Fun Facts About 59

Stephen Villee

September 1, 2018

Number theory has always fascinated me, since long before I started writing software or thinking about small government. From an early age, I studied the integers as a hobby. I learned that each natural number has its own unique properties. 6 is the first perfect number. 7 is the first odd prime for which 2 is not a primitive root.

As it happens, 59 is an especially interesting prime number. Below are some of the ways that 59 stands out.

1 Sums of Three Squares

Among primes that are 3 more than a multiple of 8, 59 is the first that can be expressed as a sum of three squares of positive integers in more than 3 ways.

Every prime p where $p \equiv 3 \pmod 8$ is a sum of three squares of positive integers. Including permutations, there are at least three such representations, except for the special case of 3 itself where there's only one.

$$3 = 1^2 + 1^2 + 1^2$$

$$\begin{aligned} 11 &= 1^2 + 1^2 + 3^2 \\ &= 3^2 + 1^2 + 1^2 \\ &= 1^2 + 3^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 19 &= 3^2 + 3^2 + 1^2 \\ &= 1^2 + 3^2 + 3^2 \\ &= 3^2 + 1^2 + 3^2 \end{aligned}$$

$$\begin{aligned} 43 &= 3^2 + 3^2 + 5^2 \\ &= 5^2 + 3^2 + 3^2 \\ &= 3^2 + 5^2 + 3^2 \end{aligned}$$

That's the complete list for 3, 11, 19 and 43. But 59 can go further. We can imagine 59 saying "hold my beer" and then showing what he's got:

$$\begin{aligned}
59 &= 5^2 + 5^2 + 3^2 \\
&= 3^2 + 5^2 + 5^2 \\
&= 5^2 + 3^2 + 5^2 \\
&= 7^2 + 1^2 + 3^2 \\
&= 3^2 + 7^2 + 1^2 \\
&= 1^2 + 3^2 + 7^2 \\
&= 1^2 + 7^2 + 3^2 \\
&= 3^2 + 1^2 + 7^2 \\
&= 7^2 + 3^2 + 1^2
\end{aligned}$$

That's a total of 9 representations, 3 times as many as 43 has.

You might think the number of ways to represent p as the sum of three squares would be fairly random, but actually for $p > 3$ it's equal to 3 times the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. More on that later. But first let's look at another intriguing characteristic of 59.

2 Fermat's Last Theorem as a Congruence

Among primes p where $p \equiv 2 \pmod 3$, 59 is the first where there are integers x, y and z satisfying

$$x^p + y^p \equiv z^p \pmod{p^2}$$

with p not dividing x, y or z.

In 1637, Pierre de Fermat first stated his famous Last Theorem: $x^n + y^n = z^n$ has no solutions in positive integers with $n > 2$. He claimed to have found a marvelous proof which wouldn't fit in the narrow margin where he was writing. The problem remained unsolved until 1995 when Andrew Wiles finally published a proof after years of effort, building on the work of many other mathematicians.

Fermat did give a proof for the exponent $n = 4$, so what remained was to prove that

$$x^p + y^p = z^p$$

has no solutions in positive integers for odd prime p. We can assume that x, y and z have no common divisor, since any such divisor could be divided out.

One of the first mathematicians to investigate Fermat's Last Theorem was Sophie Germain. She made significant headway on what is known as Case I, where p does not divide x, y or z. She proved Case I for all odd primes $p < 100$.

For now, let's take a different tack, and ask whether Case I even has any solutions as a congruence. We're going to look for a positive integer k where

$$x^p + y^p \equiv z^p \pmod{p^k}$$

has no solutions with p not dividing x, y or z. For $k = 1$, there is always a solution, but once we step up to $k = 2$, things get interesting. Let's start with $p = 3$.

$$\begin{aligned}
1^3 = 1 &\equiv 1 &\pmod{3^2}\\
2^3 = 8 &\equiv 8 &\pmod{3^2}\\
4^3 = 64 &\equiv 1 &\pmod{3^2}\\
5^3 = 125 &\equiv 8 &\pmod{3^2}\\
7^3 = 343 &\equiv 1 &\pmod{3^2}\\
8^3 = 512 &\equiv 8 &\pmod{3^2}
\end{aligned}$$

Evidently we could have stopped at 2^3, because the pattern repeats after that. In general, when $a \equiv b \pmod{p}$, we have $a^p \equiv b^p \pmod{p^2}$. In view of Fermat's little theorem, we must have $z \equiv x + y \pmod{p}$. Further, we can assume that $x = 1$, since x is invertible modulo p and we can divide it out. So the congruence to be satisfied is

$$1 + y^p \equiv (y + 1)^p \pmod{p^2}$$

It's enough to consider values of y between 1 and $p - 2$. If none of these satisfy the above congruence, then Case I is proved for that exponent p. When $p = 3$, the only candidate for y is 1, which doesn't work, so that proves Case I for the exponent 3.

When $p \equiv 1 \pmod{3}$, there are always at least 2 solutions. These are the y values of order 3, that is, where $y^3 \equiv 1 \pmod{p}$. There are 2 such y values, and each is the square of the other modulo p. The example of $p = 7$ will be instructive.

$$\begin{aligned}
1^7 = 1 &\equiv 1 &\pmod{7^2}\\
2^7 = 128 &\equiv 30 &\pmod{7^2}\\
3^7 = 2187 &\equiv 31 &\pmod{7^2}\\
4^7 = 16384 &\equiv 18 &\pmod{7^2}\\
5^7 = 78125 &\equiv 19 &\pmod{7^2}\\
6^7 = 279936 &\equiv 48 &\pmod{7^2}
\end{aligned}$$

So y can be either 2 or 4, leading to these solutions:

$$\begin{aligned}
1 + 2^7 \equiv 1 + 30 &= 31 &\equiv 3^7 &\pmod{7^2}\\
1 + 4^7 \equiv 1 + 18 &= 19 &\equiv 5^7 &\pmod{7^2}
\end{aligned}$$

The exponents 7, 13, 19, 31, 37 and 43 each have only the 2 solutions where $y^3 \equiv 1 \pmod{p}$. In general for $p \equiv 1 \pmod{3}$, if there are any other solutions, they will come in bunches of 6, as we'll see later.

What if we try increasing k, to find a proof of Case I for exponents like 7? Alas, when there is a solution modulo p^2, it can always be adjusted to become a solution modulo p^3 or any higher power. For those familiar with p-adic numbers, if our congruence with $k = 2$ has a solution, then the original Fermat equation has a p-adic solution with x, y and z all having "absolute value" 1.

When $p \equiv 2 \pmod{3}$, solutions seem to be rare. There are no solutions when p is 5, 11, 17, 23, 29, 41, 47 or 53. So Case I is proved for these exponents. We can envision 59 looking at all those lower primes with barely hidden contempt, saying "hold my Perrier" and then showing how it's done:

$$\begin{aligned}
1 + 3^{59} &\equiv 1 + 298 &&= 299 &&\equiv 4^{59} &&\pmod{59^2} \\
1 + 55^{59} &\equiv 1 + 3182 &&= 3183 &&\equiv 56^{59} &&\pmod{59^2} \\
1 + 38^{59} &\equiv 1 + 805 &&= 806 &&\equiv 39^{59} &&\pmod{59^2} \\
1 + 20^{59} &\equiv 1 + 2675 &&= 2676 &&\equiv 21^{59} &&\pmod{59^2} \\
1 + 44^{59} &\equiv 1 + 1106 &&= 1107 &&\equiv 45^{59} &&\pmod{59^2} \\
1 + 14^{59} &\equiv 1 + 2374 &&= 2375 &&\equiv 15^{59} &&\pmod{59^2}
\end{aligned}$$

$$\begin{aligned}
1 + 4^{59} &\equiv 1 + 299 &&= 300 &&\equiv 5^{59} &&\pmod{59^2} \\
1 + 54^{59} &\equiv 1 + 3181 &&= 3182 &&\equiv 55^{59} &&\pmod{59^2} \\
1 + 43^{59} &\equiv 1 + 1105 &&= 1106 &&\equiv 44^{59} &&\pmod{59^2} \\
1 + 15^{59} &\equiv 1 + 2375 &&= 2376 &&\equiv 16^{59} &&\pmod{59^2} \\
1 + 47^{59} &\equiv 1 + 1404 &&= 1405 &&\equiv 48^{59} &&\pmod{59^2} \\
1 + 11^{59} &\equiv 1 + 2076 &&= 2077 &&\equiv 12^{59} &&\pmod{59^2}
\end{aligned}$$

Not just 1, but 2 bunches of solutions. Generally, solutions come in bunches of 6, because when you find one where y is not of order 3, the following pattern will generate 5 others (where division is modulo p):

$$\begin{aligned}
1 + y^p &\equiv (y+1)^p &&\pmod{p^2} \\
1 + (-y-1)^p &\equiv (-y)^p &&\pmod{p^2} \\
1 + ((-y-1)/y)^p &\equiv (-1/y)^p &&\pmod{p^2} \\
1 + (1/y)^p &\equiv ((y+1)/y)^p &&\pmod{p^2} \\
1 + (1/(-y-1))^p &\equiv (y/(y+1))^p &&\pmod{p^2} \\
1 + (y/(-y-1))^p &\equiv (1/(y+1))^p &&\pmod{p^2}
\end{aligned}$$

3 Bernoulli Numbers

59 is one of only 3 irregular primes less than 100. The other two are 37 and 67. A prime p is irregular if it divides the numerator of at least one Bernoulli number B_k with even $k <= p-3$. Ernst Kummer proved Fermat's Last Theorem for regular prime exponents.

Jakob Bernoulli discovered the numbers which bear his name as part of generalizing this formula for the sum of the first n positive integers:

$$1+2+3+...+n = n(n+1)/2$$

The generalized formulas look like this in modern notation:

$$\begin{aligned}
1+2+3+...+n &= (B_0 n^2 - 2B_1 n)/2 \\
1^2+2^2+3^2+...+n^2 &= (B_0 n^3 - 3B_1 n^2 + 3B_2 n)/3 \\
1^3+2^3+3^3+...+n^3 &= (B_0 n^4 - 4B_1 n^3 + 6B_2 n^2)/4 \\
1^4+2^4+3^4+...+n^4 &= (B_0 n^5 - 5B_1 n^4 + 10B_2 n^3 + 5B_4 n)/5 \\
1^5+2^5+3^5+...+n^5 &= (B_0 n^6 - 6B_1 n^5 + 15B_2 n^4 + 15B_4 n^2)/6 \\
1^6+2^6+3^6+...+n^6 &= (B_0 n^7 - 7B_1 n^6 + 21B_2 n^5 + 35B_4 n^3 + 7B_6 n)/7 \\
1^7+2^7+3^7+...+n^7 &= (B_0 n^8 - 8B_1 n^7 + 28B_2 n^6 + 70B_4 n^4 + 28B_6 n^2)/8
\end{aligned}$$

and so on, where

$$\begin{aligned}
B_0 &= 1 \\
B_1 &= -1/2 \\
B_2 &= 1/6 \\
B_3 &= 0 \\
B_4 &= -1/30 \\
B_5 &= 0 \\
B_6 &= 1/42
\end{aligned}$$

and so forth are the Bernoulli numbers, and the coefficient of $B_i n^j$ is $\binom{i+j}{i}$, the binomial coefficient of $i+j$ and i.

In this case, 59 is irregular because it divides the numerator of B_{44}, given below.

$$B_{44} = -\frac{2783326957930102423 5023}{690}$$

$$= -\frac{11 \cdot 59 \cdot 8089 \cdot 2947939 \cdot 1798482437}{2 \cdot 3 \cdot 5 \cdot 23}$$

If ζ is a primitve pth root of unity, then p is irregular if and only if it divides the class number of the corresponding cyclotomic field $\mathbb{Q}(\zeta)$. When $p = 59$, the class number of $\mathbb{Q}(\zeta)$ is $41241 = 3 \cdot 59 \cdot 233$.

4 Case Study of a Number Field

A number field is obtained by starting with the rational numbers $\mathbb{Q}$ and adjoining one or more roots of a polynomial with rational coefficients. The resulting field is an extension of $\mathbb{Q}$ having some finite degree n. Its ring of integers is a free module of the same rank n over the ordinary integers $\mathbb{Z}$. This ring of integers does not necessarily have unique factorization, but its ideals do. If the number field is a Galois extension of $\mathbb{Q}$ (which it will be if we adjoin all the roots of the polynomial), then the way prime ideals of $\mathbb{Z}$ factor into prime ideals of the extension is quite fascinating and beautiful.

We're now going to do a case study of a number field, specifically $\mathbb{Q}(\sqrt{-59})$ $= \mathbb{Q}(i\sqrt{59})$. That is, we'll start with $\mathbb{Q}$ and adjoin a root of the polynomial $x^2 + 59$. This is a good example of the case where the ring of integers does not have unique factorization, so we need to look at ideals. Because this is an imaginary quadratic field, each ideal is a lattice in the complex plane, so it's easy to visualize.

Our first guess as to the ring of integers might be $\mathbb{Z}[i\sqrt{59}]$, but it turns out this would omit half the algebraic integers. If we set

$$\begin{aligned}\theta &= \frac{-1 + i\sqrt{59}}{2} \\ &\approx -0.5 + 3.84057i\end{aligned}$$

then θ is an algebraic integer, because $\theta^2 + \theta + 15 = 0$. In fact, $\mathbb{Z}[\theta]$ is the ring of integers for this number field. Let's go ahead and define K and R as our number field and its ring of integers, respectively.

$$\begin{aligned}K &= \mathbb{Q}(i\sqrt{59}) = \mathbb{Q}(\theta) \\ R &= \mathbb{Z}[\theta]\end{aligned}$$

To see that R does not have unique factorization, observe that

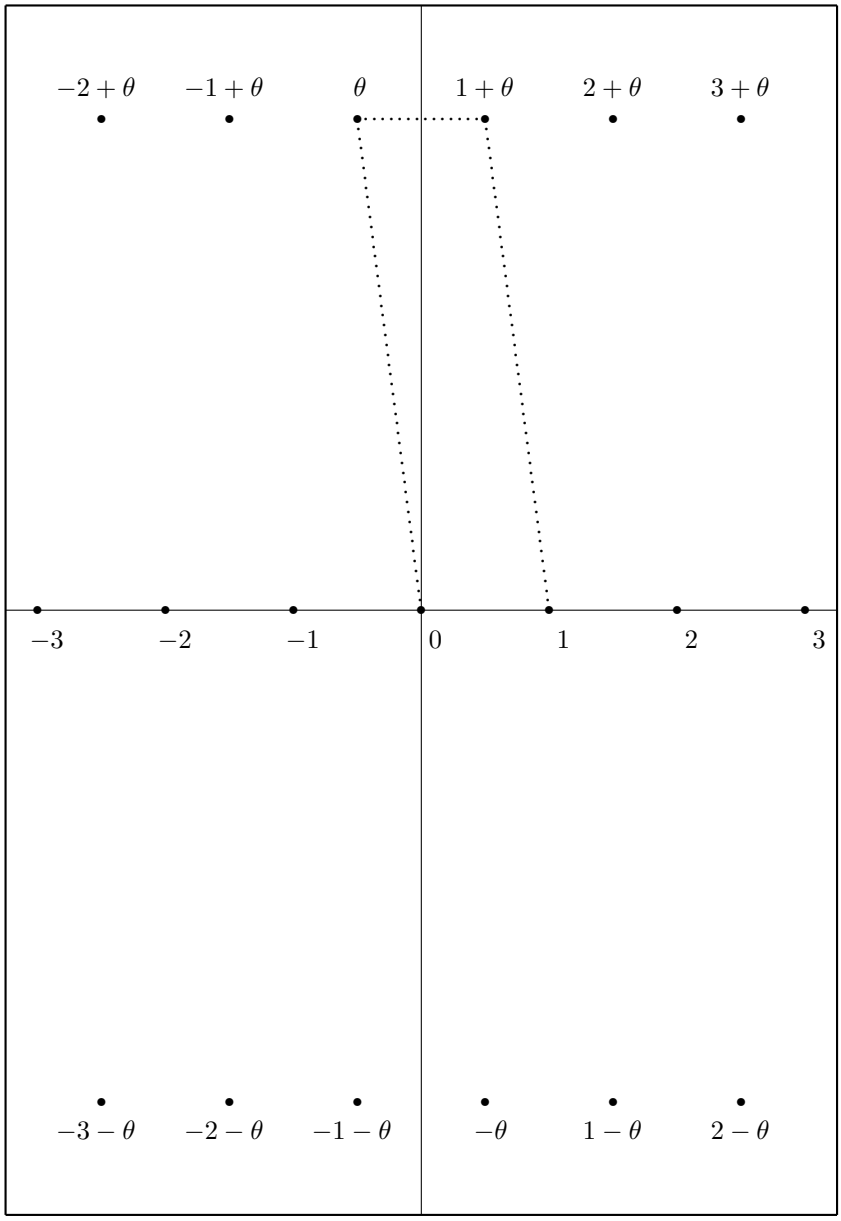
$$\begin{aligned}15 &= 3 \cdot 5 \\ &= \theta(-1 - \theta)\end{aligned}$$

where 3, 5, θ and $(-1 - \theta)$ are all irreducible elements of R.

You could say that 3 and θ "ought" to have a greatest common divisor, and that ideals were concocted to represent phantom greatest common divisors like this. Actually, an ideal of a ring is a subset of the ring that's closed under addition and also closed under multiplication by any element of the ring. A principal ideal is an ideal consisting of the multiples of some particular element. In the ordinary integers $\mathbb{Z}$, every ideal is principal. For example, $[3] = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$.

In our ring R, not every ideal is principal. For example, the ideal $[3, \theta]$ is the set of all elements you get by adding a multiple of 3 and a multiple of θ. If 3 and θ had a greatest common divisor, this ideal would consist of all the multiples of that divisor.

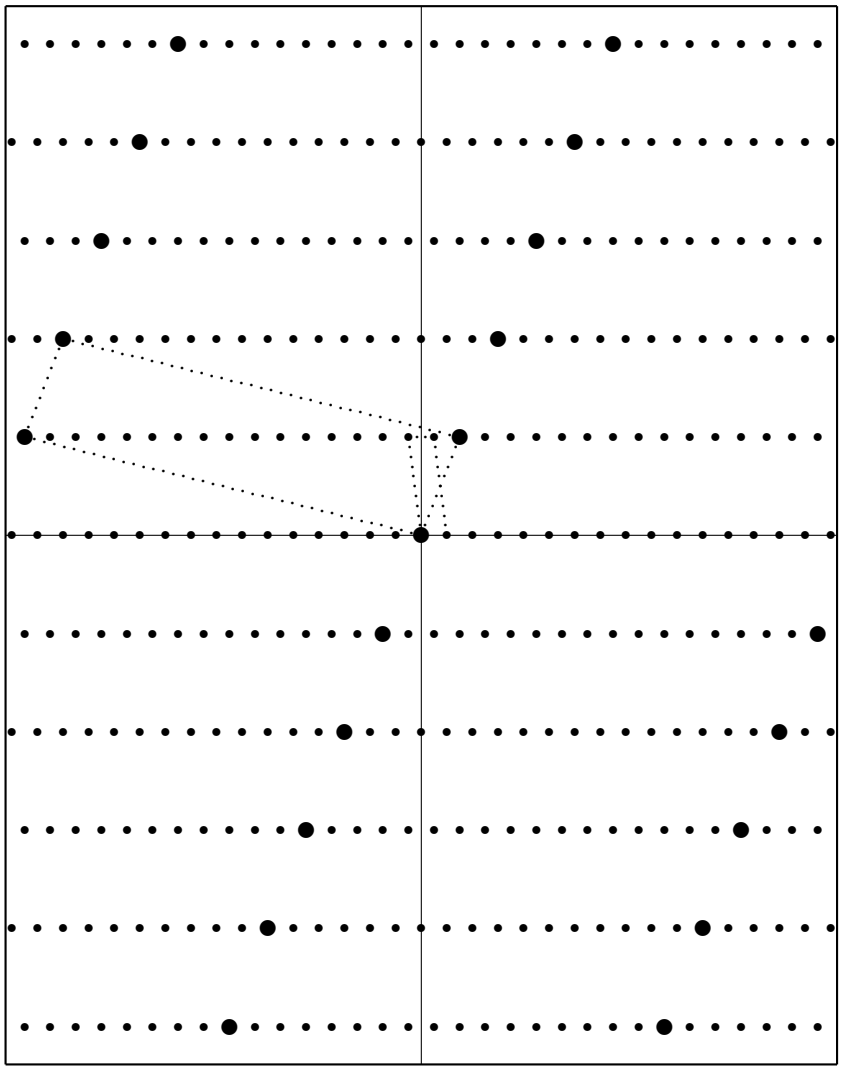
Let's see what R looks like as a lattice in the complex plane, zoomed in so we can label some points. A dotted-line parallelogram marks a fundamental domain.



Make a note of this matrix equation for later:

$$\theta \begin{bmatrix} 1 \\ \theta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -15 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ \theta \end{bmatrix}$$

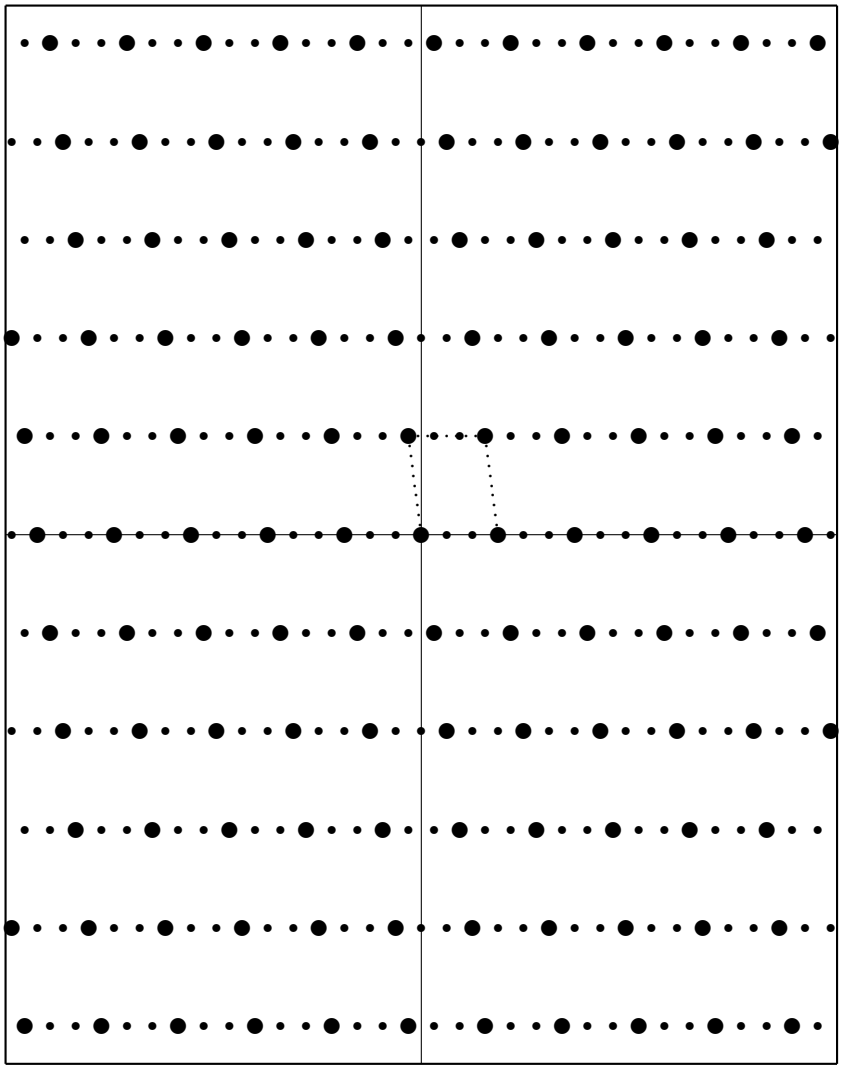
Now let's look at the principal ideal $[2+\theta]$. Here we've zoomed out quite a bit, so the original parallelogram appears much smaller. Large dots represent points of $[2+\theta]$, while small dots represent other points of R. Another parallelogram appears, marking a fundamental domain of $[2+\theta]$. If you look carefully, you can see that this parallelogram, and indeed the entire lattice, is just a copy of the one for R, but scaled and rotated. The new parallelogram has 17 times the area of the original one, but it has the same shape.



Here is the analogous matrix equation for the basis we've chosen for $[2+\theta]$:

$$\theta \begin{bmatrix} 2+\theta \\ -15+\theta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -15 & -1 \end{bmatrix} \begin{bmatrix} 2+\theta \\ -15+\theta \end{bmatrix}$$

Next we'll look at $[3, \theta]$, which is not principal. Again, large dots are points of $[3, \theta]$, and small dots are other points of R. Here, the parallelogram has 3 times the area of the one for R, but it has a different shape.



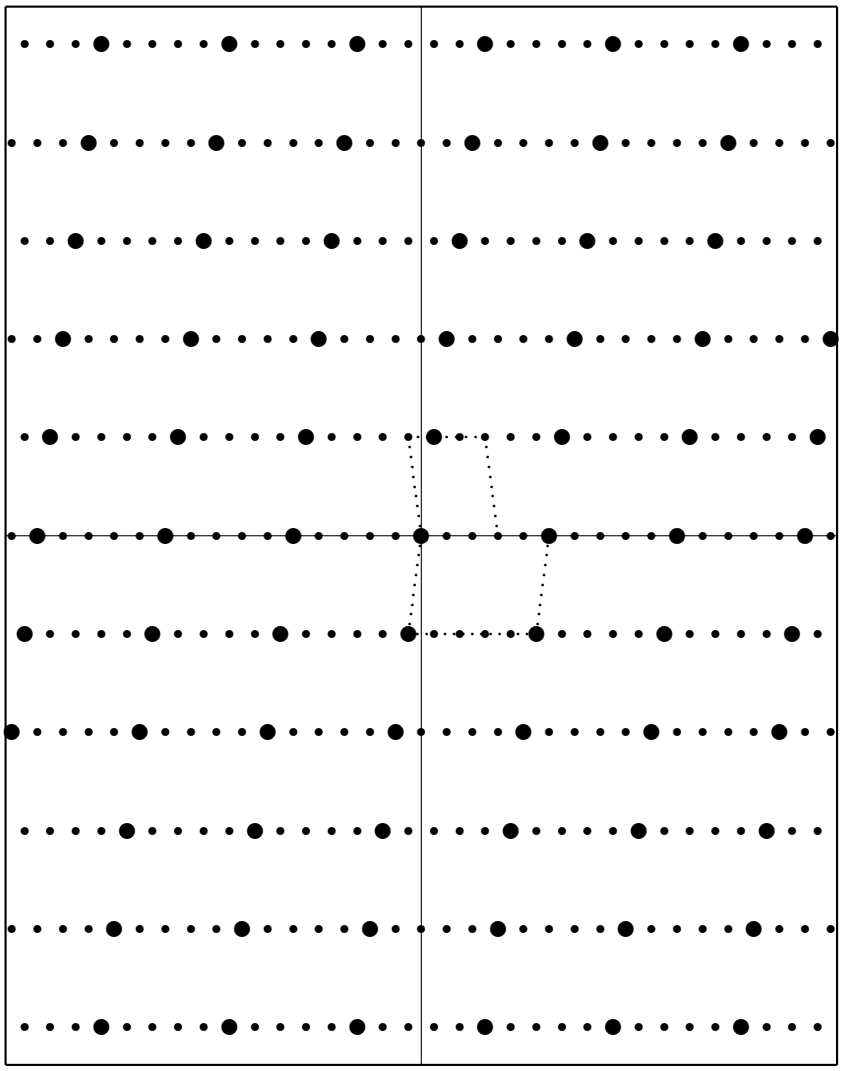
Here is the matrix equation corresponding to this basis for $[3, \theta]$:

$$\theta \begin{bmatrix} 3 \\ \theta \end{bmatrix} = \begin{bmatrix} 0 & 3 \\ -5 & -1 \end{bmatrix} \begin{bmatrix} 3 \\ \theta \end{bmatrix}$$

Each of these matrix equations shows the effect of multiplying the basis by θ. We can also say that the basis is an eigenvector of the matrix, with θ as the eigenvalue. We'll see the significance of these matrices later.

The ideal $[5, -1 - \theta]$ is also not principal. In fact, it's in the same class as $[3, \theta]$ because $[\theta][5, -1 - \theta] = [5][3, \theta]$. Generally, two ideals I and J are in the same class if there are principal ideals $[\eta_1]$ and $[\eta_2]$ such that $[\eta_1]I = [\eta_2]J$. What this means in the case of ideals of R is that one ideal's lattice is just a "scale and rotate" of the other's.

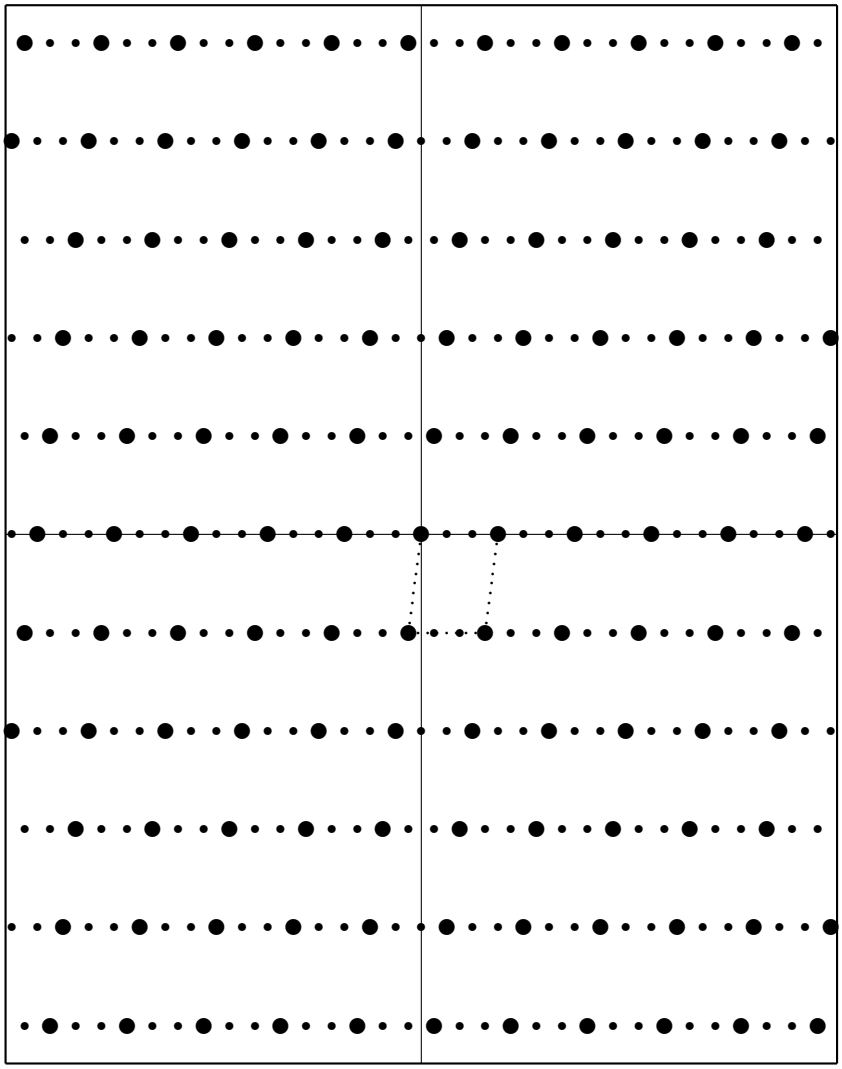
In the diagram below, the parallelogram for $[5, -1 - \theta]$ has the same shape as the one for $[3, \theta]$. It's just been scaled a bit larger, and rotated clockwise.



And here is the matrix equation corresponding to this basis for $[5, -1 - \theta]$:

$$\theta \begin{bmatrix} -1-\theta \\ 5 \end{bmatrix} = \begin{bmatrix} 0 & 3 \\ -5 & -1 \end{bmatrix} \begin{bmatrix} -1-\theta \\ 5 \end{bmatrix}$$

The ideal $[3, -1-\theta]$, shown below, belongs to the third and final class of ideals in R. You can see that it's the complex conjugate of $[3, \theta]$.



Here is the matrix equation to go with this basis for $[3, -1-\theta]$:

$$\theta \begin{bmatrix} -1-\theta \\ 3 \end{bmatrix} = \begin{bmatrix} 0 & 5 \\ -3 & -1 \end{bmatrix} \begin{bmatrix} -1-\theta \\ 3 \end{bmatrix}$$

So there are 3 classes of ideals in R, and they form a group. Since the order of the group is 3, the cube of any ideal in R is principal. For example, $[3,\theta]^3 = [3-\theta]$.

The field K has exactly two automorphisms: complex conjugation which takes θ to $-1-\theta$ and vice versa, and the identity map. These two automorphisms form a group known as the Galois group of the extension.

The norm of an element $u+v\theta$ in K (where u and v are rational numbers), denoted $\mathrm{N}(u+v\theta)$, is the product of $u+v\theta$ with its conjugate $u-v-v\theta$. The result is $u^2-uv+15v^2$, which is rational. When restricted to R (where u and v are ordinary integers), the norm is an ordinary integer. For example, $\mathrm{N}(2+\theta) = (2+\theta)(1-\theta) = 17$. When we're looking to factor the ideal $[p]$ for some prime p in $\mathbb{Z}$, we would first look for an element of R whose norm is p. If we find one, then $[p]$ splits into two principal ideals. Otherwise, we would look for an element whose norm is a multiple of p. For example, when looking to factor $[7]$, we would observe that $\mathrm{N}(2-\theta) = (2-\theta)(3+\theta) = 21 = 3\cdot 7$. Thus we would have $[7] = [7,2-\theta][7,3+\theta]$.

Below is a table showing primes of $\mathbb{Z}$ up through 59, and how their corresponding ideals factor in R. When the prime is a quadratic residue modulo 59, its ideal splits into two prime ideals in R. In this case, the second column shows the quadratic residue. When the two ideals are not principal, the one on the left is in the same class as $[3,\theta]$, and the third column shows why. If the prime is not a quadratic residue modulo 59, then its ideal stays inert, meaning it is still a prime ideal in R. 59 itself does something special: its ideal ramifies as the square of a prime ideal in R.

$[2]$ stays inert		
$[3] = [3,\theta][3,-1-\theta]$	$3 \equiv 11^2$	$[3,\theta] = [3,\theta]$
$[5] = [5,-1-\theta][5,\theta]$	$5 \equiv 8^2$	$[\theta][5,-1-\theta] = [5][3,\theta]$
$[7] = [7,2-\theta][7,3+\theta]$	$7 \equiv 19^2$	$[3+\theta][7,2-\theta] = [7][3,\theta]$
$[11]$ stays inert		
$[13]$ stays inert		
$[17] = [2+\theta][1-\theta]$	$17 \equiv 28^2$	
$[19] = [19,7+\theta][19,6-\theta]$	$19 \equiv 14^2$	$[6-\theta][19,7+\theta] = [19][3,\theta]$
$[23]$ stays inert		
$[29] = [29,8-\theta][29,9+\theta]$	$29 \equiv 18^2$	$[9+\theta][29,8-\theta] = [29][3,\theta]$
$[31]$ stays inert		
$[37]$ stays inert		
$[41] = [41,7-2\theta][41,9+2\theta]$	$41 \equiv 10^2$	$[9+2\theta][41,7-2\theta] = [41][3,\theta]$
$[43]$ stays inert		
$[47]$ stays inert		
$[53] = [53,11+2\theta][53,9-2\theta]$	$53 \equiv 17^2$	$[9-2\theta][53,11+2\theta] = [53][3,\theta]$
$[59]$ ramifies as $[1+2\theta]^2$		

So how does all this relate to the number of representations of 59 as the sum of three squares? To see the connection, let's take a deeper look at those matrix equations. For any given ideal I, we can choose a basis, i.e., a pair of elements ω_1 and ω_2 such that every element of the ideal has a unique expression as $u\omega_1 + v\omega_2$ for some u and v in $\mathbb{Z}$. In particular, we have

$$\theta\omega_1 = u_1\omega_1 + v_1\omega_2$$
$$\theta\omega_2 = u_2\omega_1 + v_2\omega_2$$

for some u_1, v_1, u_2 and v_2 in $\mathbb{Z}$. We can express this as a matrix equation:

$$\theta \begin{bmatrix}\omega_1 \\ \omega_2\end{bmatrix} = M \begin{bmatrix}\omega_1 \\ \omega_2\end{bmatrix}$$

where

$$M = \begin{bmatrix}u_1 & v_1 \\ u_2 & v_2\end{bmatrix}$$

The matrix M behaves somewhat like θ, in the sense that

$$M^2 + M + \begin{bmatrix}15 & 0 \\ 0 & 15\end{bmatrix} = \begin{bmatrix}0 & 0 \\ 0 & 0\end{bmatrix}$$

which parallels the fact that $\theta^2 + \theta + 15 = 0$. For example, in the case of the principal ideal $[2+\theta]$, recall that we chose the basis $\omega_1 = 2+\theta$ and $\omega_2 = -15+\theta$. Then we had

$$\theta \begin{bmatrix}2+\theta \\ -15+\theta\end{bmatrix} = M \begin{bmatrix}2+\theta \\ -15+\theta\end{bmatrix}$$

where

$$M = \begin{bmatrix}0 & 1 \\ -15 & -1\end{bmatrix}$$

and M behaves like θ because

$$\begin{bmatrix}-15 & -1 \\ 15 & -14\end{bmatrix} + \begin{bmatrix}0 & 1 \\ -15 & -1\end{bmatrix} + \begin{bmatrix}15 & 0 \\ 0 & 15\end{bmatrix} = \begin{bmatrix}0 & 0 \\ 0 & 0\end{bmatrix}$$

It turns out that for every ideal of R, there is a choice of basis that gives us one of the three matrices below, M_1 for a principal ideal, M_2 for an ideal in the same class as $[3, \theta]$, or M_3 for an ideal in the same class as $[3, -1-\theta]$.

$$M_1 = \begin{bmatrix}0 & 1 \\ -15 & -1\end{bmatrix}$$

$$M_2 = \begin{bmatrix}0 & 3 \\ -5 & -1\end{bmatrix}$$

$$M_3 = \begin{bmatrix}0 & 5 \\ -3 & -1\end{bmatrix}$$

For those familiar with general linear groups, we can talk about what happens if we choose a different basis. If M is the matrix for one basis, then the matrix for a different basis will be PMP^{-1} for some P in the general linear group $\mathrm{GL}_2(\mathbb{Z})$. More precisely, if $\mathrm{MC}_2(\mathbb{Z}, \theta)$ is the set of 2x2 matrices with entries in $\mathbb{Z}$ whose characteristic polynomial is the minimum polynomial of θ over $\mathbb{Z}$, then $\mathrm{GL}_2(\mathbb{Z})$ acts on $\mathrm{MC}_2(\mathbb{Z}, \theta)$ by conjugacy, and there is one orbit for each ideal class, so the number of orbits is equal to the class number. Actually, a statement similar to this is true for any monogenic field.

Each of our matrices M satisfies $M^2 + M + 15 = 0$, where scalars denote corresponding scalar matrices. From the trace we get $u_1 + v_2 = -1$, and from the determinant we get $u_1 v_2 - u_2 v_1 = 15$. Now we can define the symmetric matrix

$$A = \begin{bmatrix} 2v_1 & v_2 - u_1 \\ v_2 - u_1 & -2u_2 \end{bmatrix}$$

It's easily seen that the determinant of A is 59. Here are the matrices A_1, A_2 and A_3 corresponding to M_1, M_2 and M_3:

$$A_1 = \begin{bmatrix} 2 & -1 \\ -1 & 30 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} 6 & -1 \\ -1 & 10 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 10 & -1 \\ -1 & 6 \end{bmatrix}$$

Each A corresponds to a quadratic form. In what follows, it will be important that $v_1 > 0$, so that the quadratic form is positive definite. We have chosen M_1, M_2 and M_3 so that $v_1 > 0$. We can always swap ω_1 and ω_2 if necessary, to ensure that this is true. Then for any x and y in $\mathbb{Z}$,

$$\begin{bmatrix} x & y \end{bmatrix} A \begin{bmatrix} x \\ y \end{bmatrix}$$

is a 1x1 matrix whose single entry is $2\,\mathrm{N}(x\omega_1 + y\omega_2)/\,\mathrm{N}(I)$, where $\mathrm{N}(I)$ denotes the ideal norm.

For those familiar with special linear groups, we can continue the discussion about what happens if we choose a different basis. If $\mathrm{MC}_2^+(\mathbb{Z}, \theta)$ and $\mathrm{MC}_2^-(\mathbb{Z}, \theta)$ are the subsets of $\mathrm{MC}_2(\mathbb{Z}, \theta)$ where $v_1 > 0$ and $v_1 < 0$, respectively, then $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathrm{MC}_2^+(\mathbb{Z}, \theta)$ and $\mathrm{MC}_2^-(\mathbb{Z}, \theta)$ separately. For both actions, the number of orbits is equal to the class number. For any P in $\mathrm{SL}_2(\mathbb{Z})$, the symmetric matrix corresponding to PMP^{-1} is PAP^T.

Next, we're going to expand our symmetric matrix A by adding a third row and column, so that the resulting matrix C has determinant 1. To do this, we're going to choose a and b in $\mathbb{Z}$ such than $2v_1a^2 = 59b - 1$. This will be possible because $v_1 = \mathrm{N}(\omega_1)/\mathrm{N}(I)$ is a quadratic residue modulo 59, as is -2 since $59 \equiv 3 \pmod 8$. Then define

$$C = \begin{bmatrix} 2v_1 & v_2 - u_1 & 0 \\ v_2 - u_1 & -2u_2 & a \\ 0 & a & b \end{bmatrix}$$

Here are the values of C for each of our symmetric matrices A_1, A_2 and A_3:

$$C_1 = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 30 & 18 \\ 0 & 18 & 11 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 6 & -1 & 0 \\ -1 & 10 & 7 \\ 0 & 7 & 5 \end{bmatrix}$$

$$C_3 = \begin{bmatrix} 10 & -1 & 0 \\ -1 & 6 & 17 \\ 0 & 17 & 49 \end{bmatrix}$$

Finally, we're going to express the inverse C^{-1} as the product of some matrix B having determinant 1 with its transpose B^T. This will be possible because C^{-1} defines a positive definite ternary quadratic form with discriminant 1. The sums of the squares of the bottom row of B will then be 59.

$$C^{-1} = \begin{bmatrix} -2u_2b - a^2 & (u_1 - v_2)b & (v_2 - u_1)a \\ (u_1 - v_2)b & 2v_1b & -2v_1a \\ (v_2 - u_1)a & -2v_1a & 59 \end{bmatrix}$$

$$C_1^{-1} = \begin{bmatrix} 6 & 11 & -18 \\ 11 & 22 & -36 \\ -18 & -36 & 59 \end{bmatrix} = \begin{bmatrix} -1 & -2 & -1 \\ -3 & -3 & -2 \\ 5 & 5 & 3 \end{bmatrix} \begin{bmatrix} -1 & -3 & 5 \\ -2 & -3 & 5 \\ -1 & -2 & 3 \end{bmatrix}$$

$$59 = 5^2 + 5^2 + 3^2$$

$$C_2^{-1} = \begin{bmatrix} 1 & 5 & -7 \\ 5 & 30 & -42 \\ -7 & -42 & 59 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ -5 & -1 & -2 \\ 7 & 1 & 3 \end{bmatrix} \begin{bmatrix} -1 & -5 & 7 \\ 0 & -1 & 1 \\ 0 & -2 & 3 \end{bmatrix}$$

$$59 = 7^2 + 1^2 + 3^2$$

$$C_3^{-1} = \begin{bmatrix} 5 & 49 & -17 \\ 49 & 490 & -170 \\ -17 & -170 & 59 \end{bmatrix} = \begin{bmatrix} 0 & -2 & -1 \\ -3 & -20 & -9 \\ 1 & 7 & 3 \end{bmatrix} \begin{bmatrix} 0 & -3 & 1 \\ -2 & -20 & 7 \\ -1 & -9 & 3 \end{bmatrix}$$

$$59 = 1^2 + 7^2 + 3^2$$

If we chose a different B, still having determinant 1, and still satisfying $C^{-1} = BB^T$, could we get a different representation of 59 as the sum of three squares? Yes, but only via the obvious transformations. We can cycle the columns of B, so the first column becomes the second, the second becomes the third, and the third becomes the first. Also, we can negate any one column and swap the other two. To put it another way, we could multiply B on the right by any of these matrices:

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

These matrices generate a finite subgroup of $\mathrm{SL}_3(\mathbb{Z})$ of order 24. We can actually negate any two columns. We can also negate all three columns and swap any two of them.

Including negative numbers, there are a total of 72 triples of x, y and z in $\mathbb{Z}$ where $59 = x^2 + y^2 + z^2$. These 24 are associated with the principal ideal class:

5	5	3	3	5	5	5	3	5
−5	−5	3	−3	−5	5	−5	−3	5
5	−5	−3	3	−5	−5	5	−3	−5
−5	5	−3	−3	5	−5	−5	3	−5
−5	−5	−3	−3	−5	−5	−5	−3	−5
5	5	−3	3	5	−5	5	3	−5
−5	5	3	−3	5	5	−5	3	5
5	−5	3	3	−5	5	−5	−3	5

And these 24 are associated with the class that includes $[3, \theta]$:

7	1	3	3	7	1	1	3	7
−7	−1	3	−3	−7	1	−1	−3	7
7	−1	−3	3	−7	−1	1	−3	−7
−7	1	−3	−3	7	−1	−1	3	−7
−1	−7	−3	−3	−1	−7	−7	−3	−1
1	7	−3	3	1	−7	7	3	−1
−1	7	3	−3	1	7	−7	3	1
1	−7	3	3	−1	7	7	−3	1

Finally, these 24 are associated with the class that includes $[3, -1 - \theta]$:

1	7	3	3	1	7	7	3	1
−1	−7	3	−3	−1	7	−7	−3	1
1	−7	−3	3	−1	−7	7	−3	−1
−1	7	−3	−3	1	−7	−7	3	−1
−7	−1	−3	−3	−7	−1	−1	−3	−7
7	1	−3	3	7	−1	1	3	−7
−7	1	3	−3	7	1	−1	3	7
7	−1	3	3	−7	1	1	−3	7

5 Case Study of a Hilbert Class Field

Every number field has a Hilbert class field, which has some truly remarkable properties. It's a Galois extension where the Galois group is isomorphic to the ideal class group. Every ideal of the number field's ring of integers becomes principal when extended to the Hilbert class field's ring of integers.

Our next case study will be the Hilbert class field for the imaginary quadratic field from the last section. Recall that we had defined

$$\begin{aligned}\theta &= \frac{-1+i\sqrt{59}}{2}\\ &\approx -0.5+3.84057i\\ K &= \mathbb{Q}(i\sqrt{59}) = \mathbb{Q}(\theta)\\ R &= \mathbb{Z}[\theta]\end{aligned}$$

The class number is 3, so the Hilbert class field must be a cubic extension of K. We look around for a cubic polynomial with discriminant -59, and we find x^3+2x+1. This polynomial has three roots:

$$\begin{aligned}\alpha_1 &\approx -0.45340\\ \alpha_2 &\approx 0.22670-1.46771i\\ \alpha_3 &\approx 0.22670+1.46771i\end{aligned}$$

With a little calculation to get the sign right, we find

$$(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1) = i\sqrt{59} = 1+2\theta$$

Evidently $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$ is an extension of K. It's enough to adjoin any one of the roots to K. Let's define α as the real root, that is, $\alpha=\alpha_1$. Then $K(\alpha)$ is the Hilbert class field.

Our first guess as to the ring of integers might be $R[\alpha]$, but that doesn't quite cover all the algebraic integers. To find the missing ones, let's start by examining how the other two roots relate to the first.

$$\begin{aligned}\alpha_2\alpha_3 &= 2+\alpha^2\\ (\alpha_1-\alpha_2)(\alpha_3-\alpha_1) &= -2-3\alpha^2\\ (\alpha_2-\alpha_3)^2 &= -8-3\alpha^2\\ (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)^2(\alpha_3-\alpha_1) &= 16+30\alpha^2+9\alpha^4\\ (1+2\theta)(\alpha_2-\alpha_3) &= 16-9\alpha+12\alpha^2\end{aligned}$$

The last equation lets us calculate α_2 and α_3 from α and θ. If we also add $59(4+3\alpha)$ to both sides, then we can factor out the 12:

$$\begin{aligned}(1+2\theta)(\alpha_2-\alpha_3-(1+2\theta)(4+3\alpha)) &= 16-9\alpha+12\alpha^2+59(4+3\alpha)\\ &= 12(21+14\alpha+\alpha^2)\end{aligned}$$

We now have enough information to describe the ring of integers. If we set

$$\begin{aligned}\beta &= \frac{21 + 14\alpha + \alpha^2}{1 + 2\theta} \\ &\approx -1.93435i\end{aligned}$$

then β is an algebraic integer, because

$$\begin{aligned}(1 + 2\theta)\beta &= 21 + 14\alpha + \alpha^2 \\ -59\beta^2 &= 441 + 588\alpha + 238\alpha^2 + 28\alpha^3 + \alpha^4 \\ &= 413 + 531\alpha + 236\alpha^2 \\ \beta^2 &= -7 - 9\alpha - 4\alpha^2 \\ (1 + 2\theta)\beta^3 &= -147 - 287\alpha - 217\alpha^2 - 65\alpha^3 - 4\alpha^4 \\ &= -82 - 153\alpha - 209\alpha^2\end{aligned}$$

and from there we get $\beta^3 + (1 + 2\theta)\beta^2 - 27\beta - 4(1 + 2\theta) = 0$. It turns out that $R[\alpha, \beta]$ is the ring of integers for $K(\alpha)$, so let's define

$$\begin{aligned}L &= K(\alpha) \\ S &= R[\alpha, \beta]\end{aligned}$$

Our basis for S over R will be $\{1, \alpha, \beta\}$, so let's get representations of α^2, β^2 and $\alpha\beta$:

$$\begin{aligned}\alpha^2 &= -21 - 14\alpha + (1 + 2\theta)\beta \\ \beta^2 &= 77 + 47\alpha - (4 + 8\theta)\beta \\ \alpha\beta &= 5 + 10\theta + (3 + 6\theta)\alpha + 14\beta\end{aligned}$$

Then these matrix equations show the effect of multiplying by α and β:

$$\alpha \begin{bmatrix}1 \\ \alpha \\ \beta\end{bmatrix} = M_\alpha \begin{bmatrix}1 \\ \alpha \\ \beta\end{bmatrix}$$

$$\beta \begin{bmatrix}1 \\ \alpha \\ \beta\end{bmatrix} = M_\beta \begin{bmatrix}1 \\ \alpha \\ \beta\end{bmatrix}$$

where

$$M_\alpha = \begin{bmatrix}0 & 1 & 0 \\ -21 & -14 & 1 + 2\theta \\ 5 + 10\theta & 3 + 6\theta & 14\end{bmatrix}$$

$$M_\beta = \begin{bmatrix}0 & 0 & 1 \\ 5 + 10\theta & 3 + 6\theta & 14 \\ 77 & 47 & -4 - 8\theta\end{bmatrix}$$

Any element ξ of S has a unique representation as $\omega_1 + \omega_2\alpha + \omega_3\beta$ for some ω_1, ω_2 and ω_3 in R. Then the matrix M_ξ showing the effect of multiplying by ξ is given by

$$M_\xi = \omega_1 + \omega_2 M_\alpha + \omega_3 M_\beta$$

and the norm of ξ (for the extension L/K) is just the determinant of M_ξ.

Next we'll be looking at the Galois group of L/K, generated by σ which takes α to α_2. So σ cycles the roots of $x^3 + 2x + 1$:

$$\begin{aligned}\sigma(\alpha) &= \alpha_2\\ \sigma(\alpha_2) &= \alpha_3\\ \sigma(\alpha_3) &= \alpha\end{aligned}$$

We have these representations of α_2 and α_3:

$$\begin{aligned}\alpha_2 &= 2 + 4\theta + (1 + 3\theta)\alpha + 6\beta\\ \alpha_3 &= -2 - 4\theta - (2 + 3\theta)\alpha - 6\beta\end{aligned}$$

Now let's define

$$\beta_2 = \sigma(\beta) = \frac{21 + 14\alpha_2 + \alpha_2^2}{1 + 2\theta}$$

$$\beta_3 = \sigma(\beta_2) = \frac{21 + 14\alpha_3 + \alpha_3^2}{1 + 2\theta}$$

We can then calculate these representations of β_2 and β_3:

$$\begin{aligned}\beta_2 &= 29 - \theta + 22\alpha - (2 + 3\theta)\beta\\ \beta_3 &= -30 - \theta - 22\alpha + (1 + 3\theta)\beta\end{aligned}$$

Then the effect of σ can be expressed via this matrix equation:

$$\begin{bmatrix}\sigma(1)\\ \sigma(\alpha)\\ \sigma(\beta)\end{bmatrix} = M_\sigma \begin{bmatrix}1\\ \alpha\\ \beta\end{bmatrix}$$

where

$$M_\sigma = \begin{bmatrix}1 & 0 & 0\\ 2 + 4\theta & 1 + 3\theta & 6\\ 29 - \theta & 22 & -2 - 3\theta\end{bmatrix}$$

The matrix showing the effect of multiplying by $\sigma(\xi)$ would be $M_\sigma^{-1} M_\xi M_\sigma$.

Let's take a quick peek at the Galois group of $L/\mathbb{Q}$. This group has 6 elements. If we define ρ as complex conjugation, then the table below shows the 6 automorphisms and how they treat α, β and θ:

	takes α to ...	takes β to ...	takes θ to ...
1	α	β	θ
σ	α_2	β_2	θ
σ^2	α_3	β_3	θ
ρ	α	- β	$-1-\theta$
$\sigma\rho = \rho\sigma^2$	α_2	- β_2	$-1-\theta$
$\sigma^2\rho = \rho\sigma$	α_3	- β_3	$-1-\theta$

The Galois group of L/K is the subgroup $\{1, \sigma, \sigma^2\}$ that leaves θ unchanged.

In general, S might not have unique factorization. We know that every ideal of R becomes principal when extended to S. But if an ideal splits, the factors might not be principal. In that case, L would have its own Hilbert class field, say L'. Then the Galois group of the extension L'/L would be abelian, as is that of L/K. But L'/K would not be an abelian extension, since otherwise L' would be the Hilbert class field for K. In some cases, there may be an infinite tower of Hilbert class fields.

But in this particular case, it happens that S does have unique factorization. Keep in mind though, for any given factorization of some element, we could always multiply the left factor by a unit and then divide the right factor by the same unit. For example, even in $\mathbb{Z}$, we have $15 = 3 \cdot 5 = (-3)(-5)$. There are just 2 units in $\mathbb{Z}$: 1 and -1. The same is true of R. But S has infinitely many units. It turns out that the units of S are generated by α, α_2 and α_3. Since $\alpha\alpha_2\alpha_3 = -1$, we can always force the exponent of α to be 0, so each unit of S has a unique representation as $(-1)^t\alpha_2^u\alpha_3^v$, where t is either 0 or 1, and u and v are in $\mathbb{Z}$. For example, $\alpha = (-1)^1\alpha_2^{-1}\alpha_3^{-1}$.

With that out of the way, let's do some unique factoring. We'll start with primes of $\mathbb{Z}$ that are not quadratic residues modulo 59, whose ideals therefore stay inert in R. Each one splits into 3 primes in S:

$$
\begin{aligned}
2 &= (1+\alpha)(1+\alpha_2)(1+\alpha_3) \\
11 &= (2+\alpha)(2+\alpha_2)(2+\alpha_3) \\
13 &= (2-\alpha)(2-\alpha_2)(2-\alpha_3) \\
23 &= (2+\alpha+2\alpha^2)(2+\alpha_2+2\alpha_2^2)(2+\alpha_3+2\alpha_3^2) \\
31 &= (-1-4\alpha)(-1-4\alpha_2)(-1-4\alpha_3) \\
37 &= (1-2\alpha+2\alpha^2)(1-2\alpha_2+2\alpha_2^2)(1-2\alpha_3+2\alpha_3^2) \\
43 &= (3+2\alpha)(3+2\alpha_2)(3+2\alpha_3) \\
47 &= (6+13\alpha)(6+13\alpha_2)(6+13\alpha_3)
\end{aligned}
$$

Next we'll look at the primes of $\mathbb{Z}$ that are quadratic residues. Their ideals split in R. The first case is where the factors are principal. We only had one example of this from the last section: $[17] = [2+\theta][1-\theta]$. Each of these factors further splits into 3 primes in S:

$$2+\theta = (1-\alpha_3+\alpha_2^{-1})(1-\alpha+\alpha_3^{-1})(1-\alpha_2+\alpha^{-1})$$
$$1-\theta = (1-\alpha_2+\alpha_3^{-1})(1-\alpha+\alpha_2^{-1})(1-\alpha_3+\alpha^{-1})$$

In the case where a prime of $\mathbb{Z}$ splits in R but the factors aren't principal, those factors stay inert in S. That is, they don't split any further. But they become principal. To find the generators, we'll begin by considering these two elements of S:

$$\kappa_5 = 1-\alpha_2-\alpha_3^{-1} \qquad = 8-7\theta+(5-5\theta)\alpha-(11+\theta)\beta$$
$$\lambda_5 = 1-\alpha_3-\alpha_2^{-1} \qquad = 15+7\theta+(10+5\theta)\alpha+(10-\theta)\beta$$

These elements have the following useful properties:

$$\sigma(\kappa_5) = -\alpha_3\ \kappa_5$$
$$\sigma^2(\lambda_5) = -\alpha_2\ \lambda_5$$

It's rare that an automorphism multiplies a particular element by a unit. Normally this would indicate a prime has ramified. For example, the complex conjugate of $1+2\theta$ is $(-1)(1+2\theta)$. That's because [59] has ramified in R. But here there is no ramification. You might say that κ_5 and λ_5 are "almost" in R, in the sense that they are almost invariant under σ and σ^2.

Now recall that $[5] = [5,-1-\theta][5,\theta]$ in R. It turns out that

$$[5,-1-\theta] = [\kappa_5]$$
$$[5,\theta] = [\lambda_5]$$
$$5 = \kappa_5\ \lambda_5$$

We also had $[3] = [3,\theta][3,-1-\theta]$ in R. Now let's define

$$\kappa_3 = \kappa_5\ \theta/5 \qquad = 21+3\theta+(15+2\theta)\alpha+(3-2\theta)\beta$$
$$\lambda_3 = \lambda_5\ (-1-\theta)/5 \qquad = 18-3\theta+(13-2\theta)\alpha-(5+2\theta)\beta$$

Then we have

$$[3,\theta] = [\kappa_3]$$
$$[3,-1-\theta] = [\lambda_3]$$
$$3 = \kappa_3\ \lambda_3$$
$$\theta = \kappa_3\ \lambda_5$$
$$-1-\theta = \kappa_5\ \lambda_3$$

So the greatest common divisor that 3 and θ "ought" to have really does exist in S: it's κ_3.

The generators for the other non-principal ideals from the last section are listed below. In each case, $[p] = [p,\ \kappa_p\ \lambda_3][p,\ \kappa_3\ \lambda_p]$ in R, and

$$\begin{aligned}[p,\ \kappa_p\ \lambda_3] &= [\kappa_p] \\ [p,\ \kappa_3\ \lambda_p] &= [\lambda_p] \\ p &= \kappa_p\ \lambda_p\end{aligned}$$

p	κ_p	λ_p	$\kappa_p\ \lambda_3$	$\kappa_3\ \lambda_p$
7	$\kappa_3\ (2-\theta)/3$	$\lambda_3\ (3+\theta)/3$	$2-\theta$	$3+\theta$
19	$\kappa_3\ (7+\theta)/3$	$\lambda_3\ (6-\theta)/3$	$7+\theta$	$6-\theta$
29	$\kappa_3\ (8-\theta)/3$	$\lambda_3\ (9+\theta)/3$	$8-\theta$	$9+\theta$
41	$\kappa_3\ (7-2\theta)/3$	$\lambda_3\ (9+2\theta)/3$	$7-2\theta$	$9+2\theta$
53	$\kappa_3\ (11+2\theta)/3$	$\lambda_3\ (9-2\theta)/3$	$11+2\theta$	$9-2\theta$

Several things are worth noting here. First,

$$\begin{aligned}\sigma(\alpha) = 2+4\theta+(1+3\theta)\alpha+6\beta &\equiv -1-2\alpha &= \alpha^3 &\pmod{[3,\theta]} \\ \sigma^2(\alpha) = -2-4\theta-(2+3\theta)\alpha-6\beta &\equiv -1-2\alpha &= \alpha^3 &\pmod{[3,-1-\theta]}\end{aligned}$$

In fact, it turns out that for any element ξ of S,

$$\begin{aligned}\sigma(\xi) &\equiv \xi^3 \pmod{[3,\theta]} \\ \sigma^2(\xi) &\equiv \xi^3 \pmod{[3,-1-\theta]}\end{aligned}$$

which means that σ and σ^2 are the Frobenius automorphisms for $[3,\theta]$ and $[3,-1-\theta]$, respectively. More generally, σ is the Frobenius automorphism for any prime ideal in the same class as $[3,\theta]$ (in R), while σ^2 is the Frobenius automorphism for any prime ideal in the same class as $[3,-1-\theta]$. This provides the natural isomorphism between the ideal class group and the Galois group.

Then for each p where we've defined κ_p and λ_p, we have

$$\begin{aligned}\sigma(\kappa_p) &= -\alpha_3\ \kappa_p \\ \sigma^2(\kappa_p) &= -\alpha_2^{-1}\ \kappa_p \\ \sigma^2(\lambda_p) &= -\alpha_2\ \lambda_p \\ \sigma(\lambda_p) &= -\alpha_3^{-1}\ \lambda_p \\ \kappa_p + \sigma(\kappa_p) + \sigma^2(\kappa_p) &= \kappa_p\ \lambda_5 \\ \lambda_p + \sigma^2(\lambda_p) + \sigma(\lambda_p) &= \kappa_5\ \lambda_p\end{aligned}$$

The last two equations give the trace of κ_p and λ_p, respectively.

Now recall that the cube of any ideal in R is principal.

$$\begin{aligned}
[3,\theta]^3 &= [3-\theta] \\
[3-1-\theta]^3 &= [4+\theta] \\
[5,-1-\theta]^3 &= [11+\theta] \\
[5,\theta]^3 &= [10-\theta] \\
[7,2-\theta]^3 &= [-13+3\theta] \\
[7,3+\theta]^3 &= [-16-3\theta] \\
[19,7+\theta]^3 &= [67+15\theta] \\
[19,6-\theta]^3 &= [52-15\theta] \\
[29,8-\theta]^3 &= [-97-35\theta] \\
[29,9+\theta]^3 &= [-62+35\theta] \\
[41,7-2\theta]^3 &= [-263-\theta] \\
[41,9+2\theta]^3 &= [-262+\theta] \\
[53,11+2\theta]^3 &= [209+91\theta] \\
[53,9-2\theta]^3 &= [118-91\theta]
\end{aligned}$$

Then we get these factorizations:

$$\begin{aligned}
3-\theta &= \kappa_3\ \sigma(\kappa_3)\ \sigma^2(\kappa_3) && = \alpha_3\ \alpha_2^{-1}\ \kappa_3^3 \\
4+\theta &= \lambda_3\ \sigma^2(\lambda_3)\ \sigma(\lambda_3) && = \alpha_2\ \alpha_3^{-1}\ \lambda_3^3 \\
11+\theta &= \kappa_5\ \sigma(\kappa_5)\ \sigma^2(\kappa_5) && = \alpha_3\ \alpha_2^{-1}\ \kappa_5^3 \\
10-\theta &= \lambda_5\ \sigma^2(\lambda_5)\ \sigma(\lambda_5) && = \alpha_2\ \alpha_3^{-1}\ \lambda_5^3 \\
-13+3\theta &= \kappa_7\ \sigma(\kappa_7)\ \sigma^2(\kappa_7) && = \alpha_3\ \alpha_2^{-1}\ \kappa_7^3 \\
-16-3\theta &= \lambda_7\ \sigma^2(\lambda_7)\ \sigma(\lambda_7) && = \alpha_2\ \alpha_3^{-1}\ \lambda_7^3 \\
67+15\theta &= \kappa_{19}\ \sigma(\kappa_{19})\ \sigma^2(\kappa_{19}) && = \alpha_3\ \alpha_2^{-1}\ \kappa_{19}^3 \\
52-15\theta &= \lambda_{19}\ \sigma^2(\lambda_{19})\ \sigma(\lambda_{19}) && = \alpha_2\ \alpha_3^{-1}\ \lambda_{19}^3 \\
-97-35\theta &= \kappa_{29}\ \sigma(\kappa_{29})\ \sigma^2(\kappa_{29}) && = \alpha_3\ \alpha_2^{-1}\ \kappa_{29}^3 \\
-62+35\theta &= \lambda_{29}\ \sigma^2(\lambda_{29})\ \sigma(\lambda_{29}) && = \alpha_2\ \alpha_3^{-1}\ \lambda_{29}^3 \\
-263-\theta &= \kappa_{41}\ \sigma(\kappa_{41})\ \sigma^2(\kappa_{41}) && = \alpha_3\ \alpha_2^{-1}\ \kappa_{41}^3 \\
-262+\theta &= \lambda_{41}\ \sigma^2(\lambda_{41})\ \sigma(\lambda_{41}) && = \alpha_2\ \alpha_3^{-1}\ \lambda_{41}^3 \\
209+91\theta &= \kappa_{53}\ \sigma(\kappa_{53})\ \sigma^2(\kappa_{53}) && = \alpha_3\ \alpha_2^{-1}\ \kappa_{53}^3 \\
118-91\theta &= \lambda_{53}\ \sigma^2(\lambda_{53})\ \sigma(\lambda_{53}) && = \alpha_2\ \alpha_3^{-1}\ \lambda_{53}^3
\end{aligned}$$

[59] itself ramifies as $[1+2\theta]^2$ in R, and $[1+2\theta]$ splits into 3 primes in S:

$$1+2\theta = (\alpha-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha)$$

6 Case Study of an Elliptic Curve

Elliptic curves are a major topic of ongoing research. Roughly speaking, an elliptic curve is defined by an equation where the square of a linear polynomial in y (and maybe x) is equal to a cubic polynomial in x with nonzero discriminant. An example is $y^2 = x^3 + 4x$. Elliptic curves are useful in cryptography and in factoring large integers. Every elliptic curve over the complex numbers $\mathbb{C}$ is equivalent to a differential equation of the Weierstrass elliptic function for some lattice. If the lattice is an ideal of an imaginary quadratic field, then a property known as the j-invariant belongs to the corresponding Hilbert class field.

For our final case study, we'll examine an elliptic curve associated with $\mathbb{Q}(\sqrt{-19})$, which has class number 1. Then we'll wrap up with a brief look at the situation with $\mathbb{Q}(\sqrt{-59})$. Let's begin by defining

$$\begin{aligned}\theta_{19} &= \frac{-1 + i\sqrt{19}}{2} \\ &\approx -0.5 + 2.17945i \\ K_{19} &= \mathbb{Q}(i\sqrt{19}) = \mathbb{Q}(\theta_{19}) \\ R_{19} &= \mathbb{Z}[\theta_{19}]\end{aligned}$$

R_{19} has unique factorization. Here are the factorizations of the primes in $\mathbb{Z}$ less than 19 that split:

$$\begin{aligned}5 &= \theta_{19}(-1 - \theta_{19}) \\ 7 &= (2 + \theta_{19})(1 - \theta_{19}) \\ 11 &= (3 + \theta_{19})(2 - \theta_{19}) \\ 17 &= (4 + \theta_{19})(3 - \theta_{19})\end{aligned}$$

The Weierstrass elliptic function $\wp$ takes a complex number z along with a second parameter that specifies the lattice. When the lattice is generated by 1 and a complex number τ in the upper half plane, we can just specify τ as the second parameter. Eventually we'll be setting $\tau = \theta_{19}$, but first let's make a few general comments about $\wp$. The definition is

$$\wp(z;\tau) = \frac{1}{z^2} + \sum_{m^2+n^2 \neq 0} \left\{ \frac{1}{(z + m + n\tau)^2} - \frac{1}{(m + n\tau)^2} \right\}$$

Here the summation is over all m and n in $\mathbb{Z}$ where m and n are not both 0. In other words, we're summing over all nonzero lattice points $m + n\tau$.

As an elliptic function, $\wp$ is doubly periodic, meaning that

$$\wp(z;\tau) = \wp(z + 1;\tau) = \wp(z + \tau;\tau)$$

for all z in $\mathbb{C}$. It is also meromorphic with a second order pole at 0, hence at each lattice point.

In fact, $\wp$ satisfies this differential equation:

$$\wp'(z;\tau)^2 = 4\wp(z;\tau)^3 - \frac{4}{3}\pi^4 E_4(\tau)\wp(z;\tau) - \frac{8}{27}\pi^6 E_6(\tau)$$

where E_4 and E_6 are the Eisenstein series of weight 4 and 6, respectively, normalized so that the constant term of the q-expansion is 1. E_4 and E_6 are related by this equation:

$$(j(\tau) - 1728)E_4(\tau)^3 = j(\tau)E_6(\tau)^2$$

where j is the j-invariant.

An important feature of $\wp$ is that for any a and b in $\mathbb{C}$ satisfying

$$b^2 = 4a^3 - \frac{4}{3}\pi^4 E_4(\tau)a - \frac{8}{27}\pi^6 E_6(\tau)$$

there exists z in $\mathbb{C}$ such that

$$\wp(z;\tau) = a$$
$$\wp'(z;\tau) = b$$

Further, any two such z values differ by some lattice point $m + n\tau$.

Now let's focus on the case $\tau = \theta_{19}$. Here are some approximate values:

$$E_4(\theta_{19}) \approx 0.99972896$$
$$E_6(\theta_{19}) \approx 1.00056916$$

It turns out that $j(\theta_{19}) = -884736 = -512 \cdot 1728$, so the relation becomes

$$513E_4(\theta_{19})^3 = 512E_6(\theta_{19})^2$$
$$3^3 \cdot 19E_4(\theta_{19})^3 = 2^9 E_6(\theta_{19})^2$$

We'll divide through by $2^3 \cdot 3^6 \cdot 19^4$, so that the left side is a cube and the right side is a square, and we'll define v_{19} as the (positive real) 12th root of the result.

$$(v_{19})^{12} = \frac{E_4(\theta_{19})^3}{2^3 \cdot 3^3 \cdot 19^3} = \frac{2^6 E_6(\theta_{19})^2}{3^6 \cdot 19^4}$$
$$v_{19} \approx 0.30601616$$

$$(v_{19})^4 = \frac{E_4(\theta_{19})}{2 \cdot 3 \cdot 19} \qquad (v_{19})^6 = \frac{2^3 E_6(\theta_{19})}{3^3 \cdot 19^2}$$

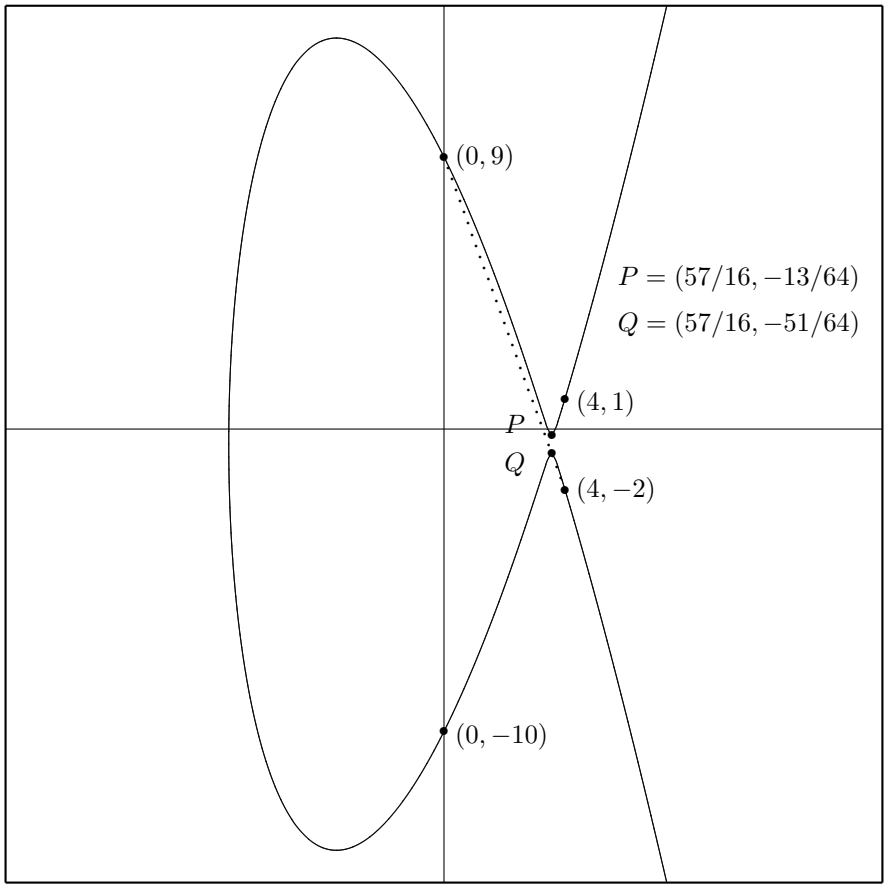
Now for any given z we can choose x and y such that

$$\wp(z;\theta_{19}) = (v_{19}\pi i)^2 x$$
$$\wp'(z;\theta_{19}) = (v_{19}\pi i)^3 (2y + 1)$$

After making these substitutions in the differential equation, and then dividing through by $4(v_{19}\pi i)^6$, we get this equation:

$$y^2 + y = x^3 - 38x + 90$$

Below is a graph of the curve defined by $y^2 + y = x^3 - 38x + 90$ over the real numbers, with all 4 of its integral points marked, plus 2 more rational points.



Now let's choose $z_{19} \approx 1.81462933i$ such that

$$\wp(z_{19}; \theta_{19}) = 0$$
$$\wp'(z_{19}; \theta_{19}) = 19(v_{19}\pi i)^3$$

The table below shows how multiples of z_{19} generate the 6 marked points.

z	$\wp(z;\theta_{19})$	$\wp'(z;\theta_{19})$	x	y
$-3z_{19}$	$57(v_{19}\pi i)^2/16$	$-19(v_{19}\pi i)^3/32$	$57/16$	$-51/64$
$-2z_{19}$	$4(v_{19}\pi i)^2$	$3(v_{19}\pi i)^3$	4	1
$-z_{19}$	0	$-19(v_{19}\pi i)^3$	0	-10
0	∞	∞	∞	∞
z_{19}	0	$19(v_{19}\pi i)^3$	0	9
$2z_{19}$	$4(v_{19}\pi i)^2$	$-3(v_{19}\pi i)^3$	4	-2
$3z_{19}$	$57(v_{19}\pi i)^2/16$	$19(v_{19}\pi i)^3/32$	$57/16$	$-13/64$

We'll be referring to the quotient space $\mathbb{C}/R_{19}$, which is just the set of complex numbers, except that any two complex numbers that differ by an element of R_{19} are considered the same. So for example, all of the lattice points $m + n\theta_{19}$ for m and n in $\mathbb{Z}$ are considered the same. We can think of R_{19} as chopping up $\mathbb{C}$ into parallelograms. Then $\mathbb{C}/R_{19}$ is any one of those parallelograms. In effect, we're "gluing" the two long edges of the parallelogram together, forming a tube, and then gluing the two short edges together, forming a torus. Since $\wp$ is doubly periodic, it's domain is really $\mathbb{C}/R_{19}$ for the case where $\tau = \theta_{19}$.

From the table, we can see that the curve naturally includes the point at infinity. So let's define E_{19} as the subset of the complex projective plane consisting of points $(x, y, 1)$ where $y^2 + y = x^3 - 38x + 90$, along with the point at infinity $(0, 1, 0)$. Now define the map ϕ_{19} from $\mathbb{C}/R_{19}$ to E_{19} taking 0 to $(0, 1, 0)$, and taking any other z to $(x, y, 1)$ where

$$\wp(z; \theta_{19}) = (v_{19}\pi i)^2 x$$
$$\wp'(z; \theta_{19}) = (v_{19}\pi i)^3 (2y + 1)$$

This is well defined and and in fact a bijection, because of the important feature of $\wp$ mentioned earlier. We'll still write (x, y) as a shorthand for $(x, y, 1)$.

The map ϕ_{19} induces an abelian group structure on E_{19}, based on ordinary addition of complex numbers. For example, if we want to add $(4, -2)$ and $(0, 9)$, the corresponding z values are $2z_{19}$ and z_{19}. Adding these gives $3z_{19}$, and the corresponding point on the curve is $(57/16, -13/64)$.

Another way to define addition of points on the curve, which turns out to be equivalent, is something called the group law. First, the "negative" of (x, y) is defined to be $(x, -1 - y)$. For example, the negative of $(4, 1)$ is $(4, -2)$. Then, to add two points, we draw a line from one to the other (a tangent if they are the same point). That line will intersect the curve at some third point. The sum is then the negative of this third point. For example, if we're adding $(4, -2)$ and $(0, 9)$, we draw a line between these two points (as indicated by the dotted line in the earlier graph). This intersects the curve at the third point $Q = (57/16, -51/64)$, whose negative is $P = (57/16, -13/64)$. One advantage of the group law is that it's well defined even for fields other than $\mathbb{C}$.

It turns out that our curve has only 4 integral points, which were shown on the graph. Further, all of its rational points are generated by $\phi_{19}(z_{19}) = (0, 9)$. The L-functions and Modular Forms Database has a lot more information about this curve, labelled 361.a2, as well as other elliptic curves.

Note that for $y^2 + y = x^3 - 38x + 90$, if we take our rough definition of an elliptic curve literally, we would need to add $1/4$ to both sides, so that the left side is the square of the linear polynomial $y + 1/2$. Then $x^3 - 38x + 90 + 1/4$ is the cubic polynomial that would need to have nonzero discriminant. In fact, it's discriminant is $-6859/16$.

From the earlier graph, it may appear that the points P and Q are at the narrows of the strait. Actually, both P and Q are at $x = 57/16 = 3.5625$, while the narrows of the strait are at $x = \sqrt{38/3} \approx 3.559026$.

Viewing the curve as defined over $\mathbb{C}$, we can use complex multiplication to find more points. If $\phi_{19}(z_1) = (x_1, y_1)$, we can "multiply" by θ_{19}, giving $\phi_{19}(z_1\theta_{19})$. This may be the point at infinity, or it may be some finite point (x_2, y_2). In the latter case, it turns out that x_2 and y_2 are in K_{19} if x_1 and y_1 were. To get formulas for x_2 and y_2, let's start by observing that every lattice point is congruent to some integer from 0 to 4 modulo θ_{19}. Therefore, if

$$\wp(z_1\theta_{19}; \theta_{19}) = \wp(z; \theta_{19})$$

then

$$\wp(z_1; \theta_{19}) = \wp((z+n)/\theta_{19}; \theta_{19})$$

for some integer n from 0 to 4. Now, for any z that's not a lattice point, define

$$r(x; z) = \prod_{n=0}^{4} \left(x - \frac{\wp((z+n)/\theta_{19}; \theta_{19})}{(v_{19}\pi i)^2} \right)$$

Then $r(x_1; z) = 0$ when x_2 is the x value for $\phi_{19}(z)$. We'll also define

$$s(x; z) = \prod_{n=1}^{2} \left(x - \frac{\wp((z+n)/\theta_{19}; \theta_{19})}{(v_{19}\pi i)^2} \right)$$

where $2z/\theta_{19}$ is a lattice point. If z itself is a lattice point, then $s(x_1; z) = 0$ when $\phi_{19}(z_1\theta_{19})$ is the point at infinity. Otherwise, $s(x_1; z) = 0$ when x_2 is the x value for $\phi_{19}(z)$ and x_1 is not the x value for $\phi_{19}(z/\theta_{19})$. Here, we're using the fact that $\wp$ is even (that is, $\wp(-z; \tau) = \wp(z; \tau)$ for any z and τ), so we can skip $n = 3$ and $n = 4$.

Now we're ready to define some polynomials:

$$\begin{aligned} f(x) &= r(x; z_{19}) \\ g(x) &= s(x; 5/2)\ s(x; \theta_{19}/2)\ s(x; (5+\theta_{19})/2) \\ h(x) &= \theta_{19}\ s(x; 0) \end{aligned}$$

The significance of these z values is that

$$\begin{aligned} \wp(z_{19}; \theta_{19}) &= 0 \\ \wp'(5/2; \theta_{19}) &= 0 \\ \wp'(\theta_{19}/2; \theta_{19}) &= 0 \\ \wp'((5+\theta_{19})/2; \theta_{19}) &= 0 \end{aligned}$$

So $f(x_1) = 0$ when $x_2 = 0$; $g(x_1) = 0$ when $y_2 = -1/2$ and $y_1 \neq -1/2$; and $h(x_1) = 0$ when $\phi_{19}(z_1\theta_{19})$ is the point at infinity.

It turns out that $f(x)$, $g(x)$ and $h(x)$ have coefficients in R_{19}:

$$\begin{aligned}
f(x) = \;& x^5 - (20+2\theta_{19})x^4 + (285+95\theta_{19})x^3 - (1900+912\theta_{19})x^2 \\
& + (5415+3249\theta_{19})x - (5415+3971\theta_{19}) \\
g(x) = \;& x^6 - (30+3\theta_{19})x^5 + 209x^4 - (247-228\theta_{19})x^3 \\
& - (2166+1083\theta_{19})x^2 + (7581+1444\theta_{19})x - 6859 \\
h(x) = \;& \theta_{19}x^2 + (5-9\theta_{19})x - (19-19\theta_{19})
\end{aligned}$$

And here are the formulas for x_2 and y_2:

$$\begin{aligned}
x_2 &= \frac{f(x_1)}{h(x_1)^2} \\
y_2 &= \frac{(y_1+1/2)g(x_1)}{h(x_1)^3} - 1/2
\end{aligned}$$

Using a similar technique, we can "multiply" by $1+2\theta_{19} = i\sqrt{19}$. Suppose $\phi_{19}(z_1) = (x_1, y_1)$ as before, and $\phi_{19}(z_1 i\sqrt{19})$ is the finite point (x_3, y_3). We'll cut straight to the chase and give the formulas for x_3 and y_3. In this case, x_3 and $(y_3+1/2)i\sqrt{19}$ are in $\mathbb{Q}$ if x_1 and y_1 were. First some polynomials:

$$\begin{aligned}
a(x) = \;& x^{19} - 76x^{18} + 5054x^{17} - 155591x^{16} + 2434945x^{15} - 19040584x^{14} \\
& + 26585484x^{13} + 918372087x^{12} - 9661738298x^{11} + 48640488756x^{10} \\
& - 138691257188x^9 + 269949265178x^8 - 1140580338964x^7 \\
& + 7880373251024x^6 - 35376761814403x^5 + 99387810915932x^4 \\
& - 180382423058461x^3 + 208456252765234x^2 - 141014523929423x \\
& + 42917463804607 \\
b(x) = \;& x^{27} - 114x^{26} + 2907x^{25} - 23826x^{24} - 92055x^{23} + 1947956x^{22} \\
& + 35659941x^{21} - 1613504301x^{20} + 35782367291x^{19} - 605388872807x^{18} \\
& + 8216082753444x^{17} - 89676741297555x^{16} + 787915711500015x^{15} \\
& - 5572200663015159x^{14} + 31531215647001103x^{13} \\
& - 140154782001161498x^{12} + 466413205975279584x^{11} \\
& - 996237601605480048x^{10} + 224697769969846628x^9 \\
& + 856666911510999 4056x^8 - 419948548230668477 19x^7 \\
& + 122614268298757271049x^6 - 253081494420620179545x^5 \\
& + 381092989394649733302x^4 - 413002350582826576439x^3 \\
& + 306566249439853960110x^2 - 139826170012004721175x \\
& + 29563247373966712477 \\
c(x) = \;& x^9 - 38x^8 + 437x^7 - 1444x^6 - 7942x^5 + 82308x^4 \\
& - 274360x^3 + 390963x^2 - 130321x - 130321
\end{aligned}$$

Then we have

$$x_3 = \frac{a(x_1)}{-19c(x_1)^2}$$
$$y_3 = \frac{(y_1 + 1/2)b(x_1)}{-19c(x_1)^3 i\sqrt{19}} - 1/2$$

Here's what complex multiplication looks like for $(0, 9)$:

$$\phi_{19}(z_{19}) = (0, 9)$$
$$\phi_{19}(z_{19}\theta_{19}) = (180 - \theta_{19})/49, (-333 + 19\theta_{19})/343)$$
$$\phi_{19}(z_{19} i\sqrt{19}) = (-133, 13357/(2i\sqrt{19}) - 1/2)$$

and for $(4, -2)$:

$$\phi_{19}(2z_{19}) = (4, -2)$$
$$\phi_{19}(2z_{19}\theta_{19}) = ((-4 - 37\theta_{19})/49, (-3686 - 555\theta_{19})/343)$$
$$\phi_{19}(2z_{19} i\sqrt{19}) = (-870755/26011, 1595297757/(1924814i\sqrt{19}) - 1/2)$$

Keep in mind that $y^2 + y = x^3 - 38x + 90$ is not the only elliptic curve with R_{19} as its lattice. We could substitute any nonzero complex number for v_{19} and get a curve that's equivalent over $\mathbb{C}$. We chose v_{19} so that the Eisenstein series would divide out, leaving integer coefficients. If we divide v_{19} by an integer, we'll get a curve whose rational points are in one to one correspondence with those of $y^2 + y = x^3 - 38x + 90$. For example, if we divide v_{19} by 3, we get

$$y^2 + y = x^3 - 3078x + 65792$$

For each point (x_1, y_1) of $y^2 + y = x^3 - 38x + 90$, there is a corresponding point $(9x_1, 27y_1 + 13)$ of $y^2 + y = x^3 - 3078x + 65792$. For example, $(4, -2)$ corresponds to $(36, -41)$.

If we divide v_{19} by the square root of an integer, we'll get another curve, known as a quadratic twist of the original curve. The twist may or may not have rational points. In the case of dividing v_{19} by $\sqrt{-19}$, an interesting thing happens, which ties into complex multiplication. The equation of the twist is

$$y^2 + y = x^3 - 13718x - 619025$$

which is labelled 361.a1. For each point (x_1, y_1) of the original curve, there is a corresponding point $(a(x_1)/c(x_1)^2, -(y_1 + 1/2)b(x_1)/c(x_1)^3 - 1/2)$ of the twist. For example, $(0, 9)$ corresponds to $(2527, 126891)$. This correspondence map consists of first doing complex multiplication by $-i\sqrt{19}$, then multiplying x by -19 and $y + 1/2$ by $-19i\sqrt{19}$. It happens that the rational points of the twist are generated by $(2527, 126891)$, so this is in fact a one to one correspondence of rational points.

Now let's consider the case of $\mathbb{Q}(\sqrt{-59})$. Recall that we had defined

$$\begin{aligned}\theta &= \frac{-1+i\sqrt{59}}{2}\\ &\approx -0.5+3.84057i\\ K &= \mathbb{Q}(i\sqrt{59}) = \mathbb{Q}(\theta)\\ R &= \mathbb{Z}[\theta]\end{aligned}$$

Here are some approximate values for the Eisenstein series:

$$\begin{aligned}E_4(\theta) &\approx 0.999999992052\\ E_6(\theta) &\approx 1.000000016690\end{aligned}$$

It turns out that

$$\begin{aligned}j(\theta) &= -2^{15}\alpha^{-18}(1+\alpha)^3(2+\alpha)^3\\ &\approx -30197682742.993\end{aligned}$$

where α is from the last section, where we studied the Hilbert class field of K. Specifically, α is the real root of x^3+2x+1. The relation between the Eisenstein series then becomes

$$11^2\alpha^4(2+\alpha+2\alpha^2)^2(3+2\alpha)^2(8+3\alpha^2)E_4(\theta)^3 = 2^9(1+\alpha)^3(2+\alpha)^5E_6(\theta)^2$$

Noting that $(2+\alpha)(6-2\alpha+\alpha^2)=11$, let's define

$$\begin{aligned}\mu &= 2^3\cdot 3^3(1+\alpha)(2+\alpha)(8+3\alpha^2)\\ \nu &= 2\cdot 3^3\alpha^2(6-2\alpha+\alpha^2)(2+\alpha+2\alpha^2)(3+2\alpha)(8+3\alpha^2)^2\end{aligned}$$

Multiplying the relation by $2^2\cdot 3^9(8+3\alpha^2)^3$ and dividing by $(2+\alpha)^2$, we get

$$3^3\nu^2E_4(\theta)^3 = 2^2\mu^3E_6(\theta)^2$$

We'll divide through by $3^6\mu^3\nu^2$, so that the left side is a cube and the right side is a square, and we'll define v_{59} as the (positive real) 12th root of the result.

$$(v_{59})^{12} = \frac{E_4(\theta)^3}{3^3\mu^3} = \frac{2^2E_6(\theta)^2}{3^6\nu^2}$$

$$v_{59} \approx 0.12064473$$

$$(v_{59})^4 = \frac{E_4(\theta)}{3\mu} \qquad\qquad (v_{59})^6 = \frac{2E_6(\theta)}{3^3\nu}$$

Substituting $\wp(z;\theta) = (v_{59}\pi i)^2x$ and $\wp'(z;\theta) = 2(v_{59}\pi i)^3y$, we then get

$$y^2 = x^3-\mu x+\nu$$

I don't know whether this curve has any points with x and y in the Hilbert class field $L=K(\alpha)$, and if so, what the structure of the Mordell-Weil group is. That would take some research to find out.

Suppose we look at the lattice for the ideal $[3, \theta]$. The corresponding τ value is $\theta/3$. The j-invariant is given by

$$j(\theta/3) = -2^{15}\alpha_3^{-18}(1+\alpha_3)^3(2+\alpha_3)^3 = \sigma^2(j(\theta))$$

Here, σ is from the last section, the automorphism that takes α to α_2. So σ^2 takes α to α_3. The corresponding elliptic curve for this lattice will be

$$y^2 = x^3 - \sigma^2(\mu)x + \sigma^2(\nu)$$

Similarly, the τ value for the $[3, -1-\theta]$ lattice is $\theta/5$, and

$$j(\theta/5) = -2^{15}\alpha_2^{-18}(1+\alpha_2)^3(2+\alpha_2)^3 = \sigma(j(\theta))$$

resulting in this curve:

$$y^2 = x^3 - \sigma(\mu)x + \sigma(\nu)$$

The Mordell-Weil group for these last two curves will be found by applying σ^2 and σ, respectively, to the Mordell-Weil group for $y^2 = x^3 - \mu x + \nu$.

7 Afterword

The link between ideal classes and sums of three squares was the subject of my senior thesis in college, almost 40 years ago. As I saw it, this was a remarkable connection that wasn't being discussed very much. It might help motivate people to learn about ideal classes, since the sum of three squares is easy to understand.

The other thing I recall from my college days was the absence of case studies. The professor would dive right into some abstract topic, with little in the way of concrete examples. When learning a new topic, I find it helpful to pick a sample case that's fairly representative, and then study that case in some depth. The case studies I've presented here are the kinds I would love to have seen in college.

For me, pure mathematics is entertainment. It's a game, like Dungeons & Dragons. Only it's more intricate and more elaborate than Dungeons & Dragons could ever be. The rules aren't created by a game writer. The rules exist naturally, and we discover them gradually.

But the game is more fun if everyone can play. I'm glad to see that Wikipedia now includes articles about a great deal of mathematics, making this information available to the general public at no charge. I've tried to make my case studies accessible to anyone with some high school math, who's willing to follow the Wikipedia links to read up on selected topics.

Another positive development is software packages like SageMath that make mathematical computations much easier. When we consider that mathematicians like David Hilbert didn't have access to modern computers, their achievements are all the more impressive.

Intelligent beings in another galaxy will likely have very different biology, history and literature. But their mathematics will be the same. They'll still have number fields, Hilbert class fields and elliptic curves, though with different names. When we meet them, we can swap stories of our respective mathematical discoveries. We can tell them that we've spent quite a bit of time on the Riemann hypothesis, but haven't been able to prove it yet. And they may confess they've been stumped on that one for a while, too.

Or they may say "hold my kanar" and then show us how it's done.