On a notable advancement of Diophantine analysis*

Leonhard Euler

§. 1.

In Diophantine analysis, when one comes upon fourth-power formulas that must equal a square, the method of handling them is as yet too little developed and requires too many tedious wanderings when we desire multiple solutions. For once a solution is found, whatever fourth-power formula you wish ought to be changed immediately into other forms through substitution, by the operations of which is soon reached numbers so enormous, that hardly anyone would be willing to undertake such work.

§. 2. When therefore, for the very familiar Problem for which two numbers are required, the sum of which is a square, while the sum of the squares is a fourth power, I recently fell upon a solution that was convenient enough and neatly arranged, I soon observed, that the same method could be made much more general. For it can always be called into use, as often as such a fourth-power formula that must be reduced to a square is put forth:

$$aax^4 + 2abx^3y + cxxyy + 2bdxy^3 + ddy^4 = \Box.$$

Because it can be reduced to this form:

$$(axx + bxy + dyy)^2 + (c - bb - 2ad)xxyy,$$

for the sake of brevity let us put $c - bb - 2ad = mn$ so that we have

$$(axx + bxy + dyy)^2 + mnx^2y^2 = \Box;$$

this will be satisfied by putting

$$axx + bxy + dyy = \lambda(mpp - nqq) \text{ and } xy = 2\lambda pq,$$

*Originally published as *De insigni promotione analysis Diophantaeae*, in *Mémoires de l'académie des sciences de St.-Petersbourg* 11, 1830, pp. 1-11. E772 in the Eneström index. Translated from the Latin by Christopher Goff, Department of Mathematics, University of the Pacific, Stockton CA 95204.

for then our formula turns out to be a square, namely $\lambda\lambda(mpp+nqq)^2$, where it is noted, that since the number mn has many factors, that this expression can thus be changed in many ways.

§. 3. Here, we consider all the numbers m, n, p, q as integers; but if however we wanted to allow fractions, then it would be permitted to write unity in place of y, and thus $x = 2\lambda pq$, which value substituted in the previous equation offers

$$4\lambda\lambda appqq + 2\lambda bpq + d = \lambda mpp - \lambda nqq,$$

seeing that this equation is quadratic with respect to both letters p and q separately, we will find by extracting the root for each separately these two formulas:[a]

$$\begin{aligned} p &= \frac{-\lambda bq \pm \sqrt{\lambda md + \lambda\lambda qq(bb-4ad+mn) - 4\lambda^3 naq^4}}{4\lambda\lambda aqq - \lambda m} \\ q &= \frac{-\lambda bp \pm \sqrt{-\lambda nd + \lambda\lambda(bb-4\ d+mn)pp + 4\lambda^3 amp^4}}{4\lambda\lambda app + \lambda n}. \end{aligned}$$

§. 4. Since the letter λ is left to our choice, it will not be at all difficult to assign to it such a value that the extraction of the square root will succeed in at least one formula. Which, if we will have obtained it, so that we have procured defined values for p and q, from there one will be able in the following way to dig up many other, indeed infinitely many, values. For let p and q be the discovered values and on account of ambiguity in the sign of the radical for p another value becomes known, which, if it is set to p', then $p+p' = \frac{-2bq}{4\lambda aqq-m}$. Here now the value p' substituted into the other formula in place of p will give also a new value for q, which is q', and in a similar way

$$q + q' = \frac{-2bp}{4\lambda app + n}.$$

And it is not truly necessary to do the other substitution, when the discovery of new values for p and q can be procured very easily in the following way.

§. 5. For once we have obtained the two values p and q, immediately from there the following series can be assigned: $p, q, p', q', p'', q'', p''', q'''$, etc. where

$$\begin{aligned} p' &= \frac{-2bq}{4\lambda aqq - m} - p; \quad q' = \frac{-2bp'}{4\lambda ap'p' + n} - q \\ p'' &= \frac{-2bq'}{4\lambda aq'q' - m} - p'; \quad q'' = \frac{-2bp''}{4\lambda ap''p'' + n} - q' \\ p''' &= \frac{-2bq''}{4\lambda aq''q'' - m} - p''; \quad q''' = \frac{-2bp'''}{4\lambda ap'''p''' + n} - q'' \\ &\qquad \text{etc.} \qquad\qquad\qquad \text{etc.} \end{aligned}$$

[a]There is an error in the expression for q, though there is an empty space in the original where the missing letter should be. The radicand should be $-\lambda nd + \lambda\lambda(bb - 4ad + mn)pp + 4\lambda^3 amp^4$.

§. 6. In fact, we can even permute both letters p and q, so that we obtain this series: q, p, q', p', q'', p'', etc., where again:

$$\begin{aligned} q' &= \frac{-2bp}{4\lambda app+n} - q; \quad p' = \frac{-2bq'}{4\lambda aq'q'-m} - p \\ q'' &= \frac{-2bp'}{4\lambda ap'p'+n} - q'; \quad p'' = \frac{-2bq''}{4\lambda aq''q''-m} - p' \\ & \quad\quad \text{etc.} \quad\quad\quad\quad\quad\quad \text{etc.} \end{aligned}$$

and thus without any transformation and substitution from both known values p and q in the beginning, we will have been able to draw out other values, as many as you wish, to such a degree that a law of progression of which comes out. From which, it is clear that this method greatly surpasses the usual one.

§. 7. For when such a sequence of letters p and q has been found, by joining two at a time together in as many ways as we wish, we will obtain just as many suitable values for the desired letter x, whose values from the former series will clearly be

$$2\lambda pq;\ 2\lambda qp';\ 2\lambda p'q';\ 2\lambda q'p'';\ \text{etc.}$$

while from the other series, the values of x will be

$$2\lambda qp;\ 2\lambda pq';\ 2\lambda q'p';\ 2\lambda p'q'';\ \text{etc.}$$

with $y = 1$ certainly; from here it happens that if these values are fractions, that their denominators can be taken for y, while the numerators are assigned to x.

§. 8. Therefore all the work comes down to this, that at least initial values for both p and q are simultaneously tracked down, which can often be done easily, since the letter λ is chosen at will[b]. Meanwhile, still, such initial values can be derived from the initial fourth-power formula via a common method. For having supposed $y = 1$, let the root of this fourth-power formula:

$$aax^4 + 2abx^3 + cxx + 2bdx + dd$$

be set[c] to $axx + bx - d$ and once the calculation has been carried out it becomes:

$$x = \frac{4bd}{bb-2ad-c} = \frac{-4bd}{mn+4ad} \text{ because } c = mn + bb + 2ad.$$

In a similar way having put the root as $axx - bx - d$ it becomes

$$x = \frac{bb-2ad-c}{4ab} = \frac{-mn-4ad}{4ab}.$$

[b] *a lubitu nostro pendet.*

[c] *statuat* is here, but I'm reading it as *statuatur*.

§. 9. These same values can also be obtained in another way. For having set the root to $axx+bx+\frac{c-bb}{2a}$, it is gathered that $x=\frac{-mn-4ad}{4ab}$, which agrees with the latter of the preceding [values]. In a similar way, if the root is formed as $d+bx+\frac{c-bb}{2d}xx$ then $x=\frac{-4bd}{mn+4ad}$, the former value of the preceding §. Yet meanwhile, having found two values these can also be counted: $x=0$ and $y=0$, though while rare can sometimes be deduced.

§. 10. Now having found a suitable value for x by keeping $y=1$, the letters p and q for it [x] can be found without much difficulty. For when we will have put[d] $axx+bx+d=\lambda(mpp-nqq)$ and $x=2\lambda pq$ then $\frac{axx+bx+d}{x}=\frac{mpp-nqq}{2pq}$. Thus from the known value let

$$\frac{axx+bx+d}{x}=A,$$

so that we have $mpp-nqq=2Apq$; it is gathered that $\frac{p}{q}=\frac{A+\sqrt{AA+mn}}{m}$, where the root can really be extracted[e], from which arises the fraction $\frac{f}{g}=\frac{p}{q}$. Therefore having supposed voluntarily $p=f$ and $q=g$ it is clear what ought to be accepted for λ so that $2\lambda pq=x$ and hence immediately both the aforementioned series will be able to be formed. All that remains is to illustrate this method through examples, because a special case was already carefully discussed in the preceding article(*)[f].

§. 11. Although the formula discussed here seems not a little restricted, nevertheless many other very different formulas can be reduced to it by the power of a suitable substitution, of which kind is the sufficiently general [formula] $\alpha A^4\pm\beta B^4=\Box$, or having put $\frac{A}{B}=C$ this simpler one $\alpha C^4\pm\beta=\Box$, provided that a case is at hand, by which it becomes a square, just as in the case $C=1$, so that then $\alpha\pm\beta=\Box$. But all formulas of this type are reduced to our form by the power of the substitution $C=\frac{1+x}{1-x}$; for then having put $\alpha+\beta=aa$, the formula will take on this form:

$$aa+4(\alpha-\beta)x+6aaxx+4(\alpha-\beta)x^3+aax^4=\Box,$$

which on account of the case, in which $a=1$, is evidently[g] reduced to this:

$$(a+2(\alpha-\beta)x+axx)^2+16\alpha\beta xx,$$

[d] There's an upside-down m in *posuerimus*. This is not the kind of typo one sees anymore!

[e] It's not clear why Euler doesn't allow for the negative root here, since there are examples later where p and q have different signs. But he really doesn't use this approach to find p and q in the examples. Rather, he finds suitable values for λ, p, and q by inspection.

[f] (*) The solution of the problem of Fermat of two numbers, the sum of which is a square, while the sum of the squares is a fourth power (*V. Mém. Tom. IX. pag.* 3.) [This footnote is Euler's, referring to E763.]

[g] It's not clear what he means by letting $a=1$, because he doesn't replace a with 1 in the next formula. My best guess is that he means $a=d$, which brings us closer to the first fourth-power formula in the paper, but still not exactly equal.

which therefore one may draw out following prescribed rules, because it will be helpful to illustrate it by a few examples.[h]

Example 1.

Of the formula $2A^4 - B^4 = \square$.

§. 12. This formula agrees with the one from which are usually derived both numbers whose sum is a square while the sum of the squares is a fourth power[i]. Therefore having set $\frac{A}{B} = C$ so that $2C^4 - 1 = \square$, then $\alpha = 2$ and $\beta = -1$, from which $\alpha + \beta = 1 = aa$, thus $a = 1$. Wherefore having put $C = \frac{1+x}{1-x}$ this expression will produce:

$$1 + 12x + 6xx + 12x^3 + x^4 = \square \text{ or this:}$$

$$(1 + 6x + xx)^2 - 32xx = \square.$$

Therefore let it be established according to the given rules

$$1 + 6x + xx = \lambda(pp + 2qq) \text{ and } 4x = 2\lambda pq,$$

or $x = \frac{1}{2}\lambda pq$ or so that we avoid fractions, if we were to write $2q$ in place of q so that we would have $1 + 6x + xx = \lambda(pp + 8qq)$ and $x = \lambda pq$, this equation arises:

$$1 + 6\lambda pq + \lambda\lambda ppqq = \lambda pp + 8\lambda qq.$$

From here the following roots are deduced

$$p = \frac{-3\lambda q \pm \sqrt{8\lambda^3 q^4 + \lambda}}{\lambda\lambda qq - \lambda}$$

$$q = \frac{-3\lambda p \pm \sqrt{\lambda^3 p^4 + 8\lambda}}{\lambda\lambda pp - 8\lambda}$$

whence, after whatever [root] you wish is assigned[j], it follows that the two values will be

$$p + p' = \frac{-6q}{\lambda qq - 1} \text{ and } q + q' = \frac{-6p}{\lambda pp - 8}.$$

Let us now see which values then for p and q come forth from the former formula at least, whence having assumed $\lambda = 1$ immediately the case $q = 0$ offers itself, from which $p = 1$: in addition meanwhile another case offers itself, in which $q = 1$, which gives[k] $p = \frac{3\pm3}{1-1}$; but meanwhile in this case the original quadratic equation gives

[h]In all of Euler's subsequent examples, $\alpha + \beta$ is a square, and $a = 1$ or is reduced to 1 via division.

[i]cf. E763.

[j]*cum quaelibet involvat.* I think Euler means that regardless of how the $\pm$ is assigned to p and p', (or to q and q'), we have the following equations for their sums.

[k]The following should read $\frac{-3\pm3}{1-1}$.

$p = +\frac{7}{6}$. Let us therefore set $\lambda = 1$, and we have twin sufficient values for p and q of which some are $q = 0$ and $p = 1$ while the others are $q = 1$ and $p = +\frac{7}{6}$ from which $x = pq$. The relations among the derived values from p and q will be:

$$p + p' = \frac{-6q}{qq - 1} \text{ and } q + q' = \frac{-6p}{pp - 8}.$$

Wherefore if we set up the series q, p, q', p', q'', etc. then

$$\begin{array}{ccc} q' = \dfrac{-6p}{pp-8} - q & ; & p' = \dfrac{-6q'}{q'q'-1} - p \\ q'' = \dfrac{-6p'}{p'p'-8} - q' & ; & p'' = \dfrac{-6q''}{q''q''-1} - p'. \\ \text{etc.} & & \text{etc.} \end{array}$$

Therefore from the values $q = 0$ and $p = 1$ this series[1] is born:

$$0;\ 1;\ \frac{6}{7};\ \frac{239}{19};\ \text{etc.}$$

Now all products of contiguous terms of this series taken two at a time will give suitable values for x (§. 7.), from which $C = \frac{1+x}{1-x}$. Therefore from here these values are obtained for x: $0; \frac{6}{7}; \frac{1434}{91}$; etc. from which the following are deduced for C: $1; 13; -\frac{1525}{1343}$; etc. The other found values $q = 1$ and $p = \frac{7}{6}$ give these numbers for the series q, p, q', p', etc. $1, \frac{7}{6}, \frac{13}{239}$, etc., from which it is evident that the former values assumed for p and q thoroughly exhaust the solution and that it is truly not necessary to solve the problem for the latter [values].

Example 2.

Of the formula $3A^4 + B^4 = \Box$.

§. 13. Now this formula $3C^4 + 1$ ought to be reduced to a square, and three values are immediately recognized to satisfy it, of course

$$C = 0,\ C = 1,\ C = 2.$$

Since therefore here $\alpha = 3$ and $\beta = 1$, after having set $C = \frac{1+x}{1-x}$ the following formula is born: $4 + 8x + 24xx + 8x^3 + 4x^4 = \Box$, which divided by 4 becomes $1 + 2x + 6xx + 2x^3 + x^4 = \Box$, which having been represented $(1 + x + xx)^2 + 3xx = \Box$ will give these substitutions:

$$1 + x + xx = \lambda(pp - 3qq) \text{ and } x = 2\lambda pq,$$

[1]The fourth term in the series should be $\dfrac{239}{13}$.

from which this equation in p and q emerges

$$1+2\lambda pq+4\lambda\lambda ppqq=\lambda pp-3\lambda qq,$$

from which on account of the case $\lambda=1$ and $q=\frac{1}{2}$ is immediately deduced $p=-\frac{7}{4}$. But both the quadratic roots for p and q will be

$$\begin{aligned} p &= \frac{-\lambda q\pm\sqrt{\lambda-12\lambda^3q^4}}{4\lambda\lambda qq-\lambda} \\ q &= \frac{-\lambda p\pm\sqrt{4\lambda^3p^4-3\lambda}}{4\lambda\lambda pp+3\lambda}. \end{aligned}$$

Thus from these formulas will

$$p+p'=\frac{-2\lambda q}{4\lambda\lambda qq-\lambda} \text{ and } q+q'=\frac{-2\lambda p}{4\lambda\lambda pp+3\lambda}.$$

Since we have already found the case $\lambda=1$ and $q=\frac{1}{2}$, from which $p=-\frac{7}{4}$, our series q,p,q',p',q'',p'', etc. can be formed immediately from this, by the power of the formulas:

$$p+p'=\frac{-2q}{4qq-1} \text{ and } q+q'=\frac{-2p}{4pp+3}.$$

and the terms of this series will become $\frac{1}{2},\frac{-7}{4},\frac{-33}{122}$, etc. from which, when $x=2pq$, we obtain from here the values, $x=\frac{-7}{4}$ and[m] $x=\frac{231}{448}$ from which $C=\frac{-3}{11}$; for then $\sqrt{3C^4+1}=\frac{122}{121}$.

Example 3.

Of the formula $\frac{3A^4-B^4}{2}=\square$.

§. 14. Now since the square ought to be $\frac{3}{2}C^4-\frac{1}{2}$, then $\alpha=\frac{3}{2}$, $\beta=-\frac{1}{2}$, and so $a=1$ and $\alpha-\beta=2$, this fourth-power formula arises

$$1+8x+6xx+8x^3+x^4=\square$$

or

$$(1+4x+xx)^2-3(2x)^2=\square.$$

On account of which let

$$1+4x+xx=\lambda(pp+3qq) \text{ and } x=\lambda pq,$$

which[n] produces this equation in p and q

$$1+4\lambda pq+\lambda\lambda ppqq=\lambda pp+3\lambda qq,$$

[m] The next value should be $\frac{231}{244}$.

[n] NB: Euler uses $mn=-3$ here and sets $2x=2\lambda pq$, rather than letting $mn=-12$.

from which we can immediately dig up certain satisfying values so that there is no need to appeal to the extraction of the root. For first having assumed $\lambda = 1$ and $q = 1$ the equation will give $p = \frac{1}{2}$ and having assumed $\lambda = 3$ and $p = 1$, then $q = \frac{1}{6}$. Thus let us pursue both these cases. First let $\lambda = 1$, so that $x = pq$ and we have found the case where $q = 1$ and $p = \frac{1}{2}$, and because the quadratic equation [becomes]

$$pp(qq-1) + 4pq + 1 = 3qq,$$

it is apparent that the sum of the roots of p is $p + p' = \frac{-4q}{qq-1}$, and in a similar way when $qq(pp-3)+4pq+1 = pp$ then $q+q' = \frac{-4p}{pp-3}$. Now from here the series q, p, q', p', etc. is formed, which will contain the numbers[o] $1, \frac{1}{2}, \frac{-3}{11}, \frac{47}{28}$, etc. from which these values are deduced[p] for x, $\frac{1}{2}, \frac{-3}{22}, \frac{-141}{308}$, and thus for C [we get] the following: $3, \frac{19}{25}, \frac{449}{167}$, etc.

In a similar way for the other case where $\lambda = 3$, $p = 1$ and $q = \frac{1}{6}$ on account of the general formulas[q] $p + p' = \frac{-4q}{\lambda qq-1}$ and $q + q' = \frac{-4p}{\lambda pp-1}$, then

$$p + p' = \frac{-4q}{3qq-1} \text{ and } q + q' = \frac{-4p}{3pp-3},$$

from here the series p, q, p', q', etc. will contain $1, \frac{1}{6}, \frac{-3}{11}, \frac{-47}{84}$, etc. Because therefore $x = 3pq$ it will again[r] be $x = \frac{1}{2}, \frac{-3}{22}, \frac{-141}{308}$, and thus I see that I have more than abundantly indicated the widest use of this method.

§. 15. These several special cases supply us with a summary, by which all this work can be unraveled much more easily and elegantly, which we will explain more clearly in the following Problem.

Problem.

Given a fourth-power formula having been restricted to this form:

$$(axx + 2bx + c)^2 - 4mnxx$$

to find infinitely many values of x for which the formula turns out to be a square.

Solution.

§. 16. First of all, the formula becomes a square if[s]

$$axx + 2bx + c = \lambda(mpp - nqq) \text{ and } x = \lambda pq$$

[o] The fourth term should be negative, i.e. $\frac{-47}{28}$.
[p] The third term should be positive, i.e. $\frac{141}{308}$.
[q] The denominator of $q + q'$ should read $\lambda pp - 3$.
[r] The third term should again be positive, i.e. $\frac{141}{308}$.
[s] The following should read $axx + bx + c = \lambda(mpp + nqq)$.

for then its root will be $\lambda(mpp-nqq)$. Thus having put $x=\lambda pq$ the former equation takes on this form:

$$\lambda\lambda appqq+2\lambda bpq+c=\lambda mpp+\lambda nqq;$$

from which immediately one case satisfying the desired [equation] is pulled forth by taking $p=0$, for then $c=\lambda nqq$. Thus having assumed $\lambda=nc$ then $q=\frac{1}{n}$, and from here this lone case will bring out countless others in the following way.

§. 17. Since the equation just found is quadratic in p and q alike, and even will sustain a twin value for either, whence if for whatever q you wish, the twin values of p are put as p and p', then from the nature of the equation

$$p+p'=\frac{2\lambda bq}{\lambda m-\lambda\lambda aqq} \text{ or } p+p'=\frac{2bq}{m-\lambda aqq}.$$

In a similar way for whatever p you wish, if the twin values of q are put as q and q' then $q+q'=\frac{2bp}{n-\lambda app}$. Whereby when we found $\lambda=nc$ according to the known case, where certainly $p=0$ and $q=\frac{1}{n}$, it will be for all the remaining cases that

$$p'=\frac{2bq}{m-nacqq}-p \text{ and } q'=\frac{2bp}{n-nacpp}-q.$$

Thus by the power of these formulas one may form the following series:

$$p,\ q,\ p',\ q',\ p'',\ q'',\ \text{etc.}$$

for which naturally[t]

$$p'=\frac{2bq}{m-nacqq}-p \quad ; \quad q'=\frac{2bp}{n-nacpp}-q$$
$$p''=\frac{2bq'}{m-nacq'q'}-p' \quad ; \quad q''=\frac{2bp'}{n-nacp'p'}-q'$$

§. 18. Therefore, since the following terms of this series can be formed with little difficulty from the known case $p=0$ and $q=\frac{1}{n}$, by the power of these formulas, it will be

$$p'=\frac{2b}{mn-ac};\ q'=\frac{4mnbb-(mn-ac)^2}{n(mn-ac)^2-4nabbc}.$$

If in this way we wish to define still more terms, we would arrive at exceedingly lengthy expressions, but certainly in numerical examples, one may continue this work with little difficulty as long as you please.

---

[t] There is an apostrophe missing on the values of p (resp. p') in the definition of q' (resp. q''), i.e. q' should be $\frac{2bp'}{n-nacp'p'}-q$ and q'' should be $\frac{2bp''}{n-nacp''p''}-q'$.

§. 19. Moreover, having found this sequence, suitable values for the quantity x can be assigned readily. For when on account of $\lambda = nc$ is $x = ncpq$ its successive values will be

$$x = ncpq, \ \ x = ncp'q = \frac{2bc}{mn - ac},$$

$$x = ncp'q' = \frac{2bc(4mnbb - (mn - ac)^2)}{(mn - ac)^3 - 4abbc(mn - ac)}$$

and so on.

§. 20. But from these individual values of x just as many other neighbors can be produced without any work. For when, having put $x = \frac{1}{y}$, the given formula takes on this form:

$$\frac{(a + 2by + cyy)^2}{y^4} - \frac{4mn}{yy} = \Box,$$

which, after being multiplied by y^4, puts forth that formula which must equal a square: $(a+2by+cyy)^2 - 4mnyy$, which does not differ from the given, except that the letters x and c are permuted[u]. On account of which, if we permute the letters a and c between themselves in all the values found for x, then we will obtain just as many values for the letter y, whose inverses will give just as many new values for x, certainly if whatever value found for x is $x = \frac{f}{g}$, and the letters a and c are permuted in the quantities f and g, from which f' and g' come out, then also will $x = \frac{g'}{f'}$, and in this way hardly any doubt can survive, but that all the satisfactory values for x will clearly be rooted out.

[u]This should read that a and c are permuted.