On the solution of Diophantine problems in whole numbers*

Leonhard Euler

[175] §1. It is often the case in solving Diophantine problems that one comes across a formula in which no more than one indeterminate is involved; typically, whole numbers are required to be put in place of the indeterminate in order to satisfy the formula. Indeed, whenever this cannot be done, it may be necessary to settle for fractional number values. However, it is observed that if in this formula the highest degree of the indeterminate is a square and the same expression is also equal to a square number, then a good many of these problems are satisfied by infinitely many whole numbers, which are linked with each other through a certain law, and form a particular series. But if the formula is to be equal to either a cube or some other higher power, or if the indeterminate has more than two dimensions, then one may not be able to produce much more than can be generated by fractional numbers.

§2. Moreover, in this manner a method for all problems is established whereby one must find by guessing one number that solves the problem, from which infinitely many others can be found in turn. In fact, the rule may not be able to reveal anything at first, as the case may occur in which there does not admit of a solution at all, as for $3x^2 + 2$, a formula which can never be made equal to a square. Therefore, we will always set forth in what follows a single instance to be found by which the condition of the problem is satisfied, and we will give the rule whereby from this one countless others can be generated.

§3. So let the formula $ax^2 + bx + c$ be given, which should be equal to a square. And let a, b and c be whole numbers, and let it be required that whole numbers be substituted in place of x. Also, let the number n be given, which put in place of x returns the formula $ax^2 + bx + c$ as a square. Then $an^2 + bn + c$ will be a square number whose root is m. Now to find from this given n another number that satisfies this, I set it equal to $\alpha n + \beta + \gamma\sqrt{an^2 + bn + c}$, and substituting this value in place of x to return the square $ax^2 + bx + c$, whose root is $\delta n + \epsilon + \zeta\sqrt{an^2 + bn + c}$. Indeed, it is clear that this number substituted in place of x will equal a rational square because $an^2 + bn + c$ is a square, and in this way whole numbers will be found, provided n is a whole number, as will soon be evident.

§4. Therefore, let $\alpha n + \beta + \gamma\sqrt{an^2 + bn + c}$ be substituted in place of x in $ax^2 + bx + c$, and from

* *Commentarii academiae scientiarum Petropolitanae* **6**, 1738, pp. 175-188. [E29]

this will be produced[1]

$$\left.\begin{array}{llll} a\alpha^2n^2 & +2a\alpha\beta n & +a\beta^2 & +2a\alpha\gamma n \\ \alpha^2\gamma^2n^2 & +ab\gamma^2n & +ac\gamma^2 & +2a\beta\gamma \\ & +b\alpha n & +b\beta & +b\gamma \\ & & +c & \end{array}\right\}\sqrt{an^2+bn+c}$$

[177] And if we put $\delta n+\epsilon+\zeta\sqrt{an^2+bn+c}$ to be the square root of ax^2+bx+c, then also it will equal the following quantity

$$\left.\begin{array}{llll} \delta^2n^2 & +2\delta\epsilon n & +\epsilon^2 & +2\delta\zeta n \\ a\zeta^2n^2 & +b\zeta^2n & +c\zeta^2 & +2\epsilon\zeta \end{array}\right\}\sqrt{an^2+bn+c}$$

Setting the two expressions equal to each other produces the following equations:

$$\begin{aligned} a\alpha^2+a^2\gamma^2 &= \delta^2+a\zeta^2, \\ 2a\alpha\beta+ab\gamma^2+b\alpha &= 2\delta\epsilon+b\zeta^2, \\ a\beta^2+ac\gamma^2+b\beta+c &= \epsilon^2+c\zeta^2, \\ 2a\alpha\gamma &= 2\delta\zeta, \\ 2a\beta\gamma+b\gamma &= 2\epsilon\zeta. \end{aligned}$$

From these, $\delta=\frac{a\alpha\gamma}{\zeta}$ and $\epsilon=\frac{2a\beta\gamma+b\gamma}{2\zeta}$ are determined, and the value δ, when substituted into the first equation, gives $\alpha^2\zeta^2+a\gamma^2\zeta^2=a\alpha^2\gamma^2+\zeta^4$, which reduces to the two solutions $\zeta^2=\alpha^2$ and $\zeta^2=a\gamma^2$. But in this last of these equations, unless a is a square, it can have no place there. Therefore we will have $\zeta=\alpha$, and similarly, by making substitutions for these quantities in the second equation, we obtain the solutions $a\gamma^2=\alpha^2$, and $\beta=\frac{b(\alpha-1)}{2a}$, of which again only the latter holds true. Finally, by this analysis the third equation will give $\alpha=\sqrt{a\gamma^2+1}$. Therefore we should find a value of γ for which $a\gamma^2+1$ is to be a square.

§5. Let p be a number which when substituted in place of γ returns a square for $a\gamma^2+1$, and let the root of it be q; so if we let $q=\sqrt{ap^2+1}$, then $\alpha=q,\gamma=p,\beta=\frac{b(q-1)}{2a},\delta=ap,\epsilon=\frac{bp}{2}$ and $\zeta=q$. From this we infer the following Theorem:

If ax^2+bx+c is a square in case $x=n$, then will it likewise be a square in case $x=qn+\frac{bq-b}{2a}+p\sqrt{an^2+bn+c}$; and its square root will be $apn+\frac{bp}{2}+q\sqrt{an^2+bn+c}$.

[178] So if bp is divisible by 2, the square root will be a whole number, and therefore the value of x will be integral if $bq-b$ can be divided by $2a$.

§6. Moreover just as from the given value n of this x, there was found another, $qn+\frac{bq-b}{2a}+pm$, obtained by putting m in place of $\sqrt{an^2+bn+c}$; so treating this quantity n in the same way, whereby in place of m there should be taken $apn+\frac{bp}{2}+qm$, another value is generated in turn, which substituted in place of x satisfies the condition, namely this: $2ap^2n+n+bp^2+2pqm$, whence indeed from the square so generated there will come the root $2apqn+bpq+2ap^2m+m$. Now

[1] [*Ed.*] The brace in this array (and the one two lines later) signifies that the radical expression to the right is a common factor of only the terms in the rightmost column of the array.

considering the first quantity as n and the second as m, we obtain a fourth value for this same solution x: $4ap^2qn + 2bp^2q + 4ap^3m + qn + \frac{b(q-1)}{2a} + 3pm$. And the corresponding square root will be $4a^2p^3n + 2abp^3 + 4ap^2qm + 3apn + \frac{3pb}{2} + qm$.

§7. Therefore, the values satisfying x, each with the roots of the resulting squares are obtained as follows: [179]

	Values of x	Values of $\sqrt{ax^2+bx+c}$
I.	n	m
II.	$qn + pm + \frac{b(q-1)}{2a}$	$apn + qm + \frac{bp}{2}$
III.	$2q^2n + 2pqm + \frac{b(q^2-1)}{a} - n$	$2apqn + 2q^2m + bpq - m$
IV.	$4q^3n + 4pq^2m + \frac{b(4q^3-3q-1)}{2a} - 3qn - pm$	$4apq^2n + 4q^3m + 2bpq^2 - apn - 3qm - \frac{bp}{2}$
V.	$8q^4 + 8pq^3m + \frac{4bq^2(q^2-1)}{a} - 8q^2n - 4pqm + n$	$8apq^3n + 8q^4m + 4bpq^3 - 4apqn - 8q^2m - 2bpq + m$
	etc. etc.	etc.
	Here is the rule for this progression.	Here is the rule for this progression.
	For any term A	E
	following this is B	F
	$2qB - A + \frac{b(q-1)}{a}$	$2qF - E$

Consequently, with a bit of work these sequences can be extended as long as is desired.

§8. It is observed from these expressions that alternate terms starting from the smallest make $ax^2 + bx + c$ a whole number square; moreover, every one of the squares becomes a whole number if bp is an even number. In addition, all the values of x are whole numbers if $b(q-1)$ is divisible by $2a$; on the other hand, if this is not true, at least every one of the other such values x is a whole number, for $qq - 1$, i.e. ap^2, is always divisible by a, if indeed we take p and q to be whole numbers. [180] Besides, it should be noted further that whenever in these terms m can be accepted as negative, then the number of solutions is doubled.

§9. Moreover, it should be understood that if a is a square number, a solution in whole numbers cannot be produced, unless it happens that $ax^2 + bx + c$ is itself a square or can be made equal to a square number. For these reasons, we exclude from consideration those in which a is a square, since we set up these problems here to deliver only whole number solutions. For if a is a square; no whole number can be found, save for 0, which put in place of p makes $ap^2 + 1$ a square. Indeed in such a case, all values of this x remain equal to n; and so no others will be found, except by guessing.

§10. However, when a is not a square, a whole number can always be determined, which put in place of p makes $ap^2 + 1$ a square. Wherefore in such cases, if we produce a single instance in which $ax^2 + bx + c$ a square, then we will be able to exhibit at the same time also infinitely many instances for which $ax^2 + bx + c$ becomes a square. Therefore the expression $ax^2 + bx + c$ ought to be handled as follows: by a first guess, a value of x should be discovered within the whole numbers which renders $ax^2 + bx + c$ a square. In addition, one should obtain a value for p which makes $ap^2 + 1$ a square. With the aid of these determined quantities an infinite progression of instances

will be revealed.

[181] §11. If c is a square, say $= dd$, a situation is immediately apparent in which $ax^2 + bx + d^2$ is a square, namely when $x = 0$. Therefore we put $n = 0$, and so $m = d$, and the values of x satisfy this series: $0, dp + \frac{b(q-1)}{2a}, 2dpq + \frac{b(q^2-1)}{a}, ----A, B, 2qB - A + \frac{b(q-1)}{a}$. Moreover, the roots of the squares which are generated from these will be: $d, dq + \frac{bp}{2}, d(2q^2-1) + bpq, ----E, F, 2qF - E$. And the law of these series is clear from above (§7.), namely that they all recur in such a way that any term is composed of the two preceding.

§12. If $b = 0$ and $d = 1$, then it takes the form $ax^2 + 1$, to which $ax^2 + bx + c$ in general reduces in largest part, as is clear from the preceding. Therefore the corresponding values of this x in the series proceed as: $0, p, 2pq, 4pq^2 - p, ----A, B, 2qB - A$. Indeed the roots of the squares so produced are the following: $1, q, 2q^2 - 1, 4q^3 - 3q, ----E, F, 2qF - E$. If then there is a single instance p, for which $ap^2 + 1$ is a square, then it is well known that among these there are infinitely many numbers which, in the general treatment of the formula $ax^2 + bx + c$, can be set in place of p and q.

§13. Moreover then, in order that this method may be adapted to any situation, we look first at those numbers which must be assigned to the letters p and q for an arbitrary value of this a. Further, such p must be a number which makes $ap^2 + 1$ a square whose root is q. Indeed, [182] it is clear that if there is a single suitable value for p, there will likewise be infinitely many: nevertheless it is appropriate to determine for this purpose the single smallest one greater than 0. For the remaining terms, which are $2pq, 4pq^2 - p$, etc., do not contribute to the number of solutions, since they produce only the values following x in §7. That is, the smallest value of p gives rise to all numbers for x; for no additional solutions arise.

§14. Therefore it is understood that if $a = e^2 - 1$, the smallest value for this p takes the value 1, and of q, e. And if $a = e^2 + 1$, then $p = 2e$, and $q = 2e^2 + 1$. And if $a = e^2 \pm 2$, then $p = e$, and $q = e^2 \pm 1$. In this manner infinitely many others can be defined, of which an extremely large number are encountered in this theorem: if $a = \alpha^2 e^{2b} \pm 2\alpha e^{b-1}$, then $p = e$, and $q = \alpha e^{b+1} \pm 1$ where for α we may also accept fractional numbers, provided that these are transformed into whole numbers through multiplication by e^{b-1}. And in the same way if $a = (\alpha e^b + \beta e^\mu)^2 + 2\alpha e^{b-1} + 2\beta e^{\mu-1}$, then $p = e$, and $q = \alpha e^{b+1} + \beta e^{\mu+1} + 1$. Also, if $a = \frac{1}{4}\alpha^2 k^2 e^{2b} \pm \alpha e^{b-1}$, then $p = ke$, and $q = \frac{1}{2}\alpha k^2 e^{b+1} \pm 1$.

§15. Thus, whenever a is a number which is found in these formulas, the value of p and q are immediately apparent. But if a is such a number which cannot be reduced to this form, there is a special method for finding p and q, which was already employed by *Pell* and *Fermat*. And this method is universal, and is likewise successful, no matter what number a denotes. Moreover, for this reason [183] it is especially recommended: because it produces the smallest value of p, which is what is desired for this.

§16. This method is described in the work of *Wallis*, so I will not explain it here. Still, it will be helpful to show the method in operation by means of an example whose study may guide any other solution: It is required to determine without doubt the smallest value of p for which $31p^2 + 1$ is a square. In order that this be executed, the following calculation is performed:

Let $\sqrt{31p^2+1} = q$. Then $q > 5p$, and we set $q = 5p + a$,

$$\begin{array}{lll}
6p^2+1 = 10ap + a^2, & p = \frac{5a+\sqrt{31a^2-6}}{6}, & p = a+b \\
5a^2 = 2ab + 6b^2 + 1, & a = \frac{b+\sqrt{31b^2+5}}{5}, & a = b+c \\
3b^2 = 8bc + 5c^2 - 1, & b = \frac{4c+\sqrt{31c^2-3}}{3}, & b = 3c+d \\
2c^2 = 10cd + 3d^2 + 1, & c = \frac{5d+\sqrt{31d^2+2}}{2}, & c = 5d+e \\
3d^2 = 10de + 2e^2 - 1, & d = \frac{5e+\sqrt{31e^2-3}}{3}, & d = 3e+f \\
5e^2 = 8ef + 3f^2 + 1, & e = \frac{4f+\sqrt{31f^2+5}}{5}, & e = 2f-g \\
f^2 = 12fg - 5g^2 + 1, & f = 6g + \sqrt{31g^2+1}. &
\end{array}$$

Of course, these operations are to be continued until one reaches the expression $\sqrt{31g^2+1}$ in the center column, which is the same form as the proposed $\sqrt{31p^2+1}$. It is now clear if we set $g = 0$, making $f = 1$. And hence, we obtain by working backwards that $e = 2, d = 7, c = 37, b = 118, a = 155, p = 273$, and $q = 1520$.

§17. Moreover, one needs to find the values of p and q from the given a without too much effort, as is seen in conjunction with the following table, in which for each one of the values of a are displayed the smallest numbers which substituted in place of p make $ap^2 + 1$ a square.

[184]

a	p	q	a	p	q
2	2	3	37	12	73
3	1	2	38	6	37
5	4	9	39	4	25
6	2	5	40	3	19
7	3	8	41	320	2049
8	1	3	42	2	13
10	6	19	43	531	3482
11	3	10	44	30	199
12	2	7	45	24	161
13	180	649	46	3588	24335
14	4	15	47	7	48
15	1	4	48	1	7
17	8	33	50	14	99
18	4	17	51	7	50
19	39	170	52	90	649
20	2	9	53	9100	66249
21	12	55	54	66	485
22	42	197	55	12	89
23	5	24	56	2	15
24	1	5	57	20	151
26	10	51	58	2574	19603
27	5	26	59	69	530
28	24	127	60	4	31
29	1820	9801	61	226153980	1766319049
30	2	11	62	8	63
31	273	1520	63	1	8
32	3	17	65	16	129
33	4	23	66	8	65
34	6	35	67	5967	48842
35	1	6	68	4	33

[185] §18. This very simple method immediately comes to mind for extracting an approximation to the square root of a number a which is not a square. That is, if $ap^2 + 1 = q^2$ then $\sqrt{a} = \frac{\sqrt{q^2-1}}{p}$, and if q is an extremely large number, then $\sqrt{a} = \frac{q}{p}$ approximately. But in place of p there can be put the individual terms of the sequence $0, p, 2pq, 4pq^2 - p, ----A, B, 2qB - A$, and in place of q the corresponding individual terms of the sequence $1, q, 2q^2 - 1, 4q^3 - 3q, ----E, F, 2qF - E$ (§12). If we let the term with index i of the latter sequence $= Q$, and also let the term of the former sequence with index i be $= P$, then $\sqrt{a} = \frac{Q}{P}$. For indeed, as the series is further extended, so the Q terms get larger, so that they become closer to $\sqrt{a}$ the further the terms of the sequence are from the initial one. For example, let $a = 6$; then $p = 2$ and $q = 5$, and in turn this sequence is written as follows, placing the subsequent values in positions one after the other: $\frac{1,\ 5,\ 49,\ 485,\ 4801,\ 47525,\ 470449,\ 46569695,\ \text{etc.}}{0,\ 2,\ 20,\ 198,\ 1960,\ 19402,\ 192060,\ 1901198,\ \text{etc.}}$ Therefore, selecting the last term produces $\frac{4656965}{1901198}$, which is so close to the square root of 6 as to not exceed it by more than this fraction: $\frac{1}{2(1901198)^2\sqrt{6}}$. In the same way it is clear that the square root of 61 will be approximately

equal to $\frac{1766319049}{226153980}$, which is only slightly larger but exceeds it by less than $\frac{1}{2(226153980)^2\sqrt{61}}$.

§19. Let there be sought all triangular numbers that are at the same time squares; that is, $\frac{x^2+x}{2}$ should be a square. Thus, each such square will be $2x^2+2x$, from which, by comparison with the expression ax^2+bx+d^2 (§11) determines $a=2, b=2, d=0$. But since $a=2$, it can be found from [186] the table above that $p=2$ and $q=3$. Whence, if in place of x there should be substituted the following values 0, 1, 8, 49, 288, 1681, 9800, etc. whereby $\frac{x^2+x}{2}$ is made a square. From this, moreover, the roots of the squares so generated produce the sequence, 0, 1, 6, 35, 204, 1189, 6930, etc. Alternately, the squares whose roots are contained in this sequence will be triangular numbers. Indeed, the terms of the latter sequence will be twice as large if they are formed from the general sequence $d, dq+\frac{bp}{2}, d(2q^2-1)+bpq$ etc., for if these terms are the roots of $2x^2+2x$, they should then be divided by 2, from which we get the roots of $\frac{x^2+x}{2}$.

§20. Polygonal numbers of side l are expressed by the general formula $\frac{(l-2)x^2-(l-4)x}{2}$, in which x denotes the root of the polygonal number. Thus if a polygonal number of this type is a square, it forces $2(l-2)x^2-2(l-4)x$ to be a square. But a single case arises immediately, in which the condition is satisfied, namely when $x=0$; here the formula $=0$. Consequently we have $n=0$ and $m=0$, and by comparing the formula with the general form ax^2+bx+c produces $a=2(l-2)$ and $b=-2(l-4)$, and also $c=0$. Therefore if $2(l-2)p^2+1=q^2$, then there are values of x for which $2(l-2)x^2-2(l-4)x$, or its fourth part $\frac{(l-2)x^2-(l-4)x}{2}$, i.e. the polygonal number, is a square, as follows: $0, \frac{-(l-4)}{2(l-2)}(q-1), \frac{-(l-4)}{(l-2)}(q^2-1), ----A, B, 2qB-A-\frac{(l-4)}{l-2}(q-1)$. Whereas all these numbers are negative if $l>4$, still we have positive values of x if we assume that q is negative, and then the alternate terms are positive. Besides, [187] if a negative number is found for x, say it is $-k$, a positive number can be given which produces the very same polygonal number, namely $x=k+\frac{l-4}{l-2}$, but unless $\frac{l-4}{l-2}$ is a whole number, these positive numbers are fractions, which we here exclude. For this reason we should keep $-q$ in place of q in alternate terms of the latter sequence. For the roots of the squares $2(l-2)x^2-2(l-4)x$ in these instances will result in the following progression: $0, (l-4)p, 2(l-4)pq, ----E, F, 2qF-E$.

§21. Furthermore, there are no other numbers, except for positive whole numbers, which will generate other instances in which $2(l-2)x^2-2(l-4)x$ is a square, as when $x=1$ produces 4. For this reason if we put $n=1$ and $m=2$, then by doing this we have the following values for x: $1, q+2p-\frac{(l-4)}{2(l-2)}(q-1), 2q^2-1+4pq-\frac{(l-4)}{l-2}(q^2-1), ----A, B, 2qB-A-\frac{(l-4)}{l-2}(q-1)$. Moreover, the square roots of the corresponding values of $\frac{(l-2)x^2-(l-4)x}{2}$ produce this sequence: $1, \frac{lp}{2}+q, lpq+2q^2-1, ----E, F, 2qF-E$. Further, when all these values of x are whole numbers, then the smallest value is not the one in place of q, but is rather the one that ought to be selected to make $\frac{l-4}{2(l-2)}(q-1)$ a whole number, and this can always be done. For if we want pentagonal numbers to be squares, then $l=5$, and $a=6$, and q will be a number from the series 1, 5, 49, etc. and the corresponding values of p will be 0, 2, 20, etc. Therefore, when $\frac{(l-4)}{2(l-2)}(q-1)=\frac{1}{6}(q-1)$ is a whole number, we should take $q=49$, and $p=20$. So the roots of [188] pentagonal numbers which are squares are, $1, 81, 7921, ----A, B, 98B-A-16$, and these numbers (§20) are contained in the above sequence, if we allow $q=-5$, making the alternate terms positive. Further, the square roots of these pentagonal numbers are $1, 99, 9701, ----E, F, 98F-E$.

§22. If $2(l-2)p^2+1=q^2$, it is clear from the preceding that if $2l-4$ is a square, no whole numbers can be substituted for p. For this reason, either all the polygonal numbers are squares or only a

few are. For instance, it turned out above that if $l = 4$, all tetragonal numbers are also squares. Then, if $2l - 4 = 16$ or 36, or 64 etc., in these situations here are no other squares besides 0 and 1. If $2l - 4 = 16$, then $l = 10$, and so the polygonal numbers are decagonal, whose form is $4x^2 - 3x$, and no decagonal number is a square in whole numbers besides 0 and 1.