Lecture 4

LEONHARD EULER (1707-1783)

Euler's algebra

The impossibility of finding a solution in integers of the equation

$$x^4 + y^4 = z^4$$

or even of the equation

$$x^4 + y^4 = z^2$$

was established by Fermat. It appears to have been Euler who in his textbook *Algebra*, published in 1770, first established the impossibility of solving the equation

$$x^3 + y^3 = z^3.$$

It is reported in a standard history that he obtained his proof sometime between 1753 and the time of publication. There is a gap in his proof that was filled by Legendre and to which we shall return. In essence, it can only be filled by understanding the decomposition into primes of numbers in $Z(\alpha)$.

I observe in passing that Euler's algebra was a widely used textbook for some time. There is still much to recommend it today to the intelligent amateur. I like to imagine Clausewitz, who began the study of mathematics as a diversion after being taken prisoner by Napoleon's troops during the battle of Jena, working through a copy of *Algebra*. He writes to his fiance of his studies, but unfortunately does not indicate what books he is using.

Euler's book starts at the beginning, and even has problems in what is presently a very hot topic, financial mathematics. I give two examples .

§II.1.36) *Ich habe einige Ellen Tuch gekauft und für jede 5 Ellen 7 Rthlr. bezahlt, davon wieder 7 Ellen für 11 Rhtlr. verkauft und dabei 100 Rthlr. gewonnen. Wie viel Tuch ist es gewesen?*

§II.1.26) *Ein Mann hinterläßt 11000 Rthlr. für seine Witwe, zwei Söhne und drei Töchter. Nach seinem Testamente soll die Frau zweimal mehr bekommen als ein Sohn, und ein Sohn zweimal mehr als eine Tochter. Wie viel bekommt jeder Erbe?*

Corrections and elaborations

There are a number of statements on the previous page that I have taken from various sources and that are doubtful, as is made clear by an examination of Weil's book on the history of the theory of numbers. First of all, Weil explains why there is good reason to believe that Fermat had not merely stated but in fact proved the impossibility of the equation

$$x^3 + y^3 = z^3, \quad xyz \neq 0,$$

in integers. The proof, however, is not extant, the first extant proof being due to Euler. Moreover, although Euler is a little careless in his *Algebra* about the matter, the "gap" in his proof is filled by theorems that he had already proved and published in 1759. A complete proof does appear in Legendre's *Théorie des nombres* published in 1798. This may be the source of the error.

I shall give two apparently different proofs of the impossibility of this equation. In essence they are the same. One is that of Euler (and perhaps also that of Fermat). The other is modelled on later, more general, methods of Kummer and is meant as an aid to the understanding of his arguments.

These problems appear about half-way through the textbook. By the end, he has arrived at Fermat's theorem for cubes. In between (§II.2.188), he asks and partially answers when an expression $ax^2 + cy^2$ is a cube. He suggests setting

$$x\sqrt{a} + y\sqrt{c} = (p\sqrt{a} + q\sqrt{-c})^3 \tag{A}$$

and

$$x\sqrt{a} - y\sqrt{c} = (p\sqrt{a} + q\sqrt{-c})^3.$$

This makes

$$\begin{aligned} ax^2 + cy^2 &= (x\sqrt{a} + y\sqrt{-c})(x\sqrt{a} - y\sqrt{-c}) \\ &= ((p\sqrt{a} + q\sqrt{-c})(p\sqrt{a} - q\sqrt{-c}))^3 \\ &= (ap^2 + cq^2)^3 \end{aligned} \tag{B}$$

If we expand the left side of (A), we obtain

$$(p^3a - 3pq^2c)\sqrt{a} + (p^2a - 3qq^3c)\sqrt{c},$$

so that (A) can be interpreted as the pair of equations,

$$x = p^3a - 3pq^2c, \qquad y = 3p^2aq - q^3c. \tag{C}$$

Thus these values for x and y ensure that $ax^2 + cy^2$ is a cube. Euler does not, however, show that, conversely, if $ax^2 + cy^2$ is a cube then integers p and q can be found that satisfy (C). None the less he uses this converse statement in his proof of Fermat's theorem for the prime 3. So his argument is incomplete. I present it nevertheless, completing it later.

It appears in the very last chapter of the very last section of the very last part of the book, in the section entitled, *von der unbestimmten Analytik*, which seems to be the late eighteenth, early nineteenth century term for the search for integral solutions to equations whose solutions are not uniquely determined. In the last chapter, the problem is to find two integers x and y such that the sum of their cubes is again a cube, thus to solve Fermat's equation

$$x^3 + y^3 = z^3.$$

Now Euler has already introduced in this section some techniques for solving such equations. I give examples that illustrate Euler's expository style and that illustrate as well some of the principal achievements of number theory before the appearance of Gauss. All of this material remained after Gauss and remains today a basic and integral part of the theory of numbers.

In §II.2.41 he asks when a rational number x can be found such that the rational number x^2+1 is a square. He observes that this is certainly possible. For example, is $x = 3/4$ then

$$x^2+1 = \frac{9}{16}+1 = \frac{25}{16} = \left(\frac{5}{4}\right)^2.$$

This is of course familiar to us as

$$3^2+4^2 = 5^2,$$

because 3 and 4 are two sides of a right-angles triangle whose hypotenuse is 5. So we are meeting the pythagorean theorem again, and of course Fermat's theorem as well, but in the case $n = 2$ in which solutions are possible.

Euler's Algebra offers two methods of solution, of which I present the first. One sets

$$\sqrt{x^2+1} = x+p,$$

and tries to find p, or rather x and p. Squaring, we obtain

$$x^2+1 = x^2+2xp+p^2 \iff 1 = 2xp+p^2.$$

The second equation yields

$$x = \frac{1-p^2}{2p}.$$

Thus if $p = m/n$,

$$x = \frac{n^2-m^2}{2mn}$$

and

$$x^2+1 = \frac{n^4-2n^2m^2+m^4}{4n^2m^2}+1 = \left(\frac{n^2+m^2}{2mn}\right)^2.$$

Euler gives a brief list of possibilities

n	2	3	3	4	4	5	5	5	5
m	1	1	2	1	3	1	2	3	4
x	$\frac{3}{4}$	$\frac{4}{3}$	$\frac{5}{12}$	$\frac{15}{8}$	$\frac{7}{24}$	$\frac{12}{5}$	$\frac{21}{20}$	$\frac{8}{15}$	$\frac{9}{40}$

He also observes that the solution leads to an infinite number of pythagorean triangles, thus to an infinite number of integral solutions of the equation

$$p^2 + q^2 = r^2.$$

He just takes

$$p = 2mn, \quad q = n^2 - m^2, \quad r = n^2 + m^2.$$

There several other equations whose integral solutions Euler discusses. Although not immediately pertinent to us, it is worthwhile to spend a little time with them. He deals with Pell's equation, which will reappear in exacerbated form as the theory of units when we return to Kummer and his treatment of Fermat's equation. He also deals with the search for rational solutions of certain equations which, in modern terminology, is the search for rational points on elliptic curves. Since the Taniyama-Shimura-Weil conjecture, about which a number of you are curious, often provides, among other things, an effective method for establishing the existence of such points, Euler's chapters may serve as an introduction not to the modern statements themselves but to their meaning and purpose.

Pell's equation

Before I begin, I observe that Euler does use the term Pell's equation and that following him the term passed into general use, but that the equation itself was introduced by Fermat in 1657 as a problem to mathematicians in general and to several English mathematicians in particular. It was solved within little more than a year by Fermat himself and by the English mathematicians.

If n is an integer and not 0, it is not possible for $n^2 + 1$ to be a square of a rational number, for that rational number would – if taken positive – have to be an integer larger than n, thus of the form $n + m$ and $(n + m)^2 = n^2 + 2mn + m^2$ is certainly larger than $n^2 + 1$ because $2mn$ and m^2 are both at least 1. On the other hand it might be possible for $an^2 + 1$ to be a square, not of course if a is negative or itself a square, but otherwise. This is the question investigated by Euler in Chapter 7 of II.2.

He begins his investigation with the following remark, in which one sees the name Pell mistakenly appearing.

"*Hiezu hat ein gelehrter Engländer, Namens Pell, eine sehr sinnreiche Methode erfunden, welche wir hier erklären wollen. Dieselbe ist nicht so beschaffen, daß sie auf allgemeine Art für jede Zahl a, sondern nur für jeden besondern Fall gebraucht werden kann.*"

The last remark is more important to us than the reference to Pell. The method is a general method, but as a number-theoretic method and not an algebraic method; it is applied to an individual equation to obtain an answer. There is no general algebraic formula.

Suppose we want to $2n^2+1$ to be the square. If it is the square of some number, that number can be taken to be positive and it will necessarily be larger than n. Write it as $n+p$. Then

$$2n^2+1 = n^2+2pn+p^2 \Longleftrightarrow n^2 = 2np+p^2-1.$$

This is a quadratic equation for n that can be solved to give

$$n = p \pm \sqrt{p^2-(1-p^2)} = p \pm \sqrt{2p^2-1}.$$

This number is only good to us if $2p^2-1$ is a square. One possibility is $p=1$. This leads to $n=0$, which is uninteresting or $n=2$ and then

$$2n^2+1 = 9 = 3^2.$$

This example was so easy, although we applied the general method, that we try another, again taken from Euler's Algebra. We want to find an integral solution of $13n^2+1=m^2$. One possibility is $n=0$, $m=1$, but we are looking for solutions of more interest.

Since $9n^2 < m^2 < 16n^2$, we conclude that $m = 3n+p$ with $p<n$, so that

$$13n^2+1 = 9n^2+6np+p^2 \Longleftrightarrow 4n^2-6pn-p^2+1=0.$$

Thus

$$n = \frac{6p \pm \sqrt{36p^2-16(1-p^2)}}{8} = \frac{3p \pm \sqrt{13p^2-4}}{4}.$$

We have to chose the +-sign. It is clear from this that $n > 6p/4$ and that $n < 7p/4$ so that $2p > n > p$ and therefore $n = p+q$, with $q<p$.

Continuing, we see that

$$n - \frac{3p}{4} = \frac{\pm\sqrt{13p^2 - 4}}{4}$$

or

$$p + 4q = \pm\sqrt{13p^2 - 4}.$$

Squaring, we obtain

$$p^2 + 8pq + 16q^2 = 13p^2 - 4 \Longleftrightarrow 12p^2 - 8pq - 16q^2 - 4 = 0.$$

The last equation can be divided by 4; the result is

$$3p^2 - 2pq - 4q^2 - 1 = 0.$$

We could decide to give these calculations up, fearing that they would continue forever, except that q is positive and smaller than p which is in turn smaller than n. Since these numbers are growing smaller and smaller, we will be forced to stop sooner or later. So we continue.

$$p = \frac{2q \pm \sqrt{4q^2 + 12(4q^2 + 1)}}{6} = \frac{q \pm \sqrt{13q^2 + 3}}{3}.$$

We might be tempted to try $q = 1$ here, so that $p = (q \pm 4q)/4$. With either sign, p is not integral, so that we have to continue.

Once again, we have to take the positive root if p is to be larger than q. Then $5q/4 > p > 4q/4$, so that $p = q + r$ with $r < q$. Thus $q = r + s$ with $s < r$. We continue and we now continue more rapidly, observing that we have at each stage to take the positive square root.

$$\begin{array}{lrl}
p = q + r; & q + r = \tfrac{q+\sqrt{13q^2+3}}{3}; & q = \tfrac{2r+\sqrt{13r^2-3}}{3}. \\
q = r + s; & r + s = \tfrac{2r+\sqrt{13r^2-3}}{3}; & r = \tfrac{s+\sqrt{13s^2+4}}{4}. \\
r = s + t; & s + t = \tfrac{s+\sqrt{13s^2+4}}{4}; & s = 3t + \sqrt{13t^2-1}. \\
s = 6t + u; & 6t + u = 3t + \sqrt{13t^2-1}; & t = \tfrac{3u+\sqrt{13u^2+4}}{4}. \\
t = u + v; & u + v = \tfrac{3u+\sqrt{13u^2+4}}{4}; & u = \tfrac{v+\sqrt{13v^2-3}}{3}. \\
u = v + x; & v + x = \tfrac{v+\sqrt{13v^2-3}}{3}; & v = \tfrac{2x+\sqrt{13x^2+3}}{3}.
\end{array}$$

At this point, we can observe that $x = 1$ makes $13x^2 + 3$ a square and that it makes v integral, namely $v = 2$. Euler takes the process two steps further. If $v = 2$ then

$$\begin{aligned}
u &= v + x = 3, \\
t &= u + v = 5, \\
s &= 6t + u = 33, \\
r &= s + t = 33 + 5 = 38, \\
q &= r + s = 38 + 33 = 71, \\
p &= q + r = 71 + 38 = 109, \\
n &= p + q = 109 + 71 = 180, \\
m &= 3n + p = 540 + 109 = 649.
\end{aligned}$$

Thus

$$13n^2 + 1 = 421201 = 649^2.$$

We could perhaps take x larger, but not smaller, since $x = 0$ does not make $13x^2 + 3$ a square. In other words, we may very well not have found all solutions. This is indeed so. It is worth while to look more carefully at these calculations and to see how we might find others.

We continue Euler's calculations. He writes

$$v = x + y,\ x + y = \tfrac{2x+\sqrt{13x^2+3}}{3},\ x = \tfrac{y+\sqrt{13y^2-4}}{4}.$$

$$x = y + z,\ y + z = \tfrac{y+\sqrt{13y^2-4}}{4},\ \ y = 3z + \sqrt{13z^2+1}.$$

At this point, we are free to take the trivial solution that we earlier rejected, namely $z = 0$, which yields $y = 1$ and then $x = 1$ as before.

This leads, as we know, to the solution $n = 180$, $m = 649$, but now we can start with this value of n, taking it for z. This gives the following results.

$$\begin{aligned}
y &= 1189,\\
x &= y + z = 1189 + 180 = 1369,\\
v &= x + y = 1369 + 1189 = 2558,\\
u &= v + x = 2558 + 1369 = 3927,\\
t &= u + v = 3927 + 2558 = 6485,\\
s &= 6t + u = 6 \times 6485 + 3927 = 42837,\\
r &= s + t = 42837 + 6485 = 49322,\\
q &= r + s = 49322 + 42837 = 92159,\\
p &= q + r = 92159 + 49322 = 141481,\\
n &= p + q = 141481 + 92159 = 233640,\\
m &= 3n + p = 3 \times 233640 + 141481 = 842401.
\end{aligned}$$

Then

$$13n^2 + 1 = 709639444801 = m^2.$$

So we have found another solution. We could continue!

Before returning to Fermat's equation, I pass to Euler's next chapter, which is entitled *Von der Art, wie die Irrationalformel* $\sqrt{a+bx+cx^2+dx^3}$ *rational gemacht wird.* In other words, he wants to find solutions of the equation

$$(D) \qquad y^2 = a + bx + cx^2 + dx^3.$$

We can take a, b, c and d to be integral, and we might at first look for integral solutions, but as Euler quickly explains, this turns out to be too difficult, and we had best content ourselves with rational solutions, and even they are difficult to find. It is useful to cite Euler's introduction to this chapter, because there is a great difference, or so it seems to me, between the present status of these problems and their status in the middle of the eighteenth century and much of the difference is the result of developments in the twentieth century, largely but not entirely in the second half. Conjectures, some, like the Taniyama-Shimura-Weil conjecture, proved, others, like the Birch-Swinnerton-Dyer conjecture, only partially established provide ways to decide, with the help of a computer, but the computer is not the essential ingredient, whether a given equation (D) has a solution, especially whether it has an infinite number of solutions. This was not the situation in which Euler found himself.

"*Es soll also die Formel* $a+bx+cx^2+dx^3$ *zu einem Quadrate gemacht, und zu diesem Zwecke geiegnete Werthe für* x *in Rationalzahlen gesucht werden. Denn da dies schon weit größeren Schwierigkeiten unterworfen ist, so erforert es auch weit mehr Kunst, nur gebrochene Zahlen für* x *zu finden, und man ist genötight sich damit zu begnügen, une keine Auflösung in ganzen Zahlen zu verlangen. Von vorn herein ist auch hier zu bemerken, daß man keine allgemeine Auflösung geben kann, wie eben geschehen, sondern jede Operation giebt uns nur einen einzigen Werth für* x *zu erkennen, während die oben gebrauchte Methode auf einmal zu unendlich vielen Auflösungen führt.*

Basically Euler is reduced to guessing. He considers for example

$$y^2 = 1 + 3x^3.$$

He observes that $x = 0$, $x = 1$ and $x = 2$ yield three possibilities, with $y = 1$, $y = 2$ and $y = 5$.

Then he begins the search for more. Since $x = 1$ is a possibility, he suggests starting from this possibility, setting $x = 1 + z$ and trying to make $1 + 3x^3$ the square of $2 + pz$. Thus

$$4 + 4pz + p^2z^2 = (2 + pz)^2 = 1 + 3(1 + z)^3 = 1 + 3 + 9z + 9z^2 + 3z^3.$$

so he takes $p = 9/4$, leaving

$$\frac{81}{16}z^2 = 9z^2 + 3z^3.$$

Dividing both sides by z^2, we obtain

$$3z = \frac{81}{16} - 9 = \frac{63}{16}$$

so that

$$x = 1 - \frac{21}{16} = -\frac{5}{16} \quad y = 2 - \frac{9}{4}\frac{21}{16} = \frac{128 - 189}{64} = -\frac{61}{64}.$$

Then

$$1 + 3x^3 = 1 - \frac{375}{4096} = \frac{3721}{4096} = y^2.$$

One example suffices for our purposes!

$$x^3 + y^3 = z^3$$

Euler begins his discussion of the impossibility of solving this equation with all three of the integers x, y and z different from 0 with an attempt to apply the various techniques developed in the previous chapters, None succeed.

If x and y have a common divisor d, that number divides z as well, and we might as well replace x by x/d, y by y/d and z by z/d and thus suppose that any two of the three numbers x, y and z are relatively prime. In particular, at least one is odd; and if one is odd, then two are odd. Since, for example, $x^3 + y^3 = z^3$ implies that $x^3 + (-z)^3 = (-y)^3$, we might as well suppose, changing the labels if necessary, that x and y are odd. We next set

$$p = \frac{x+y}{2}, \quad q = \frac{x-y}{2},$$

so that

$$x = p + q, \quad y = p - q.$$

As a result one of p and q must be even and the other odd.

Then $x^3 + y^3$ is

$$(p+q)^3+(p-q)^3 = p^3+3p^2q+3pq^2+q^3+p^3-3p^2q+3pq^2-q^3 = 2p(p^2+3q^2).$$

If this is a cube, it is certainly even – as we already arranged – and thus divisible by 8, so that either p is even or $p^2 + 3q^2$ is divisible by 4. Since one of p and q is even and the other odd, only the first possibility is tenable. Thus 4 divides p and

$$\frac{p}{4}(p^2 + 3q^2)$$

is a cube. These two factors are relatively prime unless 3 divides p. At this point, the argument branches, according as 3 does not divide p or it does.

First case: 3 does not divide p

If it does not, then $p/4$ is a cube and so is p^2+3q^2. This means, or meant for Euler, but it is a point to which we shall have to return, that

$$p+q\sqrt{-3}=(t+u\sqrt{-3})^3.$$

We had shown, following Euler that if p and q were chosen so that this were true, thus if $p=t^3-9tu^2=t(t^2-9u^2)$ and $q=3t^2u-3u^3=3u(t^2-u^2)$, then p^2+3q^2 would be a cube. Since p and q are relatively prime, so are t and u.

Since q is odd, u is odd and t even. Since $p/4$ is a cube, so is

$$2p=2t(t^2-9u^2)=2t(t-3u)(t+3u)$$

Now I observe, and that is the essence of the case we are treating, that 3 does not divide the even number t because it does not divide p. Consequently these three numbers are relatively prime and all three all cubes. Thus

$$t+3u=f^3, \quad t-3u=g^3, \quad 2t=h^3,$$

and

$$f^3+g^3=h^3.$$

At this point, Euler argues as follows.

"*Wenn es also zwei solche Kuben in den größten Zahlen gäbe, so könnte man auch in viel kleineren Zahlen ebenfalls derartige angeben, deren Summe auch ein Kubus wäre, und in solcher Art könnte man auf immer kleinere derartige Kuben kommen. Da es nun in kleinen Zahlen derartige Kuben gewiss nicht giebt, so sind sie auch in den aller größten nicht möglich. Dieser Schluß wird dadurch bestätigt, daß auch der andere Fall eben dahin führ, wie wir sogleich sehen werden.*"

We look a little closer at this argument, in particular at the other case, for, if we are not careful, our argument may simply be that if first case occurs then so does the second, but with smaller triples, and there may be no reason whatsoever that this cannot occur. After looking at the other case, we look more carefully to see in what sense the numbers are becoming smaller.

Second case: 3 divides p

Suppose that 3 divides p, so that $p = 3r$ and

$$(E) \qquad \frac{3r}{4}(9r^2 + 3q^2) = \frac{9r}{4}(3r^2 + q^2)$$

is a cube. The number r is also even, so that $3r^2 + q^2$ is divisible neither by 2 nor by 3. Consequently the two factors of (E) are relatively prime and both cubes. Thus

$$q = t(t^2 - 9u^2), \quad r = 3u(t^2 - u^2).$$

Because q is odd, t must be odd and u even. In addition, $9r/4$ is a cube and so is

$$\frac{8}{27}\frac{9r}{4} = \frac{2r}{3} = 2u(t^2 - u^2) = 2u(t+u)(t-u).$$

Once again, the three numbers $2u$, $t+u$, and $t-u$ are relatively prime, so that each is again a cube.

$$t + u = f^3, \quad t - u = g^3, \quad 2u = h^3, \quad h^3 = f^3 - g^3 = f^3 + (-g)^3.$$

What we have left to do is to assure ourselves that in both cases, we have succeeded in finding solutions that are definitely smaller. Since none of the three new numbers is 0, this cannot go on forever, so that we eventually reach a contradiction.

Are the solutions smaller?

In both the first and second case, the new numbers f and g are odd, so that the even number is still the one that stand by itself on one side of the equation. It is enough to verify that this even number is growing smaller, for that will lead to the same contradiction.

Recall that in the first case,

$$z^3 = 2p(p^2 + 3q^2) = 2p(p^2 + 3q^2) = f^3g^3h^3(t^2 + 3u^2)^3,$$

so that

$$z = \pm fgh(t^2 + 3u^2).$$

Sign aside, z is certainly larger than h because, signs again aside, f and g are both at least 1 and $t^2 + 3u^2$ is at least 3.

In the second

$$\begin{aligned} z^3 &= 2p(p^2+3q^2) = 18r(3r^2+q^2) \\ &= 54u(t+u)(t-u)(t^2+3u^2)^3 \\ &= 27f^3g^3h^3(3r^2+q^2)^3, \end{aligned}$$

so that

$$z = \pm 3fgh(3r^2+q^2).$$

Once again, h has to be smaller than z.