Leonhard Euler

Treatise on Number Theory in XVI Chapters

Original title: *Tractatus de numerorum doctrina capita sedecim, quae supersunt*.

Translator's Preface

Leonhard Euler (1707-1783) apparently worked on his Number Theory treatise (E792) sometime around 1750, but left it unfinished. It was published posthumously in 1849 in *Commentationes arithmeticae* 2, edited by P. H. Fuss and Nicolaus Fuss for the Imperial Academy of Sciences of St. Petersburg. It reappeared in Euler's *Opera omnia*, (Series 1, Volume 5) and in his *Opera postuma*, 1 (1862). The present translation is based on the original publication, as preserved on the Euler Archive, though where certain passages therein are illegible, the *Opera postuma* reprinting was consulted. I did not have access to the *Opera omnia*. Some obvious minor corrections were made, as noted in footnotes wherever this was done.

Any translation of Euler's works will be a trade-off between doing justice to his mathematical accomplishment and representing his literary accomplishment. The present translation is no different, in this respect, from any other. The main goal is, of course, to present Euler´s mathematics in an intelligible form, but at the same time I wanted to preserve some of the "flavor" of Euler's prose style. Thus, I have, for the most part, maintained the original's use of extended sentences, encumbered by many relative clauses. This may take a bit of getting used to and require some more attention on the reader's part, but it keeps the translation closer to the original. I have also often maintained the use of the subjunctive in certain "if" clauses, which gives the text a rather archaic feel, though this is perhaps not entirely inappropriate for an eighteenth-century text. I also tried, rather against the grain (!), to maintain the ambiguities and imprecisions of the original in the translation. Finally, I have avoided using standard mathematical terminology in the representation of concepts that had no such standard

in the original text, even when that meant avoiding the use of obvious cognates.

The following concrete examples may elucidate these remarks:

In the Theory of Congruences, “residue” is generally used instead of “remainder”. Nevertheless, I have consistently rendered *residuum* by “remainder” so as not to prejudice the reader’s judgement as to the extent of Euler’s anticipation of Gauss in regard to this theory.

In the same context, the congruence relation is usually referred to as an “equivalence”. Euler, in addition to this term, also uses a variety of other terms. Many, like “agrees with” (*convenit*) or “corresponds to” (*congruit*) share connotations of agreeing with, fitting in with, harmonizing, being congenial and being consistent with. Others include “answers to” (*respondet*) and “gives” (*dat*), as well as related words. I have maintained Euler’s terminology.

Even though “quantity” seems more amenable to the modern ear than “multitude”, I have consistently used the latter to translate *multitudo* because this is sanctioned by Heath’s translation of *plêthos* in Euclid’s definition of “number” and Euler is certainly harkening back to Euclid.

It would perhaps be more euphonious to delete the verb when a formula follows *est* (*erit*), letting the = in the formula do the work of the verb. Since Euler almost never uses such a construction, I also have kept the verb, but in order to avoid such contorted phrases as “it is $x = y$” or “there is $x = y$”, I changed it to “we have” (“we will have”). In many places, however, I translated *sit* by the standard mathematical idiom “let … be”.

I have, perhaps in an excess of caution, consistently translated *denotare* by “to indicate” since in a post-Fregean world the English cognate may be misleadingly specific.

I have consistently used “sequence” for *series*, since in no case (in the present text) is the word used to indicate a sum.

Lastly, it should be observed that Euler's notes, marked by (*), are given in the translation at the end of the paragraph in which they occur, whereas in the original they appear at the bottom of the page. My own notes, marked by the usual small raised numbers, are given at the bottom of the page.

Table of Contents

Treatise on Number Theory in XVI Chapters[1]

Chapter I

On the Composition of Numbers

1. A *number* is a multitude of units.

2. Any number whatever, therefore, signifies as many units as are contained in it.

3. Beginning from the unit, the numbers are 1, 2, 3, 4, 5, 6, *etc.*, each of which exceeds the previous one by a unit.

4. Because every number can be increased by a unit, the sequence of numbers proceeds to infinity.

5. Since the first, namely the unit, also exceeds the previous one by a unit, it is necessary that the previous one, 0, be nothing.

6. Herein the discussion is only about integers, to which the definition is restricted and from which fractions and, even more so, surds must be excluded.

7. If a be any number whatever, the ones following it will be $a+1$, $a+2$, $a+3$, $a+4$, *etc.*, of which the first, $a+1$, exceeds the given number a by a unit, the second, $a+2$, by two units, the third, $a+3$, by three, *etc.*

8. Similarly, for a given number a, the preceding ones will be $a-1$, $a-2$, $a-3$, $a-4$, *etc.*, of which the first, $a-1$, is less than the given number a by a unit, the second, $a-2$, by two units, the third, $a-3$, by three units, and so on.

[1] The phrase "some remains to be done" is appended to the title of this work, which was only published posthumously. This seems to indicate that the present text is unfinished.

9. If, to the number a, there be joined as many units as there are in the number b, $a+b$ results; but if as many units as there are in b be taken away from a, $a–b$ results. In the former case, the number b is said to be *added* to the number a; in the latter, it is said to be *subtracted* from it.

10. If the same number a be joined to itself, its double $a+a$ results, which is written as $2a$; if the same be adjoined once again, the triple $3a$ is produced; then, if another a be adjoined to that result, its quadruple $4a$ results; and so on. In general, these are called its *multiples*.

11. The multiples of the number a, therefore, are $2a$, $3a$, $4a$, $5a$, *etc.*, of which each exceeds the previous one by the number a itself; and, in this respect, the number a itself is called a *simple number*.[2]

12. If a be the unit, its multiples will clearly produce all the numbers; but if a is not the unit, but a multitude of units, its multiples will not produce all numbers and, in this case, there will be numbers that are not multiples of a.

13. Since the multiples of a are $2a$, $3a$, $4a$, $5a$, *etc.*, there will not be found amongst them, first of all, all the numbers less than a itself, to wit, 1, 2, 3, …, $(a–1)$; moreover, just as many non-multiples will occur from any multiple whatever up to the following multiple.

14. If, therefore, α be a number less than a, then neither α nor the numbers $a+\alpha$, $2a+\alpha$, $3a+\alpha$, $4a+\alpha$, *etc.*, will be found amongst the multiples of a.

15. Because $2a–\alpha$ is less than $2a$ and at the same time greater than a (since $\alpha < a$), the number $2a–\alpha$ will not be a multiple of a; and neither will any of the following numbers be contained amongst the multiples of a: $a–\alpha$, $2a–\alpha$, $3a–\alpha$, $4a–\alpha$, *etc.*

---

[2] *Simplum*, a single number, one taken only once, instead of multiple times. “Simple” is used for *simplum*, whereas “single” is used for *simplex*. See §31.

16. Given, therefore, any number *b* that is not a multiple of *a*, either it will be less than *a*, or it will exceed some multiple of *a* and yet be less than the next multiple.

17. Since the multiples of the dyad [*binarii*] (not excluding the simple number itself) are 2, 4, 6, 8, 10, *etc.*, the remaining numbers differ from these by a unit. Likewise, because the multiples of the triad [*ternarium*] are 3, 6, 9, 12, 15, *etc.*, the remaining numbers are separated from these either by a unit or by a dyad.

18. The double of any number *a*, namely 2*a*, is also a multiple of the dyad. For, since *a* is a multitude of units, 1+1+1+1 *etc.*, its duplication is represented thusly:

$$a = 1+1+1+1+ \textit{etc.}$$
$$a = 1+1+1+1+ \textit{etc.}$$

whence is produced by addition $2a = 2+2+2+2+ \textit{etc.}$

19. Indeed, since the number *a* is a multitude of units, the number *a* is doubled by taking each unit twice, whence there arises a multitude of dyads. From this, it is evident that the double 2*a* contains as many dyads as *a* contains units.

20. Likewise, the triple 3*a* will contain as many triads as *a* contains units and accordingly 3*a* will be a multiple of the triad. This should also be understood in regard to all multiples.

21. The number indicating how many times a multiple contains in itself a simple number is called the *index* of the multiple. Thus, the index of a double is the dyad, of a triple the triad, of a quadruple the tetrad, *etc.*

22. If the number *a* be taken as many times as the number *n* contains units, the index of the multiple derived therefrom is *n*; this multiple, moreover, is expressed by *na*, so that *na* indicates that multiple of *a* whose index is *n*.

23. Such a multiple *na* of *a* is, therefore, also a multiple of the index *n*, since it contains the index in itself as many times as the number *a* contains the unit.

24. From this, it is therefore evident that the multiple of the number *a* whose index is *n* coincides with that multiple of *n* whose index is *a*. Since the former multiple is expressed by *na* and, indeed, the latter by *an*, it will be the case that *na* = *an*.

25. Since, in any multiple *na* whatever, the number *a*, of which the multiple is taken, and *n*, the index of the multiple, can be exchanged for each other, these two numbers, *a* and *n*, are called, indiscriminately, *factors*, whereas, for the multiple *na* itself, it is usual to introduce the name *product* or *result* [*facti*].

26. Just as every number is a multiple of the unit, of which it itself is the index, so also it is its own simple, the index being the unit. In the following, therefore, we will remove both multiples of the unit and simple numbers from the denomination of multiples of any number *a*.

27. For us, then, multiples will be any numbers that are multiples (excluding simple numbers) of any number beyond the unit and will, therefore, consist of two factors, of which either can, as it were, be considered to be the index with respect to the other.

28. The result *ab*, whose factors are *a* and *b*, is, therefore, as much a multiple of *a* as it is of *b*. In so far as it is a multiple of *a*, the index is *b* but, on the contrary, in so far as it is a multiple of *b*, the index is *a*.

29. Multiples of the result *ab* are at the same time multiples both of *a* and of *b*. Let *nab* be such a multiple, whose index is *n*. Because it is also a multiple of *n*, it will be a multiple of each of the numbers *n*, *a* and *b*.

30. From this it is also clear that, in a result consisting of three factors, the three factors are permutable and that, moreover, the result

abc is not only a multiple of the several numbers *a*, *b*, *c*, but also a multiple of the factors taken two by two: *ab*, *ac*, *bc*.

31. If, in the sequence of numbers 1, 2, 3, 4, 5, 6, 7, *etc.*, all the multiples are deleted, the remaining numbers will not be multiples of any number (seeing that we exclude [from the multiples] the simple [*simpla*] numbers) and these numbers are called *single* [*simplices*] or *prime*.

32. After having deleted, for example, the multiples of the dyad, 4, 6, 8, 10, 12, *etc.*, there remains the sequence 1, 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, *etc*; further, from these, those multiples of the triad, 6, 9, 12, 15, 18, 21, *etc.*, which are still present, are extinguished, which leaves 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, *etc.*; thus, in the end, there remain the prime numbers 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, *etc*.

33. If *p*, therefore, be a prime number, it occurs neither amongst the multiples of the dyad, nor amongst the multiples of any other number and neither, therefore, can it be exhibited in any manner as a result of the type *ab*, unless either $a = 1$ or $b = 1$, which cases, however, we have excluded (26).

34. All numbers that are not prime are called *composite*; from this, it is evident that all composite numbers are multiples of some other lesser numbers, which, once again, are either prime or multiples of other lesser numbers. Moreover, multiples of any product are at the same time multiples of their several factors. It follows that, in the end, all composite numbers are reduced to multiples of prime numbers.

35. Every number is, therefore, either prime, or a multiple of some prime number; in the latter case, since the number is composite, every composite number can be exhibited as a product, whose several factors are prime.

36. Amongst the composite numbers, there occur first those consisting of only two prime factors. If *p* an *q*, for example, indicate any

two prime numbers, the product *pq* will exhibit the general form of composite numbers of the first kind, those which consist of only two prime factors.

37. A composite number of the kind *pq*, therefore, will be both a multiple of the number *q*, the index being *p*, and a multiple of the number *p*, the index being *q*, and, moreover, it will not be a multiple of any other number. For, if it were a multiple of any other number *a*, the index being *b*, the numbers *a* and *b* would be factors, contrary to the hypothesis.

38. A product of the kind *pa*, however, whose factor *p* is prime and the other, *a*, composite – having the factors α, β, γ, *etc.* –, will not only be a multiple of the numbers *p* and *a*, but also will occur amongst the multiples of the numbers α, β, γ, *etc.*

39. After composite numbers consisting of two prime factors, those deserving to be considered as coming next are those that consist of three prime factors, those, therefore, whose general form is *pqr*, where *p*, *q*, *r* indicate any prime numbers.

40. Then, certainly, the composite numbers that follow are the products of four prime numbers, whose form will be *pqrs*. The following types, moreover, will be products consisting of five, or of six or of seven, *etc.* prime factors.

41. Hence, all the numbers are assigned to classes such that the first contains all of the several prime numbers; the second, products of two primes; the third, products of three primes; the fourth, of four; the fifth, of five; and so forth.

42. After the unit, therefore, the numbers not greater than one hundred in the first class, that is, primes, are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

43. The numbers less than one hundred in the second class are clearly

2. 2 = 4,	3. 3 = 9,	5. 5 = 25,	7. 7 = 49,
2. 3 = 6,	3. 5 = 15,	5. 7 = 35,	7.11 = 77,
2. 5 = 10,	3. 7 = 21,	5.11 = 55,	7.13 = 91.
2. 7 = 14,	3.11 = 33,	5.13 = 65,	
2.11 = 22,	3.13 = 39,	5.17 = 85,	
2.13 = 26,	3.17 = 51,	5.19 = 95,	
2.17 = 34,	3.19 = 57,		
2.19 = 38,	3.23 = 69,		
2.23 = 46,	3.29 = 87,		
2.29 = 58,	3.31 = 93,		
2.31 = 62,			
2.37 = 74,			
2.41 = 82,			
2.43 = 86,			
2.47 = 94,			

44. Next, the numbers less than one hundred in the third class are clearly

2.2. 2 = 8,	2.3. 3 = 18,	3.3. 3 = 27,
2.2. 3 = 12,	2.3. 5 = 30,	3.3. 5 = 45,
2.2. 5 = 20,	2.3. 7 = 42,	3.3. 7 = 63,
2.2. 7 = 28,	2.3.11 = 66,	3.3.11 = 99,
2.2.11 = 44,	2.3.13 = 78,	
2.2.13 = 52,		
2.2.17 = 68,	2.5. 5 = 50,	3.5. 5 = 75.
2.2.19 = 76,	2.5. 7 = 70,	
2.2.23 = 92,	2.7. 7 = 98,	

45. Furthermore, the numbers of the fourth class, below 100, are[3]

2.2.2. 2 = 16,	2.2.3.3 = 36,	2.3.3.3 = 54,
2.2.2. 3 = 24,	2.2.3.5 = 60,	2.3.3.5 = 90,
2.2.2. 5 = 40,	2.2.3.7 = 84,	
2.2.2. 7 = 56,		3.3.3.3 = 81.
2.2.2 11 = 88,	2.2.5.5 = 100,	

46. The numbers of the fifth class not greater than one hundred are

2.2.2.2.2 = 32,	2.2.2.2.5 = 80,
2.2.2.2.3 = 48,	2.2.2.3.3 = 72.

47. Two numbers of this kind occur in the sixth class

2.2.2.2.2.2 = 64, 2.2.2.2.2.3 = 96.

The following classes, however, contain no numbers less than a hundred.

---

[3] Reading 2.2.3.3 = 36 for 2.2.3.3 = 63. Also 2.2.5.5 is not less than 100. Compare with paragraphs 42 and 46, where Euler uses the phrase “not greater than one hundred”.

48. The numbers of each class are distinguished from the numbers of the other classes by their specific character and, thus, any number whatever belongs to a certain class and cannot also be assigned to any other class.

49. And if, therefore, *p*, *q*, *r*, *s*, *etc.* indicate prime numbers, the forms of these classes can be exhibited thusly:

Form of class	I . . . *p*,
«	II . . . *pq*,
«	III . . . *pqr*,
«	IV . . . *pqrs*,
«	V . . . *pqrst*,
«	VI . . . *pqrstu*,
	etc.

50. Since all the numbers are contained in these classes, if we extend the natural sequence of numbers 1, 2, 3, 4, *etc.* up to *n*, so that the multitude of numbers is = *n*, and also the multitude of prime numbers contained in this sequence is = α, the multitude of numbers of the second class = β, of the third class = γ, of the fourth = δ, and so forth, it is necessary that α+β+γ+δ+ *etc.* = *n*. Thus, we saw that, if *n* is taken = 100, we will have α = 26 (the unit included amongst the prime numbers), β = 34, γ = 22, δ = 12, ε = 4, ζ = 2, η = 0 and, indeed, 26+34+22+12+4+2 = 100.

51. If *n* indicates a power of the dyad, the multitude of numbers that each class will have, all the way up to *n*, is:

number	multitude of numbers									
n	α	β	γ	δ	ε	ζ	η	θ	ι	κ
2	2									
4	3	1								
8	5	2	1							
16	7	6	2	1						
32	12	10	7	2	1					
64	19	22	13	7	2	1				
128	32	42	30	14	7	2	1			
256	55	82	60	34	15	7	2	1		
512	98	157	125	71	36	15	7	2	1	
1024	173	304	256	152	77	37	15	7	2	1

52. If we observe carefully the arrangement [*indolem*] of the numbers, we will easily perceive that at first the prime numbers occur frequently, while the composite numbers are bound to be thinly interspersed. The farther we proceed, however, the more composite numbers and, conversely, fewer primes will be found.

53. Next, it is also incumbent to observe that, in the progression of the prime numbers 1, 2, 3, 5, 7, 11, 13, 17, 19, *etc.*, no order clearly appears from which a law of this progression could be laid down, although it is certain in general that, the farther we proceed, the less frequent they should be.

54. There are tables in which the prime numbers are set out according to the hundreds. Thus, in the first hundred, from 1 to 100, there are 26 prime numbers, in the second 21, in the following fewer, to be sure. Nevertheless, their multitude does not diminish continuously,

but is extremely irregular, at times increasing and at others decreasing. Thus, from 200 to 300 there occur 16 prime numbers, but from 400 to 500 there are 17, and still the same amount from 1400 to 1500. Further on, from 79700 to 79800, only three prime numbers are to be found; not withstanding this, in the hundred from 90000 to 90100 there are still 13 prime numbers to be found.

Chapter II
On the Divisors of Numbers

55. In so far as a number is a multiple of another number, to that extent it is said to be a *divisor* of the latter and the index of the multiplication is usually called the *quotient* arising from the division.

56. Thus, if the number N be a multiple of a, with the index being n, so that $N = na$, the number a will be a divisor of the number N and the index n will furnish the quotient. If the number $N = na$ be divided by a, then, of course, the quotient will be n.

57. Since the numbers n and a are interchangeable and, in this respect, are called factors, the number $N = na$ will also have the divisor n and then the quotient will be a. In general, therefore, the divisor multiplied by the quotient reproduces the very number that was divided.

58. Since any number is its own simple, the unit is a divisor of that number and the number itself is the quotient. Also, any number is indeed its own divisor, the quotient being the unit.

59. Any number N whatever, therefore, has, first of all, the unit for a divisor and the number itself will then be the quotient. Next, any number N whatever also has itself for a divisor, the quotient being the unit.

60. No number has any other divisors except for those [numbers] of which it is a multiple (the simple not being here excluded from the idea of a multiple); for, if it were to have another divisor, it would be, by this very fact, a multiple of it, with the index of the multiplication furnishing the quotient.

61. Therefore, since a prime number is not a multiple of any other number except the unit, a prime number does not have any divisors except for the unit and itself. Clearly, if p indicates a prime number, its divisors will be 1 and p, nor does it have any others beyond these.

62. Prime numbers, or numbers of the first class, have only two divisors, excepting the unit, which of course has but one; for this reason, the unit is usually not included amongst the prime numbers.

63. Numbers of the second class, which consist of two prime factors pq, because they are multiples of each separately, also have, beyond the divisors 1 and pq, the divisors p and q, so that all of their divisors are 1, p, q, and pq.

64. The case, however, in which both factors p and q are equal to each other, should be considered separately, since the same number shouldn't be counted twice amongst the divisors. Hence, the numbers pp, which are squares of prime numbers, have only the three divisors 1, p, and pp.

65. For this reason, it is convenient for the numbers of the second class to be subdivided into two types, of which the first contains numbers of the form pp and has the three divisors 1, p, pp; the other type clearly contains numbers of the form pq, where the letters p and q indicate distinct prime numbers. Numbers of this type will have the four divisors 1, p, q, pq.

66. Similarly, the third class should be subdivided into three types, whose forms are p^3, p^2q, pqr, if indeed p, q, r indicate distinct prime

numbers, for either all the factors are equal, or only two, or all three are unequal.

67. For the third class of numbers, moreover,
of the first type p^3, there will be the four divisors 1, p, p^2, p^3,

second	p^2q	six	1, p, q, p^2, pq, p^2q,
third	pqr	eight	1 p, q, r, pq, pr, qr, pqr,

and neither can there be, in addition, other divisors in this class [*locum*].

68. The fourth class, which contains numbers consisting of four prime factors, should be subdivided into five types, as either two, or three, or all four of these factors may be equal; their forms are I. p^4, II. p^3q, III. p^2q^2, IV. p^2qr, V. $pqrs$.

69. Now it will be easy to specify all the divisors of these types in the fourth class:

Of type		the divisors will be
I. p^4,	five:	1, p, p^2, p^3, p^4,
II. p^3q,	eight:	1, p, q, p^2, pq, p^3, p^2q, p^3q,
III. p^2q^2,	nine:	1, p, q, p^2, pq, q^2, p^2q, pq^2, p^2q^2,
IV. p^2qr	twelve:	1, p, q, r, p^2, pq, pr, qr, p^2q, p^2r, pqr, p^2qr,
V. $pqrs$	sixteen:	1, p, q, r, s, pq, pr, ps, qr, qs, rs, pqr, pqs, prs, qrs, $pqrs$.

70. In the fifth class, which encompasses numbers composed out of five prime factors, on account of the equality of several factors, it will be necessary to establish the following types:

I. p^5, II. p^4q, III. p^3q^2, IV. p^3qr, V. p^2q^2r, VI. p^2qrs, VII. $pqrst$.

71. Then, indeed, the divisors of the several types will be specified thusly:

I. p^5,	six:	1, p, p^2, p^3, p^4, p^5,
II. p^4q,	ten:	1, p, q, p^2, pq, p^3, p^2q, p^4, p^3q, p^4q,
III. p^3q^2,	twelve:	1, p, q, p^2, pq, q^2, p^3, p^2q, pq^2, p^3q, p^2q^2, p^3q^2,
IV. p^3qr,	sixteen:	1, p, q, r, p^2, pq, pr, qr, p^3, p^2q, p^2r, pqr, p^3q, p^3r, p^2qr, p^3qr,
V. p^2q^2r,	eighteen:	1, p, q, r, p^2, pq, pr, q^2, qr, p^2q, p^2r, pq^2, pqr, q^2r, p^2q^2, p^2qr, pq^2r, p^2q^2r,
VI. p^2qrs,	twenty-four:	1, p, q, r, s, p^2, pq, pr, ps, qr, qs, rs, p^2q, p^2r, p^2s,

VII. $pqrst$ thirty-two: 1, p, q, r, s, t, pq, pr, ps, pt, qr, qs, qt, rs, rt, st, pqr, pqs, pqt, prs, prt, pst, qrs, qrt, qst, rst, $pqrs$, $pqrt$, $pqst$, $prst$, $qrst$, $pqrst$.

72. The types of the remaining classes will be established similarly and all the divisors of the several types will be allotted. At the same time, the form [*natura*] of the several divisors will also be evident by this reasoning, as well as both the class and type to which each should be assigned.

73. If the divisors of the number N be $1, \alpha, \beta, \gamma, \delta, \ldots, N$, and if it be multiplied by the prime number p, which is not contained in it, then the product Np will have for divisors, beyond the above $1, \alpha, \beta, \gamma, \delta, \ldots, N$, those same multiplied by p: $p, \alpha p, \beta p, \gamma p, \delta p, \ldots, Np$; and, for that reason, the number of divisors will be twice as big.

74. But if that number N be multiplied by the square of the prime number p, which is not in it as a factor, the number of divisors will be tripled. For the product Np^2 will have, firstly, the same divisors as the number N, then, to be sure, those same multiplied by p and also, thirdly, those same multiplied by p^2.

75. Likewise, if p be a prime number not contained in N and if the number N be multiplied by p^3, the product Np^3 will have firstly all the divisors of the number N, next those same multiplied by p, further those same multiplied by p^2 and, finally, those same multiplied by p^3, whereby the multitude of divisors of the product Np^3 is four times larger than that of the number N.

76. And so, in general, if the multitude of divisors of the number N be $= m$ and if it be multiplied by power p^λ of the prime number p, the multitude of divisors of the product Np^λ will be $(\lambda+1)m$; whence it will be useful to observe that the multitude of divisors of the power p^λ itself is $\lambda+1$.

77. From this, a convenient rule for determining the multitude of divisors of any number is apparent: that is, let $p^\lambda q^\mu r^\nu s^\xi$ be the form of the proposed number; and because the multitude of divisors of the number p^λ is $\lambda+1$, the multitude of divisors of the number $p^\lambda q^\mu$ will be $(\lambda+1)(\mu+1)$; for the number $p^\lambda q^\mu r^\nu$, there will clearly be $(\lambda+1)(\mu+1)(\nu+1)$, and, further, for the number $p^\lambda q^\mu r^\nu s^\xi$, there will be $(\lambda+1)(\mu+1)(\nu+1)(\xi+1)$. Moreover, the class to which this number should be assigned is indicated by the number $\lambda+\mu+\nu+\xi$, which is the sum of the exponents.

78. Infinitely many numbers, therefore, can be produced, whose multitude of divisors be given. For if the multitude of divisors be = a, a being a prime number, the number sought is contained in the formula p^{a-1}, where p indicates any prime number whatever.

79. If a, b, c, d, *etc.* indicate prime numbers, as also the letters p, q, r, s, *etc.*, the numbers, for which the multitude of divisors is ab, are either p^{ab-1}, or $p^{a-1}\ p^{b-1}$; but those, for which the multitude of divisors is abc, are either p^{abc-1}, or $p^{ab-1}q^{c-1}$, or $p^{ac-1}q^{b-1}$, or $p^{bc-1}q^{a-1}$, or $p^{a-1}q^{b-1}r^{c-1}$, where any of the letters a, b, c, *etc.* can signify the same prime number, provided that the letters p, q, r, *etc.* signify distinct ones.

80. Hence, if the multitude of divisors be = 2, only prime numbers are satisfactory, that is, numbers contained in the form p. But if it is to be that

the multitude of divisors is	the form of the numbers will be
3	p^2
4	p^3, pq
5	p^4
6	p^5, p^2q
7	p^6
8	p^7, p^3q, pqr
9	p^8, p^2q^2
10	p^9, p^4q
11	p^{10}
12	p^{11}, p^5q, p^3q^2, p^2qr.

81. Once, therefore, the form of any number whatever, that is the class and type to which it is to be assigned, is known, not only the multitude of divisors, but also the very divisors themselves can be determined by recourse to the rules.

Chapter III
On the Sum of the Divisors of Any Number

82. Any number n having been proposed, we designate the sum of its divisors by $\int n$, so that the characters $\int n$ indicate the sum of the divisors of the number n.

83. Therefore, since the unit does not have other divisors beyond itself, we will have $\int 1 = 1$; the sum of the divisors of any other number will, however, be greater than itself; clearly, we will have $\int n > n$, unless $n = 1$.

84. For prime numbers p, because they do not admit other divisors beyond themselves and the unit, we will have $\int p = p+1$. Moreover, for powers of prime numbers we will have

$$\int p^1 = p + 1 = \frac{pp-1}{p-1},$$

$$\int p^2 = pp + p + 1 = \frac{p^3-1}{p-1},$$

$$\int p^3 = p^3 + p^2 + p + 1 = \frac{p^4-1}{p-1},$$

and in general

$$\int p^n = p^n + p^{n-1} + p^{n-2} + \cdots + 1 = \frac{p^{n+1}-1}{p-1}.$$

85. Since the divisors of numbers contained in the form pq are 1, p, q, pq, their sum will be

$1+p+q+pq = (1+p)(1+q)$, and, therefore, $\int pq = (p+1)(q+1)$.

Similarly, we will have from the third class

$$\int p^2 q = (pp+p+1)(q+1) \text{ and } \int pqr = (p+1)(q+1)(r+1).$$

86. One could, in the same way, collect the divisors from [each of] the remaining classes into a single sum; but, in order to examine the character of these sums more clearly, we should investigate, in general, the number N, whose divisors are $1, \alpha, \beta, \gamma, \delta, \ldots, N$, the sum of which is $\int N$. Let this be multiplied by a prime number p, not contained in it, and the product Np will have, besides the above divisors, the same multiplied by p, whose sum will, therefore, be $p\int N$, from which will be obtained $\int Np = (p+1)\int N = \int p \int N$.

87. In the same way as is deduced in §74, if the number N is multiplied by the square of a prime number p, not contained in it, the sum of the divisors of the product Np^2 will be $(1+p+p^2)\int N$, or $\int Np^2 = \int N \int p^2$; and, in the same way, we will have $\int Np^3 = \int N \int p^3$, and so forth.

88. Hence, for the several classes and types, the sums of the divisors will be expressed thusly

$$\begin{aligned}
\int p &= 1+p \\
\int p^2 &= 1+p+p^2 \\
\int pq &= (1+p)(1+q) \\
\int p^3 &= 1+p+p^2+p^3 \\
\int p^2 q &= (1+p+p^2)(1+q) \\
\int pqr &= (1+p)(1+q)(1+r) \\
\int p^4 &= 1+p+p^2+p^3+p^4 \\
\int p^3 q &= (1+p+p^2+p^3)(1+q) \\
\int p^2 q^2 &= (1+p+p^2)(1+q+q^2) \\
\int p^2 qr &= (1+p+p^2)(1+q)(1+r) \\
\int pqrs &= (1+p)(1+q)(1+r)(1+s)
\end{aligned}$$

etc.

89. From these formulas, we deduce the following conclusions:

$$\int p^2 = p^2+\int p = 1+p\int p$$

$$\int p^3 = p^3+\int p^2 = 1+p\int p^2 = 1+p+p^2\int p$$

$$\int p^4 = 1+p\int p^3 = 1+p+p^2\int p^2 = 1+p+p^2+p^3\int p$$
$$\int p^5 = 1+p\int p^4 = 1+p+p^2\int p^3 = 1+p+p^2+p^3\int p^2 = 1+p+p^2+p^3+p^4\int p$$

etc.

from which, it is evident that we have, in general,

$$\int p^{\boldsymbol{n}} = 1+p\int p^{n-1} = 1+p+p^2\int p^{n-2} = 1+p+p^2+p^3\int p^{n-3} \text{ } etc.$$

90. Any number n having been proposed, for which it is required to determine the sum of its divisors, it should be broken up into its prime factors, and let

$N = p^\lambda q^\mu r^\nu s^\xi$, which, when this is done, will become $\int N = \int p^\lambda . \int q^\mu . \int r^\nu . \int s^\xi$.

91. Provided, therefore, that the sums of the divisors of both the prime numbers themselves, as well as their powers, can be given, the sums of the divisors of all numbers can be completely determined.

92. For prime numbers themselves, p, since we have $\int p = p+1$, the sum of the divisors will always be an even number, unless it be that $p = 2$, in which case we have $\int 2 = 3$. For, if it be that $p = 2a-1$, we will have $\int(2a-1) = 2a$. But, because $\int p^2 = p^2+p+1$, the sum of the divisors of the square of any prime number whatever will always be an odd number, and even repeatedly, a prime number, as in the case $\int 2^2 = 7$, $\int 3^2 = 13$, $\int 5^2 = 31$.

93. Next, if N be the cube of a prime number, or if

$N = p^3$, we will have $\int p^3 = 1+p+pp+p^3 = (1+p)(1+pp)$,

and, therefore, a composite number, and also, unless it be that $n = 2$, the sum of the divisors will be divisible at least by 4, because each factor $1+p$ and $1+pp$ is even. We will therefore have $\int p^3 = (1+pp)\int p$.

94. If the number N be the fourth power of a prime number, or $N = p^4$, the sum of the divisors will be $\int p^4 = 1+p+pp+p^3+p^4$, and therefore always odd, and it may even happen that it be a prime number, just as $\int 2^4 = 31$.

95. If it be that $N = p^5$, because we have $\int p^5 = 1+p+pp+p^3+p^4+p^5$, the sum of the divisors will be

$$\int p^5 = (1+p+pp)(1+p^3) = (1+p)(1+p+pp)(1-p+pp),$$

and, therefore, a composite number, which is so composed from the sums of the divisors of lesser powers, that we have

$$\int p^5 = (1-p+pp).\int p.\int p^2.$$

96. But if there be proposed the product MN, whose factors M and N have no common prime factor, we will have $\int MN = \int M.\int N$, which sum of divisors is thus all the more compounded, the more distinct prime numbers go into it.

97. Any number N whatever having been proposed, the sum of the divisors of which is $\int N$, if it be multiplied by a prime number p, the sum of the divisors of the product Np is always greater than $p\int N$. For $\int Np$ includes, firstly, all the divisors of the number N multiplied by p, whose sum is $p\int N$, and, besides, also those divisors of the number N which are not affected by p.

98. This is shown yet again in two parts. First, if the prime number p is not contained in N, we will certainly have $\int Np = \int p.\int N = (1+p)\int N = p\int N+\int N$, in which case we have, without doubt, $\int Np > p\int N$.

99. But if p is already contained in N, so that $N = Mp^n$, we will have $\int N = \int M.\int p^n$; but $\int Np = \int M.\int p^{n+1}$. Yet, it was established above that $\int p^{n+1} = 1+p\int p^n$, from which $\int Np = \int M+p\int p^n\int M$ is obtained, so that we have $\int Np = p\int N+\int M$ and, therefore, $\int Np > p\int N$.

100. Thus, the sums of the divisors of the numbers, in the natural order of their progression, are:

$\int 1 = 1$	$\int 13 = 14$	$\int 25 = 31$	$\int 37 = 38$	$\int 49 = 57$
$\int 2 = 3$	$\int 14 = 24$	$\int 26 = 42$	$\int 38 = 60$	$\int 50 = 93$
$\int 3 = 4$	$\int 15 = 24$	$\int 27 = 40$	$\int 39 = 56$	$\int 51 = 72$
$\int 4 = 7$	$\int 16 = 31$	$\int 28 = 56$	$\int 40 = 90$	$\int 52 = 98$
$\int 5 = 6$	$\int 17 = 18$	$\int 29 = 30$	$\int 41 = 42$	$\int 53 = 54$
$\int 6 = 12$	$\int 18 = 39$	$\int 30 = 72$	$\int 42 = 96$	$\int 54 = 120$

∫ 7 = 8	∫19 = 20	∫31 = 32	∫43 = 44	∫55 = 72
∫ 8 = 15	∫20 = 42	∫32 = 63	∫44 = 84	∫56 = 120
∫ 9 = 13	∫21 = 32	∫33 = 48	∫45 = 78	∫57 = 80
∫10 = 18	∫22 = 36	∫34 = 54	∫46 = 72	∫58 = 90
∫11 = 12	∫23 = 24	∫35 = 48	∫47 = 48	∫59 = 60
∫12 = 28	∫24 = 60	∫36 = 91	∫48 = 124	∫60 = 168.

101. Not every number occurs amongst these sums of divisors, and indeed, up to 60, the following are excluded:

2, 5, 9, 10, 11, 16, 17, 19, 21, 22, 23, 25, 26, 27, 29, 33, 34, 35, 37, 41, 43, 45, 46, 47, 49, 50, 51, 52, 53, 55, 58, 59.

But the numbers that express sums of divisors are:

1, 3, 4, 6, 7, 8, 12, 13, 14, 15, 18, 20, 24, 28, 30, 31, 32, 36, 38, 39, 40, 42, 44, 48, 54, 56, 57, 60.

102. Hence, it is apparent that two or more numbers sometimes produce the same sum of divisors, for example:

∫ 6 = ∫11 = 12	∫14 = ∫15 = ∫23 = 24
∫10 = ∫17 = 18	∫20 = ∫26 = ∫41 = 42
∫16 = ∫25 = 31	∫33 = ∫35 = ∫47 = 48
∫21 = ∫31 = 32	∫24 = ∫38 = ∫59 = 60.
∫34 = ∫53 = 54	
∫28 = ∫39 = 56	

103. This problem is often proposed: to find a number that bears a given ratio to the sum of its divisors. That is, it is required that $N{:}\int N = n{:}m$, or $\frac{\int N}{N} = \frac{m}{n}$, where it is necessary, in the principle case, that $m > n$; for if it were that $m = n$, we would have $N = 1$.

104. Expressing $m{:}n$ in lowest terms, the number N will be equal either to n or to some multiple of n. Let it be stipulated, therefore, that N

= an, and we will have $\int N = \int an = am$. But, unless $a = 1$, we have $\int an > a\int n$, hence[4] $m > \int n$. Wherefore, if it be that $m < \int n$, there will be no solution; but if $m = \int n$, there will be a unique solution, namely $N = n$.

105. Therefore, unless it be that either $m = \int n$, or $m > \int n$, the problem does not admit of a solution. In the former case, N will be equal to n and there will not be any other solution. In the latter case, in which $m > \int n$, the number N will be equal to a multiple of some n, say $N = an$, and there will possibly be another solution. Nevertheless, there are, at any rate, such ratios $m:n$, for which it cannot be satisfied by any means, even though it be that $m > \int n$.

106. A number, the sum of the divisors of which is twice as big as itself, is *perfect*. So, if it be that $\int N = 2N$, then N will be a perfect number. Any such number, if it be even, will be of the sort 2^nA, where A is an odd number, whether prime or composite. Therefore, since it be that

$N = 2^nA$, we will have $\int N = (2^{n+1}-1)\int A = 2^{n+1}A$, whence $\frac{\int A}{A} = \frac{2^{n+1}}{2^{n+1}-1}$.

107. Because the numerator of the fraction $\frac{2^{n+1}}{2^{n+1}-1}$ only surpasses the denominator by a unit, it cannot exceed the sum of the divisors of the denominator; therefore, it will be either equal or less. In the latter case, there is no solution and, indeed, the former cannot be, unless $2^{n+1}-1$ is a prime number. Hence, whenever $2^{n+1}-1$ be a prime number, A should be taken equal to it, and we will have a perfect number = $2^n(2^{n+1}-1)$.

108. All even perfect numbers, therefore, are contained in the formula $2^n(2^{n+1}-1)$, if, indeed, $2^{n+1}-1$ be a prime number, because it certainly cannot happen unless $n+1$ is a prime number, although not all primes chosen for $n+1$ make $2^{n+1}-1$ prime. But, up to now, no one has demonstrated whether, or not, there are, besides the even perfect numbers, any odd ones.

[4] Reading *hincque* for *hinque*.

109. If there be an odd perfect number, all its factors would necessarily be odd. Let it be, therefore = *ABCD etc.* and it necessarily makes $\int A.\int B.\int C.\int D = 2ABCD$ an oddly even[5] number. For this reason, only one amongst the sums of divisors $\int A$, $\int B$, $\int C$, $\int D$ could be oddly even, all the rest being odd; therefore, all the factors *A*, *B*, *C*, *D*, except one, will be even powers of prime numbers, but that one will be either a prime number of the form $4n+1$, or a power of the same, whose exponent is $4\lambda+1$. And thus, such a perfect number will have such a form as $(4n+1)^{4\lambda+1}PP$, *P* being an odd number, and $4n+1$ prime.

110. I omit many other problems, in which the connection between the numbers to be investigated and the sums of their divisors is proposed, that would be fittingly considered herein, because, from the beginning already made, it is not difficult to elicit a method for solving them.

Chapter IV

On Numbers Prime and Composite to Each Other

111. Two numbers that have no other factor or common divisor besides the unit are called *prime to each other*; but those that have another common divisor besides the unit are called *composite to each other*. Thus, 8 and 15 are numbers prime to each other, but 9 and 15 are numbers composite to each other.

112. The unit, therefore, is prime to all numbers. Certainly, when *n* indicates any number whatever, the numbers 1 and *n* are prime to each other, because they admit no other common divisor besides the unit.

113. Likewise, two numbers *n* and $n+1$, differing by a unit, are prime to each other; for whatever divisors the number *n* may have, none of them can divide the number $n+1$. For, indeed, if *p* be a divisor of the

[5] That is, the double of an odd number.

number n, the next greater number divisible by p will be $n+p$, so that $n+1$ certainly does not admit division by p.

114. A prime number p is prime to all numbers, except those that are its multiples; hence, the numbers a and p are prime to each other, unless it be that either $a = p$, or $a = np$. Therefore, the prime number p is prime to all numbers less than itself.

115. The multitude of numbers less than a given number a is $a-1$, amongst which it is worth the trouble to determine how many are either prime or composite to a; since, from that, the determination is easily extended to all numbers greater than a.

116. For, let $b<a$ and, if b and a be prime to each other, all the numbers $b+a$, $b+2a$, $b+3a$, *etc.* as well will be prime to a; and, further, if b and a have a common divisor, it will be a divisor of the numbers $b+a$, $b+2a$, $b+3a$, *etc.*

117. If, then, a be a prime number $= p$, because all the numbers less than it are prime to it, the multitude of these is $= p-1$.

118. If it be that $a = 2p$, there are p even numbers from 1 to a, which therefore are not prime to a, and further the number p as well is not prime to a. These, whose multitude is $= p$, are removed from all the numbers from 1 up to a and $p-1$ are left, and that amount will be prime to a.

119. If it be that $a = 3p$, amongst the numbers not greater than it, there are first those that are divisible by 3 and are not prime to it, whose multitude is $= p$, next p and $2p$, in addition, are not prime to a; all the rest, whose multitude is $3p-p-2 = 2(p-1)$ will be prime to $a = 3p$.

120. Similarly, if $a = 5p$, the numbers which have a common divisor with a are firstly all those divisible by 5, whose multitude is $= p$, and also those that are divisible by p, that is, p, $2p$, $3p$ and $4p$; since the number $5p$ has already been accounted for. Whence, the multitude of numbers

composite to a is $p+4$ and, therefore, the multitude of numbers prime to $a = 4p-4 = 4(p-1)$, which of course are not greater than a.

121. More generally, if it be that $a = pq$, both p and q being prime factors, there are, from the unit to a, p numbers divisible by q, namely q, $2q$, $3q$, …, pq; next there are q numbers divisible by p, namely p, $2p$, $3p$, …, qp, of which the last qp has already been counted. Therefore, the multitude of all the numbers not surpassing a, which are composite to a, will be $= p+q-1$, whence the rest, whose multitude is

$$= qp-p-q+1 = (p-1)(q-1),$$

will be prime to a.

122. Here we suppose distinct prime numbers for p and q. For, if we had $a = pp$, other numbers would not be composite to a, except those divisible by p, and since the multitude of those is $= p$, the multitude of the rest, those that are prime to a, will be $= pp-p = p(p-1)$.

123. Similarly, if it be that $a = p^3$, because it does not have other prime divisors besides p, all the numbers, from 1 to a, composite to a are p, $2p$, $3p$, …, p^2p, and since the multitude of these is $= p^2$, all of the remaining numbers, whose multitude is $p^3-p^2 = p^2(p-1)$, will be prime to a.

124. Hence, it is evident that, in general, if a be any power whatever p^n of a prime number p, the multitude of numbers prime to a, which indeed be not greater than a, will be $p^{n-1}(p-1)$.

125. Let $a = p^2q$, both p and q being distinct prime numbers, and since a does not have any other prime divisors besides p and q, the numbers composite to a either will be divisible by p, which are p, $2p$, $3p$, …, $pq.p$, in multitude $= pq$, or divisible by q, which are q, $2q$, $3q$, …, p^2q, in multitude $= p^2$. But, pq, $2pq$, $3pq$, …, $p.pq$, in multitude $= p$, occur amongst the latter and have already been enumerated, so that the multitude of all those composite to a is $= pq+p^2-p$. Because of this, the rest, whose multitude is $= ppq-pq-pp+p = p(p-1)(q-1)$, will all be prime to a.

126. Let $a = pqr$, with p, q and r being distinct prime numbers, and so the numbers composite to a are divisible

1) by p, namely p, $2p$, $3p$, …, $qr.p$, in multitude qr
2) by q, « q, $2q$, $3q$, …, $pr.q$, « pr
3) by r, « r, $2r$, $3r$, …, $pq.r$, « pq.

But here those divisible by pq, in multitude r, then those divisible by pr, in multitude q, and, finally, those divisible by qr, in multitude p, are counted twice, and are therefore removed; but, in so doing, the number pqr is completely taken away, and should thus be put back again. And so, the multitude of numbers composite to a will be $qr+pr+pq-r-q-p+1$; whence the rest, whose multitude is

$$pqr-qr-pr-pq+r+q+p-1 = (p-1)(q-1)(r-1),$$

will be prime to the number $a = pqr$.

127. From this, we conclude that, for all the kinds of numbers, we will have

if the proposed number be	the multitude of numbers less than a and prime to it
$a = p$	$p-1$
$a = p^2$	$p(p-1)$
$a = pq$	$(p-1)(q-1)$
$a = p^3$	$p^2(p-1)$
$a = p^2q$	$p(p-1)(q-1)$
$a = pqr$	$(p-1)(q-1)(r-1)$
$a = p^4$	$p^3(p-1)$
$a = p^3q$	$p^2(p-1)(q-1)$
$a = p^2q^2$	$p(p-1)q(q-1)$
$a = p^2qr$	$p(p-1)(q-1)(r-1)$
$a = pqrs$	$(p-1)(q-1)(r-1)(s-1)$

128. In order that this conclusion may be more firmly corroborated and not to rely too much on induction[6], we should examine the form $a =$

[6] That is, induction by enumeration, not mathematical induction.

Mp, where M is any number whatever and p a prime not contained in M. We also specify that the multitude of numbers from 1 to M, prime to M, be = μ and, thus, the multitude of numbers composite to M is = $M-\mu$.

129. Therefore, since there are $M-\mu$ numbers composite to M from 1 to M, there will be $p(M-\mu)$ numbers composite to M from 1 to Mp, which therefore will also be composite to Mp, and in addition the following are composite to Mp: p, $2p$, $3p$, …, Mp, in multitude M, but from which those that are already composite to M, whose multitude is $M-\mu$, should be taken out; and so there remain but μ numbers which are only composite to Mp and not to M also. Hence, from 1 to Mp and composite to Mp, there will be in all this many: $p(M-\mu)+\mu$, and the rest, whose multitude is $Mp-p(M-\mu)-\mu = \mu(p-1)$, will be prime to the number Mp.

130. It may be shown in a similar way that, if the number proposed be = Mp^n, with p being a prime number not contained in M, and if μ be the multitude of numbers prime to M, which are contained between the limits 1 and M, then the multitude of all the numbers below Mp^n, prime to the number Mp^n, will be = $p^{n-1}\mu(p-1)$.

131. For we should search for numbers composite to Mp^n, all of which will be composite to either M or to p. But the multitude of numbers from 1 to Mp^n, composite to M, is = $p^n(M-\mu)$; moreover, those that are composite to p will be: p, $2p$, $3p$, …, $Mp^{n-1}.p$, in multitude = Mp^{n-1}. Yet, from these, those which are already composite to M ought to be excluded, whose multitude is $p^{n-1}(M-\mu)$, so that the multitude of those that are composite to Mp^n, but not composite to M, will be = $Mp^{n-1}-p^{n-1}(M-\mu)=p^{n-1}\mu$, whence the multitude of numbers from 1 to Mp^n, composite to Mp^n, will be in all = $p^n(M-\mu)+p^{n-1}\mu$. Because of this, the rest, whose multitude is $Mp^n-p^n(M-\mu)-p^{n-1}\mu = p^{n-1}\mu(p-1)$, will be prime to Mp^n.

132. Therefore, since the multitude of numbers prime to p^n and less than it is = $p^{n-1}(p-1)$, from the preceding proposition we conclude with the highest rigor: If the number proposed be = $p^\lambda q^\mu r^\nu s^\xi$ *etc.*, the multitude of all the numbers prime to it and less than it will be

$$= p^{\lambda-1}(p-1).q^{\mu-1}(q-1).r^{\nu-1}(r-1).s^{\xi-1}(s-1)\ etc.$$

133. If, therefore, M and N be numbers prime to each other, and if the multitude of numbers from 1 to M, prime to M, be = m and the multitude of numbers from 1 to N, prime to N, be = n, then the multitude of numbers prime to the product MN and not greater to it will be = mn.

134. Hence, it is clear that the multitude of all prime numbers, just as Euclid has already demonstrated, cannot be finite. For, if the last and greatest prime number were = p, the number M may be set up equal to the product of all the prime numbers, $M = 2.3.5.7\ldots p$, which would clearly be composite to all numbers. Since the number M is certainly prime to M–1, or even M+1, it will be clear that the assertion is absurd.

135. From the above, it is also clear that, amongst the numbers less than M, not only the number M–1, but also several others are certainly prime to M, since the multitude of these numbers prime to M is = $1.2.4.6\ldots(p-1)$, which is greater than the quantity of prime numbers that are multiplied by each other.

136. Let's set $m = 1.2.4.6\ldots(p-1)$, with M being = $2.3.5.7\ldots p$; and since, from 1 to M, there are as many numbers prime to M as there are units contained in m, these, be they either prime themselves or composed of primes, are greater than p.

137. If, from 1 to M, there be m numbers prime to M, there will be $2m$ numbers prime to M from 1 to $2M$ and, in general, from 1 to NM, there will be Nm numbers prime to M. For, in any interval whatever,

$$1\ldots M,\quad M+1\ldots 2M,\quad 2M+1\ldots 3M,\quad 3M+1\ldots 4M,\ etc.,$$

the multitude of numbers prime to M is the same.

138. If n indicates any other number whatever, and if there be n numbers prime to N from 1 to N, there will be Mn numbers prime to N from 1 to MN. But, in the same interval, there are Nm numbers prime to M. Indeed, each of those that are prime to MN are prime to M and also to N.

139. However, we have already shown that, if the numbers M and N be prime to each other, then, in the interval from 1…MN, there are as many numbers prime to MN as there are units contained in mn; and these numbers occur in each of the preceding multitudes Mn and Nm. (*)

(*) *Notes written by the illustrious author in the margins*. On the greatest common divisor and on finding it. — If A and B be prime numbers, a multiple of A can be found, which, divided by B, leaves a given number C. — If these numbers be prime to each other, any of their powers whatever will be prime to each other. — If A be prime to B and also to C, it will likewise be prime to BC. — If the product AB be divisible by the prime p, one or the other factor will be divisible by it. — If A and B be prime to each other, there can be found numbers m and n, that will make $mA–nB = 1$, or any other given number whatever. — If φ be the greatest common factor of the numbers A and B, then $\frac{A}{\varphi}$ and $\frac{B}{\varphi}$ will be prime to each other. — If a divided by b produces the remainder r, then na divided by nb will produce the remainder nr. — If a divided by b produces the remainder r, a common factor of the numbers a and b, if they have one besides the unit, will likewise be a factor of the remainder r. Again, if b and r have a common factor, it will likewise be a factor of a. — If a and b be numbers prime to each other and $a > b$, we will have $a = mb+p$; and $b > p$, then also $b = np+q$ and $p > q$, and thus finally we reach the unit.

Chapter V

On Remainders Arising from Division

140. If the number a is not a multiple of the number b, division of the former by the latter does not succeed, and the excess of the number a over the nearest less multiple of b is called the *remainder* arising from the division. Thus, if it be that $a = mb+r$, then r will be the remainder arising from the division of the number a by b.

141. Hence, it is clear that the remainder r is always less than the number b, the divisor; for if it were equal, that is if $r = b$, by increasing the index m of the multiple by a unit, a would be a genuine multiple of b, that is to say $a = (m+1)b$; and if it were that $r > b$, by increasing the index of m, it would be reduced below b.

142. Therefore, any divisor b whatever being proposed, if the dividend a be a multiple of b, the remainder will be = 0; but[7] if a be not a true multiple of b, the remainder will be either 1 or 2, or 3, or some other number less than b, so that the multitude of the remainders that can occur is b–1, or exactly b if the cipher also be counted.

143. For any divisor b whatever, therefore, all the numbers can be distributed into as many classes as there are units contained in b. The first class will contain, of course, all the numbers that are multiples of b, that is of the form mb; the second, those which divided by b leave 1 for the remainder, third, those which leave 2, fourth, those which leave 3 and, finally, the last, which leave b–1.

144. Thus, taking 2 as the divisor, there are two classes, of which the first contains numbers of the form $2m$, the other numbers of the form $2m+1$. Numbers of the first class are called *even*, of the latter *odd*.

145. If the triad be selected for the divisor, all the numbers will be separated into three classes: the first is made up of numbers of the form $3m$, the second, of numbers of the form $3m+1$ and the third, of numbers of the form $3m+2$.

146. If the divisor be set = 4, the four classes of all the numbers is comprised by these four forms: I. $4m$, II. $4m+1$, III. $4m+2$, IV. $4m+3$, where the first class is assigned the name *evenly even*; the third of numbers *oddly even*. But the second and fourth present the odd numbers subdivided into two classes.

147. Similarly, the divisor 5 supplies these five classes of numbers: I. $5m$, II. $5m+1$, III. $5m+2$, IV. $5m+3$, V. $5m+4$, and also the divisor 6 provides these 6 classes:

I. $6m$, II. $6m+1$, III. $6m+2$, IV. $6m+3$, V. $6m+4$, VI. $6m+5$,

and so on for any other divisor.

---

[7] Reading *autem* for *antem*.

148. Consequently, any number you please is assigned to some fixed class by any divisor whatever, or is expressed by some fixed form, which, since the number of divisors can be increased to infinity, can be done in infinite ways.

149. For, if the number be less than the proposed divisor, it itself can be considered the remainder, the index of the multiple vanishing; thus, if it be that $a < b$, we will have $a = mb+a$, with m being = 0, and, therefore, the number 3 belongs to the class $5m+3$ with respect to the divisor 5.

150. Any class whatever contains infinite numbers in increasing arithmetic progression, the consecutive difference being equal to the divisor. Thus, in general, if the divisor be b and the remainder r, every number is assigned to a class $mb+r$: r, $b+r$, $2b+r$, $3b+r$, $4b+r$, $5b+r$, *etc.*, the general term of which arithmetic progression is the very formula $mb+r$, from which it arises.

151. Furthermore, the formula $mb+r$ can be represented by $(m+1)b-b+r$, and thus the positive remainder r is to be thought of as equivalent to the negative remainder $-(b-r)$, from which it is clear that the idea of the remainder is to be more broadly construed, even embracing negative numbers.

152. Hence, when the divisor is = 2, the formula for odd numbers, $2m+1$, may also be represented as $2m-1$; and, if the divisor b be = 3, the class of numbers, which leave the dyad upon division by 3, is also contained in the formula $3m-1$; and thus all numbers are necessarily contained in one of the three formulas $3m$, $3m+1$ and $3m-1$.

153. Because of this, if we wish to admit negative remainders, we will be able to represent all the formulas $mb\pm r$ in such a way that the remainder r does not surpass half the divisor b. For, if $r > \frac{1}{2}b$, taking $-(b-r)$ for r, we will have $b - r < \frac{1}{2}b$.

154. Similarly, since we have $mb+r = (m-1)b+b+r$, the remainder r is also equivalent to $b+r$, if we take the word in a wider sense. In general, therefore, the remainders, speaking less properly, $b+r$, $2b+r$, $3b+r$, *etc.*, are equivalent to the remainder, properly speaking, r.

155. That is to say, the divisor being b, every number, even if greater than b, can be considered as a remainder, which can be reduced to the remainder properly speaking, by taking the divisor b away from it as many times as possible and, by admitting negatives, it may even be kept below half of the divisor b.

156. Thus, if the divisor be 6 and the remainder 16, this improper remainder will be reduced to the proper remainder 4, and even to the negative remainder –2; that is, the formulas $6m+16$, $6m+4$, $6m-2$ should be considered as equivalent because all the numbers contained in one are at the same time contained in the others.

157. It behooves us to consider carefully several notable properties about remainders. If the number A be divided by the divisor d, producing the remainder α, the numbers $A+d$, $A+2d$, $A+3d$, *etc.* will leave the same remainder α, but the number $A+1$, divided by the same d, will give the remainder $\alpha+1$ and, more generally, the number $A+n$ will give the remainder $\alpha+n$, which, if it exceed the divisor d, by subtracting it as many times as possible, will be reduced to the minimum form.

158. Similarly, if the remainder α agrees with the number A when the divisor is taken to be d, the numbers $A-d$, $A-2d$, $3A-d$, *etc.* will likewise leave the same remainder, but the remainder $\alpha-1$ agrees with the number $A-1$ and the remainder $\alpha-n$ with the number $A-n$, which, if it by chance be negative, will be reduced to a positive one by the addition of the divisor d.

159. When the divisor is taken to be d, if the remainder α agrees with the number A, and the remainder β with the number B, the remainder $\alpha+\beta$ agrees with the aggregate $A+B$ of these numbers, which,

should it be that $\alpha+\beta > d$, corresponds [*congruit*[8]] to $\alpha+\beta-d$. Hence it is clear that, if it be that $\alpha+\beta = d$, $A+B$ will be a multiple of d.

160. Under the same conditions, the remainder $\alpha-\beta$ agrees with the difference of the numbers $A-B$, or even $\alpha-\beta+d$, if by chance it be that $\beta > \alpha$. Whence, if it be that $\alpha = \beta$, that is, if the numbers A and B leave equal remainders, their difference will be divisible by the divisor d.

161. Assuming the divisor d, if the number A produces the remainder α, its double $2A$ will give the remainder 2α, or even $2\alpha-d$, its triple $3A$ will give the remainder 3α, whose minimum form, if it be greater than d, will be either $3\alpha-d$, or $3\alpha-2d$. But, in general, the remainder of any multiple whatever nA will be $n\alpha$ or $n\alpha-md$.

162. If it be posited that the divisor $= d$, the remainder α answers to the number A and the remainder β to the number B, then the remainder $\alpha\beta$ agrees with the product AB, which, if it be by chance greater than the divisor d, is reduced to $\alpha\beta-d$ or $\alpha\beta-md$.

163. For we will have $A = md+\alpha$ and $B = nd+\beta$, from which the product becomes

$$AB = mnd^2+(m\beta+n\alpha)d+\alpha\beta,$$

whose last part $\alpha\beta$ can be considered as the remainder, since the first parts are divisible by d.

164. We deduce from this that, if the number A divided by d leaves the remainder α, the remainder $\alpha\alpha$ answers to its square A^2, and the remainder α^3 to its cube A^3, and the remainder α^n to any power whatever A^n, which, the division having been by d, will be reduced to minimum form as before.

165. Because of this, if the remainder = 1 be left to the number A when divided by d, all its powers A^2, A^3, A^4, *etc.*, divided by that same divisor d, will leave the same remainder = 1. But if the remainder of the

---

[8] Observe that the standard mathematical term for this relation would become "congruence".

number A be -1, equivalent to $d-1$, the remainders of the even powers A^2, A^4, A^6, A^8, *etc.* will be $+1$, but those of the odd ones -1.

166. Finally it should be noticed that, if the number A divided by d produces the remainder α, then $A-\alpha$ will be divisible by the number d. Whence, since A^n gives the remainder α^n for the divisor d, $A^n-\alpha^n$ will likewise be divisible by d.

Chapter VI
On Remainders Arising from the Division of the Terms of Arithmetic Progressions

167. Let's begin with the sequence of natural numbers, whose terms 1, 2, 3, 4, *etc.*, divided by any divisor d whatever, will give the remainders 1, 2, 3, 4, *etc.* until the term d is reached, with which the remainder = 0 agrees; the following terms $d+1$, $d+2$, $d+3$, *etc.*, up to $2d$, will, however, give back the remainders 1, 2, 3, *etc.* in the same order; the remainder of $2d$ again vanishes; and so on.

168. Now let any arithmetic progression whatever

$$a,\ a+b,\ a+2b,\ a+3b,\ a+4b,\ a+5b,\ etc.$$

be proposed, and let the several terms of it be divided by d, where the remainder a arises from the first term and does not return before the term $a+nb$ is reached, of which the part nb proves to be divisible by d, and after which the remainders of the terms will come forth in the same order as from the beginning. (*)

(*) *Written in the margin.* These remainders exceed, by the number a, the remainders arising from the progression $0,\ b,\ 2b,\ 3b,\ 4b,\ etc.$, wherefore it will be sufficient to develop these.

169. In the first place, it is immediately clear that there cannot result from this more distinct remainders than the [amount of] units

contained in the divisor d. Whence, if that many distinct remainders are already produced from the beginning, it is necessary that the former be reproduced again successively. Moreover, the term $a+db$, whose index is $d+1$, always produces the same remainder as a, the first.

170. If the difference b of the progression be a factor of the divisor d, or if, in any event, b and d have the common factor φ, so that $b = B\varphi$ and $d = D\varphi$, then the first remainder a will come back again before the term $a+bd$ is reached; this will certainly happen at the term $a+Db$, whose index is $D+1$, since $Db = BD\varphi = Bd$ is divisible by d.

171. Therefore, it is appropriate here to set out two cases, the one, in which the divisor d and the difference b[9] of the progression are numbers prime to each other, and the other, in which they are composite to each other, or in which they have some common factor besides the unit.

172. If the divisor d and the difference b of the progression be prime to each other, the first remainder a does not return before the term $a+db$; for, if it were to recur at some previous term, say $a+(d-n)b$, then $(d-n)b$, and hence also nb and, therefore, also n, would be divisible by d, which would be absurd.

173. In order to determine the remainders, therefore, it is necessary to consider the terms of the progression from the first, a, up to $a+(d-1)b$, whose multitude is d, which terms we may display, arranged in order, together with their remainders thusly:

Indexes:	1,	2,	3,	4,	5,	d
Progression:	a,	$a+b$,	$a+2b$,	$a+3b$,	$a+4b$, ...	$a+(d-1)b$,
Remainders:	α,	β,	γ,	δ,	ε,	λ

174. In the first place, therefore, I observe that all these remainders, whose multitude is d, are distinct from each other. For, just as the first,

[9] Reading b for a.

α, has been shown not to occur further, so the second, β, is shown to appear only one time. For, if this same remainder had arisen from the term $a+nb$, with $n < d$, the difference $(n-1)b$ of the terms, and therefore also $n-1$, would be divisible by d, which is absurd.

175. Since, therefore, all the remainders α, β, γ, δ, …, λ are distinct from each other, and their multitude is = d, all the numbers less than d, together with the cipher, will occur amongst them, that is, the numbers 0, 1, 2, 3, …, $(d-1)$, whose multitude altogether is = d, will occur.

176. Hence, if r be any number whatever less than the divisor d, there will certainly be a term of the progression, $a+nb$, with $n < d$, which, divided by d, leaves the remainder r. And also, taking $r = 0$, there will be a term of the kind $a+nb$ divisible by d.

177. If the term $a+nb$ produces the remainder r, then $a+nb-r$ will be divisible by d. Hence, if b and d be numbers prime to each other, and $a-r$ indicates any number whatever, there will always be a number n less than d such that the number $a-r+nb$ becomes divisible by d.

178. Let $a+mb$ be a term divisible by d, with $m < d$, thus the following term $a+(m+1)b$ will give the remainder b, but the preceding one $a+(m-1)b$ will give the remainder $-b$, that is $d-b$. Next, let $a+nb$ be a term, which leaves the unit when divided by d, then, when that number is taken away from this one, the difference $(n-m)b$ will also leave the unit.

179. Let's put $n-m = p$, so that the number pb, divided by d, leaves the unit, and assuming the term $a+mb$ divisible por d, the remainder = 1 agrees with the term $a+(m+p)b$, the remainder = 2 with the term $a+(m+2p)b$, the remainder = 3 with the term $a+(m+3p)b$, and in general the remainder = n with the term $a+(m+np)b$.

180. If $m+np$ be greater than the divisor d, this can be taken away from it so many times until the number $k < d$ remains and the term $a+kb$, divided by d, will leave the remainder = n.

181. Terms leaving given remainders can now be more easily determined, provided that the product pb, which leaves the unit on division by d, is known. For, since the first term a leaves α, the term $a+npb$ will leave $\alpha+n$.

182. If, therefore, the given remainder be $= r$, set $\alpha+n = r$, and, since $n = r-\alpha$ and p has already been found, the term producing the remainder r will be $a+(r-\alpha)pb$; or even more generally $a+((r-\alpha)p\pm\mu d)b$, where μ may be supposed such as to make $(r-\alpha)p\pm\mu d < d$.

183. The whole business, therefore, turns on tracking down, for the number b, the multiple pb, which, divided by d, leaves the unit. Since $pb-1$ would consequently be divisible by d, setting $pb-1 = qd$, it is necessary to determine p and q that make $pb-qd = 1$. But p can always be assigned below d.

184. Often a product of the kind πb, which divided by d leaves $d-1$ ou -1, is more easily found; but then the product $(d-\pi)b$ will produce the remainder $= +1$, so that, π having been found, we will have $p = d-\pi$. Then, therefore, the term $a+((\alpha-r)\pi\pm\mu d)b$ leaves the given remainder r.

185. Let's now also examine the remainders, which arise if the difference b of the progression and the divisor d be not numbers prime to each other. But we have already seen that, if the common factor be φ, so that we have $b = B\varphi$ and $d = D\varphi$, the term $a+Db$ already produces the same remainder as the first, a.

186. Whence, if φ be the maximum common factor of the numbers b and d, because the first remainder a, or eventually α, recurs at the term $a+Db$, there cannot be more distinct remainders than the number D: neither, therefore, do all the numbers less than the divisor d occur amongst the remainders.

187. In order to examine these remainders more easily, let's set $a = 0$, and the terms of the progression with their remainders are

Indexes	1	2	3	4	D

Terms	0,	$B\varphi$,	$2B\varphi$,	$3B\varphi$	$(D-1)B\varphi$	
Remainders	0,	$\beta\varphi$,	$\gamma\varphi$,	$\delta\varphi$,		$\lambda\varphi$

for it is evident that, if these terms be divided by $d = D\varphi$, the remainders are likewise divisible by φ.

188. For, if mB divided by D produces the remainder r, we will have $mB = nD+r$, and therefore $mB\varphi = nD\varphi+r\varphi$. Whence, if $mB\varphi$ is divided by $D\varphi = d$, the remainder will be $r\varphi$, a multiple of φ. Consequently, since all the numbers less than D can appear for r, all the multiples of φ, which do not surpass the divisor $d = D\varphi$, must also appear amongst those remainders, whose multitude is certainly $= D$.

189. If we add the number a to the several terms, the several remainders will be increased by this same amount, which, since $b = B\varphi$ and $d = D\varphi$, will therefore be:

Indexes	1	2	3	4	5	D
Terms	a,	$a+b$,	$a+2b$,	$a+3b$,	$a+4b$	$a+(D-1)b$
Remainders	a,	$a+\beta\varphi$,	$a+\gamma\varphi$,	$a+\delta\varphi$,	$a+\varepsilon\varphi$,	$a+\lambda\varphi$

where the sequence β, γ, δ, ε, …, λ contains all the numbers less than D.

190. In this case, therefore, all the numbers that, being diminished by the number a, are not divisible by φ, that is, the maximum common divisor of the difference b and the divisor d, are excluded from the sequence of remainders.

191. Since the numbers B and D are prime to each other, a multiple of the first, say mB, can be exhibited, which, divided by D, leaves a given remainder r; but then the term $a+mB\varphi$ of our progression, that is $a+mb$, divided by $D\varphi = d$, will leave the remainder $a+r\varphi$ (*).

(*) *Written in the margin.* A method for determining a formula $ax+b$, such that it is divisible by the given number d.

Chapter VII
On Remainders Arising from the Division of the Terms of Geometric Progressions

192. In general, we represent a geometric progression thusly: a, ab, ab^2, ab^3, ab^4, ab^5, *etc.*, the terms of which, if divided by any number d whatever, will give remainders of such a kind that they can be obtained easily from the remainders of the progression 1, b, b^2, b^3, *etc.* — of course, by multiplying them by a.

193. Thus, the investigation is reduced to that about remainders of pure powers, so that it is to be determined what remainder any power b^n whatever, divided by a given divisor d, leaves. Here it is certainly fitting to distinguish the cases in which the numbers b and d are either prime, or composite, to each other.

194. If it be that $b = p\varphi$ and $d = q\varphi$, we will look for the remainder arising from $p^n\varphi^{n-1}$, if it is divided by q; and that, multiplied by φ, will give the remainder arising from the division of the number $p^n\varphi^n$ by $q\varphi$ and, in this way, we are brought back to the division of a power b^n by d, where b and d are numbers prime to each other.

195. Let, therefore, b and d be numbers prime to each other and let the remainders arising from the division of the powers of b be indicated thusly:

Powers	1,	b,	b^2,	b^3,	b^4,	b^5,	b^6,	b^7, *etc.*
Remainders	1,	α,	β,	γ,	δ,	ε,	ζ,	η, *etc.*

all of which will also be prime to the divisor d, because d is prime to all the powers of b.

196. Because these remainders 1, α, β, γ, δ, *etc.* are all less than d, they cannot all be distinct from each other. Indeed, if the multitude of numbers that are prime to d and also less than d be μ, more distinct remainders cannot result than μ contains of units.

197. Since, therefore, countless powers produce the same remainders, if we set b^m and b^{m+n} as giving the same remainder, the difference of these powers, $b^{m+n}-b^m = b^m(b^n-1)$ will be divisible by d. Because b^m is prime to d, it follows that b^n-1 is divisible by d, that is, the power b^n gives the remainder = 1.

198. Because more than μ distinct remainders cannot occur, if the progression be extended to the term b^μ, since the number of its terms = $\mu+1$, at least one remainder occurs twice, and thus the case already considered comes to pass before $m+n$ surpasses μ, whence there will be a power b^n, reproducing the remainder = 1, such that n does not surpass μ.

199. Let's stipulate b^n to be the least power after the unit that, divided by d, leaves the unit, but the following powers, b^{n+1}, b^{n+2}, b^{n+3}, *etc.*, will produce the same remainders as the initial powers b, b^2, b^3, *etc.*, until the power b^{2n}, which again leaves the unit as remainder, is reached.

200. Since, therefore, the same remainders return, going forth from the power b^n as from the beginning, not only will all the powers b^0, b^n, b^{2n}, b^{3n}, b^{4n}, *etc.* leave the same remainder 1, but also b^1, b^{n+1}, b^{2n+1}, b^{3n+1}, b^{4n+1}, *etc.* will have the same remainder, as also will b^m, b^{n+m}, b^{2n+m}, b^{3n+m}, *etc.*, divided by d, leave equal remainders.

201. Putting, therefore, b^n for the least power leaving the unit as the remainder, so that n does not exceed μ, the multitude of numbers less than d and prime to it, all the antecedent powers 1, b, b^2, b^3, …, b^{n-1}, will produce unequal remainders, which will thereafter return in the same order. For if two of them were equal, there would be a lesser value for n, contrary to the hypothesis.

202. But if all the numbers prime to the divisor d and less than it occur in the remainders, the multitude of which is = μ, we will have $n = \mu$, and also $b^\mu-1$ will be divisible by d. But if not every number prime to d

occurs amongst the remainders, it is necessary that we have $n < \mu$. We will show, however, that, in this case, n is an aliquot part of μ.

203. If not all the numbers prime to d and less than it, whose multitude is $= \mu$, occur amongst the remainders, whose multitude $= n$, I will call those which are excluded from the rank of the remainders by the name *non-remainders*, so that the multitude of remainders n with the multitude of non-remainders must exhaust the number μ.

204. If the numbers r and s occur in the sequence of remainders $1, \alpha, \beta, \gamma$, *etc.*, the number rs, or an equivalent remainder, will likewise occur in it. For, if the remainders r and s answer to the powers b^ρ and b^σ, the remainder rs will respond to the power $b^{\rho+\sigma}$. And, hence, the number $r^f s^g$ will occur amongst the remainders, whatever may be taken for the exponents f and g.

205. Again, if the remainder r agrees with the power b^ρ, and the remainder rs, or $rs - \lambda d$, with the power $b^{\rho+\sigma}$, then the remainder s will agree with the power b^σ. For the remainder rs will agree with the product $b^\rho s$, the same as for the power $b^{\rho+\sigma}$; hence, the difference $b^{\rho+\sigma} - b^\rho s = b^\rho(b^\sigma - s)$ will be divisible by d. Because of this, since b^ρ is prime to d, it is necessary that $b^\sigma - s$ be divisible by d, and so the remainder s will answer to the power b^σ.

206. If, therefore, the numbers r and rs are found amongst the remainders, it is certain that the number s is going to be found there also. But if the sequence of remainders $1, \alpha, \beta, \gamma, \delta$, *etc.*, whose number is $= n$, does not encompass all the numbers less than d and prime to it, whose multitude is $= \mu$, there will be one, or more, which must be assigned to the class of non-remainders.

207. Let x be such a non-remainder, and it is also clear that the numbers $\alpha x, \beta x, \gamma x, \delta x$, *etc.* are to be found amongst the non-remainders, for, if αx were found in the remainders, because α occurs there, x would also have to be found there, contrary to the hypothesis. Thus, from a single non-remainder, it necessarily follows that there are as many non-

remainders as remainders, that is to say n. For these non-remainders are also unequal to each other just as the remainders 1, α, β, γ, δ, *etc.* are, and, besides, if there were two that were equal there, there would also be such here, which is absurd. (*)

(*) *Written in the margin.* If x and y be non-remainders, we will have $y = \alpha x$ and $xy = \alpha xx$; now if the number of non-remainders = the number of remainders, it must be shown that xx is contained amongst the remainders.

208. It is therefore now immediate that $n < \mu$ and there are, at a minimum, n non-remainders; if everything is encompassed, the number of both remainders and non-remainders will be = $n+n$, which must be equal to μ, whence we have $n = \frac{\mu}{2}$; hence, if $n < \mu$, it cannot be that the number of remainders supersedes n, half of the number μ.

209. If not every non-remainder occurs in the way set forth as x, αx, βx, γx, *etc.*, let y be a number $< d$ and prime to it, which is found neither in these non-remainders nor in the remainders, and similarly the numbers αy, βy, γy, *etc.*, distinct from the preceding, must be assigned to the non-remainders, and so, once again, n numbers are added to the non-remainders.

210. If these two orders do not yet exhaust all the non-remainders, a new order will be added, equally consisting of n terns, and perhaps a new one again consisting of the same number of terms; whence we deduce that the number of all the non-remainders, unless there be none, is equal either to the number n, or to its double, or its triple, or, in general, to some multiple of it.

211. Since, therefore, all the non-remainders united with the remainders must exhaust the multitude of all the numbers less than the divisor d and prime to it, we will have either $n = \mu$, or $2n = \mu$, or $3n = \mu$, *etc.* and so, the exponent n will always be an aliquot part of the number μ.

212. But if b and d be numbers prime to each other and μ indicates the multitude of all the numbers prime to d and less than it, and then if

b^n be the lowest power after the case $n = 0$, which, divided by d, leaves the unit, then we will have $n = \mu$, or n will be equal to some aliquot part of μ, so that we have $n = \frac{\mu}{m}$, with m being some divisor of μ.

213. Since, however, after b^n, each of b^{2n}, b^{3n}, b^{4n}, *etc.* also acknowledges the unit as its remainder, the power $b^{mn} = b^{\mu}$, divided by d, will always leave the unit. Hence, provided that b and d be numbers prime to each other, the formula $b^{\mu}-1$ will always be divisible by the number d.

214. Moreover, if c and d also be numbers prime to each other, seeing that $c^{\mu}-1$ admits of division by d, the difference $b^{\mu}-c^{\mu}$ of these formulas will always be divisible by the number d, provided that each of the numbers b and c be prime to d.

215. If we take the prime number p for d, we will have $\mu = p-1$, and the formula $b^{p-1}-1$ will always be divisible by p, unless the number b be a multiple of p. But it can happen that the simpler form b^n-1 also admits of division by p, whereby it is necessarily required that the exponent n be an aliquot part of $p-1$.

216. If the divisor be $d = pq$, with p and q being unequal prime numbers, and b is not included in either of these numbers, then, because $\mu = (p-1)(q-1)$, the form $b^{(p-1)(q-1)}-1$ will be divisible by d.

217. And also if p, q, r, s be unequal prime numbers and if it be that $d = p^{\lambda}q^{\mu}r^{\nu}s^{\xi}$ and also if b be any number whatever prime to d, then setting

$$m = p^{\lambda-1}(p-1)q^{\mu-1}(q-1)r^{\nu-1}(r-1)s^{\xi-1}(s-1),$$

the form b^m-1 will always be divisible by d, and also it can sometimes happen that the simpler form b^n-1, where n is some aliquot part of m, results in divisibility.

218. Yet if we retain the general divisor d and let μ be the multitude of numbers less than and prime to it, while some number prime to d is taken for b, whose smallest power, divided by d, leaving the unit be b^n, we now see that we necessarily have either $n = \mu$, or $n = \frac{1}{2}\mu$, or $n = \frac{1}{3}\mu$, or n

$= \frac{1}{4}\mu$, or $n = \frac{1}{5}\mu$, if indeed μ admits such aliquot parts; which cases it will behoove us to examine more diligently.

219. Certainly one may immediately suspect that this determination depends on the nature of the number b, so that, for a given divisor d, certain numbers taken for b may produce $n = \mu$, others $n = \frac{1}{2}\mu$, others $n = \frac{1}{3}\mu$, others $n = \frac{1}{4}\mu$, or still lesser aliquot parts of μ.

220. But letting n be some aliquot part of μ, if the two powers b^n and c^n leave the unit, the compound $(bc)^n$ will also leave the unit. Then it is clear that the power $(b \pm \lambda d)^n$, divided by d, will also leave the unit.

221. Since the power b^μ always leaves the unit, let's seek out numbers to be taken for b so that $b^{\frac{1}{2}\mu}$ also leaves the unit, in which case it is necessary, above all, that μ be an even number, which indeed always happens unless it be that $n = 2$.

222. Now, if we take $b = cc$, such that c be a number prime to d, it is certain that $b^{\frac{1}{2}\mu} = c^n$ leaves the unit, which also happens if $b = cc \pm \lambda d$. Therefore, fewer numbers, fit to be taken for b, are remainders which result from the division of square numbers by d, provided that the squares be prime to d.

223. Similarly, the power $b^{\frac{1}{3}\mu}$, divided by d, will leave the unit, if it be that $b = c^3$, and, more generally, if $b = c^3 \pm \lambda d$. Therefore, fewer values, fit for b, are remainders arising from the division, by the number d, of cube numbers prime to d. But it is evident that this cannot happen unless the number μ is divisible by 3.

224. If μ be divisible by 4, then the power $b^{\frac{1}{4}\mu}$, divided by d, will leave the unit if $b = c^4$ and, more generally, $b = c^4 \pm \lambda d$. Fewer numbers, therefore, are remainders which arise from the division of biquadratics by d, taking, of course, only those biquadratics that are prime to d.

225. In general, therefore, if the number μ be divisible by ν, the power $b^{\frac{\mu}{\nu}}$, divided by d, will leave the unit if we take $b = c^{\nu}$, or even $b = c^{\nu} \pm \lambda d$, so that the numbers fit to be substituted for b are the remainders, which arise from the division of powers of order ν by the number d, these powers being prime to d.

226. It is sufficient, therefore, to take for b numbers less than d, which are prime to it; yet, the unit, taken for b, certainly gives back all remainders equal to the unit, so that in this case we always have $n = 1$, or $n = \frac{\mu}{\mu}$. There remains this unique case: if the divisor is taken to be $d = 2$, in which, of course, we have $\mu = 1$.

227. Letting the divisor be $d = 3$, we will have $\mu = 2$, and besides the case $b = 1$, for which $n = 1$, we will have the case $b = 2$, whence arises the geometric progression with its remainders:

Geo. progr. $1, 2, 2^2, 2^3, 2^4,$ *etc.*, where we have $n = 2$,
Remainders $1, 2, 1, 2, 1,$ *etc.*, or $n = \mu$.

228. Letting the divisor $d = 4$, we will have $\mu = 2$, and besides the case $b = 1$, in which $n = 1 = \frac{1}{2}\mu$, we have the case $b = 3$.

Geo. progr. $1, 3, 3^2, 3^3, 3^4,$ *etc.*, whereby $n = 2 = \mu$,
Remainders $1, 3, 1, 3, 1,$ *etc.*

229. Letting the divisor be $d = 5$, we will have $\mu = 4$ and we will have these cases

	$b = 1$	$b = 2$	$b = 3$	$b = 4$
Geo. progr.	$1, 1$	$1, 2, 2^2, 2^3, 2^4$	$1, 3, 3^2, 3^3, 3^4$	$1, 4, 4^2$
Remainders	$1, 1$	$1, 2, 4, 3, 1$	$1, 3, 4, 2, 1$	$1, 4, 1$
	$n = 1$	$n = 4$	$n = 4$	$n = 2$

in two cases, therefore, we have $n = 4$, in one $n = 2$ and in one $n = 1$.

230. If the divisor $d = 6$, we will have $\mu = 2$ and there are two cases

	$b = 1$	$b = 5$
Geo. progr.	1, 1	$1, 5, 5^2$
Remainders	1, 1	1, 5, 1
	$n = 1$	$n = 2$

231. If the divisor $d = 7$, we will have $\mu = 6$ and there will be just that many cases

	$b = 1$	$b = 2$	$b = 3$	$b = 4$
Geo. progr.	1, 1	$1, 2, 2^2, 2^3$	$1, 3, 3^2, 3^3, 3^4, 3^5, 3^6$	$1, 4, 4^2, 4^3$
Remainders	1, 1	1, 2, 4, 1	1, 3, 2, 6, 4, 5, 1	1, 4, 2, 1
	$n = 1$	$n = 3$	$n = 6$	$n = 3$

	$b = 5$	$b = 6$
Geo. progr.	$1, 5, 5^2, 5^3, 5^4, 5^5, 5^6$	$1, 6, 6^2$
Remainders	1, 5, 4, 6, 2, 3, 1	1, 6, 1
	$n = 6$	$n = 2$

232. If the divisor $d = 8$, we will have $\mu = 4$ and just that many cases

	$b = 1$	$b = 3$	$b = 5$	$b = 7$
Geo. progr.	1, 1	$1, 3, 3^2$	$1, 5, 5^2$	$1, 7, 7^2$
Remainders	1, 1	1, 3 1	1, 5, 1	1, 7, 1
	$n = 1$	$n = 2$	$n = 2$	$n = 2$

in no case, therefore, will it be that $n = \mu$, but in three $n = \frac{1}{2}\mu$ and in one case $n = \frac{1}{4}\mu$.

233. If the divisor be $d = 9$, we will have $\mu = 6$ and just as many cases

	$b = 1$	$b = 2$	$b = 4$
Geo. progr.	1, 1	$1, 2, 2^2, 2^3, 2^4, 2^5, 2^6$	$1, 4, 4^2, 4^3$
Remainders	1, 1	1, 2, 4, 8, 7, 5, 1	1, 4, 7, 1
	$n = 1$	$n = 6$	$n = 3$

	$b = 5$	$b = 7$	$b = 8$
Geo. progr.	$1, 5, 5^2, 5^3, 5^4, 5^5, 5^6$	$1, 7, 7^2, 7^3$	$1, 8, 8^2$
Remainders	1, 5, 7, 8, 4, 2, 1	1, 7, 4, 1	1, 8, 1
	$n = 6$	$n = 3$	$n = 2$

234. If the divisor be $d = 10$, we will have $\mu = 4$

	$b = 1$	$b = 3$	$b = 7$	$b = 9$
Geo. progr.	1, 1	$1, 3, 3^2, 3^3, 3^4$	$1, 7, 7^2, 7^3, 7^4$	$1, 9, 9^2$
Remainders	1, 1	1, 3, 9, 7, 1	1, 7, 9, 3, 1	1, 9, 1
	$n = 1$	$n = 4$	$n = 4$	$n = 2$

235. Letting $d = 11$, we will have $\mu = 10$ and just as many cases

	$b = 1$	$b = 2$
Geo. progr.	1, 1	$1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}$
Remainders	1, 1	1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1
	$n = 1$	$n = 10$

	$b = 3$	$b = 4$	$b = 5$
Geo. progr.	$1, 3, 3^2, 3^3, 3^4, 3^5$	$1, 4, 4^2, 4^3, 4^4, 4^5$	$1, 5, 5^2, 5^3, 5^4, 5^5$
Remainders	1, 3, 9, 5, 4, 1	1, 4, 5, 9, 3, 1	1, 5, 3, 4, 9, 1
	$n = 5$	$n = 5$	$n = 5$

$b = 6$

Geo. progr.	$1, 6, 6^2, 6^3, 6^4, 6^5, 6^6, 6^7, 6^8, 6^9, 6^{10}$
Remainders	1, 6, 3, 7, 9, 10, 5, 8, 4, 2, 1
	$n = 10$

$b = 7$

Geo. progr.	$1, 7, 7^2, 7^3, 7^4, 7^5, 7^6, 7^7, 7^8, 7^9, 7^{10}$
Remainders	1, 7, 5, 2, 3, 10, 4, 6, 9, 8, 1
	$n = 10$

	$b = 8$
Geo. progr.	$1, 8, 8^2, 8^3, 8^4, 8^5, 8^6, 8^7, 8^8, 8^9, 8^{10}$
Remainders	$1, 8, 9, 6, 4, 10, 3, 2, 5, 7, 1$
	$n = 10$

	$b = 9$	$b = 10$
Geo. progr.	$1, 9, 9^2, 9^3, 9^4, 9^5,$	$1, 10, 10^2$
Remainders	$1, 9, 4, 3, 5, 1$	$1, 10, 1$
	$n = 5$	$n = 2$

236. Letting $d = 12$, we will have $\mu = 4$ and just as many cases

	$b = 1$	$b = 5$	$b = 7$	$b = 11$
Geo. progr.	$1, 1$	$1, 5, 5^2$	$1, 7, 7^2$	$1, 11, 11^2$
Remainders	$1, 1$	$1, 5, 1$	$1, 7, 1$	$1, 11, 1$
	$n = 1$	$n = 2$	$n = 2$	$n = 2$

here, therefore, we always have $n < \mu$, namely, in three cases $n = \frac{1}{2}\mu$ and in one $n = \frac{1}{4}\mu$.

237. If the divisor be $d = 13$, we will have $\mu = 12$ and, for the smallest powers b^n, which, divided by 13, leave the unit, we find

if $b = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$

we have $n = 1, 12, 3, 6, 4, 12, 12, 4, 3, 6, 12, 2$.

238. Just as whenever $b = 1$, we have $n = 1$, whatever the divisor d may be, so to, on taking $b = d-1$, we have $n = 2$, that is, $(d-1)^2$ divided by d leaves the unit, which never happens for the first power. Concerning the remaining values taken for b, however, it is more difficult to judge.

239. Since the power $(kd+1)^n$, divided by d, leaves 1, if it be that $kd+1 = bc$, and the power b^n, divided by d, also leaves the unit, then the power c^n will likewise leave the unit. For, since b^n leaves 1, the product $b^n c^n$ will leave c^n, but, by hypothesis, $b^n c^n$ leaves 1; therefore, in the assessment of the remainders, c^n is equivalent to the unit, that is, c^n, divided by d, will leave the unit.

240. Whence, if b^n be the least power leaving the unit when divided by d, and if it be that $bc = kd+1$, the least power of c leaving the unit will be either c^n, or a yet smaller one, the exponent being an aliquot part of n. But, if a smaller power of c, say $c^{\frac{n}{\nu}}$, leaves the unit, that power of b also leaves the unit, from which, since this is contrary to the hypothesis, it follows that, if b^n be the smallest power leaving the unit, c^n will also be the smallest power leaving 1.

241. Thus, setting $d = 13$, because 5^4 is the smallest power leaving the unit, if it be that $5c = 13k+1$, then c^4 will likewise be the smallest power leaving the unit. Indeed, to make $13k+1$ divisible by 5, we must take $k = 5\lambda-2$, and we will have $c = 13\lambda-5$, whose smallest value is $c = 8$, so that 8^4 is also the smallest power leaving the unit when divided by 13.

242. But whatever be the number b, less than d and prime to it, there will likewise be one, and not more, number c, also less than d and prime to it, such that $bc = kd+1$. For if there were two, so that both $bc = kd+1$ and $be = ld+1$, then $bc-be = b(c-e)$ would be divisible by d, whence, because b and d are prime [to each other], $c-e$ would be divisible by d, which, since c and e are less than d, is not possible unless $e = c$. It may happen, however, that $c = b$, which always comes to pass if it be that either $b = 1$ or $b = d-1$.

Chapter VIII
On Powers of Numbers which, Divided by Prime Numbers, Leave the Unit

243. If the power a^n, divided by the number d, leaves some remainder, all the powers $(a+\lambda d)^n$ with the same exponent will also leave the same remainder; moreover, if n be an even number, the powers $(\lambda d-$

$a)^n$ will also leave the same remainder, whence the investigation of remainders reduces to that of numbers a less than the divisor d.

244. Now let the divisor d be any prime number whatever, and, because the dyad offers no difficulty, we put $d = 2p+1$, and so $2p$ will be the multitude of numbers prime to d and less than it. Now, if a be any number prime to d, which happens provided that a is not a multiple of d, we saw that the power a^{2p}, divided by $d = 2p+1$, always leaves the unit.

245. Often it may happen that some lesser power a^n, with $n < 2p$, divided by the same number $d = 2p+1$, leaves the unit; then, however, the exponent n is certainly an aliquot part of $2p$. But if this happens, not only the formula $a^{2p}-1$, but also the formula a^n-1 will be divisible by the prime number $2p+1$.

246. But if the formula a^n-1 be divisible by the prime number $2p+1$, the formula $a^{mn}-1$ will also be divisible, whence, since the formula $a^{2p}-1$ certainly is divisible by $2p+1$, the difference $a^{mn}-a^{2p}$, or $a^{2p}(a^{mn-2p}-1)$, will also be divisible; because of this, since the factor a^{2p} does not admit of division, it is necessary that the other factor a^{mn-2p} be divisible, whatever number be taken for m.

247. Let λ be the maximum common divisor of the numbers n and $2p$; and if the formula a^n-1 be divisible by the prime number $2p+1$, the formula $a^\lambda-1$ will also be divisible by $2p+1$. For, let $n = \alpha\lambda$ and $2p = \beta\lambda$, so that α and β are numbers prime to each other, and, since both $a^{\alpha\lambda}-1$ and $a^{\beta\lambda}-1$ are multiples of $2p+1$, the formulas $a^{\mu\alpha\lambda}-1$ and $a^{\nu\beta\lambda}-1$ will also be multiples. But, because α and β are prime numbers[10], μ and ν can be found that make $\mu\alpha = \nu\beta+1$, whence the difference will be $a^{\nu\beta\lambda+\lambda}-a^{\nu\beta\lambda} = a^{\nu\beta\lambda}(a^\lambda-1)$, which is divisible by $2p+1$, so that it is necessary that $a^\lambda-1$ be divisible by $2p+1$.

248. If, therefore, n be a number prime to $2p$, the form a^n-1 cannot be divisible by the prime number $2p+1$, unless $a-1$ be divisible by it.

[10] That is, they are prime to each other.

Whence, if $a-1$ be not a multiple of the prime number $2p+1$, the formula a^n-1 cannot be divisible by it, unless n and $2p$ be numbers composite to each other, and if the maximum common divisor of them be λ, the formula $a^\lambda-1$ will be divisible by $2p+1$.

249. If, therefore, a^n be the least power of a, which, divided by the prime number $2p+1$, leaves the unit, then n is certainly an aliquot part of the number $2p$. But then, if it be that $ab = k(2p+1)+1$, then b^n will also be the least power of b, which, divided by $2p+1$, leaves the unit.

250. If n be a prime number and the formula a^n-1 be divisible by the prime number $2p+1$, either n will be an aliquot part of $2p$ (since there does not exist any other common divisor), or, if it be prime to $2p$, the number $a-1$ will be divisible by $2p+1$. Because of this, the formula a^n-1 does not admit other prime divisors besides those of $a-1$, unless they be of the form $2p+1$, with $2p$ a multiple of n. Hence, all of its prime factors will be contained in the form $2mn+1$.

251. Whence, the form a^3-1 does not admit other prime divisors besides the divisors of $a-1$, except those having the form $6m+1$, which are 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, *etc.* Since, therefore, $aa+a+1$ is a factor of a^3-1, it also is divisible by no other prime numbers.

252. In a similar way, the form a^5-1 does not have other divisors besides those of $a-1$, except those contained in the form $10m+1$, which are 11, 31, 41, 61, 71, *etc.* Whence, also numbers of the kind

$$a^4+a^3+a^2+a+1,$$

if they be not prime, do not admit of other divisors.

253. Whenever perfect numbers are sought after, the formula 2^n-1 is a prime number and, in the first place, it is clear that this cannot happen, unless n be a prime number. But if n be such, the formula 2^n-1 will certainly not have divisors other than those of the form $2nm+1$, whence the determination of whether it is prime or not is more easily accomplished [*negotio absolvitur*].

254. Since $a^{2p}-1$ is always divisible by the prime number $2p+1$, and that form consists of the factors a^p-1 and a^p+1, it is necessary that one or the other be divisible by $2p+1$. But we saw that if it be that $a = ee\pm\lambda(2p+1)$, then a^p-1 will be divisible; in these cases, therefore, the formula a^p+1 will certainly not be divisible by $2p+1$.

255. The question arises as to whether the formula a^p-1 might perhaps always be divisible by $2p+1$ and, therefore, never the other a^p+1? It is clear that this should be immediately denied in the case in which p is an odd number. For, because then a^p+1 has the factor $a+1$ and, taking $a = 2p$, this formula is manifestly divisible by $2p+1$.

256. In general, it can, however, be shown in the following way that the formula a^n-1, with $n < 2p$, is not always divisible by the prime number $2p+1$, but rather there certainly are numbers of the sort that, put for a, division of the formula a^n-1 does not occur. This will be most conveniently demonstrated by reduction[11] to absurdity.

257. For, whoever would deny this must affirm that all the formulas 1^n-1, 2^n-1, 3^n-1, 4^n-1, 5^n-1, …, n^n-1 are divisible by $2p+1$ and, therefore, also both their first differences 2^n-1, 3^n-2^n, 4^n-3^n, 5^n-4^n, *etc.* and their second differences $3^n-2.2^n+1^n$, $4^n-2.3^n+2^n$, $5^n-2.4^n+3^n$, *etc.*, and all the following ones.

258. But the differences of order n are constants, which, if they be indicated by the letter N, may be expressed as being $N = (n+1)^n - n.n^n + \frac{n(n-1)}{1.2}(n-1)^n - \frac{n(n-1)(n-2)}{1.2.3}(n-2)^n + etc.$, the values of which, for various values of n, are easily computed:

If $n = 1$ we have $N = 2-1 = 1$

$n = 2$ $N = 3^2-2.2^2+1 = 2 = 1.2$

$n = 3$ $N = 4^3-3.3^3+3.2^3-1 = 6 = 1.2.3$

$n = 4$ $N = 5^4-4.4^4+6.3^4-4.2^4+1 = 24 = 1.2.3.4$

etc.

[11] The Latin phrase often retained in English is, of course, *reductio ad absurdum*. Euler uses the phrase *deductionem ad absurdum*.

259. In order that this may be shown more clearly, writing n+1 for n,

$$P = (n+2)^{n+1} - (n+1).(n+1)^{n+1} + \frac{(n+1)n}{1.2}n^{n+1} - \frac{(n+1)n(n-1)}{1.2.3}(n-1)^{n+1} + etc.,$$

and, beginning with the previous term,

$$P = (n+1)^{n+1} - (n+1)n^{n+1} + \frac{(n+1)n}{1.2}(n-1)^{n+1} - etc.$$

But the value of N can be represented as

$$N = (n+1)^n - n^{n+1} + \frac{n}{1.2}(n-1)^{n+1} - \frac{n(n-1)}{1.2.3}(n-2)^{n+1} + etc.,$$

which, multiplied by n+1, produces the value of P, so that $P = (n+1)N$.

260. Therefore, since we have $N = 1$ in the case $n = 1$, in the case $n = 2$ we will have $N = 1.2$, in the case $n = 3$ we will have $N = 1.2.3$ and, in general, for any number n whatever, we will have $N = 1.2.3\ldots n$. But this difference of order n is not divisible by the prime number $2p$+1, because $n < 2p$, whence it follows that not all the terms of the sequence set out in §257 are divisible by it.

261. Let $6p$+1 be a prime number and, since a^{6p}–1 is divisible by it, unless a be a multiple of it, there will be cases in which a^{2p}–1 will also be able to be divided by it, namely taking $a = c^3 \pm \lambda(6p+1)$. But there will also be cases in which the formula a^{2p}–1 will not be divisible by the prime number $6p$+1, as is evident from the demonstration just now presented.

262. Since we have already shown that the formula a^{3p}–1 will be divisible by $6p$+1, if it be that

$$a = cc \pm \lambda(6p+1),$$

it may now be deduced that, if the number a is contained in both the form $cc \pm \lambda(6p+1)$ and $c^3 \pm \lambda(6p+1)$, then the formula a^p–1 will be divisible by $6p$+1, which will likewise happen if it be that $a = c^6 \pm \lambda(6p+1)$.

263. If $4p$+1 be a prime number, so that a^{4p}–1 is divisible by it, then even a^p–1 will be able to be divided by it, if it be that $a = c^4 \pm \lambda(4p+1)$. In fact, there are also cases in which the formula a^p–1 will not admit of division: certainly those [in which] either a^p+1 or a^{2p}+1 will be divisible by $4p$+1.

Chapter IX

On the Divisors of Numbers of the Form $a^n \pm b^n$

264. Given a prime number $2p+1$, provided that a and b are not multiples of it, then both the formulas $a^{2p}-1$ and $b^{2p}-1$ will be divisible by it; and, therefore, their difference $a^{2p}-b^{2p}$ will also always admit of division by the prime number 2p+1.

265. Let's now suppose that the number a^n-b^n is divisible by the prime number $2p+1$, and in order to investigate in what way this can happen, let's suppose that φ is the maximum common divisor of the numbers n and $2p$, so that, putting $n = \alpha\varphi$ and $2p = \beta\varphi$, the numbers α and β will be prime to each other.

266. Since, however, α and β are numbers prime to each other, it can happen that $\mu\alpha = \nu\beta+1$. Because of this, since $a^{\alpha\varphi}-b^{\alpha\varphi}$ is divisible by $2p+1$, then $a^{\mu\alpha\varphi}-b^{\mu\alpha\varphi}$, that is, $a^{(\nu\beta+1)\varphi}-b^{(\nu\beta+1)\varphi}$, will be divisible, thence, because of $a^{\beta\varphi}-b^{\beta\varphi}$, so too the number $a^{\nu\beta\varphi}-b^{\nu\beta\varphi}$, as well as the same multiplied by a^{φ}, namely $a^{(\nu\beta+1)\varphi}-a^{\varphi}b^{\nu\beta\varphi}$.

267. Removing this last form from the preceding one, the difference $a^{\varphi}b^{\nu\beta\varphi}-b^{(\nu\beta+1)\varphi} = b^{\nu\beta\varphi}(a^{\varphi}-b^{\varphi})$ will be divisible by the prime number $2p+1$. But, $b^{\nu\beta\varphi}$ is not divisible by it, therefore it is necessary that the other factor $a^{\varphi}-b^{\varphi}$ be divisible.

268. Therefore, if the number a^n-b^n be divisible by the prime number $2p+1$ and φ be the maximum common divisor of the numbers n and $2p$, then the number $a^{\varphi}-b^{\varphi}$ will also be divisible by $2p+1$ and, if the latter does not admit of division, the former likewise does not admit of it.

269. And if, therefore, n and $2p$ be numbers prime to each other, that is, the unit is their maximum common divisor, unless $a-b$ be divisible by $2p+1$, a^n-b^n will not admit of division by this prime number.

270. Hence, in investigating the prime divisors of the number a^n-b^n, besides the divisors of $a-b$, which readily present themselves, we must search for the rest amongst those prime numbers $2p+1$, for which $2p$ and n are not prime, but composite, to each other.

271. Whence, if n be a prime number, we must search for all the divisors of the number a^n-b^n, besides those that $a-b$ contains, only amongst prime numbers of the form $\lambda n+1$, if indeed a and b be numbers prime to each other, which condition, it is clear, must be added.

272. Therefore, the prime divisors of the form a^n-b^n, besides $a-b$, for various values of n, should be sought for as follows: (*)

forms	divisors should be sought for amongst these prime numbers:
a^2-b^2	$2\lambda+1$ ... 3, 5, 7, 11, 13, 17, 19, none being excluded
a^3-b^3	$3\lambda+1$ ... 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, *etc.*
a^5-b^5	$5\lambda+1$ ... 11, 31, 41, 61, 71, 101, *etc.*
a^7-b^7	$7\lambda+1$ ... 29, 43, 71, 113, 127, *etc.*
$a^{11}-b^{11}$	$11\lambda+1$ ... 23, 67, 89, 199, 331, *etc.*
	etc.

(*) *Written in the margin.* 1. The number n can also be added to the divisors of the form a^n-b^n. 2. From a^3-b^3, it follows that the number $aa+ab+bb$ cannot have other divisors except $3\lambda+1$; therefore, $3\lambda-1$ certainly are not divisors.

273. If n be not a prime number, but the product of two primes, say $n = \alpha\beta$, the prime divisors of the form $a^{\alpha\beta}-b^{\alpha\beta}$, besides $a-b$, are contained in the form $2p+1$, where $2p$ is not prime to $\alpha\beta$; whence, as either α, or β or even $\alpha\beta$ is the maximum common divisor, the form of the prime divisors will be either $\lambda\alpha+1$, or $\lambda\beta+1$ or $\lambda\alpha\beta+1$, in the first of which λ must not contain β, in the second it must not contain α, but in the third it is not limited.

274. But divisors of the form $\lambda\alpha+1$ also divide $a^\alpha - b^\alpha$, and divisors of the form $\lambda\beta+1$ also divide $a^\beta - b^\beta$, if indeed λ be prime to β in the first, but prime to α in the latter.

275. Because of this, if only those divisors of the formula $a^{\alpha\beta} - b^{\alpha\beta}$ are desired, that do not also divide either $a^\alpha - b^\alpha$ or $a^\beta - b^\beta$, they should be sought amongst prime numbers of the form $\lambda\alpha\beta+1$; but if we prefer to exclude only the divisors of the form $a^\alpha - b^\alpha$, we should seek for the rest amongst the prime numbers $\lambda\beta+1$.

276. Let $\alpha = 2$ and $\beta = 2$, and all the prime divisors of the number $a^4 - b^4$, which do not also divide $a^2 - b^2$, will be contained in the form $4\lambda+1$; and therefore these will be divisors of the numbers a^2+b^2; whence it is clear that numbers of the form a^2+b^2 do not admit of other prime divisors except those that are of the form $4\lambda+1$.

277. Let $\alpha = 2$ and $\beta = 3$, and all the prime divisors of the number $a^6 - b^6$, which do not also divide $a^3 - b^3$, will be contained in the form $2\lambda+1$; but those which also do not divide $a^2 - b^2$, in $6\lambda+1$; these, therefore, will be the divisors of the form $a^2 - ab + b^2$, and such numbers do not admit of [*agnoscunt*] other divisors.

278. From this, we deduce that, in general, if the divisors of $a^{2m} - b^{2m}$ are to be determined, which are not also divisors of the number $a^m - b^m$, that is, if the divisors of the number a^m+b^m are desired, it is required to seek for them amongst prime numbers of the form $2\lambda m+1$. But the divisor $a+b$ is excluded from these if m be an odd number.

279. Thus, we may make the following table for various values of m:

Forms of numbers	divisors should be sought for amongst prime numbers of the form
a^2+b^2	$4\lambda+1$ which are 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97
a^3+b^3	$6\lambda+1$ 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97
a^4+b^4	$8\lambda+1$ 17, 41, 73, 89, 97, 113, 137, 193
a^5+b^5	$10\lambda+1$ 11, 31, 41, 61, 71, 101, 131, 151, 181
a^6+b^6	$12\lambda+1$ 13, 37, 61, 73, 97, 109, 157, 181, 193

a^7+b^7	$14\lambda+1$ 29, 43, 71, 113, 127, 197, 211, 239
a^8+b^8	$16\lambda+1$ 17, 97, 113, 193, 241, 257, 337

etc.

The case where the exponent is a power of the dyad should be noted above all, because the divisors can, in general, be distributed amongst the others. Numbers of the kind $a^{2^n}+b^{2^n}$ do not have other prime divisors, except those contained in the form $2^{n+1}\lambda+1$.

280. But, a^n-b^n will be able to be divided by the prime number $mn+1$ if the numbers a and b be so composed as to make ax^m-by^m divisible by $mn+1$; clearly, provided that numbers can be assigned to x and y, for which this condition is satisfied, then a^n-b^n will certainly be divisible by $mn+1$.

281. For, if ax^m-by^m be divisible by $mn+1$, then $a^nx^{mn}-b^ny^{mn}$ will also be divisible. But the form $x^{mn}-y^{mn}$ is always divisible, and therefore also $a^nx^{mn}-a^ny^{mn}$, on account of which also the difference $a^ny^{mn}-b^ny^{mn}$, and so a^n-b^n will be divisible by the prime number $mn+1$.

282. If, therefore, numbers of such a kind be assumed for a and b that a^n-b^n not be divisible by somr prime number $mn+1$, then no numbers can be assigned to x and y, such that ax^m-by^m admits of division by that same prime number $mn+1$, unless indeed both x and y be a multiple of it, but x and y are stipulated prime to each other.

283. Thus, since 2^2-1 is only divisible by 3, and if $2m+1$ be a prime number, then, unless it be that $m = 1$, no number contained in the form $2x^m-y^m$ will be able to be divided by the prime number $2m+1$:

thus given	no number	will be divisible by
$m = 2$	$2x^2-y^2$	5
$m = 3$	$2x^3-y^3$	7
$m = 5$	$2x^5-y^5$	11
$m = 6$	$2x^6-y^6$	13

etc.

Chapter X
On Remainders Arising
from the Division of Squares by Prime Numbers

284. Whatever remainder is left, when the square a^2 is divided by any number d that you please, the same remainder is likewise left when the infinite squares $(nd \pm a)^2$ are divided by the same number d.

285. Because of this, if we wish to examine the remainders that are left by division of square numbers by a given number d, it will suffice to investigate the squares whose roots are less than the divisor d, therefore these:

$$1, 4, 9, 16, \ldots, (d-4)^2, (d-3)^2, (d-2)^2, (d-1)^2,$$

the number of which is $d-1$.

286. But the extreme squares 1 and $(d-1)^2$, as well as any couple equally remote from the extremes, give equal remainders; whence, if $d-1$ be an even number, more distinct remainders than $\frac{1}{2}(d-1)$ cannot result, and, if $d-1$ be an odd number, on account of the one situated in the middle, no more than $\frac{1}{2}d$.

287. Now let d be a prime number, and because it is easy[12] to judge about the dyad, it is stipulated that $d = 2p+1$; now, since all the remainders result from the squares 1, 4, 9, …, $(p-2)^2$, $(p-1)^2$, p^2, the number of them cannot be greater than p, whence it is clear that not all the numbers less than $d = 2p+1$, whose multitude is $2p$, occur amongst the remainders, but at least half of them are excluded.

288. I say first, however, that all the remainders arising from the squares 1, 4, 9, …, p^2 are unequal to each other; for, if two squares not greater than p^2, say m^2 and n^2, gave the same remainder, their difference m^2-n^2 and, therefore, either $m-n$ or $m+n$, would be divisible by the prime

[12] Reading *promptu* for *promtu*.

$d = 2p+1$, which cannot happen, since, because $m < \frac{1}{2}d$ and $n < \frac{1}{2}d$, we have $m+n$ less than d.

289. Since, therefore, all the remainders, arising from the division of the squares 1, 4, 9, …, p^2 by the prime number $2p+1$, are unequal, we represent them thusly:

roots	1	2	3	4	5	6	p
squares	1	4	9	16	25	36	p^2
remainders	1	α	β	γ	δ	ε	π

and the multitude of these remainders will be = p.

290. Since the multitude of all the numbers less than the divisor $2p+1$, which are also prime to it, is = $2p$, it is clear that half of these numbers are excluded from the class of remainders, and we therefore call them *non-remainders*. The multitude of non-remainders will thus be = p, which we indicate by German letters $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, *etc.*

291. If, therefore, we find the non-remainders for any prime divisor $2p+1$, we will be able to assert that there is no square number xx such that $xx-\mathfrak{A}$ is divisible by $2p+1$, where $\mathfrak{A}$ indicates any non-remainder whatever. And, moreover, there can always be exhibited as many formulas $xx-\mathfrak{A}$, indivisible by $2p+1$, as p contains of units.

292. For any prime divisor $2p+1$, therefore, the numbers less than it can be separated into two classes, of which one encompasses the remainders, the other the non-remainders, each of which contains the same amount of numbers, so that any remainder answers, as it were, to a non-remainder. Thus, it behooves us to examine the nature of these two classes more carefully.

293. If there occur two numbers m and n in the class of remainders, their product mn will likewise occur in it, or a remainder equivalent to it. For, if the remainder m arises from the square a^2 and n from b^2, the remainder mn arises from the product a^2b^2, which is equally a square.

294. If, therefore, any number m whatever be amongst the remainders, all its powers m^2, m^3, m^4, *etc.*, or remainders equivalent to them, will likewise be found in the same place. Then, indeed, if the number n also be there, the numbers mn, m^2n, mn^2 and in general $m^\mu n^\nu$ will likewise be present in the same class of remainders.

295. The class of remainders 1, α, β, γ, …, π of any prime divisor $2p+1$, therefore, has this notable property, that the product of any two or more terms whatever likewise occur in it, provided that, in accord with the nature of remainders, they are reduced to minimum values.

296. It is more remarkable that the class of remainders consists of a fixed number of terms, the number of which is only = p, the same number of non-remainders being excluded. Notwithstanding that in whatever way the remainders may be combined amongst themselves by multiplication, nevertheless the same numbers always occur in that class.

297. Let m be any number whatever occurring in the class of remainders, $2p+1$ being the prime divisor and, as we saw above, if the terms of the geometric progression 1, m, m^2, m^3, m^4, *etc.* be divided by $2p+1$, all the products of pairs of them are also contained amongst the remainders; and thus, no numbers will occur in the remainders of these powers that are not also found in the remainders of the squares.

298. Since, therefore, the multitude of remainders, arising from the powers, cannot surpass the multitude arising from the squares, which is = p, it is clear that either the power m^p or an inferior power produces a remainder = 1. We have already shown this, for, if m has arisen from the square aa, we will have $m = aa - k(2p+1)$; and $m^p - 1$ is clearly divisible by the prime number $2p+1$.

299. But, returning to the remainders of squares, we should observe that, if the numbers m and mn occur therein, then it is necessary that the number n must also be found in the same place. For, if the remainder m arises from the square aa and mn from the square bb, the

remainder *mn* likewise originates from *naa*, whence *bb*–*naa* will be divisible by 2*p*+1, *a* and *b* being prime to 2*p*+1.

300. But if *bb*–*naa* is divisible by 2*p*+1, then $(b+k(2p+1)^2-naa$ will also be divisible. It is, however, always permitted to suppose that *k* be such that it makes *b*+*k*(2*p*+1) = *ac*, that is, such that *k*(2*p*+1) divided by *a* leaves *b*. There is some number *c*, therefore, such that *aacc*–*naa*, that is *cc*–*n*, is divisible by 2*p*+1, whereby the square *cc* will give the remainder *n*.

301. If α be in the class of remainders, but the number $\mathfrak{A}$ in that of non-remainders, the product $\alpha\mathfrak{A}$ will certainly be found in the class of non-remainders. For, if it were in the class of remainders, $\mathfrak{A}$ would likewise be in the same place, contrary to the hypothesis.

302. If the product *mn* occurs in the class of remainders, and one factor *m* of it in the class of non-remainders, the other, *n*, will likewise certainly be found in the class of non-remainders; for, if *n* were in the remainders, *m* would likewise belong in the same place.

303. If two non-remainders $\mathfrak{A}$ and $\mathfrak{B}$ be taken together [*in se ducantur*][13], the product will fall into the class of remainders. For, since every square occurs in the class of remainders, it is evident, first of all, that every square $\mathfrak{A}^2$, $\mathfrak{B}^2$, $\mathfrak{C}^2$, *etc.* is there; it is now required further to set up a proof that the product $\mathfrak{AB}$ of the two of them be indeed also found in the same place.

304. The remainders 1, α, β, γ, *etc.*, whose number is = *p*, being known, and 2*p*+1 being the prime divisor, there are indeed for the same divisor non-remainders, whose number, since the remainders are numbers less than 2*p*+1, is likewise = *p*. But, given one non-remainder $\mathfrak{A}$, all the rest [of them] are determined thusly from the remainders: $\mathfrak{A}$, $\alpha\mathfrak{A}$, $\beta\mathfrak{A}$, $\gamma\mathfrak{A}$, *etc.*, being reduced, of course to the smallest terms. For these numbers are unequal to each other and their multitude is = *p*.

[13] The metaphor is that of marriage.

305. Any two non-remainders $\mathfrak{D}$ and $\mathfrak{E}$ whatever can be considered, therefore, as products of the kind $\delta\mathfrak{A}$ and $\varepsilon\mathfrak{A}$, where δ and ε are remainders and $\mathfrak{A}$ a non-remainder; whence, the product of any two non-remainders will be $\mathfrak{DE} = \delta\varepsilon\mathfrak{AA}$, where $\delta\varepsilon$, in as much as it is a product of two remainders, is found in the class of remainders.

306. But then $\mathfrak{AA}$ also occurs in the class of remainders, because all the squares, or equivalent remainders, are found in it. Because of this, since $\delta\varepsilon$ and $\mathfrak{AA}$ are both remainders, it is necessary that their product $\mathfrak{DE}$ likewise be a remainder, and so the product of any two non-remainders is certainly contained in the class of remainders.

307. Therefore, the joining of two numbers according to their nature of being remainders and non-remainders is done thusly:

1. The product of two remainders is a remainder.
2. The product of a remainder and a non-remainder is a non-remainder.
3. The product of two non-remainders is a remainder.

308. These things will be thoroughly illuminated, if we consider carefully the remainders and non-remainders [arising] from the division of squares by prime numbers:

divisor	3	5	7	11
remainders	1	1, 4	1, 4, 2	1, 4, 9, 5, 3
non-remainders	2	2, 3	3, 5, 6	2, 6, 7, 8, 10

divisor	13	17
remainders	1, 4, 9, 3, 12, 10	1, 4, 9, 16, 8, 2, 15, 13
non-remainders	2, 5, 6, 7, 8, 11	3, 5, 6, 7, 10, 11, 12, 14

divisor	19
remainders	1, 4, 9, 16, 6, 17, 11, 7, 5
non-remainders	2, 3, 8, 10, 12, 13, 14, 15, 18

divisor	23
remainders	1, 4, 9, 16, 2, 13, 3, 18, 12[14], 8, 6
non-remainders	5, 7, 10, 11[15], 14, 15, 17, 19, 20, 21, 22

divisor	29
remainders	1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22
non-remainders	2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27 (*).

(*) *Written in the margin*. Divisor: 59. Remainders:1, –2, 3, 4, 5, –6, 7, –8, 9, –10, –11, 12, –13, –14, 15, 16, 17, –18, 19, 20, 21, 22, –23, –24, 25, 26, 27, 28, 29. Therefore, if $4n-1$ be prime, either the form $xx+myy$ or $xx-myy$ is divisible by it.

309. We call the number, which together with the remainder makes up the divisor, the *complement* of the remainder; so, if the divisor be = d and some remainder be = r, its complement will be $d-r$.

310. If the complement of any remainder occurs in the class of remainders, the complements of all the remainders will occur in that same place. For, if $d-\alpha$, with d being the divisor, occurs in the class of remainders $1, \alpha, \beta, \gamma, \delta$, *etc.*, the remainder $d-\alpha$ can also be represented by $-\alpha = -1.\alpha$, because of which, since both α and the product $-1.\alpha$ are remainders, -1 will also be a remainder, and, therefore, $-\beta, -\gamma, -\delta$, *etc.*, which are equivalent to the rest of the complements, will also be remainders.

311. Therefore, either none or all of the complements will occur in the sequence of remainders. It is clear from the examples above, if the divisor be either 3, or 7, or 11, or 19, or 23, the complement of no remainder is to be found amongst the remainders, but they are all non-remainders. But if the divisor be 5, or 13, or 17, or 29, the complements of each remainder is likewise to be found in the class of remainders.

312. If the prime divisor be $2p+1$, and the complements of each [remainder] likewise occur amongst the remainders, seeing that they are

[14] Reading 12 for 11.
[15] Reading 11 for 12.

joined to each other in pairs, so that either one [of the pair] is the complement of the other, and neither can any one be its own complement, since $2p+1$ does not admit of a half, the number of remainders will necessarily be even.

313. Since, therefore, the number of the remainders is = p, it cannot happen that the complements of the remainders are also remainders, unless p be an even number. Because of this, if p be an odd number, it is certain that the complement of no remainder is contained in the class of remainders, and hence the complements of all the remainders make up the class of non-remainders.

314. Let, therefore, p be the odd number = $2p-1$, so that the prime divisor is $4q-1$, and all the complements of remainders are non-remainders. Thus, if α be any remainder whatever, its complement $4q-1-\alpha$ will be a non-remainder, that is, there is no square, which divided by $4q-1$, leaves $4q-1-\alpha$.

315. Since, therefore, α can indicate any square whatever, say nn, there is no square reduced by the number, $4q-1-nn$, that can be divided by $4q-1$. Hence, $mm-(4q-1-nn)$, or $mm+nn$, never proves to be divisible by a prime number of the form $4q-1$, unless by chance each of the numbers m and n be divisible by it.

316. It has been demonstrated, therefore, that the sum of two squares prime to each other cannot be divided by any prime number of the form $4q-1$. But if such a sum of pairs of squares has prime divisors, they certainly are of the form $4q+1$, discounting, of course, the dyad, which also can be a divisor whenever both squares are assumed odd.

317. When the complements of the remainders are discovered amongst the remainders, the complements of the non-remainders will also be non-remainders; but if the complement of one remainder be a non-remainder, all the complements of the remainders will be non-remainders, and the complements of the non-remainders will, in turn, be remainders.

318. If the divisor be $2p+1$, it is only in the case that p be an even number that the complements of the remainders are likewise remainders; that they are always remainders, however, has not yet been established [*evictum*]. But, for this, these remainders should be compared with the remainders arising from the sequence of powers, for the same divisor $2p+1$, [as to] whether the sequence of powers is constituted in such a way that the multitude of remainders be equal to the multitude of non-remainders.

319. Let $1, a, a^2, a^3$, *etc.* be a sequence of powers of this kind, which produces p distinct remainders, the prime divisor being $= 2p+1$, so that all the remainders will be $1, a, a^2, a^3, \ldots, a^{p-1}$, which powers, of course, being used, as it were, as equivalent to the remainders. But the non-remainders, just as many in number, are expressed thusly: $A, Aa, Aa^2, Aa^3, \ldots, Aa^{p-1}$.

320. Here the remainders, just as the remainders of squares, are so composed that 1) they begin with the unit, 2) the product of a pair of remainders is likewise a remainder, 3) the product of a remainder and a non-remainder occurs amongst the non-remainders, whence one may conclude that the product of a pair of non-remainders crosses over again into the class of remainders.

321. If a^p-1 be divisible by $2p+1$, then a is certainly a remainder of the squares. For, if it were a non-remainder, all the rest of the remainders, which are $a\alpha$, $a\beta$, $a\gamma$, *etc.*, would have the very same property and, therefore, all of the numbers x would be so constituted that x^p-1 could be divided by $2p+1$, which is absurd (*).

(*) This paragraph was inserted handwritten in the margin.

322. For, since it is contained amongst the remainders of squares, where the number of non-remainders is equal to the number of remainders, if it turns out otherwise in the remainders of powers, and the product of a pair of non-remainders gives a non-remainder again, the

multitude of non-remainders will surpass the multitude of remainders, contrary to the hypothesis.

323. This can also be shown more convincingly thus: Since A can indicate any non-remainder whatever, and also any non-remainder can be represented as being Aa^n, the product of a pair of non-remainders will be AAa^n, which, if it were a non-remainder, would be equivalent to a form of the kind Aa^m, or of the kind $Aa^{m+\nu p}$, such that m is greater than n, and therefore the difference $A^m - AAa^n$ would be divisible by $2p+1$.

324. But since neither A nor a^n can be divided by $2p+1$, $a^{m-n} - A$ would be divisible by $2p+1$, that is, the power a^{m-n}, divided by $2p+1$, would leave the remainder A. But, since A is not a remainder, it follows that this hypothesis is absurd, and therefore the product of two non-remainders is not contained in the form Aa^m, which encompasses all the non-remainders, and therefore it is necessary that it occur amongst the remainders.

325. Because of this, if a be such a number that a^p is the least power which, divided by the prime number $2p+1$, leaves the unit, and therefore as many distinct remainders arise from the division of the terms of the geometric progression $1, a, a^2, a^3, a^4, \ldots, a^{p-1}$ as p contains of units, and there are just that many non-remainders, it is certain that all the products of pairs of non-remainders are contained in the class of remainders.

326. But since all the numbers less than the divisor $2p+1$ are contained either in the remainders or in the non-remainders, the squares of each one will certainly occur in the class of remainders, which also happens in the remainders arising from squares, so it follows that both classes of remainders, both that arising from squares and that from the geometric progression above, clearly agree with each other.

327. And if $1, \alpha, \beta, \gamma, \delta$, *etc.* be the remainders of the squares divided by the prime divisor $2p+1$, and $\mathfrak{A}$ be any non-remainder whatever, the number $\mathfrak{A}$ will also be found amongst the non-remainders which answer

to the geometric progression 1, a, a^2, a^3, …, a^{p-1}, if indeed a^p be the least power producing the unit for its remainder.

328. We already saw above that, if a be a remainder arising from squares, a^p-1 will certainly be divisible by $2p+1$; now, however, it is clear that, if a be a non-remainder with respect to squares, then a^p is not the least power of this a, which, divided by $2p+1$, leaves the unit. Therefore, either a^p will not leave the unit, or there will also be a lesser one $a^{\frac{p}{\nu}}$, which leaves the unit.

329. If a be a number of such a kind that its power a^p, divided by the prime number $2p+1$, leaves the unit, then a is certainly contained amongst the remainders of the squares. This is evident if a^p be the least power of this type. But, if on the contrary, it be not the least, it would appear to be all the more true of it. For, if there be a lesser one, some of them will cross over from those remainders, in number p, into the class of non-remainders. For, if $a^{\frac{1}{2}p}$ be the least, then a will be contained amongst the remainders of the biquadratics, but if $a^{\frac{1}{3}p}$, amongst the remainders of the sixth powers, *etc.*, therefore it will always be contained amongst the remainders of squares.

330. If, therefore, a be a non-remainder in regard to squares, then a^p-1 is certainly not divisible by $2p+1$, whence, if a be a complement of any remainder whatever, say $a = d-\alpha$, putting $d = 2p+1$, then $(d-\alpha)^p-1$ is not divisible by 2p+1, but α^p-1 is certainly divisible, because α is a remainder, whence the difference $(d-\alpha)^p-\alpha^p$ will also not be divisible.

331. But this difference would be divisible if p were an even number, because, unless p be an odd number, that situation cannot be the case and we may suppose any $(d-\alpha)^p-1$ undividable by $2p+1$, that is, any $d-\alpha$ is a non-remainder.

332. But if p be an even number, any complement of a remainder α, say $d-\alpha$, is certainly a remainder, and for this reason $(d-\alpha)^p-1$ is

divisible by $2p+1$; for, if it were a non-remainder, this divisibility could not happen.

333. If, therefore, it be that $p = 2q$ and the number $= 4q+1$ be the proposed prime divisor, then the complements of every [remainder] will be found amongst the remainders of squares, that is, if the remainders be 1, α, β, γ, *etc.*, then -1, $-\alpha$, $-\beta$, $-\gamma$, *etc.* will also be remainders.

334. Thus, for any of the squares taken from the progression 1, 4, 9, 16, …, $4qq$, there will be another, which, added to that one, produces a sum divisible by $4q+1$, that is, since the multitude of these square be $= 2q$ and each one has, as it were, its conjugate[16], there will be q pairs of two distinct squares, whose sum is divisible by $4q+1$. (*)

(*) *Written in the margin*: Two squares can always be produced, whose sum is divisible by the prime number $4q+1$, and indeed one of the squares may be taken at will.

335. And because each square does not surpass $4qq$, the sum of the pair is certainly less than $8qq$, whence, if such a sum be divided by $4q+1$, the quotient will certainly be less than $2q$. This quotient, however, unless it be $= 2$, will also be either a prime number of the form $4n+1$, or some product of such primes (316).

336. Therefore, $4q$, and hence also q, the complement, as it were, of the unit, to which -1 is equivalent, occurs amongst the remainders of the squares as many times as there is a prime divisor of the form $4q+1$; and, in the same way, all the remaining negative squares, -4, -9, -16, *etc.*, also occur in that very place, so that the included remainders encompass [those] of both the squares and of those taken negatively, and, together with the products of all their pairs, the multitude of all of which numbers, if they be brought to their least form by division by $4q+1$, will still be $= 2q$, so that the same amount is excluded.

[16] Or, more literally, “consort”; once again, the metaphor is that of marriage.

337. Contrarywise, however, if the prime divisor be of the form $4q-1$, then -1 and all the negative squares are returned to the non-remainders (*). For, if -1 were a remainder, $(-1)^{2q-1}-1$ would be divisible by $4q-1$, which, however, cannot happen. But in the previous case, if -1 be a non-remainder, when the divisor is $4q+1$, then $(-1)^{2q}-1$ would not be divisible by $4q+1$, which, in the same way, is false.

(*) *Written in the margin*: Therefore, there are not any sums of two squares divisible by a prime number $4q-1$.

338. Only squares, however, are always found in the class of the remainders, the remaining numbers indeed fall now amongst the remainders, now amongst the non-remainders, depending on the divisor, just as we saw that -1 is a remainder, if the divisor be $4q+1$, but -1 is a non-remainder, if the divisor be $4q-1$.

339. For other, non-square numbers, a similar criterion is observed: The number $+2$ is of course found amongst the remainders, as often as the prime divisor is either of the form $8q+1$ or of the form $8q-1$, that is, $8q+7$. In the remaining cases, in which the divisor is either $8q+3$ or $8q+5$, the number $+2$ occupies a place amongst the non-remainders. (*)

(*) *Written in the margin*: But this cannot, as the preceding, be fortified by a demonstration.

340. But the number -2 occurs amongst the remainders in the cases in which the prime divisor is either $8q+1$ or $8q+3$; the same number -2, however, falls amongst the non-remainders in the cases in which the prime divisor is either $8q+5$ or $8q+7$.

341. Further, the number $+3$ is a remainder, if the prime divisor be either $12q+1$ or $12q+11$; but the same will be a non-remainder, if the divisor be either $12q+5$ or $12q+7$. The number -3, however, is a remainder, if the prime divisor be either $12q+1$ or $12q+7$; but -3 will be a non-remainder, if the divisor be $12q+5$ or $12q+11$.

342. The number +4 is always assigned to the remainders, and the decision about –4 is the same as for –1. The number 5, however, is found amongst the remainders, if the divisor be either $20q+1$, or $20q+9$ or $20q+11$, or $20q+19$; but –5 is found amongst the remainders, if the divisor be either $20q+1$, or $20q+3$, or $20q+7$, or $20q+9$.

343. Let's bring together these results, so that they may be surveyed in a single view:

Number will be in remainders	if the prime divisor be
+1	$4q+(1, 3)$
–1	$4q+1$
+2	$8q+(1, 7)$ (*)
–2	$8q+(1, 3)$
+3	$12q+(1, 11)$
–3	$12q+(1, 7)$
+5	$20q+(1, 9, 11, 19)$
–5	$20q+(1, 3, 7, 9)$
+6	$24q+(1, 5, 19, 23)$
–6	$24q+(1, 5, 7, 11)$
+7	28q+(1, 3, 9 19, 25, 27)
–7	$28q+(1, 9, 11, 15, 23, 25)$
+10	$40q+(1, 3, 9, 13, 27, 31, 37, 39)$
–10	$40q+(1, 7, 9, 11, 13, 19, 23, 37)$
+11	$44q+(1, 9, 25, 5, 7, 37, 39, 19, 35, 43)$
–11	$44q+(1, 9, 25, 5, 37, 3, 15, 23, 27, 31)$
+12	$48q+(1, 11, 13, 23, 25, 35, 37, 47)$
–12	$48q+(1, 13, 25, 37, 7, 19, 31, 43)$
+14	$56q+(1, 5, 9, 13, 25, 45, 11, 31, 43, 47, 51, 55)$
–14	$56q+(1, 5, 9, 13, 25, 45, 3, 15, 19, 23, 27, 39)$
+15	$60q+(1, 7, 11, 17, 43, 49, 53, 59)$
–15	$60q+(1, 17, 49, 53, 19, 23, 31, 47)$(**)

etc.

Written in the margin:

(*) $xx-2yy$ does not admit other divisors except those of the form $8q+(1, 7)$.

(**) 1) If $xx = mn+r$, then the square xx, divided by m or by n, leaves the same remainder r. Therefore, if the remainder r agrees with the divisor m, it will also agree with the divisor n.

2) If

divisor	in non-remainders	remainder
$4n-1$	-1	
$8n-1$	-2	$+2$
$8n-3$	± 2	
$12n-1$	-3	$+3$
$12n-7$	± 3	
$8n\pm 3$	$+2$	

This can be demonstrated; but, if divisor be $8n+1$, then $+2$ is in remainders, which, however, cannot be demonstrated from this.

344. Up to here, however, these results only rest upon induction[17], but, in order that a demonstration be found out, it will be helpful to observe the following. First of all, any number whatever $\pm n$ will be found amongst the remainders, if the prime divisor be of the form $4nq+1$, or even $4nq+ii$, where i indicates any odd number whatever. Next, a positive number $+n$ will be a remainder, if the prime divisor be of the form $4nq-1$, or more generally $4nq-ii$; for these divisors, however, a negative number $-n$ will be found amongst the non-remainders.

345. If a positive number n be a remainder for the divisor d, it will also be a remainder for any prime divisor of the form $4nq\pm d$, or even $4nq\pm dii$; but, if a negative number $-n$ be a remainder for the divisor d, it will likewise be a remainder for the divisor $4nq+d$, but a non-remainder for the divisor $4nq-d$.

346. If a positive number n be a remainder for the divisor d, and further also for the divisor e, it will also be a remainder for any prime divisor of the form $4nq\pm de$. But if a negative number $-n$ be a remainder for the divisors d and e, it will likewise be a remainder for any prime divisor of the form $4nq+de$; for the divisors $4nq-de$, however, it will be assigned to the non-remainders.

347. If a positive number n be a non-remainder for the divisors d and e, it will certainly be a remainder for all the prime divisors of the form

[17] That is, induction by enumeration, not mathematical induction.

$4nq \pm de$; but if the negative number $-n$ be a non-remainder for the divisors d and e, it will be a remainder for all prime divisors of the form $4nq+de$; for divisors of the form $4nq-de$, however, it will be a non-remainder.

348. Any number $\pm n$ being proposed, it will always be a remainder, if the prime divisor be contained in anyone of the forms of the kind $4nq+A$, $4nq+B$, $4nq+C$, *etc.*, the number of which is equal to half of the multitude of the numbers prime to $4n$ and less than it. But if, however, the divisor is contained in the remaining forms, it will be a non-remainder.

349. The case in which the number n is a square and, of course, always occurs amongst the remainders, whatever divisors be taken, should, however, be removed. And, moreover, if n be a negative square, the same reasoning applies as for -1.

350. It should be demonstrated first, therefore, that, if the prime divisor be $4nq+ii$, where i is an odd number, both the numbers n and q, as well as their negatives $-n$ and $-q$, always occur amongst the remainders of squares. Let $i = 2m+1$ and because the divisor $4nq+4mm+4m+1$ is of the form $4p+1$, the negative square $-4mm-4m-1$ is contained amongst the remainders and, therefore, the number $4nq$ and, because 4 is a remainder, also the number nq, and likewise $-nq$; because of this, either both numbers n and q must occur at the same time amongst the remainders, or at the same time amongst the non-remainders, whence it is necessary that, provided either one be amongst the remainders, the other will be found in the same place.

351. If n were not a remainder, there would be no square xx, such that $xx-n$ would be divisible by $4nq+4mm+4m+1$. If, therefore, it could be demonstrated that there is such a square, the truth of the proposition would be established. Actually, if n were a non-remainder, the expression $n^{2nq+2mm+2n}-1$ would not be divisible by the prime number, and, therefore, if the contrary could be demonstrated, we would have what we want [*intendimus*]. (*)

(*) *Written in the margin*: If n were a non-remainder, nzz would likewise be a non-remainder, and therefore also

$$\pm nzz \mp y(4nq + 4mm + 4m + 1),$$

which expression, if it were the case for even one square, would establish the proposition. In this respect, it would seem that, because of the ambiguous sign, it must occur in at least one case; and all the more so, since n and q are interchangeable, and moreover it is true even if the divisor be not prime. Question, if $n = 3$, $q = 5$, $2m+1 = 5$, $\pm 3zz \pm 85y$, or $\pm 5zz \pm 85y$, cannot be made a square. Therefore, the demonstration should be set up so that the divisor be a prime.

352. Further, it is necessary to demonstrate that, if the prime divisor be $4nq-4mm-4m-1$, the number n occurs amongst the remainders of the squares, but the number $-n$ amongst the non-remainders. Equally so, that the number q will be amongst the remainders and $-q$ amongst the non-remainders. However, since $(2m+1)^2$ is certainly amongst the remainders, $4nq$ and therefore also nq, will be in the same place.

353. Conceding these propositions, even though the demonstration be not yet known, assuming that i is an odd number and that $4nq \pm ii$ is prime, for the prime divisor $4nq+ii$, since n and $-n$ are remainders, and likewise naa and $-naa$, there will always be a square xx such that $xx-naa$ be divisible by $4nq+ii$, and further also a square yy such that $yy+naa$ be divisible by $4nq+ii$.

354. But when the prime divisor be $4nq-ii$, because of the remainder naa, there will always be a square xx, such that $xx-naa$ is divisible by $4nq-ii$; there does not exist, however, any square yy, such that $yy+naa$ is made divisible by $4nq-ii$, because in this case $-naa$ is a non-remainder.

355. When $4nq+ii$ is a number of the form $4p+1$, there will always be a sum of two squares $ff+gg$ divisible by it, one of which can be selected at will. Because of this, if $xx-naa$ be divisible by $4nq+ii$, a square yy can be found, such as to make $xx+yy$ divisible by $4nq+ii$ and, moreover, $yy+naa$ will also be divisible by it.

356. When $4nq-ii$ is of the form $4p-1$, there are no sums of squares divisible by $4nq-ii$; because of this, if $xx-naa$ were divisible by $4nq-ii$, it

could not happen that $yy+naa$ be divisible by it; for then the sum $xx+yy$ would likewise be divisible, which is absurd.

357. Assuming $d = 4nq+ii$ as the prime divisor, because there is a form $xx+naa$ divisible by it, there will also be a form $yy+qaa$ divisible by it, whence also $qxx–nyy$. Indeed, there will also be a divisible form $yy–qaa$, and also, for this reason, one of the form $qxx+nyy$.

358. If the prime divisor be $d = 4nq–ii$, because there are such formulas as $xx–naa$ and $yy–qaa$ divisible by it, the form $qxx–nyy$ will also be divisible by d. Since, however, the form $yy+qaa$ is not divisible by d, no form of the kind $qxx+nyy$ will be divisible by d.

359. Although these propositions can indeed be demonstrated, the others, as we have observed above, have not yet been established. From 345, if there be a square leaving, when divided by d, the positive remainder n, there will also be one leaving naa; then, however, $4nq\pm d$ being a prime number, there will be some square xx, which, divided by $4nq\pm d$, leaves the same remainder, that is, $xx–naa$ will be divisible by $4nq+d$.

360. Of course, if $bb–naa$ be divisible by d, there will always be a number $xx–naa$ divisible by the prime number $4nq\pm d$. Moreover, when i indicates an odd number, a form of the kind $xx–naa$ can be produced, which is divisible by the prime number $4nq\pm dii$.

361. If there be a square bb, which leaves a negative remainder $–n$ or $–naa$ on division by d, there will also be a square xx, which, divided by the prime number $4nq+dii$, leaves $–n$ or $–naa$. Of course, if d be a divisor of the form $bb+ncc$, there will be an x such that $xx+naa$ is divisible by the prime number $4nq+dii$.

362. Indeed, if d be a divisor of the form $bb+ncc$, there will not be any form $xx+naa$, which is divisible by the prime number $4nq–dii$. If, for example, it be that $n = 3$, take $d = 7$, because $2^2+3.1 = 7$, and it is certain

that no numbers of the form $xx+3aa$ admit divisors of the form $12q-7ii$, some of which are: 5, 17, 29, 41, 53, 65, 77, 89, 101, 9, 21, 33, 45.

363. It follows from §346 that, if d and e be divisors of any number of the form $aa-nbb$, then there always is a square xx, such that $xx-ncc$ is divisible by the prime number $4nq\pm deii$, which can also be deduced from the preceding, demonstrating that if $aa-nbb$ has the divisor d, and another similar form $ff-ngg$ the divisor e, there will also be an $hh-nkk$ divisible by the product de. This will be clear if we consider carefully remainders of squares divided by composite numbers.

364. Further, it is noteworthy that the number n, and also, therefore, naa, cannot occur amongst the remainders of squares, unless the prime divisor be of the form $4nq+\alpha$, where α does not signify all the numbers prime to $4n$ and less than it, but only half of them, the other half being completely excluded. And thus, all prime divisors of the form $xx-naa$ have a form of the kind $4nq+\alpha$, where α indicates several numbers, with just as many being excluded.

365. The reckoning is similar for numbers of the form $aa+naa$, whose prime divisors are restricted to the form $4nq+\alpha$, so that the same amount of numbers are excluded from α as are admitted. In either case, however, all odd squares ii are valid for α and, if α is valid, αii will also be valid.

366. In order to attempt these desired demonstrations, we consider the prime divisor $4p+1$, and since the sum of two squares $aa+bb$ divisible by it can be exhibited, for which one can be taken at will, $(4p+1)bb$ is removed and $aa-4pbb$ will be divisible by $4p+1$, that is, there will be a square aa, which, divided by $4p+1$, leaves $4pbb$, therefore leaving p, that is, there will be a form $aa-pbb$ that is divisible by $4p+1$.

367. Since there is a form $aa-bb$ divisible by $4p+1$, adding $(4p+1)bb$, there will also be a form $aa+pbb$ divisible by 4p+1, which is already clear because, if the squares be divided by the prime number $4p+1$, both $+p$ and $-p$ will be found in the remainders.

368. But, let the prime divisor be $4ffp+ii$, where i indicates an odd number, and because both forms $aa+bb$ and $aa-bb$, divisible by it, can be exhibited, hence $iiaa+iibb$ and $iiaa-iibb$; taking away from there and adding here $(4ffp+ii)bb$, the formulas $iiaa-4ffpbb$ and $iiaa+4ffpbb$ will be divisible by $4ffp+ii$, that is, $\pm 4ffpbb$ will be amongst the remainders of the squares and, therefore also $\pm p$. Thus, there will be numbers of the forms $xx+pyy$ and $xx-pyy$ divisible by $4ffp+ii$. (*)

(*) *Written in the margin*: The preceding is manifest; for $\frac{xx+pyy}{4ffp+ii}$ = integer if $x = i$, $y = 2f$;
that $xx-2yy$ be divisible by 41 $x = 7, 10, 13, 14, 17$
$y = 2, 3, 8, 4, 1$
that $xx-2yy$ be divisible by 17,

$x =$	12, 5	11, 6	10, 7	16, 1	17, 4
$y =$	2	1	4	3	5

369. Therefore, if, the observations above being granted, the prime divisor is contained in any of these forms: $4rq+1$, $4rq+\alpha$, $4rq+\beta$, $4rq+\gamma$, $4rq+\delta$, *etc.*, where the numbers $1, \alpha, \beta, \gamma, \delta$, *etc.* are prime to $4r$ and less than it, only half of which occur here, then the number r certainly occurs amongst the remainders of the squares; and for the remainder $-r$, the formulas for the divisors are treated in a similar way, agreeing with them if the divisor be of the form $4p+1$, but disagreeing with them if the form of the divisor be $4p-1$.

370. It is also worthwhile to observe that, from the form $4rq+4m+1$, half are to be excluded both for the remainder $+r$ and for $-r$, the divisors of which are common for this form. But, from the form $4rq+4m-1$, half are valid for the remainder $+r$, the other half for the remainder $-r$, and here the divisors that are valid for one remainder are excluded from the other.

Chapter XI
On Remainders Arising from the Division of Cubes by Prime Numbers

371. When the prime divisor be $d = 2p+1$, whatever remainder is left by the cube a^3, the same will also be left by the cubes $(a+d)^3$, $(a+2d)^3$, *etc.* and in general $(a+nd)^3$; because of this, it suffices to consider only those cubes, whose roots are less than d, which are:

$$1, 8, 27, 64, \ldots, (d-4)^3, (d-3)^3, (d-2)^3, (d-1)^3.$$

372. Let r be the remainder which any one of these cubes, a^3, leaves; it is clear that the cube $(d-a)^3$ will leave the remainder $-r$, or $d-r$. Because of this, if any number r whatever occurs amongst the remainders of the cubes, its negative $-r$, or $d-r$, which is called the complement of the former, will likewise occur in the very same place.

373. Let $1, \alpha, \beta, \gamma, \delta$, *etc.* be the remainders arising from the division of the cube numbers by the prime number $d = 2p+1$, of which, if they be all mutually distinct, the number will be $= d-1$; and therefore all the numbers less than d will occur there. But if any numbers occur two or more times, then some numbers will be excluded and assigned to the non-remainders. (*)

(*) All the cubes less than d^2, reduced to minimum values, as well as their products two at a time, three at a time *etc.*, occur in these remainders.

374. To investigate whether it can happen that the same number r occurs amongst the remainders twice, let's assume that the same remainder r results from the cubes a^3 and b^3, whose roots a and b are unequal and less than the divisor d, and so their difference $b^3-a^3 = (b-a)(aa+ab+bb)$ will be divisible by d. But, since d is prime to the factor $b-a$ (because d is prime), it is necessary that the other factor $aa+ab+bb$ be divisible by d.

375. But if the cube b^3 produces the same remainder as the cube a^3, to any other cube c^3 there will answer the cube e^3, likewise leaving the same remainder as the former. For, if the cubes a^3 and b^3 produce the same remainder, so also will a^3x^3 and b^3x^3, reduced to minimum values, that is, $(ax–md)^3$ and $(bx–nd)^3$, bring forth the same remainder. But because a and d are numbers prime to each other, it is always permitted to take x and m such that $ax–md$ be equal to the given number c, and hence we will have $e = bx–nd$, distinct from c and less than d; for, if it were that $e = c$, we would have $ax–md = bx–nd$, and hence $(a–b)x$ would be divisible by d, although neither $a–b$ nor x is divisible.

376. Thus, it is immediate that, if one remainder occurs twice, they will all occur twice; and, therefore, the multitude of distinct remainders is reduced by half. This cannot happen, however, unless the divisor d be a divisor of the form $aa+ab+bb$, where a and b are less than d. But if the divisor be not of that form, all the remainders will be distinct and their multitude = $d–1 = 2p$.

377. Let the cubes a^3 and b^3 produce the same remainder r, so that a^2+ab+b^2 is divisible by d, and also $3a^3+3a^2b+3ab^2$ will be divisible by d; $a^3–b^3$ is taken away, so that we have that

$$2a^3+3a^2b+3ab^2+b^3 = a^3+(a+b)^3$$

is divisible by d. Therefore, because a^3 leaves r, the cube $(a+b)^3$ will leave the remainder $–r$ and, hence, the cube $(d–a–b)^3$, or $(2d–a–b)^3$, will give the remainder $+r$.

378.[18] And immediately, therefore, if there are two cubes a^3 and b^3, leaving the same remainder r, there will also be a third $(d–a–b)^3$, or $(2d–a–b)^3$, leaving the same remainder, the root of which will be less than d and distinct from both the preceding a and b. For, neither can it be that $d–a–b = a$, nor that $2d–a–b = a$; for, if it were [the case] that $b = d–2a$, or $b = 2d–2a$, then b^3 would leave the remainder $–8a^3$, or $–8r$. But, because it leaves r by hypothesis and the two remainders r and $–8r$ cannot be

[18] Reading 378 for 387.

equivalent, because the difference = $9r$ is not divisible by d, except for the case $d = 3$, which is obvious, it follows that two equal remainders always suppose a third.

379. If therefore two cubes a^3 and b^3 produce the same remainder r, there will consequently be a third c^3 exhibiting the same remainder, the root of which is so constituted that the sum of all of them $a+b+c$ is either $= d$, or $= 2d$, for $c = d-a-b$ or $c = 2d-a-b$, because of which, each of them is less than d. And, thus, from two it is always easy to find the third.

380. From this one may deduce, moreover, that there are never more than three cubes a^3, b^3, c^3 below the cube d^3, which leave the same remainder; for, if there were a fourth e^3 distinct from those, these also

$$(\lambda d-a-e)^3,\ (\lambda d-b-e)^3,\ (\lambda d-c-e)^3,$$

would produce the same remainder and would be distinct from the preceding ones. For, if it were that $\lambda d-a-e = b$, then $a+b+e$ would be divisible by d and, therefore, $e = c$, contrary to the hypothesis; hence, we would have not only four, but seven cubes giving the same remainder.

381. Hence, by combining them two at a time, more cubes less than d^3 could be elicited in turn, leaving the same remainder, so that in the end all the cubes would be produced. But, since, one remainder r being granted, there would be a distinct other one $-r$, it is clear that there are not more than three cubes less than d^3 that may exhibit the same remainder.

382. Therefore, in the sequence of remainders 1, α, β, γ, *etc.*, the multitude of which is $= d-1 = 2p$, either they are all unequal, or they are equal three at a time; but the latter cannot happen, unless $2p$ be a number divisible by 3. Because of this, if p be not divisible by 3, it is certain that all the remainders will be unequal to each other, and, therefore, all the numbers less than d will occur in the remainders.

383. Since all the prime numbers, excepting 2 and 3, are contained in one or the other of the formulas $6q+1$ and $6q-1$, if the prime divisor be $6q-1$, all the numbers less than it occur in the remainders, and there are

not any non-remainders. But if the divisor be $6q+1$, it can happen that the multitude of distinct remainders be only $2q$, and thus there would be $4q$ non-remainders.

384. We saw in addition that this last case happens if the divisor be of the form $aa+ab+bb$, whence it is clear, as we have already observed, that such a form does not admit of other prime divisors except those of the form $6q+1$. But the quadruple of the former $4aa+4ab+4bb = (2a+b)^2+3b^2$ returns the form $aa+3bb$, whose prime divisors enjoy that notable property.

385. One should search, therefore, for those divisors of squares that leave -3 or $-3bb$ for the remainder, which, as was observed above (341), are contained in the two forms $12q+1$ and $12q+7$, which are reducible to the single form $6q+1$, whence again it is permitted to conclude that all the prime numbers of the form $6q+1$ are endowed with that property; although a satisfactory demonstration of this thing is still needed.

386. But, this being granted, we obtain this proposition: Whenever the prime divisor be of the form $6q+1$, the remainders of the cubes from 1 to $216q^3$ are not all unequal to each other, but, because [they are] equal in threes, the multitude of unequal remainders is only $2q$, and the rest of the numbers less than the divisor, the multitude of which is $4q$, will be non-remainders. But whenever the prime divisor is not of the form $6q+1$, all the remainders are unequal to each other, so that there are not any non-remainders.

387. Therefore, it is apposite to consider only divisors of the form $6q+1$, for which the multitude of non-remainders is twice as large as the multitude of remainders. Let's present [*evolvamos*, "roll out"] the simpler cases:

for divisor:	7	13	19
remainders:	1, 6	1, 8, 5, 12	1, 8, 7, 11, 12, 18
non-remainders:	2, 3 5, 4	2, 4, 3, 6 11, 9, 10, 7	.2, 3, 4, 5, 6, 9 17, 16, 15, 14, 13, 10

for divisor: 31

remainders: 1, 8, 27, 2, 16, 15, 29, 4, 23, 30

non-remainders: { 3, 5, 6, 7, 9, 10, 11, 12, 13, 14
{ 28, 26, 25, 24, 22, 21, 20, 19, 18 17

for divisor: 37

remainders: 1, 8, 27, 14, 31 10, 6. 23, 29, 11, 26, 36

non-remainders: { 2, 3, 4, 5, 7, 9, 12, 13, 15, 16, 17, 18
{ 35, 34, 33, 32, 30, 28, 25, 24, 22, 21, 20, 19

for divisor: 43

remainders: 1, 8, 27, 21, 39, 11, 4, 32, 22, 16, 35, 2, 41, 42

non-remainders: { 3, 5, 6, 7, 9, 10, 12, 13, 14, 15, 17, 18, 19, 20
{ 40, 38, 37, 36, 34, 33, 31, 30, 29, 28, 26, 25, 24, 23 .

388. For any prime divisor of the form $6q+1$, therefore, all the cubes less than it occur in the remainders, and then their complements $6q$, $6q-7$, $6q-26$, $6q-63$, *etc.* Continuing, also their products two by two. Then also, if any product mn, with one factor m, be there, the other factor n is likewise found in the very same place.

389. For, if a^3 leaves mn and b^3 leaves m, assuming the divisor $6q+1 = d$, we can make $a = fb-gd$ and, therefore, f^3b^3 leaves mn, but nb^3 also leaves mn, and so $f^3b^3-nb^3$ and, besides, f^3-n will be divisible by d, that is, f^3 will leave n.

390. If the prime divisor be $d = 6q+1$ and the number α occurs amongst the remainders of the cubes, then $\alpha^{2q}-1$ will be divisible by d. Whence, the remainders, which arise from the division of the geometric sequence $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \ldots, \alpha^{2q}$ by the same divisor, will agree with the remainders of the cubes.

391. Again, however, it must be shown that, if $a^{2q}-1$ be divisible by the prime divisor $6q+1$, the number a certainly occurs amongst the remainders of the cubes, which is easily done, at least if $2q$ is not divisible

by 3. For, if it be that $2q = 3k \pm 1$, since $a^{2q} = a^{3k \pm 1}$ occurs amongst the remainders of the cubes, in as much as it is equivalent to the unit, it is necessary that a be found in the same place.

392. It remains to be shown, therefore, that, if it be that $2q = 3k$ and $a^{3k}-1$ can be divided by $6q+1 = 9k+1$, then a will be amongst the remainders of the cubes (*); a^{3k}, as a cube, is likewise certainly found there, but a demonstration must be sought for that the remainder of a^{3k} is equivalent to the unit.

(*) *Written in the margin*: For, if a were non-remainder, all the rest of the non-remainders, which are a, $a\alpha$, $a\beta$, $a\gamma$, $a\delta$, and a^2, $a^2\alpha$, $a^2\beta$, $a^2\gamma$, *etc.* would enjoy the same property that their powers to the exponent $2q$, minus the unit, would be divisible by $6q+1$; therefore, all the numbers would have this property, which is absurd.

393. But since the distinct remainders of the powers 1, a, a^2, a^3, *etc.*, in number $2q$, are equally in the remainders of the cubes, and both classes begin with the unit and have the common terms a^3, a^6, a^9, *etc.*, then the rest of their properties are common to them and the class of powers can contain no terms distinct from the other class.

394. If, however, we attend to the non-remainders of the cubes, divided by the prime number $6q+1$, it is indeed certain that, if mn be a remainder, and m a non-remainder, n will likewise be a non-remainder. But again, not all the products of two non-remainders produce a remainder; however, all the products of any remainder with a non-remainder are non-remainders.

395. For, first, the square of every non-remainder is likewise contained amongst the non-remainders; certainly, if A be a non-remainder, A^2 will likewise be a non-remainder, however, this non-remainder A^2 multiplied by the non-remainder A certainly gives a remainder, because it is a cube.

396. For, if A^2 were a remainder, $A^{4q}-1$ would be divisible by $6q+1$; and since $A^{6q}-1$ is certainly divisible, $A^{6q}-A^{4q}$ would also be divisible, as would $A^{2q}-1$ and, therefore, A would be a remainder of the cubes, contrary

to the hypothesis. Because of this, if AA be a remainder, A will also be a remainder, and, on the contrary, if A be a non-remainder, AA will likewise be a non-remainder.

397. Therefore, if the remainders of the cubes be 1, α, β, γ, δ, *etc.*, the prime divisor being = $6q+1$, and if A be the only non-remainder we have, first, all the numbers A, $A\alpha$, $A\beta$, $A\gamma$, *etc.*, then also A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, *etc.*, will be non-remainders, and, since these numbers are all distinct from one another, it is clear, as we have already demonstrated, that the multitude of non-remainders is twice that of the remainders.

398. Hence it is also clear that, if the prime divisor be $6q+1$, there can only be $2q$ distinct remainders; for, if all the numbers could occur amongst the remainders, $a^{2q}-1$ would in general be divisible by $6q+1$ whenever $a < 6q+1$, but since this is absurd, there is, therefore, at least one non-remainder, from which the $4q$ non-remainders follow.

399. Since, therefore, two classes of non-remainders are obtained from a single non-remainder A, the first being A, $A\alpha$, $A\beta$, $A\gamma$, *etc.* and the second being A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, *etc.* and each contains as many terms as the class of remainders, the products two at a time from one class are found in the other class and the products two at a time from both classes make remainders.

400. If we may still be uncertain as to whether all the non-remainders are obtained in this manner from a single one, let B be a non-remainder contained in neither class, and then B, $B\alpha$, $B\beta$, $B\gamma$, *etc.* as well as B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$, *etc.* will be non-remainders, there being the same number in both places as there are remainders, and all these numbers will be distinct from the preceding ones. In addition, either AB or AB^2 will not be a remainder; one of them certainly proves to be a remainder, the other a non-remainder. (*)

(*) *Written in the margin*: It must be demonstrated that both of them cannot simultaneously be remainders. If AB be a non-remainder, it is contained either in class A, or B, or A^2, or B^2. But each of these is absurd, therefore AB is a remainder.

401. If AB be not a remainder, we can represent the classes of non-remainders in pairs thusly:

First class: A, $A\alpha$, $A\beta$, $A\gamma$, *etc.* B, $B\alpha$, $B\beta$, $B\gamma$, *etc.*

Second class: A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, *etc.* B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$, *etc.*

and any number A whatever from the first class, multiplied by any number you please from the second class, produces a remainder distinct from whichever you please; whence more remainders will appear than in fact there are, which is absurd.

402. Since, therefore, there are only $2q$ remainders for the prime divisor $6q+1$, given any cube a^3 whatever, there will be another b^3, less than $(6q+1)^3$, the difference of which will be divisible by $6q+1$, and therefore $aa+ab+bb$ will likewise be divisible by it. Hence, every prime number $6q+1$ is a divisor of numbers of the form $aa+3bb$, or of the form $aa+3$, or $3aa+1$.

403. As an example, let the divisor be 373, and the remainders of the cubes, as well as the non-remainders of both classes, are as follows:

Remainders	Non-remainders	
±	Class I. ±	Class II. ±
1, 7, 8, 12, 13, 17	2, 3, 5, 14, 16, 21	4, 6, 9, 10, 11, 15
18, 19, 20, 22, 23	24, 26, 34, 35, 36	25, 28, 29, 32, 37
27, 30, 31, 33, 41	38, 39, 40, 44, 46	42, 43, 48, 52, 63
45, 49, 50, 55, 56	47, 51, 53, 54, 57	68, 70, 71, 72, 73
58, 64, 67, 74, 75	59, 60, 61, 62, 65	76, 77, 78, 79, 80
84, 86, 87, 91, 96	66, 69, 81, 82, 83	88, 92, 94, 102, 103
97, 104, 109, 111, 113	85, 89, 90, 93, 95	105, 106, 108, 114, 117
119, 125, 126, 129, 133	98, 99, 100, 101, 107	118, 120, 122, 124, 127
136, 137, 139, 140, 142	110, 112, 115, 116, 121	130, 131, 132, 138, 141
144, 145, 146, 152, 154	123, 128, 134, 135, 147	143, 149, 153, 159, 162
156, 157, 158, 160, 161	148, 150, 151, 155, 165	164, 166, 170, 171, 173
163, 167, 169, 176, 184	168, 172, 174, 179, 181	175, 177, 178, 180, 183
185	182	186
in number 2.62 = 124.	in number = 124.	in number = 124.

404. Since, therefore, the prime divisor is $6q+1$ and the multitude of non-remainders is twice that of the multitude of remainders, there will also be fewer divisors, for which a given number be contained amongst the remainders. Thus, a given number a will be a remainder, if the divisor be a factor of the form $x^3 \pm ay^3$, or the form $x^3 \pm aay^3$; for, if it be that $x^3 \pm ay^3 = dn$, the cube x^3, divided by d, gives the remainder ay^3, and thus a will also be in the remainders.

405. Therefore, prime divisors of the numbers $x^3 \pm ay^3$ should be sought for and, for our purposes, only those that are at the same time of the form $6q+1$. In this way, putting $a = 2$, the dyad will be found amongst the remainders, whenever the divisor of the form $6q+1$ be a number from the sequence:

31, 43, 109, 127, 157, 223, 229, 277, 283, 307, 397, 433, 439, 457, 499, 601, 643, 691, 727, 733, 739, 811, 919, 997, 1021, 1051, 1069, 1093, *etc.*

406. Therefore, if $6n+1$ be such a number, both 2 and 2^2 will be remainders; then $2^{2n}-1$ will be divisible by it and, therefore, either 2^n-1, or 2^n+1. But, if $6n+1$ be either of the form $8m+1$ or $8m+7$, that is, either $n = 4m$, or $n = 4m+1$, then $2^{3n}-1$ is also divisible by $6n+1$; whence it is clear that in this case, in which n be either $4m$ or $4m+1$, 2^n-1 will be divisible by $6n+1$; in the case, however, in which n is either $4m+2$ or $4m+3$, not 2^n-1, but 2^n+1 will be divisible by $6n+1$.

407. Thus, transporting the numbers given above

by	is divisible	by	is divisible
31	$2^{10}-1$ and $2^{5}-1$	499	$2^{166}-1$ and $2^{83}+1$
43	$2^{14}-1$ « $2^{7}+1$	601	$2^{200}-1$ « $2^{100}-1$
109	$2^{36}-1$ « $2^{18}+1$	643	$2^{214}-1$ « $2^{107}+1$
127	$2^{42}-1$ « $2^{21}-1$	691	$2^{230}-1$ « $2^{115}+1$
157	$2^{52}-1$ « $2^{26}+1$	727	$2^{242}-1$ « $2^{121}-1$
223	$2^{74}-1$ « $2^{37}-1$	733	$2^{244}-1$ « $2^{122}+1$
229	$2^{76}-1$ « $2^{38}+1$	739	$2^{246}-1$ « $2^{123}+1$
277	$2^{92}-1$ « $2^{46}+1$	811	$2^{270}-1$ « $2^{135}+1$
283	$2^{94}-1$ « $2^{47}+1$	919	$2^{306}-1$ « $2^{153}-1$
307	$2^{102}-1$ « $2^{51}+1$	997	$2^{332}-1$ « $2^{166}+1$
397	$2^{132}-1$ « $2^{66}+1$	1021	$2^{340}-1$ « $2^{170}+1$
433	$2^{144}-1$ « $2^{72}-1$	1051	$2^{350}-1$ « $2^{175}+1$
439	$2^{146}-1$ « $2^{73}-1$	1069	$2^{356}-1$ « $2^{178}+1$
457	$2^{152}-1$ « $2^{76}-1$	1093	$2^{364}-1$ « $2^{182}+1$

408. If we consider attentively these divisors, for which the dyad comes about [*convenit*] as a remainder, we will notice that they all result from the form $27pp+qq$, whenever that be a prime number; although this observation is not yet supported with a demonstration.

409. If we want those prime divisors of the form $6q+1$, for which 3 comes about as a remainder, we will find these:

61, 67, 73, 103, 193, 307, 367, 439, 577, 1021, *etc.*

which, if we may rely on conjecture, are contained in the form $3pp+qq$, if it be that either $p = 9n$, or $p \pm q = 9n$.

410. Those prime divisors, however, of the form $6q+1$, that have 5 in the remainders of cubes, are found from the form $x^3 \pm 5y^3$, of which the divisors must be 13, 67, 127, 181, 199, 241, 487, 739, *etc.*, which we observe to be contained in the form $3pp+qq$ under the conditions: 1) if $p = 15n$, 2) if $p = 3m$ and $q = 5n$, 3) if $p \pm q = 15n$ and 4) if $p \pm 2q = 15n$.

411. If 6 should occur amongst the remainders, the divisors are found to be

7, 37, 139, 163, 181, 241, 307, 337, 349, 379, 631, 727, 751, 997, *etc.*,

which are discovered to be contained in the form $3pp+qq$, if it be that $p = 9n$, or $2p \pm q = 9n$. The truth of these observations, however, are only

supported by conjecture, neither can we conveniently make further progress by induction. (*)

(*) *Written in the margin*: For 7 to be a remainder and $3pp+qq$ the divisor, it must be that either $p = 3m$ and $q = 7n$, or $p \pm q = 21n$, or $4p \pm q = 7n$, or $p = 21m$, or $p \pm 2q = 7n$. — For 10 to be a remainder, for the divisor $3pp+qq$, it must be that either $p = 5n$, or $q = 5n$.

Chapter XII
On Remainders Arising from the Division of Biquadratics by Prime Numbers

412. If the prime divisor be d, whatever remainder is left by the biquadratic a^4, the same is left, not only by the biquadratics $(d+a)^4$, $(2d+a)^4$, *etc.*, but also by $(d-a)^4$, whence, if $d = 2p+1$, more than p distinct remainders cannot occur.

413. If the remainders be 1, α, β, γ, δ, *etc.*, the multitude of which cannot be more than p, all the biquadratics, reduced of course to their minimum form, will occur amongst them and moreover they will enjoy the property that their products, two by two, are found amongst them.

414. These remainders, therefore, originate from the biquadratics 1, 16, 81, 256, ..., p^4, and it behooves us to inquire diligently whether, or not, they will all be distinct from one another for the given prime divisor $2p+1$.

415. But it is certainly clear, first of all, that should one occur twice, say from the biquadratics a^4 and b^4, then, because b^4-a^4 would be divisible by $d = 2p+1$, it will be possible to make $b = md \pm na$, whence $n^4a^4-a^4$ will be divisible and, thus, also n^4-1. Then, likewise c^4 and n^4c^4 will produce equal remainders, and every remainder will occur twice.

416. If, therefore, d be a divisor of the formula b^4-a^4 (taking a and b less than $\frac{1}{2}d$) and, therefore, of the formula b^2+a^2, because neither $b-$

a nor $b+a$ can be divisible by it, then each remainder occurs twice. But, on the contrary, if it is not a factor of the formula b^2+a^2, all the divisors will be distinct.

417. But by §279 all the prime divisors of the form $bb+aa$ are contained in the form $4q+1$, because of which, if the proposed divisor be of the form $4q-1$, certainly $2q-1$ distinct remainders emerge from the division of the biquadratics and there will be just as many non-remainders, not more. Let's explain this case first.

418. Thus, let the prime divisor be $4q-1$ and the distinct remainders arising from the biquadratics be 1, α, β, γ, δ, *etc.*, the number of which will be $2q-1$, and let the non-remainders be A, B, C, D, *etc.*, of the same number. And also, it is clear, in the first place, that, if A be a non-remainder, $A\alpha$, $A\beta$, $A\gamma$ will also be non-remainders. For, if $A\alpha^4$ were a remainder, arising from the biquadratic b^4, then $b^4-A\alpha^4$ would be divisible by d. But we have $b = m\alpha \pm nd$, whence $m^4\alpha^4-A\alpha^4$ and, therefore, m^4-A would be divisible by d and m^4 would leave A, contrary to the hypothesis.

419. This property indeed extends to all divisors, so that the product of a remainder and a non-remainder is always a non-remainder. But the product AB of two non-remainders, at least if the prime divisor be $4q-1$, is certainly a remainder; for, if it were a non-remainder, it would agree with a term $A\alpha^4$, so that $A\alpha^4-AB$, and therefore α^4-B, would be divisible by d, contrary to the hypothesis.

420. In this case, in which the divisor is $= 4q-1$, the remainders of the biquadratics are provided with the same property as the remainders of squares and, moreover, clearly agree with them for the same divisor. For every remainder of the biquadratics is contained in the remainders of squares and, since they are equal in multitude, it is necessary that they be absolutely the same, whence the same thing that we explained above, about remainders and non-remainders, is true here.

421. Now let the prime divisor be $4q+1$ and all the remainders 1, α, β, γ, δ, *etc.* have the property that α^q-1 is divisible by $4q+1$. These

remainders will certainly also be contained in the remainders of the squares for the same divisor $4q+1$; but, in contrast, not all the remainders of the squares are at the same time remainders of biquadratics, which is shown thusly.

422. Any remainder whatever of squares can be represented by x^2, but if it were a remainder of biquadratics, $x^{2q}-1$ would be divisible by $4q+1$, where x indicates any number you please less than the divisor; that is to say, $1^{2q}-1$, $2^{2q}-1$, $3^{2q}-1$, $4^{2q}-1$, …, $(2q)^{2q}-1$, can be divided by $4q+1$, which cannot be done, so that not every square occurs in the remainders of the biquadratics.

423. If x^2 does not occur in the remainders of the biquadratics, αx^2, βx^2, γx^2, δx^2, *etc.* likewise will not occur in that place, which, since they are remainders of squares, are clearly amongst the remainders of the squares, the multitude of which is $2q$; but, at minimum, there are the same number of non-remainders of biquadratics as there are remainders of biquadratics; whence it is clear that the multitude of remainders of biquadratics is either = q or less than this, which last, however, cannot be.

424. So that we may investigate this more easily, we may examine the simpler divisors of the form $4q+1$, both with regard to the remainders and non-remainders of the biquadratics:

for the divisor	5	13	17	29
remainders	1	1, 3, 9	1, 4, 13, 16	1, 16, 23, 24, 20, 7, 25
non-remainders	2	2, 6, 5	3, 12, 5, 14	2, 3, 17, 19, 11, 14, 21
	4	4, 12, 10	9, 2, 15, 8	4, 6, 5, 9, 22, 28, 13
	3	8, 11, 7	10, 6, 11, 7	8, 12, 10, 18, 15, 27, 26

for the divisor	37
remainders	1, 16, 9, 12, 33, 10, 26, 34, 7
non-remainders	2, 32, 14, 31, 29, 15, 24, 20, 18
	4, 27, 28, 25, 21, 30, 11, 3, 36
	8, 17, 19, 13, 5, 23, 22, 6, 35

425. From these examples, we see that the number of remainders is = q, than which it cannot be greater, as we already demonstrated. The number of non-remainders is three times as many; we have separated

them into three classes, since the numbers of each class enjoy their own special properties.

426. One may most conveniently constitute these three classes thusly: since there are squares not occurring in the remainders, let xx be such a square; and it is certain that neither x nor x^3 can be found amongst the remainders. Therefore, if the remainders be 1, α, β, γ, δ, ε, *etc.*, the three classes of non-remainders will be:

I. x, αx, βx γx, δx, *etc.*

II. x^2, αx^2, βx^2, γx^2, δx^2, *etc.*

III. x^3, αx^3, βx^3, γx^3, δx^3, *etc.*

427. Each class contains as many terms as there are remainders, and all the terms of these classes are distinct from one another. Indeed, terms of the same class are manifestly distinct; on the other hand, the diversity of the terms in different classes is shown thusly.

428. If αx were equivalent to βx^2, then $\beta x^2 - \alpha x$, and therefore $\beta x - \alpha$, would be divisible by $4q+1$, whence, since α is a remainder, βx, being equivalent to it, would also be a remainder, which is absurd. In a similar way, if αx, or αx^2, agreed with βx^3, either $\alpha - \beta x^2$ or $\alpha - \beta x$ would be divisible by $4q+1$, and therefore βx^2, or βx, would go over into the remainders, contrary to the hypothesis.

429. Hence, if the number of remainders be = n, the number of non-remainders will be $3n$, or at least it will not be less than $3n$. And besides, if all the non-remainders be contained in the three mentioned classes, it is necessary that the multitude of both remainders and non-remainders taken together be = $4q$ and, therefore, $n = q$.

430. When these classes are arranged in the manner that we have fashioned them, it is clear that the product of two non-remainders from both the first and the third classes is contained in the second class; further, the product either of two terms of the second class, or one of the first class with one of the third class crosses over to the class of the remainders. But the product of a term from the first class with one from

the second is found in the third class and the product of one from the second class with one from the third is found in the first.

431. From this, one discerns that a square number can have no place either in the first or the third classes, since it would be led into the remainders by multiplying it by itself. Therefore, the second class contains only squares and, since remainders can also be considered as squares, the multitude of all the squares is = $2n$.

432. If the second class, with the remainders, includes all the squares which can be considered as distinct remainders with respect to the divisor $4q+1$, and their number is = $2q$, as we saw in the remainders of the squares, because $2n = 2q$ and hence $4n = 4q$, they are all the numbers less than the divisor and neither are there non-remainders not contained in our three classes, and we will have $n = q$.

433. Now, should anyone doubt whether all the numbers which are not remainders occur in our three classes of non-remainders, this doubt will be removed if we point out that there are no square non-remainders that are not contained in the second class. For, if yy were such a square, on account of that, three new classes of non-remainders would immediately emerge and then the number of non-remainders would be = $6n$, and besides, if the non-remainders were now completed, we would have $7n = 4q$.

434. That there is not such a square yy, dragging along behind it three new classes of non-remainders, is indeed shown thusly: Let, in addition to the others, the three classes arising from such a square be:
IV. y, αy, βy, γy, *etc.* V. y^2, αy^2, βy^2, γy^2, *etc.* VI. y^3, αy^3, βy^3, γy^3, *etc.*
each of which will contain n terms; it is necessary to examine two cases, the first in which xy would be a remainder, the second in which it would be a non-remainder.

435. Let ay be a remainder and then all the terms of the fourth class, multiplied by x, that is xy, αxy, βxy, γxy, *etc.*, in number n, will be remainders. Also, to be sure, all the terms of the third class, multiplied

by x, that is x^4, αx^4, βx^4, γx^4, *etc.*, are remainders, just as many in number, and distinct from the former ones; for, if αxy and βx^4 agreed with each other, $\alpha y - \beta x^3$ would be divisible by the divisor and αy would fall into the third class, contrary to the hypothesis. Thus, $2n$ distinct remainders would appear; but, because this is absurd, xy cannot be made a remainder.

436. Having, therefore, disposed of the case in which xy is a remainder, we may assume xy to be a non-remainder and, since all the non-remainders are comprehended in six classes, xy must occur in one of them; moreover, we may put xy as equivalent to either αx, or αx^2, or αx^3, or αy, or αy^2, or αy^3, from which an absurdity follows, in as much as y would be a remainder and would fall into either class I or II of non-remainders, or x would be a remainder and would fall into class IV or V.

437. But since six classes of non-remainders cannot be granted, either they should be constituted by only three, as we would have it, or by more than six. The latter would happen if all the square non-remainders do not yet occur in classes II and V. Let, therefore, zz be a non-remainder contained in neither of these classes, and three new classes will spring up from it, each consisting of n terms:

VII. z, αz, βz, *etc.* VIII. z^2, αz^2, βz^2, *etc.* IX. z^3, αz^3, βz^3, *etc.*

438. Now indeed, as is shown in §435, neither xy, nor xz, nor yz can be a remainder because more remainders would follow from that than there actually are. Further, if xy were contained in any of the first six classes, the same inconvenience would arise as before; because of this, xy must be in one of the latter three classes. We should consider, therefore, whether xy can be equivalent to αz.

439. But if xy were equivalent to αz, then xz, because it is certainly a non-remainder, would be equivalent to either βy, or βy^2, or βy^3; because of this, since $xy - \alpha z$ and $xz - \beta y^\nu$, where ν indicates either 1, or 2 or 3, would be divisible by $4q+1$, $z(xy - \alpha z) - y(xz - \beta y^\nu)$, that is $\beta y^{\nu+1} - \alpha z^2$, would be

divisible, and thus αz^2 would be equivalent to $\beta y^{\nu+1}$, and therefore would be contained in a different class, which would be absurd.

440. Thus it is demonstrated that, if the prime divisor be $4q+1$, the distinct divisors of the biquadratics will be = q in number, neither more, nor less, but the non-remainders will be comprehended in three classes, of which each consists of q terms.

441. Because of this, since the distinct remainders arise from the biquadratics $1, 2^4, 3^4, 4^4, \ldots, 16q^4$, the multitude of which is = $2q$, they must be equal in pairs. Hence, if a is any number less than $2q$, there will always be another b, unique and likewise not greater than $2q$, such that b^4 and a^4 leave equal remainders, that is, such that b^4-a^4 is divisible by $4q+1$.

442. But since both $b-a$ and $b+a$ are less than $4q+1$, $bb+aa$ will be divisible by $4q+1$. Hence, for a proposed prime number $4q+1$, a sum of two squares $aa+bb$, divisible by it, can be produced such that neither root surpasses $2q$ and one of the squares can be selected at will.

443. We have already shown above that the sum of two squares $aa+bb$, prime to each other, does not admit prime divisors, other than the dyad, except those of the form $4n+1$. From which it appears that one can conclude that all prime numbers of the form $4q+1$ are sums of two squares and also certainly that $2(4q+1)$, or $5(4q+1)$ or $13(4q+1)$, *etc.* will be the sum of two squares.

444. Although it has already been taken care of, that there are not more than two biquadratics, whose roots do not exceed $2q$, that leave the same remainder, this can nevertheless also be demonstrated in another way. For, let a, b, c be three numbers not exceeding $2q$, such that $aa+bb$, $aa+cc$ and $bb+cc$ are all divisible by $4q+1$, and, moreover, their differences $aa-cc$, $aa-bb$ and $bb-cc$ would also be divisible. But, since neither $a-c$ nor $a+c$ can be divided by $4q+1$, their product $aa-cc$ likewise cannot be divided.

445. Thus, we have given a new proof that, if the prime divisor be $4q+1$, the multitude of distinct remainders arising from the division of the biquadratics is = q, and cannot be less; whence, the multitude of non-remainders will be $3q$, distributed in the three above mentioned classes.

446. Therefore, the remainders of the biquadratics arising from the prime divisor $4q+1$, which are 1, α, β, γ, δ, *etc.*, have the property that α^q-1, β^q-1, γ^q-1, *etc.* admit of division by the prime number $4q+1$. However, whether, or not, all remainders[19] upholds [*refragentur*] this property should be considered.

447. Let xx be a non-remainder and then x and x^3 will equally be non-remainders. Now, if $(xx)^q-1$, or $x^{2q}-1$, were divisible by $4q+1$, all the terms αx^2, βx^2, γx^2, *etc.* would enjoy the same property, whereby, since the remainders, properly speaking, enjoy it, all the squares from 1 to $4qq$ would be provided with the same property.

448. All the numbers from 1 to $2q$, would thus have the property that their power with the exponent $2q$, divided by $4q+1$, would leave the unit; and, so, all the differences between two terms of the sequence 1, 2^{2q}, 3^{2q}, 4^{2q}, …, $(2q)^{2q}$, would be divisible by $4q+1$, which, however, is absurd, as was shown above.

449. This accomplishes what was proposed, namely, if the square xx be a non-remainder, then $x^{2q}-1$ certainly is not divisible by $4q+1$. Since x and x^3 are also non-remainders, however, much less will the formulas x^q-1 and $x^{3q}-1$ be divisible by $4q+1$, whence it is clear that, if a^q-1 admits of division by $4q+1$, then the number a will necessarily be found amongst the remainders of the biquadratics.

450. When, therefore, the power a^q, divided by the prime number $4q+1$, leaves the unit, then every remainder arising from the sequence of powers 1, a, a^2, a^3, a^4, *etc.*, will be contained in our remainders of

[19] That is, including quadratics that are non-residues of the biquadratics.

biquadratics. And in turn, if a be not a remainder of the biquadratics, the formula a^q-1 certainly will not be divisible by $4q+1$.

451. If q be an odd number, the number -1, or $4q$, will not occur amongst the remainders, because $(-1)^q-1$ certainly cannot be divided by $4q+1$. In this case, therefore, if the remainders be $1, \alpha, \beta, \gamma, \delta$, *etc.*, their negatives $-1, -\alpha, -\beta, -\gamma$, *etc.*, that is $4q, 4q+1-\alpha, 4q+1-\beta, 4q+1-\gamma$, *etc.* will certainly be found amongst the non-remainders.

452. Hence, it follows that, if q be an odd number, there are not two biquadratics a^4 and b^4, whose sum a^4+b^4 is divisible by the number $4q+1$. For, if a^4 agreed with the remainder α, another b^4 would agree with $-\alpha$, which, however, we have just now shown cannot happen.

453. But contrarywise, if q be an even number, -1 certainly occurs amongst the remainders of the biquadratics, for, if it were a non-remainder, $(-1)^q-1$ would not be divisible by $4q+1$. Since it is divisible, however, it is clear that the negative of every biquadratic, or its complement, is also contained amongst the remainders.

454. If, therefore, q be an even number and $4q+1$ a prime number, or if $8q+1$ be a prime number, for any given biquadratic a^4, there will be another b^4, such that their sum a^4+b^4 is divisible by $8q+1$. Thus, for the given number a, a number x can always be found, such that the sum of the biquadratics a^4+x^4 is divisible by 17, or 41, or 73, or 89, or 97, *etc.*

455. On the contrary, however, there will be no sum of two biquadratics which is divisible by any prime number from the sequence 5, 13, 29, 37, 53, 61, 101, *etc.*; much the less by any prime number of the form $4q-1$, because not even the sum of two squares is divisible by such a number.

456. Therefore, the sum of two biquadratics, prime to each other, cannot have, besides the dyad, other divisors, except those contained in the form $8q+1$; thus we have:

$1+2^4 = 17$	$2^4+3^4 = 97$	$4^4+5^4 = 881$	$7^4+8^4 = 73.89$
$1+3^4 = 2.41$	$2^4+5^4 = 641$	$4^4+7^4 = 2657$	$7^4+9^4 = 2.4481$

$1+4^4 = 257$	$2^4+7^4 = 2417$	$4^4+9^4 = 17.401$	$7^4+10^4 = 12401$
$1+5^4 = 2.313$	$2^4+9^4 = 6577$	$5^4+6^4 = 17.113$	$8^4+9^4 = 10657$
$1+6^4 = 1297$	$3^4+4^4 = 337$	$5^4+7^4 = 2.17.89$	$9^4+10^4 = 16561$[20].
$1+7^4 = 2.1201$	$3^4+5^4 = 2.353$	$5^4+8^4 = 4721$	
$1+8^4 = 17.241$	$3^4+7^4 = 2.17.73$	$5^4+9^4 = 2.3593$	
$1+9^4 = 2.17.193$	$3^4+8^4 = 4177$	$6^4+7^4 = 3697$	
$1+10^4 = 73.137$	$3^4+10^4 = 17.593$[21]		

457. Now, let's seek out those divisors for which the dyad is to be found amongst the remainders, which indeed never happened in the cases presented in §424. But wherever 2 occurs, 2α also occurs; and, therefore, the divisor $4q+1$ must be a factor of such numbers as a^4-2b^4, or $2b^4-a^4$; whence these divisors are deduced:

73, 89, 113, 233, 281, 353, 593, 617, 937, 1249, 1889, 2273, 2393, 4177, 4721, 4801, 6529, *etc.*,

which numbers seem to be contained in the form $64pp+qq$. (*)

(*) *Written in the margin*: For 3 to be a remainder, the divisor must be $pp+qq$, so that either $p = 12m$, or $p = 3(2m+1)$ and $q = 4n+2$. For 5 to be a remainder, the divisor is made $= 100pp+qq$.

458. But the numbers contained in the formula $64pp+qq$ are:

73, 89, 113, 233, 257, 281, 337, 353, 577, 593, 601, 617, 881, 937, 1033, 1049, 1097, 1153, 1193, 1201, 1249, *etc.*

Since all the preceding occur therein and the rest satisfy the question, there is nothing that should make us doubt the truth of the conjecture and, since all these numbers are of the form $8n+1$, both -2 and 2 are to be found in the remainders.

459. Examining all the prime divisors of the form $4q+1$ up to 101, the number q always occurs amongst the remainders, so that q^q-1 is divisible by $4q+1$; insofar as it is true in general, the numbers q, q^2, q^3, $16q$, $81q$, $256q$, $16qq$, $81qq$ and hence -4, $q-20$, -64, and $-4q$ would likewise be amongst the remainders.

[20] Reading "16561" for "16511".
[21] Reading "17.593" for "2.17.593".

460. This observation is confirmed by what was reported in §339[22] above, where we decided that the number 2 is amongst the remainders of the squares, if the prime divisor be of the form $8p+1$, but it is a non-remainder, if the divisor be of the form $8p+5$, whereby $2^{4p}-1$ is divisible by $8p+1$, but $2^{4p+2}-1$ is not divisible by $8p+5$, whence, since $2^{8p+4}-1$ is divisible, it is necessary that $2^{4p+2}+1$ be divisible by $8p+5$.

461. Thus, since the form $4q+1$ answers to $8p+1$, if q be an even number, in this case $2^{2q}-1$, or 4^q-1, is divisible by $4q+1$ and, therefore, the number 4 and its negative -4 must be found amongst the remainders of the biquadratics. But if q be an odd number, in which case $4q+1$ answers to $8p+5$, $2^{2q}+1$, or 4^q+1, which answers to $(-4)^q-1$, is divisible by $4q+1$; thus, even in this case -4 should be found amongst the remainders of the biquadratics.

462. For the divisor $4q+1$, therefore, whether p be an even number, or an odd one, -4 is always found in the remainders of the biquadratics, whence, since $-4q$, because of 1, is present there, q must likewise be present, and thus one observation is confirmed by the other.

Chapter XIII
On Remainders Arising from the Division of Surdosolids[23] by Prime Numbers

463. If the divisor be d and a^5 leaves α, then $(d-a)^5$ will leave $-\alpha$, and thus the number of all the remainders originating from the powers $1, 2^5, 3^5, 4^5, \ldots, (d-1)^5$, if they be all distinct, is $= d-1$.

464. Let $1, \alpha, \beta, \gamma$, *etc.* be all the distinct remainders and their products, two by two, will occur amongst them; moreover, if any product

[22] Reading "§339" for "§389".
[23] That is, fifth powers.

mn appears there along with one factor m, the other n also will appear there. For, if mn arises from a^5, and m from b^5, mn will also originate from nb^5, and $a^5 - nb^5$ will be divisible by d. But we can put $a = fb \pm gd$, and therefore a^5 leaves the same remainder as f^5b^5, thus, since $f^5b^5 - nb^5$, and therefore also $f^5 - n$, is divisible by d, n will be in the remainders.

465. If a be in the remainders, a^2, a^3, a^4, will likewise be there, but a^5 is always there. Hence, in its turn, if a^2 be in the remainders, $a^3 = a^5 : a^2$ will likewise be in the very same place; and, because a^4 is a remainder, a will also be a remainder. Therefore, if any power whatever a^n (provided that n be not a multiple of five) be a remainder, all its powers a, a^2, a^3, *etc.* will also be remainders.

466. Let m be the multitude of the remainders $1, \alpha, \beta, \gamma, \delta$, *etc.* for the prime divisor $2q+1$ and, if all the numbers less than the divisor occur in the remainders, we will have $m = 2q$ and, besides, that there are such cases will be clear soon.

467. If it be that $m < 2q$, there will be a number that is a non-remainder; let A be of this kind and, hence, the non-remainders will be, firstly, A, $A\alpha$, $A\beta$, *etc.*, m in number; but then, because A^2, A^3, A^4 are non-remainders, m new ones are obtained from each of them, so that one non-remainder A envelops four classes of non-remainders:

I. A, $A\alpha$, $A\beta$, $A\gamma$, *etc.* III. A^3, $A^3\alpha$, $A^3\beta$, $A^3\gamma$, *etc.*

II. A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, *etc.* IV. A^4, $A^4\alpha$, $A^4\beta$, $A^4\gamma$, *etc.*

468. Therefore, as soon as there is one non-remainder, $4m$ non-remainders are immediately generated and, if that be all of them, it is necessary that we have $m+4m = 2q$ and, therefore, $5m = 2q$ and $m = \frac{2q}{5}$; therefore, unless q be a multiple of five, non-remainders cannot appear.

469. But if there be a new non-remainder B beyond the four classes, there would once more arise from it four classes:

V. B, $B\alpha$, $B\beta$, $B\gamma$, *etc.* VII. B^3, $B^3\alpha$, $B^3\beta$, $B^3\gamma$, *etc.*

VI. B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$, *etc.* VIII. B^4, $B^4\alpha$, $B^4\beta$, $B^4\gamma$, *etc.*

Now, whether AB be designated a remainder or a non-remainder, an absurdity follows; whence it is necessary that all the non-remainders, if there be any, be exhausted by the four former classes.

470. It is therefore certain that whenever the number q in the prime divisor $2q+1$ is not a multiple of five, all the numbers occur in the remainders, and their multitude is = $2q$. Hence, there will not be two numbers a and b, less than $2q+1$, such that a^5-b^5 would be divisible by $2q+1$; and thus $a^4+a^3b+aabb+ab^3+b^4$ can be divided by no prime number $2q+1$, in which q is not a multiple of five.

471. All the prime divisors, therefore, of numbers of the form $a^4+a^3b+aabb+ab^3+b^4$, or of a^5-b^5, excepting the divisor $a-b$, are contained in the formula $10p+1$, and these numbers can in no way be divided by any number contained in the formulas $10p+3$, $10p+7$ and $10p+9$.

472. But if the prime divisor be $10p+1$, not all the numbers will occur in the class of remainders, for, if they were all to occur, $x^{2p}-1$ would always be divisible by $10p+1$, whatever x may be, or the differences of all the powers $1, 2^{2p}, 3^{2p}, 4^{2p}, \ldots, (2p+1)^{2p}$ would be divisible by $10p+1$, whose absurdity was already shown above.

473. Whence, if the prime divisor be $10p+1$, the number of distinct remainders is only = $2p$, and there will be $8p$ non-remainders, and thus there will always be five numbers a, b, c, d, e less than $10p+1$, whose fifth powers product the same remainders.

474. Of course, for any given number a, four others b, c, d, e, each less than the divisor $10p+1$, can always be assigned, so that

these numbers	and therefore also these
b^5-a^5	$b^4+ab^3+a^2b^2+a^3b+a^4$
c^5-a^5	$c^4+ac^3+a^2c^2+a^3c+a^4$
d^5-a^5	$d^4+ad^3+a^2d^2+a^3d+a^4$
e^5-a^5	$e^4+ae^3+a^2e^2+a^3e+a^4$

are divisible by it. The demonstration can be adapted from the same one for the preceding powers.

475. Therefore, the differences of the first minus the three following can be divided by the same divisor; moreover, these differences, since they are divisible by $b-c$, $b-d$, $b-e$, will be reduced to these

$$b^3+b^2c+bc^2+c^3+ab^2+abc+ac^2+a^2b+a^2c+a^3,$$
$$b^3+b^2d+bd^2+d^3+ab^2+abd+ad^2+a^2b+a^2d+a^3,$$
$$b^3+b^2e+be^2+e^3+ab^2+abe+ae^2+a^2b+a^2e+a^3.$$

476. Next, one should take the differences of these, which divided in turn by $c-d$ and $c-e$, become

$$c^2+cd+d^2+bc+bd+b^2+ac+ad+ab+a^2,$$
$$c^2+ce+e^2+bc+be+b^2+ac+ae+ab+a^2,$$

which are also divisible by $10p+1$. And, once again, the difference of these, divided by $d-e$, is

$$e+d+c+b+a.$$

477. Hence, it is apparent that the five numbers a, b, c, d, e, the fifth powers of which leave equal remainders, when divided by the prime number $10p+1$, are so composed that their sum

$$a+b+c+d+e$$

is also divisible by the same [number]. But, since each of them is less than $10p+1$, their sum is either $10p+1$, or $2(10p+1)$, or $3(10p+1)$, or $4(10p+1)$.

478. Since it is also permitted to consider negative numbers as remainders, the sum $a+b+c+d+e$ can be looked at as equal to nothing[24], whence, given the four a, b, c, d, the fifth is automatically given, namely $e = -a-b-c-d$, and, since it is unique, it is clear that there are not more than five.

479. Behold, then, a new demonstration that the number of distinct remainders for any prime divisor $2q+1$ be either $= 2q$ or $= \frac{2q}{5}$, and that the first always happens if q be not a multiple of five, the second whenever

[24] That is, zero.

we have $q = 5p$. In the first case, all the numbers less than the divisor are remainders, in the second only a fifth part of them.

480. Given, therefore, a prime divisor $10p+1$, the multitude of distinct remainders is $= 2p$, amongst which the negative of any remainder whatever likewise occurs, from which their multitude is even. But then the same remainder agrees with five distinct powers, the roots of which are less than the divisor; it will be helpful to list some of them.

481. Since such divisors are 11, 31, 41, 61, 71, 101, *etc.*, let's examine first the divisor $10p+1 = 11$, which makes $p = 1$:

Remainders	from the powers	Classes of non-remainders			
		I.	II.	III.	IV.
1	$1^5, 3^5, 4^5, 5^5, 9^5$	2	4	8	5
10	$2^5, 6^5, 7^5, 8^5, 10^5$	9	7	3	6.

482. Let the divisor be $10p+1 = 31$ and $p = 3$; we will have

Remainders	from the powers	Classes of non-remainders			
		I.	II.	III.	IV.
1	$1^5, 2^5, 4^5, 8^5, 16^5$	2	4	8	16
5	$7^5, 14^5, 19^5, 25^5, 28^5$	10	20	9	18
26	$3^5, 6^5, 12^5, 17^5, 24^5$	21	11	22	13
6	$11^5, 13^5, 21^5, 22^5, 26^5$	12	24	17	3
25	$5^5, 9^5, 10^5, 18^5, 20^5$	19	7	14	28
30	$15^5, 23^5, 27^5, 29^5, 30^5$	29	27	23	15

483. Let the prime divisor be $10p+1 = 41$ and, therefore, $p = 4$; we will have

Remainders	from the powers	Classes of non-remainders			
		I.	II.	III.	IV.
1	$1^5, 10^5, 16^5, 18^5, 37^5$	2	4	8	16
40	$4^5, 23^5, 25^5, 31^5, 40^5$	39	37	33	25
3	$11^5, 12^5, 28^5, 34^5, 38^5$	6	12	24	7
38	$3^5, 7^5, 13^5, 29^5, 30^5$	35	29	17	34
9	$5^5, 8^5, 9^5, 21^5, 39^5$	18	36	31	21
32	$2^5, 20^5, 32^5, 33^5, 36^5$	23	5	10	20

14	15^5,	22^5,	24^5,	27^5,	35^5	28	15	30	19
27	6^5,	14^5,	17^5,	19^5,	26^5	13	26	11	22

484. Letting the prime divisor be $10p+1 = 61$ and $p = 6$, we will have

Remainders	from the powers					Classes of non-remainders			
						I.	II.	III.	IV.
1	1^5,	9^5,	20^5,	34^5,	58^5	2	4	8	16
60	3^5,	27^5,	41^5,	52^5,	60^5	59	57	53	45
13	12^5,	25^5,	42^5,	47^5,	57^5	26	52	43	25
48	4^5,	14^5,	19^5,	36^5,	49^5	35	9	18	36
14	5^5,	39^5,	45^5,	46^5,	48^5	28	56	51	41
47	13^5,	15^5,	16^5,	22^5,	56^5	33	5	10	20
11	8^5,	11^5,	28^5,	37^5,	38^5	22	44	27	54
50	23^5,	24^5,	33^5,	50^5,	53^5	39	17	34	7
21	10^5,	17^5,	29^5,	31^5,	35^5	42	23	46	31
40	26^5,	30^5,	32^5,	44^5,	51^5	19	38	15	30
29	6^5,	21^5,	43^5,	54^5,	59^5	58	55	49	37
32	2^5,	7^5,	18^5,	40^5,	55^5	3	6	12	24

485. Any prime divisor of the form $10p+1$ being proposed, therefore, there will be a number a, such that a^5-1 is divisible by it, which property the numbers a^2, a^3, a^4 will likewise have, that is, their fifth powers also leave the unit. The following terms a^5, a^6, *etc.* are not distinct from these since $a^5 = a(10p+1)+1$, and so a^5 is equivalent to 1, a^6 to a, a^7 to a^2, *etc.*

486. Since the five numbers whose fifth powers, divided by $10p+1$, leave the unit can be represented by 1, a, a^2, a^3, a^4, if b^5 gives the remainder α, there will be five numbers b, ab, a^2b, a^3b, a^4b, whose fifth powers, divided by $10p+1$, leave the same remainder α.

487. Because the same thing can be extended to the higher powers, given any prime number $mn+1$, there will always be a number a, such that a^m-1 is divisible by it; and all its powers are provided with the same property. But a will be less than the divisor $mn+1$ and as many such distinct numbers as m contains of units can be exhibited.

488. Further, a prime number $mn+1$ being proposed, if the powers 1^m, 2^m, 3^m, 4^m, *etc.*, up to $(mn)^m$, be divided by it, more than n distinct remainders will not be left and, therefore, there will be $(m-1)n$ numbers less than the divisor that are not remainders.

489. If a be the smallest number after the unit whose power a^m, divided by $mn+1$, leaves the unit — and there will always be some unique number of this kind —, then, if the power b^m leaves α, the powers with exponent m of all the numbers b, ab, a^2b, a^3b, …, $a^{m-1}b$, whose multitude is $= m$, will leave the same remainder α.

490. If $m = 2$, the smallest power a^2, which, divided by the prime number $2n+1$, leaves the unit, is as follows

$2n+1$	n	a^2
3	1	2^2
5	2	4^2
7	3	6^2
11	5	10^2

and so on; in this case, we always have $a = 2n$.

491. If $m = 3$, the powers a^3, which, divided by $3n+1$, leave the unit, are

$3n+1$	n	powers	$3n+1$	n	powers
7	2	1^3, 2^3, 4^3	61	20	1^3, 13^3, 47^3
13	4	1^3, 3^3, 9^3	67	22	1^3, 29^3, 37^3
19	6	1^3, 7^3, 11^3	73	24	1^3, 8^3, 64^3
31	10	1^3, 5^3, 25^3	79	26	1^3, 23^3, 55^3
37	12	1^3, 10^3, 26^3	97	32	1^3, 35^3, 61^3
43	14	1^3, 6^3, 36^3	103	34	1^3, 46^3, 56^3.

492. Let m =4 and the powers a^4, which, divided by $4n$+1, leave the unit are

$4n$+1	n	powers	$4n$+1	n	powers
5	1	1^4, 2^4, 4^4, 3^4	53	13	1^4, 23^4, 52^4, 30^4
13	3	1^4, 5^4, 12^4, 8^4	61	15	1^4, 11^4, 60^4, 50^4
17	4	1^4, 4^4, 16^4, 13^4	73	18	1^4, 27^4, 72^4, 46^4
29	7	1^4, 12^4, 28^4, 17^4	89	22	1^4, 34^4, 88^4, 55^4
37	9	1^4, 6^4, 36^4, 31^4	97	24	1^4, 22^4, 96^4, 75^4
41	10	1^4, 9^4, 40^4, 32^4	101	25	1^4, 10^4, 100^4, 91^4

493. If m = 5, the powers a^5, which, divided by $5n$+1, leave 1, are, as we have already seen,

$5n$+1	n	powers
11	2	1^5, 3^5, 9^5, 5^5, 4^5
31	6	1^5, 2^5, 4^5, 8^5, 16^5
41	8	1^5, 10^5, 18^5, 16^5, 37^5
61	12	1^5, 9^5, 20^5, 58^5, 34^5
71	14	1^5, 5^5, 25^5, 54^5, 57^5
101	20	1^5, 36^5, 84^5, 95^5, 87^5

494. Let m = 6, and the sixfold powers a^6, which, divided by $6n$+1, leave the unit are

$6n$+1	n	powers
7	1	1^6, 2^6, 4^6, 6^6, 5^6, 3^6
13	2	1^6, 3^6, 9^6, 12^6, 10^6, 4^6
19	3	1^6, 7^6, 11^6, 18^6, 12^6, 8^6

of course, the same powers as for the case m = 3 appear here, to which are adjoined those arising from negative roots.

495. Let $m = 7$ and the powers a^7, which, divided by $7n+1$, leave the unit, are

$7n+1$	n	powers
29	4	1^7, 7^7, 20^7, 24^7, 23^7, 16^7, 25^7
43	6	1^7, 4^7, 16^7, 21^7, 41^7, 35^7, 11^7
71	10	1^7, 20^7, 45^7, 48^7, 37^7, 30^7, 32^7
113	16	1^7, 16^7, 30^7, 28^7, 109^7, 49^7, 106^7

496. We have already observed that, one of these numbers being known, the rest arise from its powers. Indeed, a method of investigating such numbers is most readily seen: Given a prime divisor $mn+1$, two powers a^m and b^m producing the same remainder are sought out; then x is sought, such that we have $x = \frac{b+p(mn+1)}{a}$ and x^m will leave the unit. Moreover, p can always be taken so as to make the number an integer.

497. If the divisor be $mn+1$, the powers with exponent m leaving the unit being

$$1^m, \alpha^m, \beta^m, \gamma^m, \delta^m, \textit{etc.} \quad \text{in number } m,$$

then, 1, α, β, γ, δ, *etc*, will be remainders arising from the geometric progression 1, α, α^2, α^3, α^4, *etc.*; therefore, they will also originate from the sequence of powers 1^n, 2^n, 3^n, 4^n, 5^n, 6^n, *etc.*

498. Behold, therefore, a most easy method for finding at least one number α, such that $\alpha^m - 1$ be made divisible by $mn+1$; of course, 2^n can always be taken for α, or the remainder arising from this power of the dyad, moreover suitable values can be sought for from 3^n, 5^n, *etc.*; but, knowing one, the rest become known easily.

499. If the prime divisor be $mn+1$ and the number N occurs in the remainders of the powers 1, 2^n, 3^n, 4^n, *etc.*, the number Na^n will likewise occur there; and there will be a number x, such that $x^n - Na^n$ is made divisible by $mn+1$, and $N^m - 1$ will also be divisible by $mn+1$.

500. Again, if $N^m - 1$ be divisible by $mn+1$, N will be a remainder of a power of x^n; for, if it were a non-remainder, all the rest of the non-

remainders, and therefore all numbers, would enjoy the same property; and all the numbers 1^m-1, 2^m-1, 3^m-1, *etc.* would be divisible by $mn+1$, which however cannot happen.

501. Specifying the prime divisor $mn+1$, and 1, A, B, C, D, *etc.* being the remainders of the powers 1^m, 2^m, 3^m, 4^m, *etc.* and 1, α, β, γ, δ, *etc.* the remainders of the powers 1^n, 2^n, 3^n, 4^n, *etc.*, then all the powers

$$1^m,\ \alpha^m,\ \beta^m,\ \gamma^m,\ \delta^m,\ \textit{etc.}$$

will leave 1; moreover, the powers 1^n, A^n, B^n, C^n, *etc.* will leave remainder 1 and, therefore, the forms $\alpha^m - A^n$ will be divisible by $mn+1$.

Inserted Page

An attempt to demonstrate that, if the prime divisor be 8q+7, *then* 2 *is to be found in the remainders*. Let's suppose that 2 is in the remainders and, since $(2q+m)^2$ is in the same place, $8qq+8mq+2mm$ will be likewise, and therefore

$$8mq+2mm-7q \text{ and } 2mm-7m-7q \text{ and } 2mm-7m+q+7,$$

but if there are never any non-remainders, the proposition will be clear. But non-remainders can be represented by negative squares, the doubles of which will be remainders by hypothesis; thus, let

$$2mm-7m+q+7 = -2aa+8bq+7b, \text{ and make}$$

$$q = \frac{2aa+2mm-7m+7-7b}{8b-1} \text{ and } 8q+7 = \frac{(4a)^2+(4m-7)^2}{8b-1},$$

and $8q+7$ would be a divisor of $(4a)^2+(4m-7)^2$, but, since this cannot happen, it follows that no absurdity is to be deduced from 2 as a remainder, which would necessarily result if 2 was not a remainder. (*)

(*) *Written in the margin*: If $2mm-7m+q$ is put $= -aa$, it makes

$$8q+7 = \frac{2(2a)^2+(4m-7)^2}{8b-1},$$

now it remains to be demonstrated that $2xx+yy$ is never divisible by $8q+7$. *Another note, as it seems, pertinent here*. $8xx-(2y+1)^2$ does not have prime divisors other than of the forms $8n-1$ and $8n+1$.

$\frac{8xx-1}{7}$ int.[25] if $x = 7a \pm 1$, $\frac{8xx-1}{23}$ int. if $x = 23a \pm 7$, $\frac{8xx-1}{31}$ int. if $x = 31a \pm 2$,
$\frac{8xx-1}{47}$ « « $x = 47a \pm 10$, $\frac{8xx-1}{17}$ « « $x = 17a \pm 7$, $\frac{8xx-1}{41}$ « « $x = 41a \pm 6$.

[25] That is, "integer".

Theorem. If the divisor [be] $12q+11$, 3 will be a remainder.

Assume that 3 is a remainder and, if no absurdity follows from that, it should be taken for the truth. Therefore, –3 will be a non-remainder and all non-remainders will be $-3aa$. But, $(2q+m)^2$ is a remainder and $12qq+12mq+3mm$ and, hence, $3mm-11q-11m$, likewise $3mm+q-11m+11$, which can never be a non-remainder $-3aa$: for, putting

$$3mm-11m+11+q = -3aa+12bq+11b,$$ we will have

$$q = \frac{3aa+3mm-11m+11-11b}{12b-1},$$ from which we obtain $12q + 11 = \frac{(6a)^2+(6m-11)^2}{12b-1}$,

but, since that is absurd, $3mm-11m+11+q$ will never be contained amongst the non-remainders.

Or thus for the divisor $8q+7$.

If 2 were a non-remainder, in general $2mm-7m-7q\pm\alpha(8q+7)$ would be a non-remainder; but in general the remainders are $(4q+n)^2 = 16qq+8nq+nn = 8nq+nn-14q = nn-14q-7n = nn+2q-7n+14\pm\beta(8q+7)$, thus all the numbers are contained in one or the other of these formulas:

$$2mm-7m-7q\pm\alpha(8q+7)$$
$$nn-7n-14q\pm\beta(8q+7).$$

If but a single number, not therein contained, can be determined, the demonstration would be complete; or if the same number were contained in both of them, which happens if, putting $m = f+g$, $n = f+2g$, $ff-2gg+7g+7q$ were divisible by $8q+7$.

Chapter XIV
On Remainders Arising from the Division of Squares by Composite Numbers

502. Let 1, α, β, γ, δ, *etc.* be the remainders, which emerge from the division of squares by a prime number $2p+1$, the number of which is $= p$; and also we may see first just what remainders arise, if the division is made by its double $2(2p+1)$, although here we exclude even squares; for, we will consider only those squares which are prime to the divisor.

503. But the multitude of squares, whose roots are less than the divisor, is $= 2p$, and because the squares aa and $(4p+2-a)^2$ leave the same

remainder, the multitude of distinct remainders cannot be greater than p; therefore, it will be either = p, or less than p.

504. Of course, it would be less if there were two squares aa and bb, which leave the same remainder and are such that it is not the case that $b = 4p+2-a$. But, then, were $bb-aa = (b-a)(b+a)$ divisible by $2(2p+1)$, one factor would have to be divisible by 2 and the other by $2p+1$. Yet, one being even, the other will likewise be even and, therefore, divisible by the whole divisor, whence we would have $b = 2(2p+1)-a$.

505. Therefore, the multitude of distinct remainders, which indeed arise from squares prime to the divisor, will be = p, just as many in number as are begotten from the prime divisor $2p+1$. And also, if the remainders, arising from the divisor $2(2p+1)$, be 1, A, B, C, D, *etc.*, their number will be = p and their products, two by two, will occur in the very same place.

506. There are, however, $2p$ numbers prime to this divisor and less than it, whence, since only half of them make up the remainders, the other half will give the class of non-remainders; letting them be $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, *etc.*, their number will be = p, and their products two at a time will make remainders again.

507. We consider some examples, in which the remainders originate both from the prime divisor $2p+1$ and from its double $2(2p+1)$, setting down at the same time the non-remainders prime to the divisor:

divisor	3	6	5	10	7	14
remainders	1	1	1, 4	1, 9	1, 2, 4	1, 9, 11
non-remainders	2	5	2, 3	3, 7	3, 5, 6	3, 5, 13

divisor	11	22
remainders	1, 3, 9, 5, 4	1, 9, 3, 5, 15
non-remainders	2, 6, 7, 8, 10	7, 13, 17, 19, 21

divisor	13	26
remainders	1, 3, 4, 9, 10, 12	1, 3, 9, 17, 23, 25
non-remainders	2, 5, 6, 7, 8, 11	5, 7, 11, 15, 19, 21

divisor	17	34
remainders	1, 2, 4, 8, 9, 13, 15, 16	1, 9, 13, 15, 19, 21, 25, 33
non-remainders	3, 5, 6, 7, 10, 11, 12, 14	3, 5, 7, 11, 23, 27, 29, 31

508. We will represent things in general

divisor	$2p+1$	$2(2p+1)$
remainders	1, α, β, γ, δ, *etc.*	1, *A*, *B*, *C*, *D*, *etc.*
non-remainders	$\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, $\mathfrak{e}$, *etc.*	$\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$, *etc.*

and we observe, in the first place, that all the remainders of the divisor $2(2p+1)$, either they themselves, or reduced by the number $2p+1$, make up the remainders of the divisor $2p+1$.

509. Of course, either *A* or $A-(2p+1)$ occurs in the remainders 1, α, β, γ, *etc.* For, since there is an odd square *aa*, such that $aa-A$ is divisible by $2(2p+1)$, it will likewise be divisible by $2p+1$, whence it is necessary that *A*, or $A-(2p+1)$, if it be that $A > 2p+1$, also be found amongst the remainders of the divisor $2p+1$.

510. Next, the odd numbers in the sequence 1, α, β, γ, *etc.* occur in the sequence 1, *A*, *B*, *C*, *D*, *etc.*, but the even ones are not found there, but rather those same ones increased by the number $2p+1$. For, let α be an odd number and, since $aa-\alpha$ is divisible by $2p+1$, we will have $aa-\alpha = n(2p+1)$. Now, *a* is either even or odd. If it be odd, $aa-\alpha$ will be even and, because of this, *n* is also even and, thus, $aa-\alpha$ will be divisible by $2(2p+1)$.

511. But if *a* be even, $2p+1-a$ will be odd and, moreover, $(2p+1-a)^2-\alpha = n(2p+1)$, where *n* is even, so that this formula is likewise divisible by $2(2p+1)$; whence, if α be an odd number, it will certainly be contained amongst the remainders 1, *A*, *B*, *C*, *etc.*

512. But if α be an even number, $\alpha+2p+1$, which is odd, can be considered in its place amongst the remainders of the divisor $2p+1$ and,

for the reasons given [above], it must also be found amongst the remainders of the divisor $2(2p+1)$.

513. Given, therefore, the remainders 1, α, β, γ, *etc.* arising from the prime divisor $2p+1$, the sequence of remainders 1, *A*, *B*, *C*, *etc.* arising from the double divisor $2(2p+1)$ can be immediately put together from them, putting, of course, those that are odd themselves, but increasing those that are even by the number $2p+1$.

514. In like manner, the sequence of non-remainders answering to the divisor $2(2p+1)$ is fashioned from the sequence of non-remainders $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, $\mathfrak{e}$, *etc.* answering to the divisor $2p+1$, provided that the odd ones themselves be taken and the even ones be increased by the number $2p+1$.

On the divisor $d = 4(2p+1)$.

515. The multitude of numbers less than this divisor and prime to it is $2.1.2p = 4p$ and not only do the squares aa and $(d-a)^2$ leave the same remainder, but there are in addition two others bb and $(d-b)^2$. For, we can make $bb-aa = (b-a)(b+a) = 4n(2p+1)$ by taking $(b-a) = 2n$ and $b+a = 2(2p+1)$, whence we have $b = 2(2p+1)-a$ and, thus, the roots of the four squares leaving the same remainder are: a, $2(2p+1)-a$, $2(2p+1)+a$, $4(2p+1)-a$.

516. But there cannot be more than four, whence, in this case, the number of remainders is only p, just as for the prime divisor $2p+1$. But the number of non-remainders is $3p$, as one may see from the subjoined examples:

divisor	3	12	5	20	7	28
remainders	1	1	1, 4	1, 9	1, 2, 4	1, 9, 25
non-remainders	2	5 7 11	2, 3	3, 7, 11, 19 13, 17	3, 5, 6	3, 27, 19 5, 17, 13 11, 15, 23

divisor	11	44
remainders	1, 3, 9, 5, 4	1, 9, 25, 5, 37
non-remainders	2, 6, 7, 8, 10	3, 27, 31, 15, 23 7, 19, 43, 35, 39 13, 29, 17, 21, 41

divisor	13	52
remainders	1, 3, 4, 9, 10, 12	1, 9, 25, 49, 29, 17
non-remainders	2, 5, 6, 7, 8, 11	3, 27, 23, 43, 35, 51 5, 45, 21, 37, 41, 33 7, 11, 19, 31, 47, 15.

517. Let 1, α, β, γ, δ, *etc.* be the remainders for the divisor $2p+1$ and 1, *A*, *B*, *C*, *D*, *etc.* the remainders for the divisor $4(2p+1)$, equal in multitude; and, first of all, it is clear that those remainders found in the sequence 1, *A*, *B*, *C*, *D*, *etc.* that are less than $2p+1$ are contained in the sequence 1, α, β, γ, δ, *etc.*; but those that are greater must be reduced by the number $2p+1$, or its double, or its triple.

518. Next, I observe that no number of the form $4q-1$ is contained amongst the remainders 1, *A*, *B*, *C*, *D*, *etc.* For, since the square *aa*, reduced by the number $4q-1$, cannot be divisible by 4, $aa-(4q-1)$ cannot be a multiple of $4(2p+1)$, whence the numbers 3, 7, 11, 15, 19, 23, are always amongst the non-remainders.

519. If an odd number of the form $4q+1$ occurs in the sequence 1, α, β, γ, δ, *etc.*, it will likewise occur in the sequence 1, *A*, *B*, *C*, *D*, *etc.*; for, if $aa-(4q+1)$ be divisible by $2p+1$, then $(2p+1\pm a)^2-(4q+1)$ will likewise be divisible; and, because one of the numbers a and $2p+1\pm a$ is certainly even and the other odd, a is taken as odd and $aa-(4q+1)$ will be divisible by 4, whence also by $4(2p+1)$, so that $4q+1$ will be a remainder for this divisor.

520. On the contrary, if an odd number $4q-1$ be a remainder of the divisor $2p+1$, it will not be a remainder of the divisor $4(2p+1)$, as we have already seen; but then $2(2p+1)+4q-1$, because it reduces to the form $4r+1$, will certainly be contained amongst the remainders of the divisor $4(2p+1)$.

521. If an even number $2q$ be a remainder of the divisor $2p+1$, then either

$$2q+2p+1, \quad \text{or} \quad 2q+3(2p+1)$$

will be a remainder of the divisor $4(2p+1)$, as either the former or the latter will be of the form $4r+1$; the other one, being of the form $4r-1$, is always excluded.

522. Of course, if it be that $p = 2m$ and $4m+1$ a prime number, if $4q$ be a remainder of the divisor $4m+1$, then $4q+4m+1$ will be a remainder of the divisor $4(4m+1)$; but if $4q+2$ be a remainder of the divisor $4m+1$, then $4q+2+3(4m+1)$ will be a remainder of the divisor $4(4m+1)$.

523. Let $p = 2m-1$ and $4m-1$ a prime number: If $4q$ be a remainder of the divisor $4m-1$, then $4q+3(4m-1)$ will be a remainder of the divisor $4(4m-1)$. But if $4q+2$ be a remainder of the divisor $4m-1$, then $4q+2+4m-1 = 4q+4m+1$ will be a remainder of the divisor $4(4m-1)$.

524. With the help of these rules, from the several remainders of the prime divisor $2p+1$ the same number of remainders for the divisor $4(2p+1)$ are found; for each one either itself, or increased by the number $2p+1$, or $2(2p+1)$, or $3(2p+1)$, produces a number of the form $4q+1$ and will be a remainder of the divisor $4(2p+1)$.

525. Moreover, from any remainder of the divisor $2p+1$, one non-remainder, of the form $4q-1$, for the divisor $4(2p+1)$ is elicited; and also, from each non-remainder of the divisor $2p+1$, two non-remainders for the divisor $4(2p+1)$ are produced; for, if it be even, two non-remainders are obtained by adding $2p+1$ and $3(2p+1)$,[26] but if it be odd, adding 0 and $2(2p+1)$.

On the divisor $d = 8(2p+1)$.

526. Here there are always eight numbers less than d, whose squares, divided by d, leave the same remainder, namely, one number being a, the other seven are

[26] Reading "$3(2p+1)$" for "$2(2p+1)$".

$$2(2p+1)\pm a,\ 4(2p+1)\pm a,\ 6(2p+1)\pm a,\ 8(2p+1)-a$$

and neither can any more be produced.

527. Because of this, since the multitude of numbers less than d and prime to it is = $4.1.2p = 8p$ and of these the same remainder is furnished in groups of eight, it is clear that the number of remainders will be = p, but that of non-remainders = $7p$.

528. Next, it is clear that any number of the form $4q-1$, that is, of the form $8q-1$ or $8q-5$, cannot occur amongst the remainders; but neither can numbers of the form $8q+5$ be amongst the remainders, because the form $xx-(8q+5)$ can never be divided by 8 and therefore neither by $8(2p+1)$, because $xx = 8n+1$ on account of x being odd.

529. Therefore, there can be no other remainders, except for those of the form $8n+1$ and, because the divisor is $16p+8$, all the numbers from 0 up to $2p$ can be taken for n. But, whenever either $2p+1$, or $3(2p+1)$, or $5(2p+1)$ or $7(2p+1)$ is of the form $8n+1$, they are to be excluded, so that there are only $2p$ numbers of this kind left, only half of which make up the remainders.

530. However, from these numbers of the form $8n+1$, whose multitude is $2p$, if it be established that one is a non-remainder, the remaining p non-remainders are obtained by multiplying it by each remainder, and in addition the rest of the odd numbers, whether of the form $8n+3$, or $8n+5$ or $8n+7$, supply the other $6p$ non-remainders[27].

531. Therefore, the divisor $8(2p+1)$ produces the same number of remainders as the divisor $2p+1$ and, if they be 1, α, β, γ, δ, *etc.*, from each, one by one, the remainders of the divisor $8(2p+1)$ are elicited, by adding a multiple of $2p+1$, so that the aggregate becomes of the form $8n+1$, just as one may see from this example:

[27] Reading *non-residua* for *residua*.

For the divisor 13, remainders	1, 3, 4, 9, 10, 12
add	0, 6.13, 13, 0, 3.13, 13
For the divisor 104, remainders	1, 81, 17, 9, 49, 25.

532. If A be a remainder for the divisor $8(2p+1)$, A^p-1 will be divisible by $8(2p+1)$, and also, if this happens, A will in turn be a remainder of squares. Of course, if A^p-1 be divisible by $8(2p+1)$, it can always be assigned a square xx, such that $xx-A$ be divisible by $8(2p+1)$.

On the divisor $d = 3(2p+1)$.

533. The multitude of numbers less than this divisor and prime to it is $= 2.2p = 4p$, amongst which there are at least two, whose squares leave the same remainder, namely a^2 and $(d-a)^2$, whence the number of distinct remainders cannot be greater than $2p$.

534. In addition, since a is not divisible by 3, either $2p+1-2a$, or $2(2p+1)-2a$, will be divisible by 3; let the quotient be $= m$, and the square of the number $3m+a$ will leave the same remainder, therefore either $2p+1-a$, or $2(2p+1)-a$, and therefore also either $2(2p+1)+a$, or $2p+1+a$ will likewise leave the same remainder.

535. In this way, since the squares always leave the same remainder in groups of four, the number of distinct remainders will only be $= p$ and, therefore, will be the same as for the divisor $2p+1$. However, any number of the form $3n-1$ cannot be in the remainders, since no square, minus such number, can be divided by 3, and thus neither by $3(2p+1)$.

536. Therefore, all the remainders of the divisor $3(2p+1)$ will be numbers of the form $3n+1$, and, if the remainders of the divisor $2p+1$ be $1, \alpha, \beta, \gamma$, *etc.*, each of them, either itself, or increased by either the number $2p+1$, or $2(2p+1)$, by which a number of the form $3n+1$ is produced, will be a remainder of the divisor $3(2p+1)$.

For the divisor $d = (2p+1)(2q+1)$.

537. Let the remainders for the divisor $2p+1$ be 1, α, β, γ, δ, *etc.*, in number = p, and the remainders for the divisor $2q+1$ be 1, π, ρ, σ, τ, *etc.*, in number = q, and the numbers common to each class will be remainders of the divisor $d = (2p+1)(2q+1)$.

538. But the number $m(2p+1)+\alpha$ is reckoned to belong to the first class, where m can be so defined that it becomes equal to either $n(2q+1)+1$, or $n(2q+1)+\pi$, *etc.*, and, so, q remainders of the divisor $2q+1$ are produced from any remainder whatever of the divisor $2p+1$, and, so, pq distinct remainders are obtained altogether for the divisor $(2p+1)(2q+1)$.

539. Let 5.7 = 35 be the composite divisor of this kind and, since 1 and 4 are the two remainders for 5, and 1, 2, 4 the three for 7, therefore, for the divisor 35, the remainders will be the $7n+1$, $7n+2$, $7n+4$ that, of course, are contained in the form $5m+1$, or $5m+4$. Therefore, these remainders will be six in number: 1, 29; 9, 16; 4, 11.

540. Since there are only pq distinct remainders for the divisor $(2p+1)(2q+1)$, four squares at a time will produce the same remainder, one of which, if it be = aa, will be the base of the other three:

$$(2p+1)(2q+1)-a, \quad m(2p+1)-a, \quad n(2p+1)-a,$$

taking the numbers m and n so that $m(2p+1)-2a$ and $n(2p+1)+2a$ can be divided by $2q+1$, which, because $2p+1$ and $2q+1$ are prime to each other, can always be done in such a way that m and n are less than $2q+1$.

Chapter XV

On Divisors of Numbers of the Form *xx+yy*

541. First of all, the case in which the numbers x and y have a common divisor is excluded; for, if the maximum common divisor were = φ and $x = p\varphi$ and $y = q\varphi$, so that p and q be prime to each other, we would

have $xx+yy = (pp+qq)\varphi\varphi$, and discovering the divisors would reduce to that of the form $pp+qq$.

542. Therefore, let x and y be prime to each other, and it can also happen that $xx+yy$ become a prime number, for the testing of which but a single case, the simplest of which is 2, may suffice. However, for $xx+yy$ to become a prime number, the case in which both the numbers x and y are odd is immediately excluded.

543. One is, therefore, supposed to be even, the other odd, and it is evident that all prime numbers $xx+yy$ must be contained in the form $4n+1$ and, thus, no number of the form $4n-1$ can be the sum of two squares.

544. But, on the contrary, if x and y be odd numbers, that is, if $x = 2p+1$ and $y = 2q+1$, it will be possible that its half $\frac{xx+yy}{2} = 2pp+2p+2qq+2q+1$ become a prime number. And also,

$$2pp+2p+2qq+2q+1 = (p+q+1)^2+(p-q)^2$$

is again the sum of two squares, of which one is even, the other odd, on account of the odd sum of the roots, $2p+1$.

545. If a sum of two squares $aa+bb$ be multiplied by another sum of two squares $cc+dd$, the product $(aa+bb)(cc+dd)$ will again be a sum of two squares, since it is $= (ac\pm bd)^2+(ad\mp bc)^2$, which, because of the ambiguity of the signs, can happen in two ways.

546. Here the reciprocal proposition presents itself: if a sum of two squares $pp+qq$ admits of division by a sum of two squares $aa+bb$, the quotient will also be a sum of two squares, the truth of which, however, does not follow thereupon, but requires a special demonstration.

547. In order to demonstrate this, I stipulate that the form $pp+qq$ be divisible by $aa+bb$; then, whatever numbers p and q may be, they can always be reduced to numbers less than $aa+bb$, and even less than $\frac{1}{2}(aa+bb)$, since, if $pp+qq$ be divisible by $aa+bb$,

$$(\pm\alpha(aa+bb)\pm p)^2+(\pm\beta(aa+bb)\pm q)^2$$

also turns out to be divisible.

548. But if $\frac{pp+qq}{aa+bb}$ be the sum of the two squares $cc+dd$, or if $p = ac+bd$ and $q = ad-bc$, taking $p = ac+bd+\alpha(aa+bb)$ and $q = ad-bc+\beta(aa+bb)$, then $pp+qq$ certainly admits of division by $aa+bb$ and the quotient will be

$$= cc+dd+2\alpha(ac+bd)+2\beta(ad-bc)+(\alpha\alpha+\beta\beta)(aa+bb),$$

which is also a sum of two squares $(c+\alpha a-\beta b)^2+(d+\alpha b+\beta a)^2$.

549. The truth of these things should be investigated more deeply; I assert, first of all, that, if the divisor $aa+bb$ be a prime number, by which some form $pp+qq$ is divisible, the quotient is the sum of two squares; yet, this is true in general, even when $aa+bb$ is a composite number, the demonstration of which is seen to be derived from this case.

550. Since a and b are numbers prime to each other, p can be so related to them that $p = ma-nb$, and that in an infinite number of ways; now, if it were that $q = na+mb$, we would certainly have $\frac{pp+qq}{aa+bb} = mm+nn$; but if it not be that $q = na+mb$, we may put $q = na+mb+s$, and we will have

$$pp+qq = (aa+bb)(mm+nn)+2s(na+mb)+ss.$$

551. Since, therefore, $2s(na+mb)+ss$ is divisible by $aa+bb$, it is necessary that either s, or $s+2(na+mb)$ is divisible. In the first case, putting $s = t(aa+bb)$, we will have

$$\frac{pp+qq}{aa+bb} = mm+nn+t(t(aa+bb)+2(na+mb))$$
$$= mm+2mbt+ttbb+nn+2nat+aatt = (m+bt)^2+(n+at)^2,$$

and, therefore, the sum of two squares.

552. In the other case, putting $s+2(na+mb) = t(aa+bb)$, we will have $s = t(aa+bb)-2(na+mb)$, and therefore $\frac{pp+qq}{aa+bb} = mm+nn+tt(aa+bb)-2t(na+mb)$ $= (m-bt)^2+(n-at)^2$, so that in both cases the quotient is a sum of two squares.

553. Therefore, if $pp+qq$ be divisible by the prime number $aa+bb$, it is demonstrated that the quotient is likewise a sum of two squares. Hence,

if the quotient were not a sum of two squares, the divisor would not be a prime number of the form $aa+bb$, that is, either, if it were prime, it would not be of the form $aa+bb$, or, if it were of the form $aa+bb$, it would not be prime; moreover, the words quotient and divisor may be interchanged.

554. Indicating, for the sake of brevity, prime numbers of the form $aa+bb$ by the letters A, B, C, D, *etc.*, if the sum of two squares $pp+qq$ be divisible by the product ABC of such numbers, the quotient will likewise be a sum of two squares. For, we have $\frac{pp+qq}{A} = rr+ss$, then also $\frac{rr+ss}{B} = tt+uu$, and also $\frac{tt+uu}{C} = xx+yy$, whence we have $\frac{pp+qq}{ABC} = xx+yy$.

555. If, therefore, the sum of two squares $pp+qq$ were divisible by a number not the sum of two squares, the quotient, if it were prime, would not be a sum of two squares and, if it were composite, it would not be a product of prime numbers of such a kind, that is, each of which is a sum of two squares.

556. Because of this, if the sum of two squares $pp+qq$ have one factor that is not a sum of two squares, it is necessary that there be found, amongst the remaining prime factors, at least one that is also not a sum of two squares.

557. Now let's investigate whether the sum of two squares $pp+qq$, prime to each other, can be divided by any number $\mathfrak{A}$ that is not a sum of two squares. In order to do this, we may suppose $pp+qq$ to be divisible by such a number $\mathfrak{A}$, and then $(p-m\mathfrak{A})^2+(q-n\mathfrak{A})^2$ will also be divisible by $\mathfrak{A}$ (*).

(*) *Written in the margin*: The roots of which, if p and q be prime to each other, will also be prime to each other.

558. Therefore, a sum of two squares $pp+qq$ can be produced, the roots p and q of which are less than $\mathfrak{A}$, even less than $\frac{1}{2}\mathfrak{A}$; indeed, if p and q were greater than it, since $(\mathfrak{A}-p)^2+(\mathfrak{A}-q)^2$ must admit of the division, the roots of these squares will be less than $\frac{1}{2}\mathfrak{A}$.

559. Therefore, there will be a sum of two squares $pp+qq$ less than $\frac{1}{2}\mathfrak{AA}$ (since it be that $p < \frac{1}{2}\mathfrak{A}$ and $q < \frac{1}{2}\mathfrak{A}$) and divisible by the number $\mathfrak{A}$; putting the quotient = $\mathfrak{B}$, either it itself will not be a sum of two squares, or it will have a factor of that kind, and we will have $\mathfrak{B} < \frac{1}{2}\mathfrak{A}$.

560. Now, since $pp+qq$ be divisible by $\mathfrak{B}$, a sum of two squares $rr+ss$, less than $\frac{1}{2}\mathfrak{BB}$ and divisible by $\mathfrak{B}$, can be produced, and the quotient $\mathfrak{C}$, which will be less than $\frac{1}{2}\mathfrak{B}$, will equally not be a sum of two squares, but since $rr+ss$ be divisible by the latter, there will be a $tt+uu < \frac{1}{2}\mathfrak{CC}$ and divisible by $\mathfrak{C}$, and the quotient $\mathfrak{D} < \frac{1}{2}\mathfrak{C}$ in the same way will not be a sum of two squares.

561. In this way, we finally arrive at a sum of two squares as small as you like, which is divisible by a number that is not a sum of two squares, from which, since this is absurd, it necessarily follows that a sum of two squares, prime to each other, is not divisible by any number that is not itself a sum of two squares.

562. Moreover, given any prime number whatever of the form $4n+1$, because -1, or $4n$, is amongst the remainders of the squares, a sum of two squares divisible by it can always be produced, whence it follows that all prime numbers of the form $4n+1$ are sums of two squares.

563. Further, since numbers of the form $4n-1$ can never be a sum of two squares, no sum of two squats prime to each other can be divisible by any number of the kind $4n-1$.

564. If, however, a more concise demonstration be wanted, which proves that, if the sum of two squares $pp+qq$ be divisible by the sum of two squares $aa+bb$, the quotient is necessarily likewise a sum of two squares, we may try to accomplish this by the following argument.

565. We may suppose that the numbers a and b in the divisor $aa+bb$ are prime to each other; for, if they were not prime to each other, they will be rendered such by taking out the common factor; therefore,

$aa+bb$ will be prime to both a and b. Whence, p and q being any numbers whatever, they can be represented suchly:

$$p = m(aa+bb)\pm fa \quad \text{and} \quad q = n(aa+bb)\pm gb,$$

and this can be done in an infinite number of ways.

566. Therefore, since $pp+qq$ is divisible by $aa+bb$, then $ffaa+ggbb$ will also be divisible by $aa+bb$, and, because of those infinite resolutions, it must happen in all the cases in which $ffaa+ggbb$ is divisible by $aa+bb$, therefore it also happens in the case $g = f$, because the division is successful. (*)

(*) *Written in the margin*: Here it may be doubtful whether the case $g = f$ necessarily follows from the divisibility of the formula $pp+qq$. This doubt is confirmed, for, letting
$a = 7$, $b = 4$, $p = 17$, $q = 6$, we will have $aa+bb = 65$, $pp+qq = 325$;
however, it cannot happen that $17 = 65m\pm 7f$ at the same time $6 = 65n\pm 4f$, whence the latter demonstration should be rejected.
$\frac{17^2+6^2}{7^2+4^2} = 1^2+2^2$, although in no way is $17 = 1.7\pm 2.4$,[28] or $17 = 2.7\pm 1.4$.

567. This being granted, we will have $p = m(aa+bb)\pm fa$ and $q = n(aa+bb)\pm fb$; whence we have

$$\frac{pp+qq}{aa+bb} = \begin{cases} mm(aa+bb) \pm 2fma \\ nn(aa+bb) \pm 2fnb \end{cases} + ff,$$

which expression is $= (f\pm ma\pm nb)^2+(\pm na\mp mb)^2$ and, therefore, the sum of two squares.

568. Thus, it follows immediately from this that, if the quotient be not a sum of two squares, neither can the divisor be of such a kind, neither, therefore, can the product of two numbers, one of which is the sum of two squares, the other not, be a sum of two squares.

569. Together with what was proposed in §558 and the following, it is conclusively proved that the sum of two squares, prime to each other, have no divisors, except those that are themselves a sum of two squares and, also, that all prime numbers of the form $4n+1$ are sums of two squares.

[28] Reading "2.4" for "2 4".

570. If any number N whatever be a sum of two squares in two ways, that is

$$N = aa+bb = cc+dd,$$

then it is not prime. For, since it be that $aa-cc = dd-bb$, we will have $d+b = \frac{m(a+c)}{n}$ and $d-b = \frac{n(a-c)}{m}$, whence $b = \frac{m(a+c)}{2n} - \frac{n(a-c)}{2m}$; hence,

$$N = aa+bb = \frac{(mm+nn)}{4mmnn}(nn(a-c)^2+mm(a+c)^2) = \frac{(mm+nn)}{4mm}((a-c)^2+(b+d)^2),$$

where the factor in the denominator cannot be cancelled. (*)

(*) *Written in the margin*: $(a+c)(a-c) = (b+d)(d-b) = pqrs$, $a+c = pq$, $a-c = rs$, $b+d = pr$, $d-b = qs$; $a = \frac{pq+rs}{2}$, $b = \frac{pr-qs}{2}$, $aa+bb = \frac{1}{4}(pp+ss)(qq+rr)$.

Chapter XVI

On Divisors of Numbers of the Form $xx+2yy$

571. Taking x an y prime to each other, either both are odd, or only one or the other even, therefore, either x, or y, will be even; it will be helpful to investigate the three cases that result from this and to carefully consider by what conditions even and odd numbers may be produced.

572. If both numbers x and y be odd, their squares will be numbers of the form $8n+1$ and $xx+2yy$ is made into a number of the form $8n+3$; but if x is odd and y even, because

$$xx = 8m+1 \quad \text{and} \quad 2yy = 2.4n,$$

$xx+2yy$ is made into a number of the form $8n+1$.

573. If x be even and y odd, putting $x = 2z$, it makes $xx+2yy = 2(2zz+yy)$; now, since y is odd, according as z may be either even or odd, we will have either

$$xx+2yy = 2(8n+1) \quad \text{or} \quad xx+2yy = 2(8n+3).$$

574. Therefore, all the numbers contained in the form $xx+2yy$, provided that x and y be prime to each other, or at least not both even, if they be odd, will belong either to the form $8n+1$, or to $8n+3$; but if these numbers be even, they should be assigned either to the form $2(8n+1)$ or $2(8n+3)$, and in the latter case their halves, that is $2zz+yy$, are also numbers of the form $xx+2yy$.

575. Odd numbers, therefore, that are of the form $8n+5$, or of the form $8n+7$, certainly are not numbers of the form $xx+2yy$, neither are the doubles of their forms contained in that one, whence there are an infinity of numbers not contained in the form $xx+2yy$.

576. Moreover, the product of two numbers of this form are contained in the same form; for, we have $(aa+2bb)(cc+2dd) = (ac\pm 2bd)^2+2(ad\mp bc)^2$, it is at once clear that such products are contained in this form in two ways.

577. Now, it should be demonstrated that, if the number $pp+2qq$ can be divided by $aa+2bb$, the quotient will also be of this form. Observe that, because a and b are prime to $aa+2bb$,

$$p = m(aa+2bb)\pm fa \quad \text{and} \quad q = n(aa+2bb)\pm gb$$

can be realized in an infinite number of ways, and hence $ffaa+2ggbb$ will be divisible by $aa+2bb$.

578. In this way, if it be granted that all formulas $ffaa+2ggbb$ are to be held divisible by $aa+2bb$, the case $gg = ff$, that is $g = \pm f$, will also be contained there, which gives raise to

$$\frac{pp+2qq}{aa+2bb} = \begin{cases} mm(aa+2bb) \pm 2mfa \\ 2nn(aa+2bb) \pm 4ngb \end{cases} + ff = (f \pm ma \pm 2nb)^2 + 2(mb \mp na)^2.$$

579. But, that which I requested that should granted can be proved. Let 1, α, β, γ, δ, *etc.* be the remainders, which arise from the division of squares by the number $aa+2bb$, and also all the squares, $-2bb$ and -2, or all the negative double squares, that is -2, -2α, -2β, -2γ, *etc.*, will be contained in these remainders.

580. Now, any square qq whatever, divided by $aa+2bb$, leaves a remainder that can be exhibited by $ggbb$, since it is possible to put $q = n(aa+2bb)\pm gb$, and the remainder, arising from the division of $2qq$, by $2ggbb$; therefore, the square pp, divided by $aa+2bb$ must leave $-2ggbb$; in the place of which can be put $aagg$, and thus the squares pp and $aagg$ leave equal remainders, and thus we can make

$$p = m(aa+2bb)\pm ag.$$

581. But this demonstration should be rejected unless $aa+2bb$ be a prime number, for, if it be prime, because $ffaa+2ggbb$ and $ggaa+2ggbb$ are divisible by $aa+2bb$, it is necessary that $ff-gg$ and, therefore, either $f-g$, or $f+g$, be divisible; but in whichever case you please, because $aa+2bb$ is already contained in one or the other of the parts, we have either $g = +f$, or $g = -f$; the conclusion does not follow if $aa+2bb$ be a composite number, since then $f-g$ can be divisible by one of the factors and $f+g$ by the other.

582. If the number $pp+2qq$ can be divided by the number $\mathfrak{A}$, which is not of the form $xx+2yy$, the quotient will not be a prime number of the form $xx+2yy$, because of which, if the quotient be prime, it will not be of the form $xx+2yy$; and, if it be composite, not all its prime factors, at any rate, will be of this form.

583. For, let A, B, C, D, *etc.* indicate prime numbers of the form $xx+2yy$, and, if $pp+2qq$ were divisible by $ABCD$ *etc.*, the quotient would certainly be of the form $xx+2yy$; therefore, if the quotient, that is one multiplier, be not of the form $xx+2yy$, it cannot happen that the other factor be a product of prime numbers of this kind.

584. Because if this, if $pp+2qq$ can be divided by a number $\mathfrak{A}$ excluded from the form $xx+2yy$, the quotient, if it be prime, will not be of this form, or, if it be composite, will certainly have a factor not of this form. (*)

(*) *Written in the margin*: Therefore, $pp+2qq$ cannot be divided by any prime number of the forms $8n+5$ and $8n+7$; whence, if squares be divided by such numbers, –2 will be amongst the non-remainders.

If $\frac{xx+nyy}{aa+nbb}$ = an integer, we will have $\frac{bbxx-aayy}{aa+nbb}$ = int.[29] and $\frac{aaxx-nnbbyy}{aa+nbb}$ = int.

585. Let $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, *etc.* indicate prime numbers excluded from the form $xx+2yy$, and we saw that $pp+2qq$ cannot be $A\mathfrak{A}$, nor $AB\mathfrak{A}$, nor $ABC\mathfrak{A}$, because of which it is certain that either no numbers, or at least two $\mathfrak{A}$, $\mathfrak{B}$ are contained amongst the prime factors of the numbers $pp+2qq$.

586. From this, however, it cannot yet be concluded that, if one factor, even if it be composite, of $pp+2qq$ be of the form $xx+2yy$, the other will also be of this form. It remains to be demonstrated that a number $pp+2qq$ cannot be either of the form $\mathfrak{AB}$, or $A\mathfrak{AB}$, or $AB\mathfrak{AB}$, because if it were, $\mathfrak{AB}$ would by all means be a number of this form.

587. In order to see whether $pp+2qq$ can be divided by a number $\mathfrak{A}$ not of the form $xx+2yy$, with respect to which, if it could happen, we would have $p < \frac{1}{2}\mathfrak{A}$ and $q < \frac{1}{2}\mathfrak{A}$, whence $pp+2qq < \frac{3}{4}\mathfrak{AA}$, and the quotient $< \frac{3}{4}\mathfrak{A}$, which would either itself not be a number $xx+2yy$, or would have a factor $\mathfrak{B}$ such that, since it would also be a factor of $pp+2qq$, it could be imputed to be the smallest number $\mathfrak{B}$ of this kind which is a divisor of some form $xx+2yy$; but because this cannot happen, the numbers $pp+2qq$ have no prime divisors, which are not themselves of the form $xx+2yy$.

[29] Integer.