Lecture 6 (and Lecture 8)

Final stages

We are in the middle of two proofs of the impossibility of solving Fermat's equation for $n = 3$. To complete the classical proof, we need to establish with Euler that if an integer $p^2 + 3q^2$ is a cube, then

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

To complete the proof in the style of Kummer, we need to show that there is unique factorization into primes in the domain $\mathbb{Z}(\alpha)$.

Although more abstract, it is easier; so I begin with the proof of unique factorization. It employs a variant of Euclid's algorithm that I prove, taking advantage of a certain modern freedom and informality, pictorially. I begin with the representation of the numbers of $\mathbb{Z}(\alpha)$ as complex numbers in the plane. These are then the numbers of the form

$$a + b\alpha = (a - b/2) + ib\sqrt{3}/2.$$

When represented in the plane, they form a regular triangular lattice as in Figure 1. One point and the six adjacent points are shown in Figure.1a. If for example, the point is $(0, 0)$, then the neighboring points are $(1/2 + i\sqrt{3}/2)$, $-1/2 + i\sqrt{3}/2)$, -1, $-1/2$, $-i\sqrt{3}/2$, $1/2 - i\sqrt{3}/2$. These are in fact the points $\cos(2k\pi/6) + i\sin(2k\pi/6)$, $k = 0, \ldots, 5$ and thus all at a distance 1 from $(0, 0)$. They are the 6-th roots of unity.

If instead of all the numbers in $Z(\alpha)$ we consider those that are multiples of some other ξ, then we simply take this lattice and stretch and rotate it, because multiplying by a complex number amounts, as we saw to a stretching and a rotation. The points that are multiples of ξ are the vertices of the triangles in Figure 2. The sides of the new triangles will be the length L of ξ. I superimpose Figure 2 on Figure 1 obtaining Figure 3.

Suppose we have some other number η. It lies inside or on the boundary of one of the triangles. I look more carefully at this triangle or indeed at any equilateral triangle with vertices A, B and C as in Figure 4. The point D is in the center of the triangle. Suppose the side of the triangle has length L. Then the distance from D to any of the points A, B or C is $L/\sqrt{3}$. Thus the distance of the point A to any point of the small triangle in Figure 4 that contains it is at most $L/\sqrt{3}$. We return to Figure 3 and to an arbitrary number η in the domain $Z(\alpha)$. It is contained in one of the triangles of the figure (imagined as extending off to infinity), thus in one of the three smaller triangles into which that triangle is divided as in Figure 5. In other words it lies at a distance at most $L/\sqrt{3}$ from one of the vertices. If this vertex is $\zeta\xi$ then the length of $\eta - \zeta\xi$ is at most $L/\sqrt{3}$.

In other words, if we start from ξ and η, we can perform the same sequence of operations as in Euclid. We take η to have the larger distance from 0, thus the larger length and the larger norm as the norm is the square of the length. Then we subtract an appropriate multiple of ξ from η. The result μ has a length smaller than ξ. We begin again with the pair μ and ξ, subtracting an appropriate multiple of μ from ξ to obtain a number ν with length smaller than μ. Continuing in this way we eventually arrive at 0. Therefore the penultimate number, the one δ reached immediately before 0, divides all the immediate ones and is the greatest common divisor of ξ and η.

Expressed in another way, the collection of all numbers $\beta\xi+\gamma\eta$ with β and γ in the domain $Z(\alpha)$ is just the collection of multiples of δ, the collection $\beta\delta$ with β in the domain $Z(\alpha)$. This δ may not be unique. If there were another δ', we would have

$$\delta' = \beta\delta, \quad \delta = \beta'\delta',$$

but then

$$\beta\beta' = 1$$

and both β and β' are units. Thus, up to a unit, the greatest common divisor of ξ and η is well defined.

We then show, just as in the modern treatment of Proposition 30 of Book VII and its consequences, that every number of $Z(\alpha)$ is a product of primes in an essentially unique way.

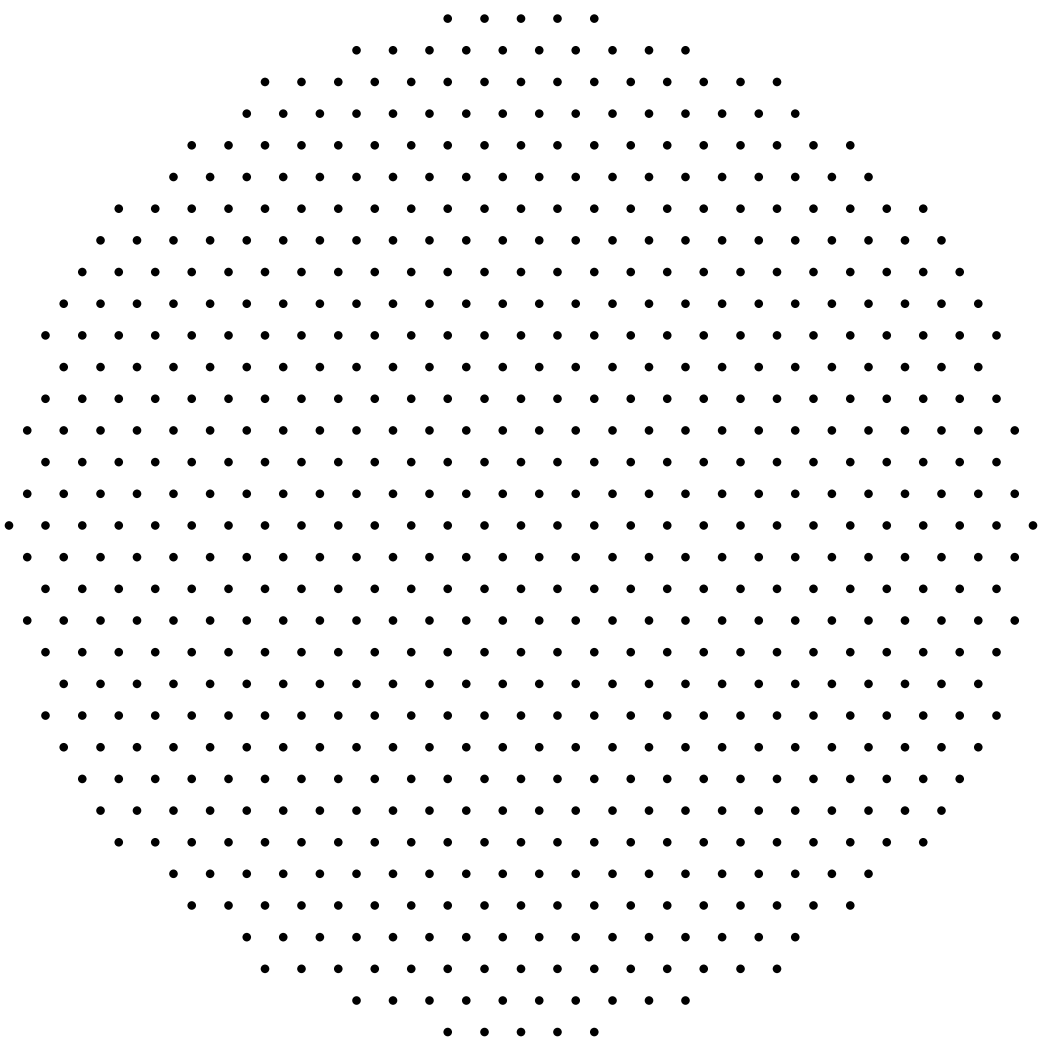

Figure 1

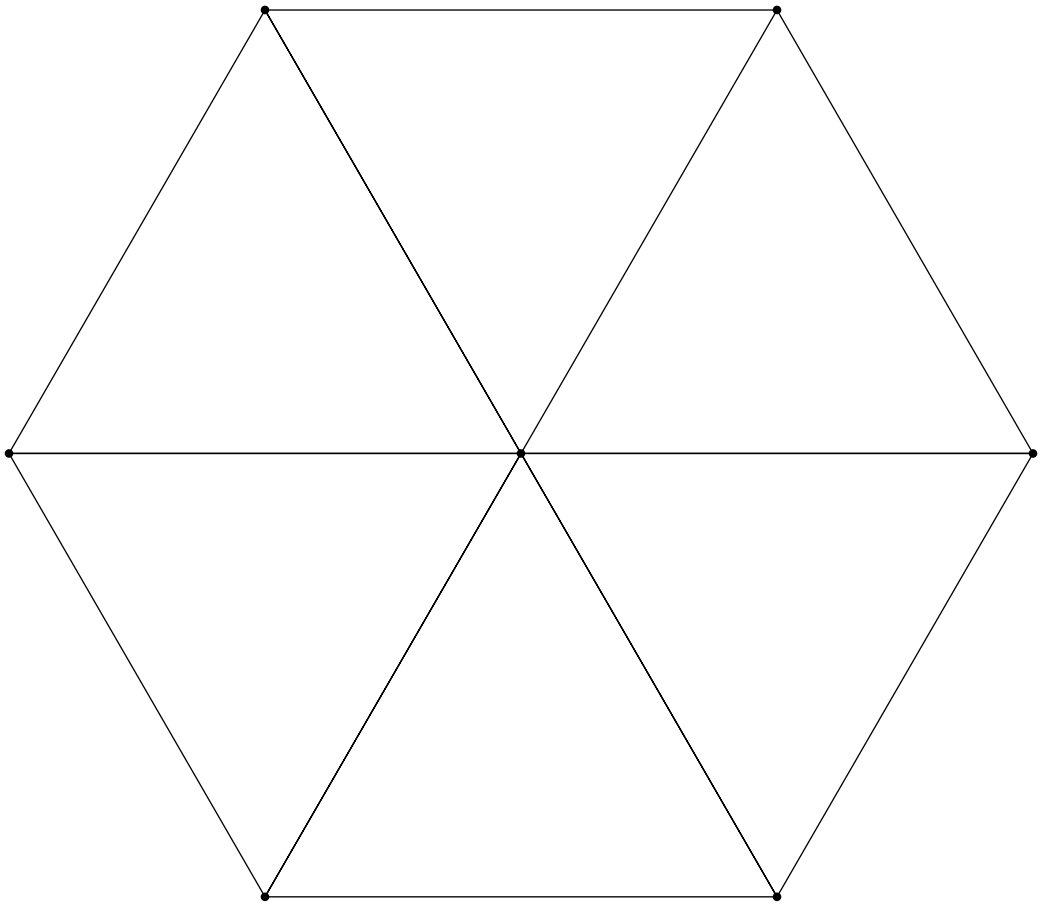

Figure 1a

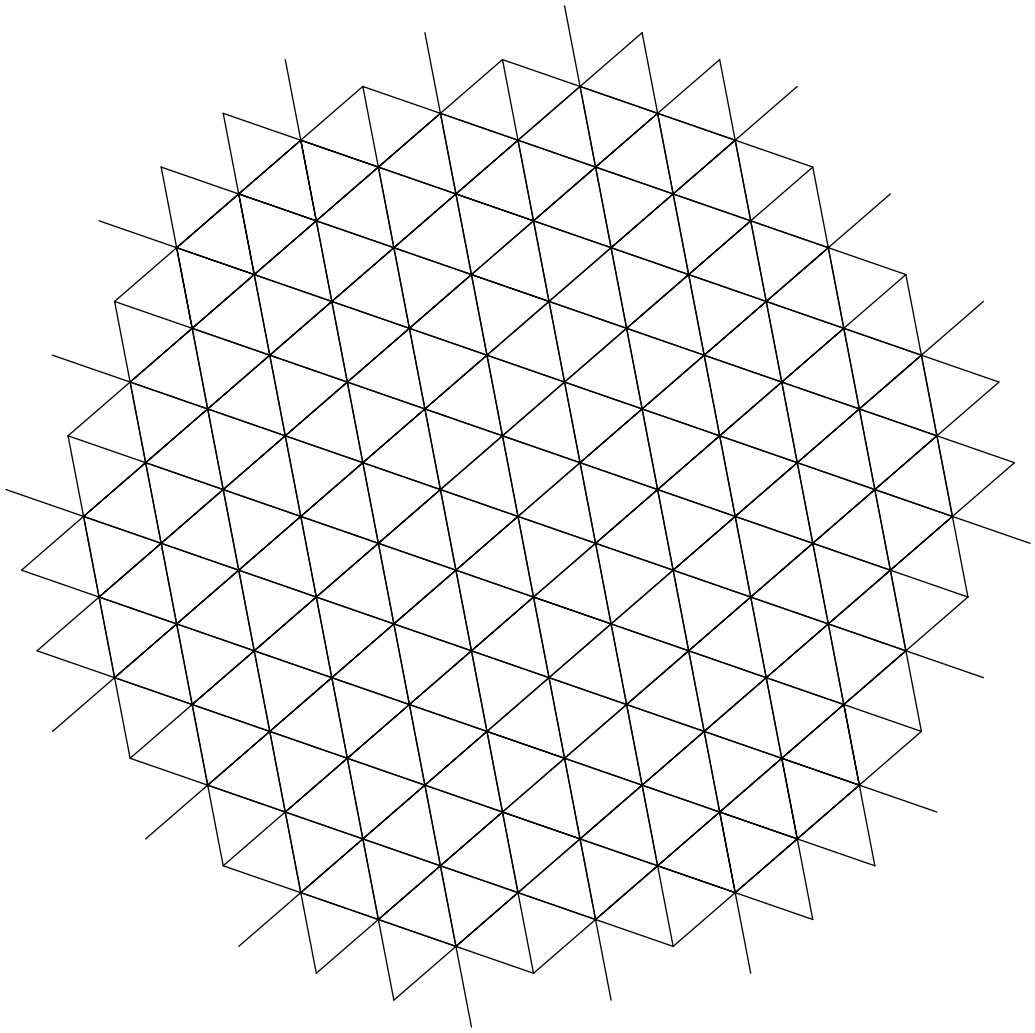

Figure 2

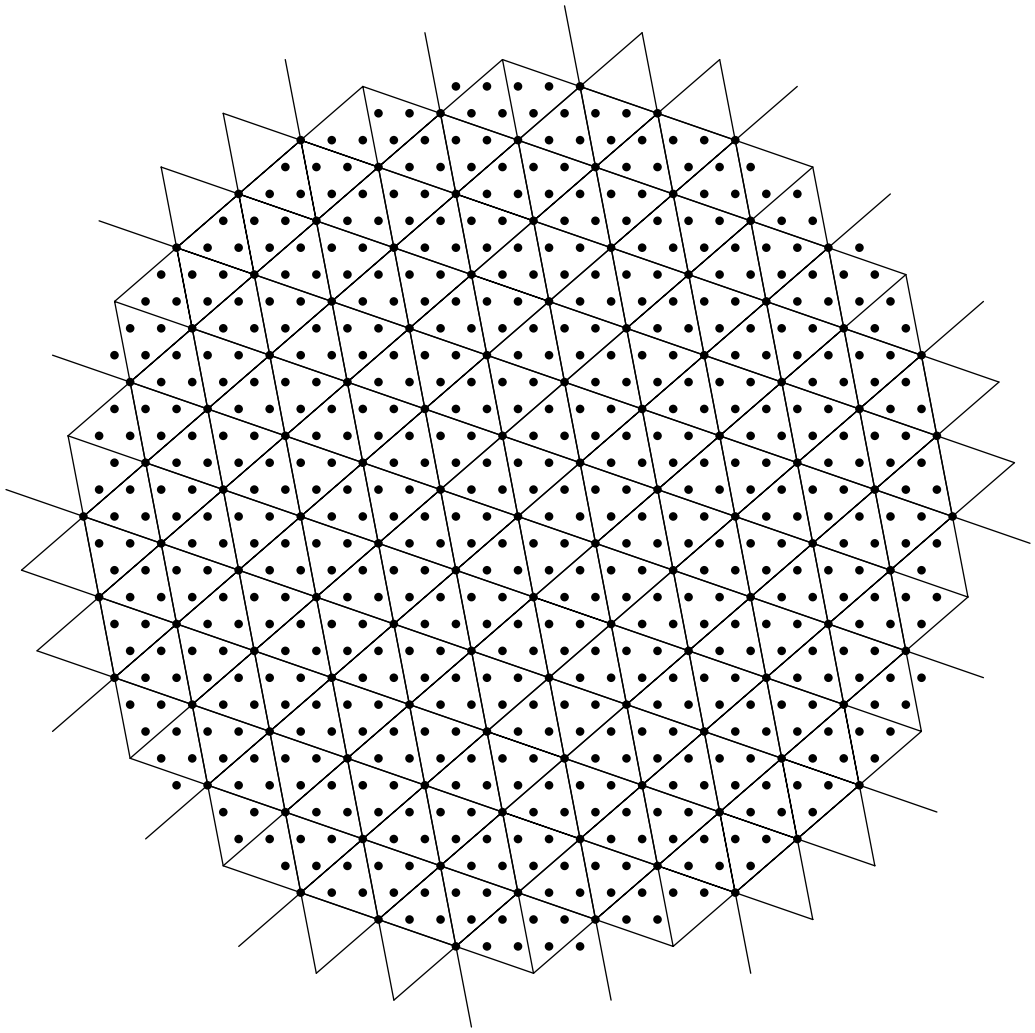

Figure 3

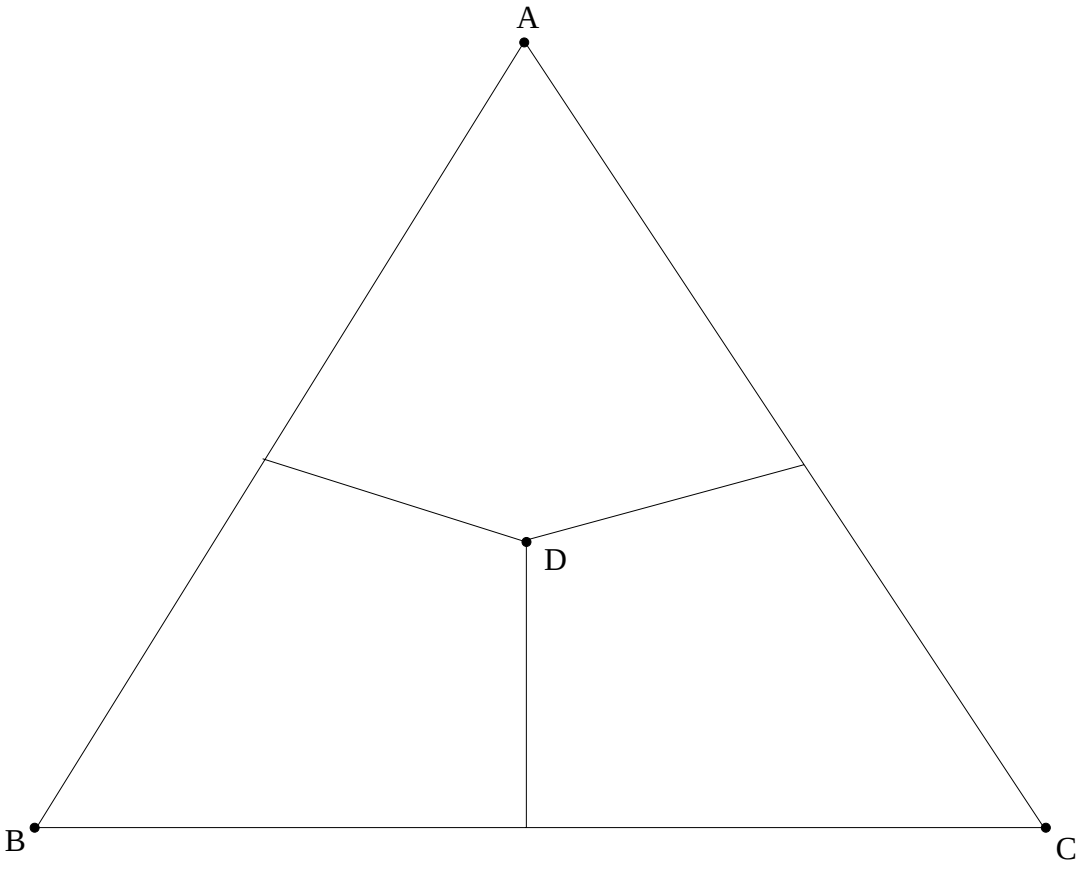

Figure 4

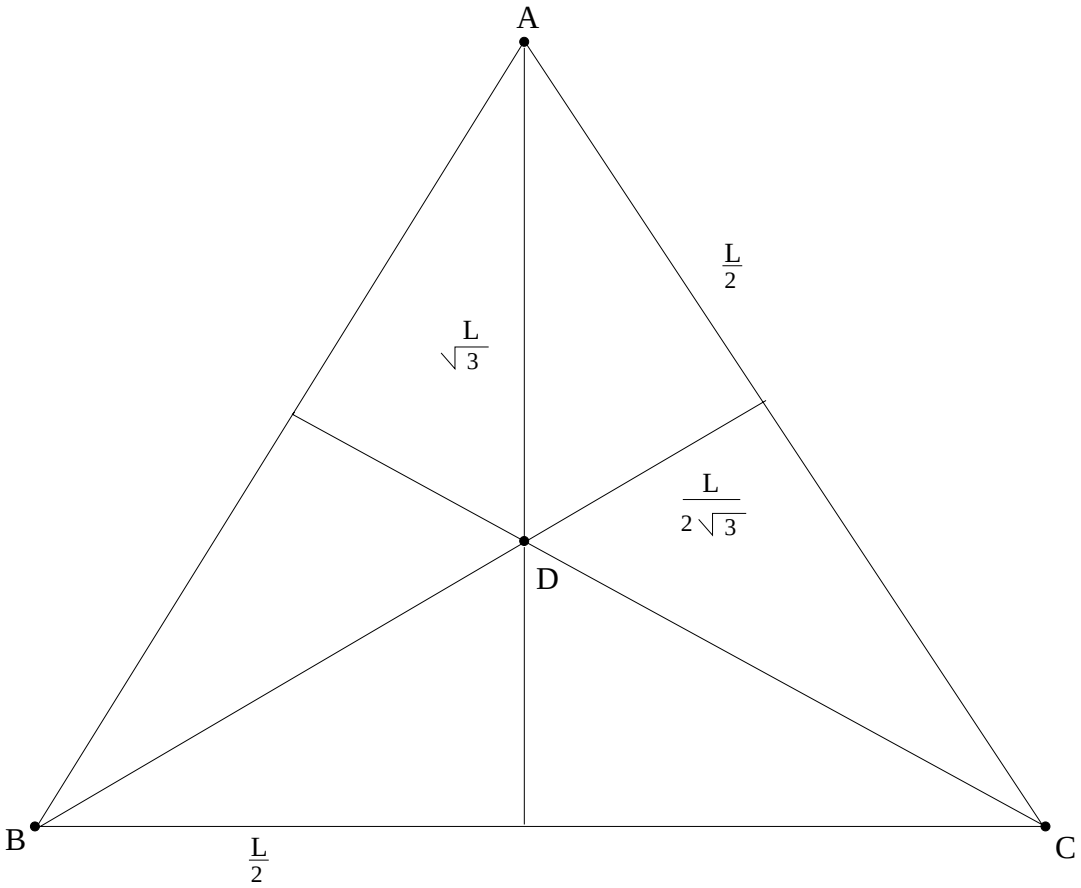

Figure 5

Completion of Euler's argument

Recall what was missing from our argument. We needed to show that if $a^2 + 3b^2$, with a and b relatively prime, was a cube then we could find t and u such that $a = t^3 - 9tu^2$, $b = 3t^2u - 3u^3$. Thus

$$\begin{aligned} a^2 + 3b^2 &= (t^3 - 9tu^2)^2 + 3(3t^2u - 3u^3) \\ &= t^6 - 18t^4u^2 + 81t^2u^4 + 27(t^4u^2 - 2t^2u^4 + u^6) \\ &= t^6 + 9t^4u^2 + 27t^2u^4 + 27u^6 \\ &= (t^2 + 3u^2)^3. \end{aligned}$$

The pertinent argument appears in the Memoirs of the Saint Petersburg Scientific Academy for 1760 (vol. 1.II of Euler's *Opera omnia*). Those who read Latin, even if with difficulty, are advised to turn directly to the paper itself, which contains nothing but the argument about to be presented. The discussion of Euler could not be more leisurely.

There is, however, one thing that we need to know that is not in the paper itself. So I begin with it. I fix a prime p. We want to consider integers, but we do not want to distinguish between two whose difference is a multiple of p. Thus we only need consider the integers $0, 1, 2, \ldots, p-1$ because any integer positive or negative is equal to one of these numbers plus a multiple of p.

$$-14 = 3 + (-1)17, \quad 103 = 1 + 6 \times 17, \quad 212 = 8 + 12 \times 17.$$

We use the symbol $a \equiv b \pmod{p}$ to mean that $a - b$ is a multiple of the prime p. If the prime is understood, we write $a \equiv b$. We are here dealing with a basic notion of number theory. If a and b are not equal to 0 modulo p, then, by Proposition VII.30, neither is ab. Thus if $ab \equiv ac$ or $ab - ac \equiv 0$, then $a(b - c) \equiv 0$ and $b - c \equiv 0$ or $b \equiv c$. Starting from a which is not equivalent to 0 modulo p, we form a^2, a^3, a^4 and so on. Since modulo p there are only $p - 1$ possibilities – except for 0 – there will be a repetition.

$$a^m \equiv a^n, \quad n > m.$$

Then

$$a^m(a^{n-m} - 1) \equiv 0 \Longrightarrow a^{n-m} \equiv 0.$$

Cautionary remarks

When I first turned to this aspect of Euler's argument, I was persuaded that Weil's reconstructions in his book *Number Theory* would convince me that the necessary materials for a complete proof were in Euler. I am no longer so sure. Certainly only details are missing and these details, although they require fastidious care, are not difficult, but even Weil's arguments seem to me at times to be just a little too facile. Providing all the details is time-consuming and they are of little or no interest to a general audience, so that, even though I include it in the notes, I shall omit from the lectures a great deal of the material that follows.

Thus for each a there is a smallest positive integer r that depends on a and is such that $a^r \equiv 1$. If $a^s \equiv 1$ and $s > r$ then, by the euclidean algorithm $s = mr + n$, $0 \leq n < r$, and then $1 \equiv a^s \equiv a^{rm}a^n \equiv a^n$, so that $n = 0$. We refer to this number r as the order of a modulo p. This order has already played an important role in our discussion of Gauss's periods. For $p = 17$, the order of 2 is 8 and that of 3 is 16. Notice that if a^s is any power of a then we can always find a t such that $s + t$ is divisible by r and then $a^{s+t} \equiv 1$. So $a^s a^t \equiv 1$. For example $8 \equiv 2^3 \pmod{17}$ and $3 + 5$ is divisible by 8. Thus if we multiple 8 by $32 = 2^5$ we obtain $256 = 1 + 15 \times 17$.

The powers 2^n, $n = 1, \ldots, 16$ are

$$2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536.$$

Taken modulo 17, they become

$$2, 4, 8, 16, 15, 13, 9, 1, 2, 4, 8, 16, 15, 13, 9, 1$$

We see that they repeat themselves with a period 8 so that 2 has the order 8 modulo 17.

The powers 3^n, $n = 1, \ldots, 16$ are

$$3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,$$
$$177147, 531441, 1594323, 4782969, 14348907, 43046721.$$

Taken modulo 17, they are

$$3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1.$$

We exploited this without discussing congruences in our discussion of Gauss's periods.

Both examples suggest that the order of any integer a modulo p always divides $p - 1$. To verify this we let a be any integer not divisible by p and r its order. I first observe that if b and c are two other integers not divisible by p, then the residues modulo p of the two collections

$$b, ab, a^2b, \ldots, a^{r-1}b.$$

$$c, ac, a^2c, \ldots, a^{r-1}c$$

are either exactly the same or completely different.

Consider for example $a = 12$, $p = 29$. Then

$$a^2 \equiv 28, \quad a^3 \equiv 17, \quad a^4 \equiv 1,$$

so that the order of 12 modulo 29 is 4. Then

$$\{2, 12 \times 2, 28 \times 2, 17 \times 2\} = \{2, 24, 27, 5\},$$
$$\{3, 12 \times 3, 28 \times 3, 17 \times 3\} = \{3, 7, 26, 22\},$$
$$\{5, 12 \times 5, 28 \times 5, 17 \times 5\} = \{5, 2, 24, 27\}.$$

Thus if $b = 2$ and $c = 5$, the two collections are the same, but if $b = 2$ and $c = 3$, they are completely disjoint.

The proof proceeds by observing that if $a^m b = a^n c$ and, for example, $n \geq m$ then $a^m(a^{n-m}c - b) \equiv 0$, so that $a^{n-m}c \equiv b$. Thus the residue of b is in the collection for c and so is that of $a^s b$ for any s.

This means that $\{1, 2, \ldots, p-1\}$ is obtained as the union of various collections $\{b, ac, a^2c, \ldots, a^{r-1}c\}$ (all numbers being taken modulo p,) each with r elements. In other words, in Euclid's language, r measures $p-1$ or, in ours, r divides $p-1$. For example, if $p = 17$ and $a = 2$ then

$$\{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7\} = \{1, 2, 4, 8, 16, 15, 13, 9\},$$
$$\{3, 2 \cdot 3, 2^2 \cdot 3, 2^3 \cdot 3, 2^4 \cdot 3, 2^5 \cdot 3, 2^6 \cdot 3, 2^7 \cdot 3\} = \{3, 6, 12, 7, 14, 11, 5, 10\},$$

and these two sets together make up

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}.$$

There is another important point. For any p, we can always find an a whose order is exactly $p-1$. For $p = 17$, we used without much comment that one such a was $a = 3$. We can get by with a slightly weaker statement.

Let p be given. There is no integer m dividing $p-1$ except $p-1$ itself such that $a^m \equiv 1 \pmod{p}$ for all a not dividing p.

If this were so then every a would be a solution of

$$x^m - 1 \equiv 0 \pmod{p}.$$

Then, by long division of polynomials but only modulo p,

$$x^m - 1 \equiv (x-1)(x^{m-1} + cx^{m-2} + dx^{m-3} + \dots) + f,$$

but we must have $f \equiv 0$. Continuing and dividing by $x-2$, then by $x-3$ and so on, we finally arrive at

$$x^m - 1 \equiv (x-1)(x-2)(x-3)\dots(x-m).$$

If $m \neq p-1$, we substitute $x = m+1$ and arrive at a contradiction.

To what use does Euler put this conclusion? He proves the following assertion.

Suppose p is given and p leaves the remainder 1 upon division by 6. Then there is a pair of relatively prime integers a and b such that $a^2 + 3b^2$ is divisible by p.

Since p cannot be 2, it must be odd. Suppose that $f^2 + fg + g^2$ is divisible by p but not by p^2. Replacing f by $f + p^2$ or g by $g + p^2$ if necessary, we may suppose that f and g are both odd. then

$$f^2 + fg + g^2 = \left(\frac{f-g}{2}\right)^2 + 3\left(\frac{f+g}{2}\right)^2,$$

so that it is enough to show that we can find f and g relatively prime and such that p divides $f^2 + fg + g^2$.

I observe in passing that we can then arrange that p divides $f^2 + fg + g^2$ but that p^2 does not. For if p^2 divides this expression, then

$$(f \pm p)^2 + (f \pm p)g + g^2 = f^2 + fg + g^2 + (\pm 2f + p \pm g)p$$

will for one of the two signs not be divisible by p^2 unless p divides $2f + g$, but that is excluded by hypothesis.

The assumption is that $p = 6n + 1$ because it leaves the remainder 1 on division by 6. Consider the identity,

$$a^{6n} - 1 = (a^{2n} - 1)(a^{4n} + a^{2n} + 1).$$

The left side is divisible by p if a is not. Moreover we can choose an a such that $a^{2n} - 1$ is not divisible by p. As a result, we can find an a such that $a^{4n} + a^{2n} + 1$ is divisible by p. So we take $f = a^{2n}$ and $g = 1$.

Our major task now is to deduce from this that if $p = 6n+1$ then we can always find a pair of relatively prime integers a and b such that $a^2 + 3b^2 = p$.

We first deduce this from unique factorization in the domain $\mathbb{Z}(\alpha)$, because the argument will explain some of Kummer's calculations, and only afterwards return to Euler's, and therefore presumably also Fermat's, more elementary arguments. Choose f and g such that

$$N(f - g\alpha) = f^2 + fg + g^2$$

is divisible by p but not by p^2. Consider the greatest common divisor η of p and $\xi = f - g\alpha$. It cannot be 1 because the norm of any number $\mu p + \nu\xi$ is equal to

$$\mu\bar{\mu}p^2 + p\mu\bar{\nu}\bar{\xi} + \nu\bar{\nu}\, N\,\xi$$

and is therefore divisible by p. In particular $N\,\eta$ is divisible by p. But $N\,\eta$ divides $N\,p = p^2$. So $N\,\eta = p$. Thus $\eta = k + l\alpha$ and

$$k^2 - kl + l^2 = p.$$

There are 12 numbers with this property $\epsilon\eta$ and $\epsilon\bar{\eta}$, if ϵ is any unit. We have

$$\alpha\eta = \alpha(k + l\alpha) = -l + (k - l)\alpha,$$
$$\alpha^2\eta = \alpha^2(k + l\alpha) = (l - k) - k\alpha.$$

Since p is odd, either k or l is odd. Thus either they are both odd or one is odd and one is even. Thus of the three numbers η, $\alpha\eta$ and $\alpha^2\eta$, exactly one

$$\zeta = c + 2b\alpha = (c - b) + b\sqrt{-3} = a + b\sqrt{-3}, \quad a = c - b,$$

in which the coefficient of α is even. This is then also true of $-\zeta$, $\bar{\zeta}$ and $-\bar{\zeta}$ which equal

$$-a - b\sqrt{-3}, \quad a - b\sqrt{-3}, \quad -a + b\sqrt{-3}.$$

Moreover

$$p = N(a + b\sqrt{-3}) = a^2 + 3b^2.$$

Replacing if necessary, ζ by one of the other three numbers, we can even arrange that a and b are positive. So there seems to be an essentially unique way to represent a prime p of the form $6n+1$ as a^2+3b^2 with a and b positive.

Interjection

At this point, we should tie up some loose ends and clarify the argument on the previous page, as it contains a gap. Dividing a number n by 6 leaves the remainder 0, 1, 2, 3, 4 or 5. If n leaves the remainder 1 upon division by 3 then it must leave the remainder 1 or 4 upon division by 6 and if it is a prime, then it must leave the remainder 1 for otherwise it would be even. Thus every prime p that is congruent to 1 modulo 3 can be represented as

$$N\,\eta = \eta\bar{\eta}, \quad \eta = k + l\alpha$$

We saw some time ago that η and $\bar{\eta}$ could not differ by multiplication by a unit. Thus they are relatively prime, so that p is indeed the product of two relatively prime numbers η and $\bar{\eta}$ in the domain $\mathbb{Z}(\alpha)$. Consequently p can be represented in a unique way as $a^2 + 3b^2$.

Interjection continued

We have discovered three kinds of primes in $Z(\alpha)$: the prime λ; the ordinary primes 2, 5, 11 that are congruent to 2 modulo 3 and that, therefore, continue to be prime in $Z(\alpha)$; and those primes ξ such that $N\,\xi$ is a prime congruent to 1 modulo 3. These are, up to multiplication by a unit, the only primes.

If ξ is a prime then $\xi\bar{\xi} = N\,\xi$ is a number n that admits a factorization

$$n = p_1^{a_1} p_2^{a_2} \dots$$

and each p_i admits a factorization that involves only the three kinds of primes just described. Thus so does n. Since the factorization of n is unique, ξ is equal to a unit times one of those primes.

We now, following Euler, attempt to show this directly, starting from the fact that we can find a pair of relatively prime integers c and d such that p divides $c^2 + 3d^2$.

An important step is the observation that if we have such a c and d, then we can find c' and d' such that $c_1 = kp \pm c$ and $d_1 = lp \pm d$, with $-p/2 < c_1, d_1 < p/2$. All we do is to lay the multiples of p out on the line and to choose the ones kp and lp that are closest to c and d. Since the distance between adjacent multiples is p, the closest multiple to, for example, c has to be at a distance at most $p/2$ from it. It cannot be exactly at a distance $p/2$ because $p/2$ is not an integer. Since

$$c_2 + 3d_1^2 = c^2 + d^2 \pm 2c_1kp \pm 6d_1lp + k^2p^2 + 3l^2p^2$$

differs from $c^2 + 3d^2$ by a multiple of p, we might as well suppose that $-p/2 < c, d < p/2$. Then

$$N = c^2 + 3d^2 < \frac{p^2}{4} + 3\frac{p^2}{4} = p^2,$$

so that N/p is smaller than p.

Notice that

$$(A) \qquad (x^2 + 3y^2)(u^2 + 3v^2) = (xu \pm 3yv)^2 + 3(xv \mp yu)^2,$$

so that if we can represent M and N as the sum of a square and 3 times a square then we can so represent MN.

Suppose that

$$(B) \qquad N = c^2 + 3d^2, \quad N < p^2.$$

It may happen that N is even, a disagreeable possibility. But then c and d are both odd. Moreover $4 = 1^2 + 3 \cdot 1^2$. We apply (A).

$$(C) \qquad 4N = (c \pm 3d)^2 + 3(c \mp d)^2.$$

If 4 divides $c + d$ then it also divides $c - 3d$ and we choose $c_2 = (c - 3d)/4$ $d_2 = (c + d)/4$. Otherwise 4 divides $c - d$ and $c + 3d$ and we choose $c_2 = (c + 3d)/4$ and $d_2 = (c - d)/4$. The equation (C) becomes

$$\frac{N}{4} = c_2^2 + 3d_2^d.$$

Thus 4 divides N and $N/4 < p^2$ has a representation of the type (B). We replace N by $N/4$. The new N is odd because $c_2 - d - 2$ is either $-d$ or d and thus odd. So we suppose in addition that N is odd.

If 3 divides N then 3 divides c and

$$\frac{N}{3} = c_2^2 + 3d_2^2, \quad c_2 = d, \quad d_2 = \frac{c}{3}.$$

So we remove 3 from N. The result is not divisible by 3, because c and d are relatively prime.

Suppose some other odd prime q divides N. It then divides neither c nor d. Moreover q divides $4c^2 + 12d^2$. Set $y = 2d$, $x = c - d$. Then

$$x^2 + xy + y^2 = (c-d)^2 + (c-d)2d + 4d^2 = c^2 + 3d^2$$

is divisible by q. So is

$$x^3 - y^3 = (x-y)(x^2 + xy + y^2).$$

Moreover q cannot divide both x and y. So it can divide neither. Choose z such that $zy \equiv 1 \pmod{(q)}$. Then if $w = zx$,

$$w^3 - 1 \equiv (zx)^3 - (zy)^3 \equiv z^3(x^3 - y^3) \equiv 0 \pmod{(q)}.$$

Finally, w is not equivalent to 1 modulo q, for if were then x would be equivalent to y and

$$x^2 + xy + y^2 \equiv 3x^2 \pmod{(q)},$$

So the left side would not be divisible by q. The order of w is therefore 3 and 3 must therefore divide $q - 1$. Since q is odd it must leave the remainder 1 on division not only by 3 but also by 6.

$$6k + r = 3(2k) + r, \quad r = 1, 4$$

If $r = 4$ then $6k + r = 2(3k + 2)$ is even.

Penultimate step

We now want to show that every prime that leaves the remainder 1 on division by 6 can be represented as a^2+3b^2 with a and b necessarily relatively prime. We have seen that this is so for the prime 7 and some other small primes. If it is not generally true, then there is certainly a smallest prime p for which it is false. This could be p. Then we find an N smaller than p^2 which can be represented as c^2+3d^2. If $N=p$, there is nothing to do, but if N is larger than p, we have to make it smaller – and smaller – until it is equal to p. If N is not p, then $N/p<p$ is divisible by a prime q and that prime is necessary smaller than p. Consequently, by assumption, $q=x^2+3y^2$ and

$$(D) \qquad qN=(c^2+3d^2)(x^2+3y^2)=(cx\pm 3dy)^2+3(cy\mp dx)^2.$$

None of the numbers c, d, x and y is divisible by q, because both q and N are divisible by q and c is relatively prime to d and x to y. Moreover

$$c^2+3d^2\equiv x^2+3y^2\equiv 0.$$

Thus

$$3c^2y^2\equiv 3d^2x^2 \Leftrightarrow cy\equiv \pm dx.$$

Changing the sign of one of the numbers if necessary, we arrange that $cy-dx$ is divisible by q. Then

$$dy(cx+3dy)\equiv d^2x^2+3d^2y^2\equiv d^2(x^2+3y^2)\equiv 0.$$

So we can divide (D) by q^2, obtaining

$$\frac{N}{q}=c_1^2+d_1^2, \quad c_1=\frac{cx+3dy}{q}, \quad d_1=\frac{cy-dx}{q}.$$

So we have succeeded in replacing N by N/q, thereby making it smaller.

A property of relatively prime numbers that needs to be mentioned

Suppose that a and b are relatively prime. Then there are two numbers k and l such that $ka + lb = 1$. Suppose the some number d divides the two numbers ac and bc, so that $ac = md$ and $bc = nd$. Then

$$c = (ka + lb)c = kac + lbc = kmd + lnd = (km + ln)d$$

is divisible by d.

Final step

The final step is in fact composed of several small steps and a large digression. I want to show first of all that, if N is any positive number leaves the remainder 1 upon division by 6, then the number of representations of N in the form $c^2 + 3d^2$ with a and b positive and relatively prime is $2^{\rho-1}$ if ρ is the number of different prime divisors of N. For example $343 = 7^3$ has exactly one and $57967 = 7^3 \cdot 13^2$ has two.

Digression

We vacillate between two methods, that of Euler (perhaps even Fermat) and one based on later considerations of Kummer (perhaps even Gauss). Euler's method demands that we demonstrate more, in particular an assertion that I now explain. We say that a number N is properly represented as $c^2 + 3d^2$ if c and d are relatively prime and positive. We know that a number N not divisible by 2 or by 3 has a proper representation exactly when all of its prime divisors leave the remainder 1 upon division by 6.

Why? Suppose N has such a representation,

$$N = c^2 + 3d^2.$$

If p divides N and $b = 2d$, $a = c - d$, then

$$a^2 + ab + b^2 = (c-d)^2 + 2(c-d)d + 4d^2 = c^2 + 3d^2.$$

Moreover the only common divisor of a and b could be 2. Finally

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

is divisible by p and $a - b$ is not, for if it were then

$$a^2 + ab + b^2 \equiv 3a^2 \pmod{(p)},$$

would not be divisible by p. (If p divided a, it would then also have to divide b.) We can find an e such that $eb \equiv 1 \pmod{(p)}$ and then

$$0 \equiv e^3(a^3 - b^3) \equiv f^3 - 1 \pmod{(p)}, \quad f = ea$$

and, at the same time, f is not equivalent to 1 modulo p. As a consequence, the order of f modulo p is 3 and 3 divides $p-1$. Thus p leaves the remainder 1 upon division by 3 and therefore, as it is odd, the remainder 1 upon division by 6.

On the other hand, suppose that

$$N = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots p_\rho^{m_\rho}$$

and that each

$$p_i = \pi_i \bar{\pi}_i$$

is the product of two conjugate primes in $\mathbb{Z}(\alpha)$. We can even suppose that

$$\pi_i = c_i + d_i\sqrt{-3}, \quad \bar{\pi}_i = c_i - d_i\sqrt{-3}.$$

Consider then

$$\xi = \pi_1^{m_1}\pi_2^{m_2}... = c + d\sqrt{-3}$$

Its norm is

$$(E) \qquad c^2 + 3d^2 = (N\,\pi_1)^{m_1}(N\,\pi_2)^{m_2}(N\,\pi_3)^{m_3}\cdots = N$$

On the other hand it is not divisible by any ordinary prime because an ordinary prime is either a prime in $\mathbb{Z}(\alpha)$ or has as prime factors both π and $\bar{\pi}$, π being a prime of $\mathbb{Z}(\alpha)$, and no such pairs appear in (E). Thus c and d are relatively prime.

At each i there are four choices. We can replace c_i and d_i by their negatives $-c_i$ and $-d_i$, which has little effect on the final result. Both c and d are also replaced by their negatives. On the other hand, we can leave c_i alone and replace d_i by $-d_i$, thus replacing ξ_i by $\bar{\xi}_i$, which is prime to it. This leads, because of unique factorization, to a completely different number ξ. Ignoring signs, we obtain 2^ρ different numbers ξ, thus 2^ρ ways of representing N as c^2+3d^2. If we change all of the ξ_i to $\bar{\xi}_i$, the result is to replace ξ by $\bar{\xi}$, thus to replace d by $-d$. In conclusion, we see that only $2^{\rho-1}$ of the representations will have both c and d positive.

Further cautionary remarks

On turning, finally, to Legendre's argument in his *Théorie des nombres* it appears at first that we could have stopped here if, instead of using Euler's initial argument, we had used the variant of it found there. Curiously enough, although still in the classical mode, thus still working with ordinary integers and not with surds of any kind, it is closer to Kummer's arguments. It appears that all we need know is that an odd number N not divisible by 3 can be represented as

$$N = a^2 + 3b^2$$

if and only all its prime divisors leave the remainder 1 upon division by 6. On closer examination, however, Legendre's argument (4th edition, vol. II, pp. 357-360) seems to suffer from the same defect as Euler's

It runs as follows. Since one of the three numbers in Fermat's equation

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

is necessarily even, we suppose it to be z and write $z = 2^m u$, with u odd. Then

$$(x + y)(x^2 - xy + y^2) = 2^{3m} u^3.$$

Legendre next attempts to establish the important fact that u is necessarily divisible by 3. Suppose not.

Since

$$x^2 - xy + y^2 = (x + y)^2 - 3xy,$$

the only possible common divisor of $x + y$ and $x^2 - xy + y^2$ is 3 x and y are then odd, but as u is supposed not to be divisible by 3, this is out of the question. Thus $x+y$ and $x^2 - xy + y^2$ are both cubes. Moreover $x+y$ is even and $x^2 - xy + y^2$ is odd. Let

$$\left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2 = x^2 - xy + y^2 = \sigma^3.$$

Since σ^3 can be represented as the sum of a square and 3 times a square so can σ because they have the same prime divisors. Thus

$$\sigma = f^2 + 3g^2.$$

Thus if

$$(A) \qquad F = f(f^2 - 9g^2), \quad G = 3g(f^2 - g^2),$$

then

$$\sigma^3 = F^2 + 3G^2.$$

Legendre then, unfortunately, concludes that

$$(B) \qquad \frac{x+y}{2} = F, \quad \frac{x-y}{2} = G,$$

a completely unwarranted conclusion, because if σ is composite there are several ways of representing it as the sum of a square and 3 times a square. This error is repeated again later in the argument. To correct the argument, it is necessary to show, and for that the following discussion is necessary, that f and g can be so chosen that both (A) and (B) are satisfied.

Euler's argument

Euler's argument seems to require that he show directly that if N is a number all of whose prime divisors leave the remainder 1 upon division by 6 and ρ is the number of distinct prime divisors of N, then the number of proper representations of N in the form $c^2 + 3d^2$ is $2^{\rho-1}$. We have seen that this can be established as a consequence of unique factorization in the domain $\mathbb{Z}(\alpha)$. How can it be established directly?

I begin with an earlier formula. Suppose

$$M = a^2 + 3d^2, \quad N = c^2 + 3d^2.$$

Then

$$MN = (a^2 + 3b^2)(c^2 + 3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2 = e^2 + 3f^2.$$

where

$$e = ac \pm 3bd \quad f = ad \mp bc,$$

the signs being chosen consistently, either $+$ in the first and $-$ in the second or $-$ in the first and $+$ in the second. I suppose that both M and N leave the remainder 1 upon division by 6.

Then

$$(F) \qquad \begin{aligned} ae \mp 3bf &= a(ac \pm 3bd) \mp 3b(ad \mp bc) = a^2c + 3b^2c = Mc, \\ af \pm be &= a(ad \mp bc) \pm b(ac \pm 3bd) = a^2d + 3b^2d = Md. \end{aligned}$$

As a result any number that divides both e and f divides M. The same argument with c and d replacing a and b shows that it also divides N. Thus if M and N are relatively prime, then e and f are relatively prime.

To remove any possible doubt that the same argument applies, I write out the analogue of (F) in which M is replaced by N.

$$(G) \qquad \begin{aligned} ce + df &= c(ac \pm 3bd) + 3d(ad \mp bc) = ac^2 + 3ad^2 = aN, \\ \mp cf \pm de &= \mp c(ad \mp bc) \pm (d)(ac \pm 3bd) = bc^2 + 3bd^2 = bN. \end{aligned}$$

Notice that if

$$ae - 3bf, \quad af + be$$

are both divisible by M then

$$ae + 3bf, \quad af - be$$

are not both divisible by M, for then M would divide $2ae$ and $2af$, and therefore, being odd, a. It would also divide $3bf$ and be and thus e and thus $3b$ and therefore b as M is prime to 3. Thus the signs appearing in (F) are determined; there is no choice and we can recover c and d from e and f. Changing the sign of both e and f changes the sign of c and d. Changing the sign of just one forces us to modify the choice of signs in (F) and causes the sign of either c or d to change.

Since the signs of both e and f can be changed, this yields eight representations of MN as $e^2 + 3f^2$, of which only two will have e and f positive. If

$$M = p_1^{a_1} \ldots, p_\sigma^{a_\sigma}$$

has σ distinct prime factors and

$$N = p_1^{b_1} \ldots, p_\sigma^{b_\tau}$$

has τ, then MN has $\rho = \sigma + \tau$ and from each of the

$$2^{\sigma-1}2^{\tau-1} = 2^{\sigma+\tau-2} = 2^{\rho-2}$$

representations of M together with N we obtain 2 of MN, leading to $2 \cdot 2^{\rho-2} = 2^{\rho-1}$ representations of MN. Thus, if the assertion to be proved is valid for M and N, then it is true for their product.

As a consequence, if we can show that for a power p^m of a prime that leaves the remainder 1 upon division by 6, there is exactly one proper representation $p = c^2 + 3d^2$ with c and d positive, we will be done, because then the assertion is true for p^m and any of our numbers N is a product $p^m M$ with $M = 1$ or with p and M relatively prime, and with M smaller than N. Thus if the assertion is true for M, it is true for N and we can work our way down.

Let p be such a prime. We first show, repeating an argument, that p has a unique representation with c and d positive. Suppose

$$p = a^2 + 3b^2, \quad p = c^2 + 3d^2.$$

Then, as in formula (D),

$$(H) \qquad p^2 = (ac \pm 3bd)^2 + 3(ad \mp bc)^2 = e^2 + 3f^2.$$

We can arrange, by the same argument as before, that p divides $ad - bc$, although this may require changing the sign of d. But then p divides not only $f = ad - bc$, but also $ac + bd$. This can only be so if $ad = bc$ and $ac + 3bd = p$. Since a, b and c are still positive, d must also be positive. Since $a : c = b : d$ and both a and b and c and d are relatively prime, we conclude from Euclid's Proposition VII.21, or otherwise, that $a = c$, $b = d$.

On the other hand, if we take $a = c$, $b = d$ in (H), we obtain

$$(I) \qquad p^2 = (c^2 - 3d^2)^2 + 3(2cd)^2 = e^2 + 3f^2, \quad e = \pm(c^2 - 3d^2) \quad f = 2cd$$

Since one of c and d must be odd and the other even, and since 3 does not divide c, $e = 2cd$ and $f = \pm(c^2 - 3d^2)$ are relatively prime. Choosing the sign correctly, we arrange that both e and f are positive.

Conversely, if

$$(J) \qquad p^2 = e^2 + 3f^2,$$

then

$$p^3 = (ce \pm 3df)^2 + 3(cf \mp de)^2 = a^2 + 3b^2, \quad a = ce \pm 3df, \quad b = cf \mp de$$

Once again, one choice of sign leads to p dividing b and therefore also a and the second leads to a representation of p^3 by relatively prime a and b.

Choose, however, the sign for which p divides $cf \mp de$ and therefore also $ce \pm 3df$. Then we obtain

$$p = \left(\frac{ce \pm 3df}{p}\right)^2 + 3\left(\frac{cf \mp de}{p}\right)^2.$$

Since there is only one representation of p, we conclude that

$$(K) \qquad ce \pm 3df = \pm pc, \quad \pm cf - de = \pm pd,$$

where the signs on the right are, at first, independent of each other and of those on the left. On the left, they are the same.

Set $f' = \pm f$, so that (K) becomes

$$(L) \qquad ce + 3df' = \pm pc, \quad cf' - de = \pm pd.$$

Multiply the first of these equations by d and the second by c and add to obtain

$$pf' = 3d^2 f' + c^2 f' = \pm pdc \pm pcd.$$

Since $f' \neq 0$, the two signs on the right must be the same and $f' = \pm 2cd$. Multiplying the equations (L) by c and $3d$ and subtracting, we obtain

$$pe = c^2 e + 3d^2 e = \pm pc^2 \mp 3pd^2 = \pm p(c^2 - 3d^2),$$

as the signs on the right are the same. Thus the possible new solutions (J) are in fact the same as those deduced from (I).

At this point we have found that there is at least one proper, positive representation of p^m for $m = 1, 2, 3$ and exactly one if $m = 1, 2$. The argument, however, clearly allows us to pass to higher and higher powers of m and to establish this in general.

At last

Recall what we needed to establish to complete Euler's argument. We had a number

$$M = c^2 + 3d^2$$

although we were then following Euler, using p or q for c and q or r for d. This number was a cube $M = N^3$ and c and d were relatively prime. We needed to write

$$(M) \qquad c = t(t^2 - 9u^2), \quad d = 3u(t^2 - u^2).$$

The signs are not important here, changing the sign of t changes that of u and changing the sign of u changes that of d.

Suppose that $M = p^{3m}$ and $N = p^m$. If

$$N = t^2 + 3u^2$$

then, as we have seen, we can construct a representation of N^2 as

$$N^2 = (t^2 - 3u^2) + 3(2tu),$$

and this representation, apart from the determination of sign, is unique.

We construct a representation of N^3 as

$$N^3 = (t(t^2 - 3u^2) \pm 6tu^2)^2 + 3(t(2tu) \mp u(t^2 - 3u^2))^2,$$

The second coefficient here is

$$2t^2u \mp (t^2u - 3u^3) = \begin{cases} u(t^2 + 3u^2) = pu \\ 3t^2u - 3u^3, \end{cases}$$

so that only the +-sign is permissible, and that yields

$$N^3 = (t(t^2 - 3u^2))^2 + 3(3u(t^2 - u^2))^2.$$

Since the positive proper representation of N^3 is unique, this is it and (M) is established.

To complete the argument, we proceed as usual, passing from smaller to larger N. Thus suppose $N = N_1N_2$, with N_1 and N_2 relatively prime. Then we have seen that any proper representation

$$N^3 = c^2 + 3d^2$$

is given, apart from signs, as

$$(c_1c_2 \pm 3d_1d_2)^2 + 3(c_1d_2 \mp d_1c_2)^2,$$

where $N_1 = c_1^2 + 3d_1^2$ and $N_2 = c_2^2 + 3d_2^2$ are proper representations of N_1 and N_2. Moreover the four possible choices of sign for c_1 and d_1 and the four for c_2 and d_2 yields exactly eight choides for c and d, as a simultaneous change of the signs of c_1, d_1, c_2 and d_2 has no effect on c and d. These eight results come as two sets of four, the values of c and d in one set being obtained by making all possible sign changes.

If

$$c_1 = t_1(t_1^2 - 9u_1^2), \quad d_1 = 3u_1(t_1^2 - u_1^2)$$

and

$$c_2 = t_2(t_2^2 - 9u_2^2), \quad d_2 = 3u_2(t_2^2 - u_2^2),$$

consider

$$t = t_1t_2 \pm 3u_1u_2, \quad u = t_1u_2 \mp t_2u_1$$

Then $c_1c_2 \pm 3d_1d_2$ is equal to

$$t_1t_2(t_1^2 - 9u_1^2)(t_2^2 - 9u_2^2) \pm 27u_1u_2(t_1^2 - u_1^2)(t_2^2 - u_2^2) =$$
$$t_1t_2(t_1^2t_2^2 - 9t_1^2u_2^2 - 9t_2^2u_1^2 + 81u_1^2u_2^2) \pm 27u_1u_2(t_1^2t_2^2 - t_1^2u_2^2 - u_1^2t_2^2 + u_1^2u_2^2),$$

from which we remove the two terms $t_1^3t_2^3$ and $\pm 27u_1^3u_2^3$ to obtain

$$(N) \qquad t_1t_2(-9t_1^2u_2^2 - 9t_2^2u_1^2 + 81u_1^2u_2^2) \pm 27u_1u_2(t_1^2t_2^2 - t_1^2u_2^2 - u_1^2t_2^2).$$

On the other hand, $t^3 - 9tu^2$ is equal to

$$t_1^3t_2^3 \pm 9t_1^2t_2^2u_1u_2 + 27t_1t_2u_1^2u_2^2 \pm 27u_1^3u_2^3 - 9(t_1t_2 \pm 3u_1u_2)(t_1u_2 \mp t_2u_1)^2$$

from which we remove the same two terms to obtain

$$\pm 9t_1^2t_2^2u_1u_2 + 27t_1t_2u_1^2u_2^2 - 9(t_1t_2 \pm 3u_1u_2)(t_1u_2 \mp t_2u_1)^2 =$$
$$\pm 9t_1^2t_2^2u_1u_2 + 27t_1t_2u_1^2u_2^2 - 9(t_1t_2 \pm 3u_1u_2)(t_1^2u_2^2 \mp 2t_1t_2u_1u_2 + t_2^2u_1^2).$$

This we separate into the terms with the arbitrary and those with no sign. The first are

$$\pm(27t_1^2t_2^2u_1u_2 - 27(t_162u_1u_3 - t_262u_1^3u_2),$$

while the second are

$$27t_1t_2u_162u_2^2 - 9t_1^3t_2u_162 - 9t_1t_2^3u_1^2 + 81t_1t_2u_1^2u_2^2.$$

They are the same as the terms in (N). We conclude that

$$c = c_1c_2 \pm 3d_1d_2 = t(t^2 - 9u^2),$$

and this is one-half of what we want to show.

For the second half we calculate $c_1d_1 \mp d_1c_2$ and $3u(t^2 - u^2)$. The first is

$$(O) \qquad 3t_1u_2(t_1^2 - 9u_1^2)(t_2^2 - u_2^2) \mp 3t_2u_1(t_2^2 - 9u_2^2)(t_1^2 - u_1^2);$$

and the second

$$(P) \qquad 3(t_1u_2 \mp t_2u_1)((t_1t_2 \pm 3u_1u_2)^2 - (t_1u_2 \mp t_2u_1)^2).$$

With the wisdom of experience, we separate in both (O) and (P), the terms without an arbitrary sign from those with. Moreover, we discard the 3 that is common to all terms in both these expressions.

This is easy for (O) and leads to

$$t_1u_2(t_1^2t_2^2 - t_1^2u_2^2 - 9u_1^2t_2^2 + 9u_1^2u_2^2)$$

and to

$$t_2u_1(t_2^2t_1^2 - t_2^2u_1^2 - 9u_2^2t_1^2 + 9u_2^2u_1^2),$$

the second expression being obtained from the first by interchanging the indices 1 and 2.

For (P), there is more to sort out. The terms without the sign yield

$$t_1u_2(t_1^2t_2^2 + 9u_1^2u_2^2 - t_1^2u_2^2 - t_2^2u_1^2) - t_2u_1(6t_1t_2u_1u_2 + 2t_1u_2t_2u_1).$$

On collecting terms and rearranging, this becomes

$$t_1u_2(t_1^2t_2^2 + 9u_1^2u_2^2 - t_1^2u_2^2 - 9t_2^2u_1^2)$$

The terms with sign yield

$$t_1u_2(6t_1t_2u_1u_2 + 2t_1u_2t_2u_1) + -t_2u_1(t_1^2t_2^2 + 9u_1^2u_2^2 - t_1^2u_2^2 - t_2^2u_1^2),$$

or

$$-t_2u_1(-8t_1^2u_2^2 + t_1^2t_2^2 + 9u_1^2u_2^2 - t_1^2u_2^2 - t_2^2u_1^2),$$

which is

$$-t_2u_1(t_1^2t_2^2 + 9u_1^2u_2^2 - 9t_1^2u_2^2 - t_2^2u_1^2)$$

We conclude that

$$d = -3u(t^2 - u^2)$$

Since we are free to change the sign of u, this is sufficient for our purposes

TWO LIVES

Ernst Eduard Kummer (1810-1893)

Evariste Galois (1811-1832)


Galvez 1848 A.G.

E. E. Kummer

Galois theory

Suppose we have an equation with rational coefficients

$$(A) \qquad Z^n + a_1 Z^{n-1} + a_2 Z^{n-2} + \dots a_{n-2} Z^2 + a_{n-1} Z^1 + a_n = 0$$

and that no factorization of

$$Z^n + a_1 Z^{n-1} + a_2 Z^{n-2} + \dots a_{n-2} Z^2 + a_{n-1} Z^1 + a_n$$

as

$$(Z^k + b_1 Z^{k-1} + \cdots + b_{k-1} Z^1 + b_k)(Z^l + c_1 Z^{l-1} + \cdots + c_{l-1} Z^1 + a_l),$$

with all the b_i and c_j also rational is possible. If such a factorization exists, then necessarily $k + l = n$.

The equation (A) will have n roots,

$$z_1, z_2, \dots, z_n$$

Notice that if we have an expression

$$z_1^{m_1} z_2^{m_2} \dots z_n^{m_n}$$

and if one of the m_i is larger than $n - 1$, then we can use the relation

$$z_i^{m_i} = z_i^{m_i - n} z_i^n = -z_i^{m_i - n}(a_1 z_i^{n-1} + a_2 z_i^{n-2} + \dots)$$

to replace it by a combination of terms that involve no power of z_i greater than $m_i - 1$. Thus all the numbers that can be obtained from $z_1, z_2, \dots, z_n$ by multiplying them together, multiplying the results by fractions, and adding the results together can be expressed by a finite number of them.

An example well known to us is the equation

$$Z^n + Z^{n-1} + Z^{n-2} + \dots Z^2 + Z^1 + 1 = 0,$$

in which n is a prime. Its roots are

$$z_j = \cos(2\pi j/n) + i \sin(2\pi j/n), \quad i = \sqrt{-1}, \quad j = 1, \dots, n-1.$$

Since $z_j z_k = z_l$ if $l - j - k$ is divisible by n, the numbers obtained in the above way can all be expressed as

$$a_1 z_1 + a_2 z_2 + \cdots + a_{n-1} z_{n-1}.$$

In general, it is not possible to predict in advance the size of a collection of expressions $\{w_1, \ldots, w_N\}$ of this form such that any other can be expressed as

$$a_1 w_1 + a_2 w_2 + a_3 w_3 + \cdots + a_N w_N$$

The smallest possible size N is extremely important in Galois theory, because it is exactly the number of symmetries provided we include the trivial one. This is the basic theorem of the theory, a theory that sprung fully armed from the head of Galois.

Consider again our example. The number N is $n - 1$. The symmetries were

$$z_1 \to z_1^k = z_k, \quad k = 1, 2, \ldots, n-1.$$

This symmetry took $z_l = z_1^l$ to $(z_1^k)^l = z_1^{kl} = z_m$ if $m - kl$ is divisible by n. There are certainly N symmetries and we saw that there were no more, because z_1 has to go to a number with the same properties, thus to another root of

$$Z^{n-1} + Z^{n-2} + \cdots + Z + 1 = 0.$$

Thus in this case, we are familiar with the main theorem of Galois theory.

In general any two of the N symmetries can be multiplied together

$$\begin{aligned} \rho : z_i \to \rho(z_i) = z_j, \\ \sigma : z_j \to \sigma(z_j) = z_k, \\ \tau = \sigma \circ \rho : z_i \to \tau(z_i) = z_k. \end{aligned}$$

It is by no means always the case that $\sigma \circ \rho = \rho \circ \sigma$. One important symmetry is the one for which every root is its own reflection. We denote it ι. Associated to any symmetry ρ there is a reverse symmetry $\sigma = \rho^{-1}$.

$$\begin{aligned} \rho : z_i \to z_j, \\ \sigma : z_j \to z_i, \\ \sigma \circ \rho : z_i \to z_i. \end{aligned}$$

This is usually expressed by saying that the symmetries form a group.

There are two other assertions of the Galois theory that it is worth mentioning. First of all, the only numbers with maximal symmetry, thus which remain unchanged no matter which symmetry is applied are the rational numbers, which form the *field* of reference. If the field of reference is changed, thus if for example the coefficients of the polynomials in question are arbitrary numbers of the form $a + b\alpha$, with a and b rational, then the symmetries are then symmetries that preserve all relations with coefficients from this field. The field is larger; therefore there are more constraints and fewer symmetries. The valid statements of the theory remain the same, but it has to be understand that in each of them there are more coefficients and fewer symmetries allowed!

Not knowing quite what to say about a single number, since a number has in itself almost no properties, all its properties being defined by its relations to other numbers, mathematicians attach a great deal of importance to the group of symmetries, calling it the Galois group. If you look carefully at various advanced theories, you will see that they all treat the group and that the roots themselves are largely – but not entirely –neglected. We shall return to some simple applications of the notion, but first we turn to Galois himself.