ELLIPTIC CURVES AND NUMBER FIELDS — AN EXAMPLE

N. P. STRICKLAND

Let E be the elliptic curve $y^2 = x^3 - x$ and let K be the subfield of $\mathbb{C}$ obtained from $\mathbb{Q}$ by adjoining the coordinates of the points of order nine on E. In this note we record the structure of K.

Definition 1. We write

$$\begin{aligned}
\rho &= \sqrt{3} \\
u &= 2 + \rho \\
v &= u^{1/3} \\
w &= v + 1/v \\
\zeta_m &= \exp(2\pi i/m) \\
\xi &= \zeta_9 + \zeta_9^{-1} \\
\theta &= (1-i)(1-\rho)/2 \\
\alpha &= 3^{1/8}2^{-1/2}u^{1/4} \\
x_3 &= 2\alpha^2/\rho \\
y_3 &= 2\alpha/\rho \\
x_9 &= (4 - 3\rho + (-5+4\rho)w + (4-\rho)w^2 + \\
&\quad (-4+2\rho)\xi + (-4+\rho)w\xi - w^2\xi + \\
&\quad (-2+2\rho)\xi^2 + w\xi^2 + (-2+\rho)w^2\xi^2)2\alpha^2/9 \\
y_9 &= (-30 + 20\rho + (-3-\rho)w + (9-7\rho)w^2 + \\
&\quad (-6-2\rho)\xi + (-15+\rho)w\xi + (-9+\rho)w^2\xi + \\
&\quad (12-4\rho)\xi^2 + (3+5\rho)w\xi^2 + (-3+5\rho)w^2\xi^2)\alpha/9.
\end{aligned}$$

All the roots occurring here are understood to be the positive roots of positive real numbers.

Proposition 2. *We have the following relations.*

$$\begin{aligned}
\zeta_{36} &= -i + \rho(-1 + \xi + \xi^2/2)/3 + i\xi^2/2 \\
\zeta_9 &= -2i\rho/3 + (1 + i\rho/3)\xi/2 + i\rho\xi^2/3 \\
\zeta_3 &= (-1 + i\rho)/2 \\
v &= w/2 - (w^2 - 2w - 2)\rho/6 \\
w^3 &= 3w + 4 \\
\xi^3 &= 3\xi - 1
\end{aligned}$$

Proof. For the first three equations, write $\zeta = \zeta_{36}$ and note that $i = \zeta^9$ and $\rho = 2\sin(\pi/3) = -i(\zeta^{12} - \zeta^{-12})$ and $\xi = \zeta^4 + \zeta^{-4}$. Moreover, one checks that the cyclotomic polynomial $\phi_{36}(t)$ is $t^{12} - t^6 + 1$, and thus that $\{\zeta^i \mid -6 < i \leq 6\}$ is a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Using the above remarks, we can write both sides of the first three equations in terms of our basis and observe that they coincide. The remaining equations can be checked directly. □

Proposition 3. *The elements u, v, θ, ξ, $\xi^2 - 2$ and $2 - \xi - \xi^2$ are units in the ring of integers of $\mathbb{Q}(i, \rho, \xi, w)$. In fact, u and θ are the fundamental units in $\mathbb{Q}(\rho)$ and $\mathbb{Q}(i, \rho)$ respectively. We have relations $v^3 = u$, $\theta^2 = -i/u$ and $\xi(\xi^2 - 2)(2 - \xi - \xi^2) = -1$.*

Proof. One can check directly that $\theta^2 = -i(2-\rho)$. This is clearly an algebraic integer, so the same is true of θ. It is also clear that u, v, ξ, ξ^2-2 and $2-\xi-\xi^2$ are integral. Another calculation shows that $\theta^2 ui = -\xi(\xi^2-2)(2-\xi-\xi^2) = 1$. This proves everything except that u and θ are fundamental units. I saw this in print somewhere so it must be true. □

Proposition 4. *The curve E has complex multiplication by $\mathbb{Z}[i]$. We have*

$$\begin{aligned}
i(x,y) &= (-x, iy)\\
-(x,y) &= (x,-y)\\
2(x,y) &= \left(\frac{\left(1+x^2\right)^2}{4\,x\,\left(-1+x^2\right)}, \frac{1-5\,x^2-5\,x^4+x^6}{8\,x\,\left(-1+x^2\right)\,y}\right)\\
3(x,y) &= \left(\frac{x\left(-3+6\,x^2+x^4\right)^2}{\left(-1-6\,x^2+3\,x^4\right)^2}, \frac{\left(-3+90\,x^2-185\,x^4+92\,x^6-165\,x^8-22\,x^{10}+x^{12}\right)\,y}{\left(-1-6\,x^2+3\,x^4\right)^3}\right)
\end{aligned}$$

Moreover, we have $3(x_9,y_9) = (x_3,y_3)$ and $3(x_3,y_3) = \infty$.

Proof. It is clear by inspection that the map $(x,y) \mapsto (-x,iy)$ is an automorphism of the curve of order four. A standard formula shows that the invariant differential is $dx/(2y)$, and this clearly gets multiplied by $(-1)/i = i$ under our automorphism. We thus have complex multiplication as claimed. The formula for $2(x,y)$ is standard. Write $(x',y') = 2(x,y)$ and let (x'',y'') be the right hand side of the last displayed equation. We claim that $3(x,y) = (x'',y'')$, or equivalently that $(x,y)+(x',y')+(x'',-y'')$ is the zero element. The group law is essentially defined by the requirement that three distinct points add to zero if and only if they lie on a line. It is thus enough to check that

$$\det\begin{pmatrix} 1 & x & y\\ 1 & x' & y'\\ 1 & x'' & -y'' \end{pmatrix} = 0.$$

This can be done by direct computation. One can also check directly that $3x_3^4 - 6x_3^2 - 1 = 0$, which implies that $3(x_3,y_3) = \infty$. (Another way to see this without having to derive the triplication formula is to note that the points of order three are precisely the inflection points of the curve, in other words the points where $y = \sqrt{x^3-x}$ and $d^2\sqrt{x^3-x}/dx^2 = 0$). I don't know a way to check by hand that $3(x_9,y_9) = (x_3,y_3)$ but it's straightforward using a suitable computer algebra system. □

Definition 5. We write $W = \mathbb{Z}[i]/9$, and $\omega = 2(1-i) \in W^\times$. Note that $\omega^2 = i$ and $\overline{\omega} = \omega^3 = -1/\omega$. We have $W^\times \simeq C_8 \times C_3^2$, with generators ω, $1+3$ and $1+3i$. Let G be the group generated by $W^\times$ and an element c subject to $c^2 = 1$ and $cz = \overline{z}c$.

Proposition 6. *The field K has a basis over $\mathbb{Q}$ consisting of monomials $i^a\rho^b w^c \xi^d \alpha^e$ for which $a,b \leq 1$ and $c,d \leq 2$ and $e \leq 3$. In particular, it has degree 144 over $\mathbb{Q}$. The Galois group can be naturally identified with G. (We will write $[z]$ for the Galois automorphism corresponding to an element $z \in W^\times$.)*

Proof. Write $L = \mathbb{Q}(i,\rho,w,\xi,\alpha)$, so we need to show that $L = K$. It is clear from Proposition 2 that L is spanned over $\mathbb{Q}$ by the given list of monomials. Thus, L has degree at most 144 over $\mathbb{Q}$.

We know that (x_9,y_9) is a point of exact order nine. From the formulae it is clear that x_9 and y_9 lie in L, and by complex multiplication (using $i \in L$) we deduce that all points of order nine are defined over L, so $K \subseteq L$.

We next observe that the complex multiplication on E gives a faithful algebraic action of $W^\times$ on $E[9]$ and thus a faithful action of $W^\times$ on K that fixes $\mathbb{Q}(i)$. It follows that K has degree at least $72 = |W^\times|$ over $\mathbb{Q}(i)$, and thus at least 144 over $\mathbb{Q}$. As $K \subseteq L$, we deduce that $K = L$ and that this field has degree exactly 144. If we let $c \in G$ act by complex conjugation we find that the action of $W^\times$ on K extends to one of G. By counting we find that G is the whole Galois group.

It is unsatisfying to rely so heavily on the computational fact that (x_9,y_9) has exact order nine, so we give a more conceptual proof of part of the proposition. Let (x,y) be a point of exact order nine, so x and y lie in K. Then $2(x,y) \neq 0$ so $(x,y) \neq -(x,y) = (x,-y)$, so $y \neq 0$. Moreover, $i(x,y) = (-x,iy)$ is another point of exact order nine, so $iy \in K$ and thus $i \in K$. We also know that there is an alternating bilinear Weil pairing

$e_9\colon E[9]\otimes E[9]\to\mu_9$, where $E[9]$ is the group of points of order nine in E and μ_9 is the group of ninth roots of unity. One can check that this is algebraically defined, and thus that $\mu_9\subseteq K$. As $\mu_4=\{\pm1,\pm i\}$ is also contained in K, we see that the cyclotomic field $\mathbb{Q}(\zeta_{36})$ is contained in K. It has degree 12 over the $\mathbb{Q}$, and it contains $\rho=-i(\zeta_3-\zeta_3^{-1})$. As we saw earlier, the inflection points of E are defined over K, so $\alpha\in K$. Using Proposition 2, we see that $\mathbb{Q}(\zeta_{36},\alpha)=\mathbb{Q}(i,\rho,\xi,\alpha)$. I still do not have a conceptual proof that u has a cube root in K, although I suspect that class field theory should provide one. If so, we could conclude that $L\subseteq K$. If we also knew that $[F(\alpha):F]=4$ and $[F(v):F]=3$ (where $F=\mathbb{Q}(\zeta_{36})$) then we could conclude that $[L:\mathbb{Q}]=144$ and with a little more work that $K=L$. □

Proposition 7. *The action of the generators of G on K is as follows, where $w'=(-w+(w^2-2w-2)i)/2$:*

	ω	i	$1+3$	$1+3i$	c
i	i	i	i	i	$-i$
ρ	$-\rho$	ρ	ρ	ρ	ρ
w	w	w	w	w'	w
ξ	ξ	ξ	ξ^2-2	ξ	ξ
α	$\theta\alpha$	$i\alpha$	α	α	α
ζ_9	$1/\zeta_9$	ζ_9	$1/\zeta_9^2$	ζ_9	$1/\zeta_9$
u	$1/u$	u	u	u	u
v	$1/v$	v	v	$\zeta_3 v$	v
θ	$-i/\theta$	θ	θ	θ	$-i\theta$

Proof. We have $\omega^2=i$, so the second column follows from the first. The action of c (by complex conjugation) is elementary. Thus, we need only study the action of ω, $1+3$ and $1+3i$. By construction, all these generators fix i.

For the action on ρ, note that $\mathbb{Q}(\rho)$ is a Galois extension of $\mathbb{Q}$. Thus, we have a surjective homomorphism $\mathrm{Gal}(K/\mathbb{Q})\to\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})\simeq C_2$. Moreover, c is in the kernel because ρ is real. As $1+3$ and $1+3i$ have order three, it is easy to check that the only possible homomorphism is the one indicated in the table. The action on $u=2+\rho$ follows from that on ρ. The action on $\theta=(1-i)(1-\rho)/2$ follows from that on ρ and i.

For the action on ζ_9, let e_9 denote the Weil pairing. As this is natural, and multiplication by i is an automorphism of the curve, we see that $e_9(iP,iQ)=e_9(P,Q)$ for all points P and Q of order nine. It follows that $e_9(iP,Q)=e_9(P,iQ)^{-1}$ and thus that

$$\begin{aligned}[a+ib]e_9(P,Q)&=e_9((a+ib)P,(a+ib)Q)\\&=e_9(P,Q)^{a^2}e_9(P,iQ)^{ab}e_9(iP,Q)^{ab}e_9(iP,iQ)^{b^2}\\&=e_9(P,Q)^{a^2+b^2}.\end{aligned}$$

Thus $[a+ib](\zeta_9)=\zeta_9^{a^2+b^2}$, which gives the action shown in the table.

Next, as $[i](u)=u$ and $v^3=u$ we must have $[i](v)=\lambda v$ where λ is a power of ζ_3, and thus $[i](\lambda)=\lambda$. It follows that $v=[i^4](v)=\lambda^4 v$ so $\lambda^4=1$ but also $\lambda^3=1$ so $\lambda=1$. Thus $[i](v)=v$. Next, as $[\omega](u)=1/u$ we must have $[\omega](v)=\lambda/v$ where λ is again a power of ζ_3. We have $c[\omega]=[\omega^{-1}]c=[\omega][-i]c$ in G. By applying this to v, we find that $\lambda^{-1}v=[\omega](\lambda)[\omega](v)=\lambda^{-1}\lambda v=v$, and it follows that $\lambda=1$. Thus $[\omega](v)=v$. Similarly, we have $[1+3](v)=\lambda v$ for some λ but $[1+3]$ commutes with c and thus preserves $K\cap\mathbb{R}$ so $[1+3](v)=v$. If $[1+3i](v)=v$ then Galois theory would tell us that $v\in\mathbb{Q}(\rho)$ which is clearly false, so

$[1+3i](v) = \zeta_3^{\pm 1} v$. One can check by numerical computation that $[1+3i](v) = \zeta_3 v$. In more detail, one can use the formulae for the group law and the complex multiplication to compute the action on x_9 and y_9. One can then deduce the action on γ, which is defined to be the trace of $x_9 y_3/(x_3 y_9)$ under the action of the group generated by $[1+3]$. Galois theory tells us that γ lies in $\mathbb{Q}(v)$ and by numerical computation we find that $v = (1+\rho)/(\gamma - 1)$. Using this we can deduce the action on v exactly.

Finally, we need to determine the action on α. As $3(x_3, y_3) = \infty$ we find that x_3 and y_3 are fixed under $[1+3]$ and $[1+3i]$, and thus that $\alpha = x_3/y_3$ is also fixed. We also have $i(x_3, y_3) = (-x_3, iy_3)$, which gives $[i](\alpha) = [i](x_3/y_3) = (-x_3)/(iy_3) = i\alpha$. Moreover, as $\omega = i - 1 \pmod 3$ we have $\omega(x_3, y_3) = i(x_3, y_3) - (x_3, y_3)$, so $\omega(x_3, y_3) + (-x_3, -iy_3) + (x_3, y_3) = \infty$. A simple calculation shows that $(-2\alpha^2\theta^2/\rho, -2\alpha\theta/\rho)$, $(-x_3, -iy_3)$, and (x_3, y_3) lie on E and are colinear. It follows that $\omega(x_3, y_3) = (-2\alpha^2\theta^2/\rho, -2\alpha\theta/\rho)$ and thus that $[\omega](\alpha) = (-2\alpha^2\theta^2/\rho)/(-2\alpha\theta/\rho) = \alpha\theta$ as claimed. □

1. Rings of integers

It is standard that the ring A_1 of integers in $K_1 = \mathbb{Q}(\rho)$ is just $\mathbb{Z}(\rho)$ (which is a PID), and that the discriminant of this ring over $\mathbb{Z}$ is 12. The primes 2 and 3 ramify in A_1, with $2 = u(1-\rho)^2$ and $3 = \rho^2$. All other primes are unramified. The unit group is generated by u.

Next, consider the field $K_2 = K_1(\alpha^2)$. This contains the element

$$\lambda = \frac{(1+\rho)(1+\alpha^2)}{2} = \frac{1+\alpha^2}{1-\rho}.$$

One checks that $K_2 = K_1(\lambda)$ and that

$$\lambda^2 = (1+\rho)(\lambda + u).$$

It follows that λ is an algebraic integer. I think that in fact the ring A_2 of integers in K_2 is $A_1(\lambda)$. The discriminant of A_2 over A_1 is thus $(1+\rho)^2 + 4(1+\rho)u = 24 + 14\rho$, which turns out to be the same as $2\rho u^2$. Thus, the discriminant ideal is generated by 2ρ. By the standard transitivity formula, the discriminant of A_2 over $\mathbb{Z} = A_0$ is $(12)^2 N_{A_1/A_0}(2\rho)$, which is equal to $2^6 3^3$ (up to a unit).

The obvious embedding $K_1 \to \mathbb{R}$ extends to give two embeddings of K_2 in $\mathbb{R}$. The other embedding $K_1 \to \mathbb{R}$ (sending ρ to $-\rho$) extends to give a conjugate pair of embeddings of K_2 in $\mathbb{C}$. In the usual notation, we have $s = 2$, $t = 1$ and $n = 4$. It follows that the rank of the unit group is $s + t - 1 = 2$. The element $u_1 = (\rho - 2)\lambda + \rho$ is a unit, with inverse $u_1^{-1} = (2-\rho)\lambda + 1$. I think that u and u_1 generate the units.

The primes $1 - \rho$ (over 2) and ρ (over 3) ramify in A_2, with $1 - \rho = u^{-2} u_1 \lambda^2$ and $\rho = u^{-2} u_1^2 (\lambda + 1)^2$. All other primes are unramified.

The standard classgroup estimate says that any ideal class for K_1 has a representative $\mathfrak{a}$ of norm at most

$$\left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|d|} = \frac{9\rho}{\pi} \simeq 4.96196.$$

Any ideal of norm less than 5 is a product of prime ideals whose norms are prime numbers less than 5. We have seen that 2 and 3 are totally ramified in A_2, and that the prime above 2 is generated by λ, and the prime above three is generated by $\lambda + 1$. In particular, both these ideals are principal, and it follows that A_2 is a PID.

Next, consider $K_3 = K_2(\alpha)$. If we put $\mu = (1+\rho)\alpha$ then we also have $K_3 = K_2(\mu)$. One checks that $\mu^2 = u u_1 (1 + \lambda)$, which shows that μ is a prime integer in A_3 and that $1 + \lambda \in A_2$ is ramified in A_3.

Consider the point $P = [\mu : 1 + \rho : \mu^3/u^2]$ in the projective plane over A_3. I think that this is of exact order 3, and that the resulting map $\mathrm{spec}(A_3) \to C\langle 3 \rangle$ is an isomorphism.

2. Subschemes

I think that when 2 is inverted, the subscheme $E[3]$ is $\mathrm{spec}(\mathbb{Z}[1/2, x]/(x^9 - 3x^5/2 - 3x/16))$, embedded by the map $x \mapsto [x : 1 : 7x^3 - 4x^7]$. The vector $u = (1 + 14x^4 - 8x^8, 9x^2 - 4x^6)$ (in the xz-plane) is doubly tangent to E at this point, and is universally nonzero because $u.v = 1$ where $v = (1 + 7x^4/4 - x^8, -11x^2/8 + x^6/2)$. On $E[3]$ regarded as a subscheme of the x-line, complex multiplication is as follows. We can embed $\mathbb{F}_3 =$

$\{0, 1, -1\}$ in $\mathbb{Z}$ in an obvious way, and this gives an embedding of $\mathbb{F}_9 = \mathbb{F}_3[i]$ in $\mathbb{Z}[i]$. Using this, we have

$$[a](x) = \begin{cases} ax & \text{if } a \in \{\pm 1, \pm i\} \\ ax(x^4 - 5/4) & \text{if } a \in \{\pm 1 \pm i\}. \end{cases}$$

Addition in $E[3]$ is given by the following formula:

$$\begin{aligned} F =& (x_0 + x_1) + \\ & (121x_0x_1^4 + 121x_0^4x_1 - 25x_0^2x_1^3 - 25x_0^3x_1^2)/8 + \\ & (-19x_0x_1^8 - 19x_0^8x_1 + 3x_0^2x_1^7 + 3x_0^7x_1^2 + 7x_0^3x_1^6 + 7x_0^6x_1^3 - 7x_0^4x_1^5 - 7x_0^5x_1^4)/2 + \\ & 2x_0^5x_1^8 + 2x_0^8x_1^5 - 2x_0^6x_1^7 - 2x_0^7x_1^6. \end{aligned}$$

3. History

I end with a brief account of how I found the formulae presented here, particularly those for x_9 and y_9. I used the computer programs *Mathematica* and *PARI*. The former is considerably more flexible and user-friendly and better able to deal with symbolic computation, but the latter is faster with numerical computation, and has algorithms for algebraic number theory built in. I used *Mathematica* to find the formula for $3(x, y)$ given above. Using this, I found a point (x_9, y_9) with $3(x_9, y_9) = (x_3, y_3)$, accurate to 1000 decimal places. Using the formulae for complex multiplication, I found all the other points of order nine. As mentioned above, one can compute from this the trace of $\kappa = x_9y_3/(x_3y_9)$ with respect to the subgroup of $W^\times$ generated by $1 + 3$. We denote this trace by γ. The formulae for complex multiplication show that γ is fixed under $[i]$, and it is clearly real. By Galois theory we deduce that it has degree at most three over $\mathbb{Q}(\rho)$, and thus six over $\mathbb{Q}$. This is small enough that one can use the LLL algorithm (implemented in the *Mathematica* package `NumberTheory‘Recognize‘`, or the *PARI* function `lindep()`) to find the minimal equation of γ. After some experimentation, I found that $\mathbb{Q}(\rho, \gamma)$ contained the element v, which seemed a more pleasant choice of generator. Next, Galois theory shows that $\kappa + [\omega](\kappa)$ and $(\kappa - [\omega](\kappa))/\rho$ lie in $\mathbb{Q}(w, \xi)$. This has degree nine over $\mathbb{Q}$, which is again small enough that the LLL algorithm is practicable (whereas the more direct approach involving $\mathbb{Q}(\rho, v, \xi)$ overwhelmed my computer). This gives expressions for $\kappa \pm [\omega](\kappa)$ and thus for κ. As $x_3/y_3 = \alpha$ this gives in turn an expression for x_9/y_9. Similar methods then give x_9 and y_9 separately.