of the group of all points. More generally, show that this is true for the elliptic curve $y^2 = f(x)$ if $f(x) \in K[x]$.

7. Consider the subgroup of all points on $y^2 = x^3 - n^2x$ with real coordinates. How many points in this subgroup are of order 2? 3? 4? Describe geometrically where these points are located.

8. Same as Problem 7 for the elliptic curve $y^2 = x^3 - a$, $a \in \mathbb{R}$.

9. If $y^2 = f(x)$ is an elliptic curve in which $f(x)$ has real coefficients, show that the group of points with real coordinates is isomorphic to (a) $\mathbb{R}/\mathbb{Z}$ if $f(x)$ has only one real root; (b) $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if $f(x)$ has three real roots.

10. Letting a approach zero in Problem 8, show that for the curve $y^2 = x^3$ the same geometric procedure for finding $P_1 + P_2$ as for elliptic curves makes the smooth points of the curve (i.e., $P \neq (0, 0)$, but including the point at infinity) into an abelian group. Show that the map which takes $P = (x, y)$ to x/y (and takes the point at infinity to zero) gives an isomorphism with the additive group of complex numbers. This is called "additive degeneracy" of an elliptic curve. One way to think of this is to imagine both ω_1 and ω_2 approaching infinity (in different directions). Then g_2 and g_3 both approach zero, so the equation of the corresponding elliptic curve approaches $y^2 = 4x^3$. Meanwhile, the additive group $\mathbb{C}/L$, where $L = \{m\omega_1 + n\omega_2\}$, approaches the additive group $\mathbb{C}$, i.e., the fundamental parallelogram becomes all of $\mathbb{C}$.

11. Let $a \to 0$ in the elliptic curve $y^2 = (x^2 - a)(x + 1)$. Show that for the curve $y^2 = x^2(x + 1)$ the same geometric procedure for finding $P_1 + P_2$ as for elliptic curves makes the smooth points of the curve into an abelian group. Show that the map which takes $P = (x, y)$ to $(y - x)/(y + x)$ (and takes the point at infinity to 1) gives an isomorphism with the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers. This is called "multiplicative degeneracy" of an elliptic curve. Draw the graph of the real points of $y^2 = x^2(x + 1)$, and show where the various sections go under the isomorphism with $\mathbb{C}^*$. One way to think of multiplicative degeneracy is to make the linear change of variables $y \mapsto \frac{1}{2}y$, $x \mapsto -x - \frac{1}{3}$, so that the equation becomes $y^2 = 4x^3 - \frac{4}{3}x - \frac{8}{27}$ (compare with Problem 8 of §I.6). So we are dealing with the limit as t approaches infinity of the group $\mathbb{C}/\{mit + n\pi\}$, i.e., with the vertical strip $\mathbb{C}/\{n\pi\}$ (rather, a cylinder, since opposite sides are glued together), and this is isomorphic to $\mathbb{C}^*$ under the map $z \mapsto e^{2iz}$.

§8. Points of finite order

In any group, there is a basic distinction between elements of finite order and elements of infinite order. In an abelian group, the set of elements of finite order form a subgroup, called the "torsion subgroup". In the case of the group of points in $\mathbb{P}^2_{\mathbb{C}}$ on the elliptic curve $y^2 = f(x)$, we immediately see that a point $P_z = (x, y)$ has finite order if and only if $Nz \in L$ for some N, i.e., if and only if z is a *rational* linear combination of ω_1 and ω_2. In that case, the least such N (which is the least common denominator of the coefficients of ω_1 and ω_2) is the exact order of P_z. Under the isomorphism from $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ to the elliptic curve given by $(a, b) \mapsto P_{a\omega_1 + b\omega_2}$, it is the image of $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$ which is the torsion subgroup of the elliptic curve.

This situation is the two-dimensional analog of the circle group, whose torsion subgroup is precisely the group of all roots of unity, i.e., all $e^{2\pi i z}$ for $z \in \mathbb{Q}/\mathbb{Z}$. Just as the cyclotomic fields—the field extensions of $\mathbb{Q}$ generated by the roots of unity—are central to algebraic number theory, we would expect that the fields obtained by adjoining the coordinates of points $P = (x, y)$ of order N on an elliptic curve should have interesting special properties. We shall soon see that these coordinates are algebraic (if the coefficients of $f(x)$ are). This analogy between cyclotomic fields and fields formed from points of finite order on elliptic curves is actually much deeper than one might have guessed. In fact, a major area of research in algebraic number theory today consists in finding and proving analogs for such fields of the rich results one has for cyclotomic fields.

Let N be a fixed positive integer. Let $f(x) = ax^3 + bx^2 + cx + d = a(x - e_1)(x - e_2)(x - e_3)$ be a cubic polynomial with coefficients in a field K of characteristic $\neq 2$ and with distinct roots (perhaps in some extension of K). We are interested in describing the coordinates of the points of order N (i.e., exact order a divisor of N) on the elliptic curve $y^2 = f(x)$, where these coordinates may lie in an extension of K. If $N = 2$, the points of order N are the point at infinity 0 and $(e_i, 0)$, $i = 1, 2, 3$. Now suppose that $N > 2$. If N is odd, by a "nontrivial" point of order N we mean a point $P \neq 0$ such that $NP = 0$. If N is even, by a "nontrivial" point of order N we mean a point P such that $NP = 0$ but $2P \neq 0$.

Proposition 13. *Let K' be any field extension of K (not necessarily algebraic), and let $\sigma: K' \to \sigma K'$ be any field isomorphism which leaves fixed all elements of K. Let $P \in \mathbb{P}^2_{K'}$ be a point of exact order N on the elliptic curve $y^2 = f(x)$, where $f(x) \in K[x]$. Then σP has exact order N (where for $P = (x, y, z) \in \mathbb{P}^2_{K'}$ we denote $\sigma P \underset{\text{def}}{=} (\sigma x, \sigma y, \sigma z) \in \mathbb{P}^2_{\sigma K'}$).*

Proof. It follows from the addition formulas that $\sigma P_1 + \sigma P_2 = \sigma(P_1 + P_2)$, and hence $N(\sigma P) = \sigma(NP) = \sigma 0 = 0$ (since $\sigma(0, 1, 0) = (0, 1, 0)$). Hence σP has order N. It must have exact order N, since if $N'\sigma P = 0$, we would have $\sigma(N'P) = 0 = (0, 1, 0)$, and hence $N'P = 0$. This proves the proposition. □

Proposition 14. *In the situation of Proposition 13, with K a subfield of $\mathbb{C}$, let $K_N \subset \mathbb{C}$ denote the field obtained by adjoining to K the x- and y-coordinates of all points of order N. Let K_N^+ denote the field obtained by adjoining just their x-coordinates. Then both K_N and K_N^+ are finite galois extensions of K.*

Proof. In each case K_N and K_N^+, we are adjoining a finite set of complex numbers which are permuted by any automorphism of $\mathbb{C}$ which fixes K. This immediately implies the proposition. □

As an example, if $N = 2$, then $K_2 = K_2^+$ is the splitting field of $f(x)$ over K.

Recall that the group of points of order N on an elliptic curve in $\mathbb{P}^2_{\mathbb{C}}$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$. Because any $\sigma \in \mathrm{Gal}(K_N/K)$ respects addition of points, i.e., $\sigma(P_1 + P_2) = \sigma P_1 + \sigma P_2$, it follows that each σ gives an invertible linear map of $(\mathbb{Z}/N\mathbb{Z})^2$ to itself.

If R is any commutative ring, we let $GL_n(R)$ denote the group (under matrix multiplication) of all $n \times n$ invertible matrices with entries in R. Here invertibility of a matrix A is equivalent to $\det A \in R^*$, where R^* is the multiplicative group of invertible elements of the ring. For example:

(1) $GL_1(R) = R^*$;
(2) $GL_2(\mathbb{Z}/N\mathbb{Z}) = \{(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) | a, b, c, d \in \mathbb{Z}/N\mathbb{Z}, ad - bc \in (\mathbb{Z}/N\mathbb{Z})^*\}$.

It is easy to construct a natural one-to-one correspondence between invertible linear maps $R^n \to R^n$ and elements of $GL_n(R)$. There is no difference with the more familiar case when R is a field.

In our situation of points of order N on an elliptic curve, we have seen that $\mathrm{Gal}(K_N/K)$ is isomorphic to a subgroup of the group of all invertible linear maps $(\mathbb{Z}/N\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2$. Thus, any $\sigma \in \mathrm{Gal}(K_N/K)$ corresponds to a matrix $(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in GL_2(\mathbb{Z}/N\mathbb{Z})$. The matrix entries can be found by writing

$$\sigma P_{\omega_1/N} = P_{a\omega_1/N + c\omega_2/N}, \qquad \sigma P_{\omega_2/N} = P_{b\omega_1/N + d\omega_2/N}.$$

Notice that this is a direct generalization of the situation with the N-th cyclotomic field $\mathbb{Q}_N \underset{\text{def}}{=} \mathbb{Q}(\sqrt[N]{1})$. Recall that $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q}) \approx (\mathbb{Z}/N\mathbb{Z})^* = GL_1(\mathbb{Z}/N\mathbb{Z})$, with the element a which corresponds to σ determined by

$$\sigma(e^{2\pi i/N}) = e^{2\pi i a/N}.$$

But one difference in our two-dimensional case of division points on elliptic curves is that, in general, $\mathrm{Gal}(K_N/K) \to GL_2(\mathbb{Z}/N\mathbb{Z})$ is only an injection, not an isomorphism.

In the case $K \subset \mathbb{C}$, say $K = \mathbb{Q}(g_2, g_3)$, where $y^2 = f(x) = 4x^3 - g_2 x - g_3$ is in Weierstrass form, we shall now use the $\wp$-function to determine the polynomial whose roots are the x-coordinates of the points of order N. That is, K_N^+ will be the splitting field of such a polynomial.

We first construct an elliptic function $f_N(z)$ whose zeros are precisely the nonzero values of z such that P_z is a point of order N. We follow the prescription in the proof of Proposition 9 of §I.5. If $u \in \mathbb{C}/L$ is a point of order N, then so is the symmetric point $-u$ (which we denoted u^* when we were thinking in terms of points in a fundamental parallelogram). We consider two cases:

(i) N is odd. Then the points u and $-u$ are always distinct modulo L. In other words, u cannot be $\omega_1/2$, $\omega_2/2$ or $(\omega_1 + \omega_2)/2$ if u has odd order N. We define

$$f_N(z) = N \prod (\wp(z) - \wp(u)), \tag{8.1}$$

where the product is taken over nonzero $u \in \mathbb{C}/L$ such that $Nu \in L$, with one u taken from each pair $u, -u$. Then $f_N(z) = F_N(\wp(z))$, where $F_N(x) \in \mathbb{C}[x]$ is a polynomial of degree $(N^2 - 1)/2$. The even elliptic function $f_N(z)$ has $N^2 - 1$ simple zeros and a single pole at 0 of order $N^2 - 1$. Its leading term at $z = 0$ is N/z^{N^2-1}.

(ii) N is even. Now let u range over $u \in \mathbb{C}/L$ such that $Nu \in L$ but u is *not* of order 2, i.e., $u \neq 0, \omega_1/2, \omega_2/2, (\omega_1 + \omega_2)/2$. Define $\tilde{f}_N(z)$ by the product in (8.1). Then $\tilde{f}_N(z) = F_N(\wp(z))$, where $F_N(x) \in \mathbb{C}[x]$ is a polynomial of degree $(N^2 - 4)/2$. The even elliptic function $\tilde{f}_N(z)$ has $N^2 - 4$ simple zeros and a single pole at 0 of order $N^2 - 4$. Its leading term at $z = 0$ is N/z^{N^2-4}.

If N is odd, the function $f_N(z)$ has the property that

$$f_N(z)^2 = N^2 \prod_{0 \neq u \in \mathbb{C}/L, Nu \in L} (\wp(z) - \wp(u)).$$

If N is even, then the function $f_N(z) \underset{\text{def}}{=} \frac{1}{2}\wp'(z)\tilde{f}_N(z)$ has the property that

$$\begin{aligned} f_N(z)^2 &= \tfrac{1}{4}\wp'(z)^2\tilde{f}_N(z)^2 \\ &= N^2(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3) \prod_{u \in \mathbb{C}/L, Nu \in L, 2u \notin L} (\wp(z) - \wp(u)) \\ &= N^2 \prod_{0 \neq u \in \mathbb{C}/L, Nu \in L} (\wp(z) - \wp(u)). \end{aligned}$$

We see that a point $(x, y) = (\wp(z), \wp'(z))$ has odd order N if and only if $F_N(x) = 0$. It has even order N if and only if either $y = 0$ (i.e., it is a point of order 2) or else $F_N(x) = 0$.

Because of Propositions 13 and 14, we know that any automorphism of $\mathbb{C}$ fixing $K = \mathbb{Q}(g_2, g_3)$ permutes the roots of F_N. Hence, the coefficients of F_N are in $K = \mathbb{Q}(g_2, g_3)$.

If we started with an elliptic curve not in Weierstrass form, say $y^2 = f(x) = ax^3 + bx^2 + cx + d$, and if we wanted to avoid using the $\wp$-function, then we could repeatedly apply the addition formulas (7.1)–(7.4) to compute the rational function of x and y which is the x-coordinate of NP, where $P = (x, y)$. We would simplify algebraically as we go, making use of the relation $y^2 = f(x)$, and would end up with an expression in the denominator which vanishes if and only if NP is the point at infinity, i.e., if and only if P has order N (recall: "order N" means "exact order N or a divisor of N").

What type of an expression would we have to get in the denominator of the x-coordinate of NP? Suppose, for example, that N is odd. Then this denominator would be an expression in $K[x, y]$ (with y occurring at most to the first power), where $K = \mathbb{Q}(a, b, c, d)$, which vanishes if and only if x is one of the $(N^2 - 1)/2$ values of x-coordinates of nontrivial points of order N. Thus, the expression must be a polynomial in x alone with $(N^2 - 1)/2$ roots. Similarly, we find that when N is even, this denominator has the form

$y \cdot$(polynomial in x alone), where the polynomial in $K[x]$ has $(N^2-4)/2$ roots.

It is important to note that the algebraic procedure described in the last two paragraphs applies for any elliptic curve $y^2=f(x)$ over any field K of characteristic $\neq 2$, not only over subfields of the complex numbers. Thus, for any K we end up with an expression in the denominator of the x-coordinate of NP that vanishes for at most N^2-1 values of (x, y).

For a general field K, however, we do not necessarily get exactly N^2-1 nontrivial points of order N. Of course, if K is not algebraically closed, the coordinates of points of order N may lie only in some extension of K. Moreover, if K has characteristic p, then there might be fewer points of order N for another reason: the leading coefficient of the expression in the denominator vanishes modulo p, and so the degree of that polynomial drops. We shall soon see examples where there are fewer than N^2 points of order N even if we allow coordinates in $K^{\mathrm{alg\,cl}}$.

This discussion has led to the following proposition.

Proposition 15. *Let $y^2=f(x)$ be an elliptic curve over any field K of characteristic not equal to 2. Then there are at most N^2 points of order N over any extension K' of K.*

Now let us turn our attention briefly to the case of K a finite field, in order to illustrate one application of Proposition 15. We shall later return to elliptic curves over finite fields in more detail.

Since there are only finitely many points in $\mathbb{P}^2_{\mathbb{F}_q}$ (namely, q^2+q+1), there are certainly only finitely many $\mathbb{F}_q$-points on an elliptic curve $y^2=f(x)$, where $f(x) \in \mathbb{F}_q[x]$. So the group of $\mathbb{F}_q$-points is a *finite abelian group.*

By the "type" of a finite abelian group, we mean its expression as a product of cyclic groups of prime power order. We list the orders of all of the cyclic groups that appear in the form: $2^{\alpha_2}, 2^{\beta_2}, 2^{\gamma_2}, \ldots, 3^{\alpha_3}, 3^{\beta_3}, 3^{\gamma_3}, \ldots, 5^{\alpha_5}, 5^{\beta_5}, \ldots$. But Proposition 15 implies that only certain types can occur in the case of the group of $\mathbb{F}_q$-points on $y^2=f(x)$. Namely, for each prime l there are at most two l-th power components l^{α_l}, l^{β_l}, since otherwise we would have more than l^2 points of order l. And of course $l^{\alpha_l+\beta_l}$ must equal the power of l dividing the order of the group.

As an example of how this works, let us consider the elliptic curve $y^2=x^3-n^2x$ over $K=\mathbb{F}_q$ (the finite field of $q=p^f$ elements), where we must assume that p does not divide $2n$. In the case when $q \equiv 3 \pmod 4$, it is particularly easy to count the number of $\mathbb{F}_q$-points.

Proposition 16. *Let $q=p^f$, $p \nmid 2n$. Suppose that $q \equiv 3 \pmod 4$. Then there are $q+1$ $\mathbb{F}_q$-points on the elliptic curve $y^2=x^3-n^2x$.*

PROOF. First, there are four points of order 2: the point at infinity, $(0, 0)$, and $(\pm n, 0)$. We now count all pairs (x, y) where $x \neq 0, n, -n$. We arrange these $q-3$ x's in pairs $\{x, -x\}$. Since $f(x)=x^3-n^2x$ is an odd function, and -1 is not a square in $\mathbb{F}_q$ (here's where we use the assumption that $q\equiv 3 \pmod 4$), it follows that exactly one of the two elements $f(x)$ and $f(-x)=-f(x)$ is a square in $\mathbb{F}_q$. (Recall: In the multiplicative group of a finite field, the squares are a subgroup of index 2, and so the product of two nonsquares is a square, while the product of a square and a nonsquare is a nonsquare.) Whichever of the pair x, $-x$ gives a square, we obtain exactly two points $(x, \pm\sqrt{f(x)})$ or else $(-x, \pm\sqrt{f(-x)})$. Thus, the $(q-3)/2$ pairs give us $q-3$ points. Along with the four points of order two, we have $q+1$ $\mathbb{F}_q$-points in all, as claimed. □

Notice that when $q\equiv 3 \pmod 4$, the number of $\mathbb{F}_q$-points on the elliptic curve $y^2=x^3-n^2x$ does not depend on n. This is not true if $q\equiv 1 \pmod 4$.

As an example, Proposition 16 tells us that for $q=7^3$ there are $344=2^3\cdot 43$ points. Since there are four points of order two, the type of the group of $\mathbb{F}_{343}$-points on $y^2=x^3-n^2x$ must be $(2, 2^2, 43)$.

As a more interesting example, let $q=p=107$. Then there are $108=2^2\cdot 3^3$ points. The group is either of type $(2, 2, 3^3)$ or of type $(2, 2, 3, 3^2)$. To resolve the question, we must determine whether there are 3 or 9 points of order three. (There must be nontrivial points of order 3, since 3 divides the order of the group.) Recall the equation for the x-coordinates of points of order three (see Problem 4 of §7): $-3x^4+6n^2x^2+n^4=0$, i.e., $x=\pm n\sqrt{1\pm 2\sqrt{3}/3}$. Then the corresponding y-coordinates are found by taking $\pm\sqrt{f(x)}$. We want to know how many of these points have both coordinates in $\mathbb{F}_{107}$, rather than an extension of $\mathbb{F}_{107}$. We could compute explicitly, using $\sqrt{3}=\pm 18$ in $\mathbb{F}_{107}$, so that $x=\pm\sqrt{13}$, $\pm\sqrt{-11}$, etc. But even before doing those computations, we can see that not all 9 points have coordinates in $\mathbb{F}_{107}$. This is because, if (x, y) is in $\mathbb{F}_{107}$, then $(-x, \sqrt{-1}y)$ is another point of order three, and its coordinates are not in $\mathbb{F}_{107}$. Thus, there are only 3 points of order three, and the type of the group is $(2, 2, 3^3)$.

Notice that if K is any field of characteristic 3, then the group of K-points has *no* nontrivial point of order three, because $-3x^4+6n^2x^2+n^4=n^4\neq 0$. This is an example of the "dropping degree" phenomenon mentioned above. It turns out that the same is true for any $p\equiv 3 \pmod 4$, namely, there are no points of order p over a field of characteristic p in that case. This is related to the fact that such p remain prime in the ring of Gaussian integers $\mathbb{Z}[i]$, a ring which is intimately related to our particular elliptic curve (see Problem 13 of §6). But we will not go further into that now.

Problems

1. For the elliptic curve $y^2=4x^3-g_2x-g_3$, express $\wp(Nz)$ as a rational function of $\wp(z)$ when $N=2$.

2. Let $f_N(z)$ be the elliptic functions defined above. Express $f_3(z)$ as a polynomial in $\wp(z)$.

9. Each of the following points has finite order N on the given elliptic curve. In each case, find its order.
   (a) $P = (0, 4)$ on $y^2 = 4x^3 + 16$
   (b) $P = (2, 8)$ on $y^2 = 4x^3 + 16x$
   (c) $P = (2, 3)$ on $y^2 = x^3 + 1$
   (d) $P = (3, 8)$ on $y^2 = x^3 - 43x + 166$
   (e) $P = (3, 12)$ on $y^2 = x^3 - 14x^2 + 81x$
   (f) $P = (0, 0)$ on $y^2 + y = x^3 - x^2$
   (g) $P = (1, 0)$ on $y^2 + xy + y = x^3 - x^2 - 3x + 3$.

§9. Points over finite fields, and the congruent number problem

We have mainly been interested in elliptic curves E over $\mathbb{Q}$, particularly the elliptic curve $y^2 = x^3 - n^2x$, which we shall denote E_n. But if K is any field whose characteristic p does not divide $2n$, the same equation (where we consider n modulo p) is an elliptic curve over K. We shall let $E_n(K)$ denote the set of points on the curve with coordinates in K. Thus, Proposition 16 in the last section can be stated: If $q \equiv 3 \pmod 4$, then $\# E_n(\mathbb{F}_q) = q + 1$.

The elliptic curve E_n considered as being defined over $\mathbb{F}_p$, is called the "reduction" modulo p, and we say that E_n has "good reduction" if p does not divide $2n$, i.e., if $y^2 = x^3 - n^2x$ gives an elliptic curve over $\mathbb{F}_p$. More generally, if $y^2 = f(x)$ is an elliptic curve E defined over an algebraic number field, and if $\mathfrak{p}$ is a prime ideal of the number field which does not divide the denominators of the coefficients of $f(x)$ or the discriminant of $f(x)$, then by reduction modulo $\mathfrak{p}$ we obtain an elliptic curve defined over the (finite) residue field of $\mathfrak{p}$.

At first glance, it may seem that the elliptic curves over finite fields—which lead only to finite abelian groups—are not a serious business, and that reduction modulo p is a frivolous game that will not help us in our original objective of studying $\mathbb{Q}$-points on $y^2 = x^3 - n^2x$. However, this is far from the case. Often information from the various reductions modulo p can be pieced together to yield information about the $\mathbb{Q}$-points. This is usually a subtle and difficult procedure, replete with conjectures and unsolved problems. However, there is one result of this type which is simple enough to give right now. Namely, we shall use reduction modulo p for various primes p to determine the torsion subgroup of $E_n(\mathbb{Q})$, the group of $\mathbb{Q}$-points on $y^2 = x^3 - n^2x$.

In any abelian group, the elements of finite order form a subgroup, called the "torsion subgroup". For example, the group $E(\mathbb{C})$ of complex points on an elliptic curve is isomorphic to $\mathbb{C}/L$, which for any lattice L is isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ (see Problem 2 of §I.5). Its torsion subgroup corresponds to the subgroup $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$, i.e., in $\mathbb{C}/L$ it consists of all rational linear combinations of ω_1 and ω_2.

A basic theorem of Mordell states that the group $E(\mathbb{Q})$ of $\mathbb{Q}$-points on an elliptic curve E defined over $\mathbb{Q}$ is a finitely generated abelian group. This means that (1) the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is finite, and (2) $E(\mathbb{Q})$ is isomorphic to the direct sum of $E(\mathbb{Q})_{\text{tors}}$ and a finite number of copies of $\mathbb{Z}$: $E(\mathbb{Q}) \approx E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$. The nonnegative integer r is called the "rank" of $E(\mathbb{Q})$. It is greater than zero if and only if E has infinitely many $\mathbb{Q}$-points. Mordell's theorem is also true, by the way, if $\mathbb{Q}$ is replaced by any algebraic number field. This generalization, proved by Andre Weil, is known as the Mordell–Weil theorem. We shall not need this theorem for our purposes, even in the form proved by Mordell. For a proof, the reader is referred to Husemuller's forthcoming book on elliptic curves or else to [Lang 1978b].

We shall now prove that the only rational points of finite order on E_n are the four points of order 2: 0 (the point at infinity), $(0, 0)$, $(\pm n, 0)$.

Proposition 17. $\# E_n(\mathbb{Q})_{\text{tors}} = 4$.

PROOF. The idea of the proof is to construct a group homomorphism from $E_n(\mathbb{Q})_{\text{tors}}$ to $E_n(\mathbb{F}_p)$ which is injective for most p. That will imply that the order of $E_n(\mathbb{Q})_{\text{tors}}$ divides the order of $E_n(\mathbb{F}_p)$ for such p. But no number greater than 4 could divide all such numbers $\# E_n(\mathbb{F}_p)$, because we at least know that $\# E_n(\mathbb{F}_p)$ runs through all integers of the form $p + 1$ for p a prime congruent to 3 modulo 4 (see Proposition 16).

We begin the proof of Proposition 17 by constructing the homomorphism from the group of $\mathbb{Q}$-points on E_n to the group of $\mathbb{F}_p$-points. More generally, we simply construct a map from $\mathbb{P}^2_{\mathbb{Q}}$ to $\mathbb{P}^2_{\mathbb{F}_p}$. In what follows, we shall always choose a triple (x, y, z) for a point in $\mathbb{P}^2_{\mathbb{Q}}$ in such a way that x, y, and z are integers with no common factor. Up to multiplication by ± 1, there is a unique such triple in the equivalence class. For any fixed prime p, we define the image $\bar{P}$ of $P = (x, y, z) \in \mathbb{P}^2_{\mathbb{Q}}$ to be the point $\bar{P} = (\bar{x}, \bar{y}, \bar{z}) \in \mathbb{P}^2_{\mathbb{F}_p}$, where the bar denotes reduction of an integer modulo p. Note that $\bar{P}$ is not the identically zero triple, because p does not divide all three integers x, y, z. Also note that we could have replaced the triple (x, y, z) by any multiple by an integer prime to p without affecting $\bar{P}$.

It is easy to see that if $P = (x, y, z)$ happens to be in $E_n(\mathbb{Q})$, i.e., if $y^2 z = x^3 - n^2 x z^2$, then $\bar{P}$ is in $E_n(\mathbb{F}_p)$. Moreover, the image of $P_1 + P_2$ under this map is $\bar{P}_1 + \bar{P}_2$, because it makes no difference whether we use the addition formulas (7.1)–(7.4) to find the sum and then reduce mod p, or whether we first reduce mod p and then use the addition formulas. In other words, our map is a homomorphism from $E_n(\mathbb{Q})$ to $E_n(\mathbb{F}_p)$, for any prime p not dividing $2n$.

We now determine when this map is not injective, i.e., when two points $P_1 = (x_1, y_1, z_1)$ and $P_2 = (x_2, y_2, z_2)$ in $\mathbb{P}^2_{\mathbb{Q}}$ have the same image $\bar{P}_1 = \bar{P}_2$ in $\mathbb{P}^2_{\mathbb{F}_p}$.

Lemma. $\bar{P}_1 = \bar{P}_2$ *if and only if the cross-product of* P_1 *and* P_2 *(considered as vectors in* $\mathbb{R}^3$*) is divisible by* p*, i.e., if and only if* p *divides* $y_1 z_2 - y_2 z_1$, $x_2 z_1 - x_1 z_2$, *and* $x_1 y_2 - x_2 y_1$.

Proof of Lemma. First suppose that p divides the cross-product. We consider two cases:

(i) p divides x_1. Then p divides x_2z_1 and x_2y_1, and therefore divides x_2, because it cannot divide x_1, y_1 and z_1. Suppose, for example, that $p \nmid y_1$ (an analogous argument will apply if $p \nmid z_1$). Then $\bar{P}_2 = (0, \bar{y}_1\bar{y}_2, \bar{y}_1\bar{z}_2) = (0, \bar{y}_1\bar{y}_2, \bar{y}_2\bar{z}_1) = (0, \bar{y}_1, \bar{z}_1) = \bar{P}_1$ (where we have used the fact that p divides $y_1z_2 - y_2z_1$).

(ii) p does not divide x_1. Then $\bar{P}_2 = (\bar{x}_1\bar{x}_2, \bar{x}_1\bar{y}_2, \bar{x}_1\bar{z}_2) = (\bar{x}_1\bar{x}_2, \bar{x}_2\bar{y}_1, \bar{x}_2\bar{z}_1) = (\bar{x}_1, \bar{y}_1, \bar{z}_1) = \bar{P}_1$.

Conversely, suppose that $\bar{P}_1 = \bar{P}_2$. Without loss of generality, suppose that $p \nmid x_1$ (an analogous argument will apply if $p \nmid y_1$ or $p \nmid z_1$). Then, since $\bar{P}_1 = \bar{P}_2 = (\bar{x}_2, \bar{y}_2, \bar{z}_2)$, we also have $p \nmid x_2$. Hence, $(\bar{x}_1\bar{x}_2, \bar{x}_1\bar{y}_2, \bar{x}_1\bar{z}_2) = \bar{P}_2 = \bar{P}_1 = (\bar{x}_2\bar{x}_1, \bar{x}_2\bar{y}_1, \bar{x}_2\bar{z}_1)$. Since the first coordinates are the same, these two points can be equal only if the second and third coordinates are equal, i.e., if p divides $x_1y_2 - x_2y_1$ and $x_1z_2 - x_2z_1$. Finally, we must show that p divides $y_1z_2 - y_2z_1$. If both y_1 and z_1 are divisible by p, then this is trivial. Otherwise, the conclusion will follow by repeating the above argument with x_1, x_2 replaced by y_1, y_2 or by z_1, z_2. This concludes the proof of the lemma.

We are now ready to prove Proposition 17. Suppose that the proposition is false, i.e., that $E_n(\mathbb{Q})$ contains a point of finite order greater than 2. Then either it contains an element of odd order, or else the group of points of order 4 (or a divisor of 4) contains either 8 or 16 elements. In either case we have a subgroup $S = \{P_1, P_2, \ldots, P_m\} \subset E_n(\mathbb{Q})_{\text{tors}}$, where $m = \#S$ is either 8 or else an odd number.

Let us write all of the points P_i, $i = 1, \ldots, m$, in the form in the lemma: $P_i = (x_i, y_i, z_i)$. For each pair of points P_i, P_j, consider the cross-product vector $(y_iz_j - y_jz_i, x_jz_i - x_iz_j, x_iy_j - x_jy_i) \in \mathbb{R}^3$. Since P_i and P_j are distinct points, as vectors in $\mathbb{R}^3$ they are not proportional, and so their cross-product is not the zero vector. Let n_{ij} be the greatest common divisor of the coordinates of this cross-product. According to the lemma, the points P_i and P_j have the same image $\bar{P}_i = \bar{P}_j$ in $E_n(\mathbb{F}_p)$ if and only if p divides n_{ij}. Thus, if p is a prime of good reduction which is greater than all of the n_{ij}, it follows that all images are distinct, i.e., the map reduction modulo p gives an *injection* of S in $E_n(\mathbb{F}_p)$.

But this means that for all but finitely many p the number m must divide $\#E_n(\mathbb{F}_p)$, because the image of S is a subgroup of order m. Then for all but finitely many primes congruent to 3 modulo 4, by Proposition 16 we must have $p \equiv -1 \pmod{m}$. But this contradicts Dirichlet's theorem on primes in an arithmetic progression. Namely, if $m = 8$ this would mean that there are only finitely many primes of the form $8k + 3$. If m is odd, it would mean that there are only finitely many primes of the form $4mk + 3$ (if $3 \nmid m$), and that there are only finitely many primes of the form $12k + 7$ if $3 | m$. In all cases, Dirichlet's theorem tells us that there are infinitely many primes of the given type. This concludes the proof of Proposition 17. □

Notice how the technique of reduction modulo p (more precisely, the use of Proposition 16 for infinitely many primes p) led to a rather painless proof of a strong fact: There are no "non-obvious" rational points of finite order on E_n. As we shall soon see, this fact is useful for the congruent number problem. But a far more interesting and difficult question is the existence of points of infinite order, i.e., whether the rank r of $E_n(\mathbb{Q})$ is nonzero. As we shall see in a moment, that question is actually *equivalent* to the question of whether or not n is a congruent number.

So it is natural to ask whether mod p information can somehow be put together to yield information about the rank of an elliptic curve. This subtle question will lead us in later chapters to consideration of the Birch–Swinnerton-Dyer conjecture for elliptic curves.

For further general motivational discussion of elliptic curves over finite fields, see [Koblitz 1982].

We now prove the promised corollary of Proposition 17.

Proposition 18. *n is a congruent number if and only if $E_n(\mathbb{Q})$ has nonzero rank r.*

PROOF. First suppose that n is a congruent number. At the beginning of §2, we saw that the existence of a right triangle with rational sides and area n leads to a rational point on E_n whose x-coordinate lies in $(\mathbb{Q}^+)^2$. Since the x-coordinates of the three nontrivial points of order 2 are 0, $\pm n$, this means that there must be a rational point not of order 2. By Proposition 17, such a point has infinite order, i.e., $r \geq 1$.

Conversely, suppose that P is a point of infinite order. By Problem 2(c) of §I.7, the x-coordinate of the point $2P$ is the square of a rational number having even denominator. Now by Proposition 2 in §I.2, the point $2P$ corresponds to a right triangle with rational sides and area n (under the correspondence in Proposition 1). This proves Proposition 18. □

Notice the role of Proposition 17 in the proof of Proposition 18. It tells us that the only way to get nontrivial rational points of the form $2P$ is from points of infinite order. Let $2E_n(\mathbb{Q})$ denote the subgroup of $E_n(\mathbb{Q})$ consisting of the doubles of rational points. Then Proposition 17 is equivalent to the assertion that $2E_n(\mathbb{Q})$ is a torsion-free abelian group, i.e., it is isomorphic to a certain number of copies (namely, r) of $\mathbb{Z}$. The set $2E_n(\mathbb{Q}) - 0$ (0 denotes the point at infinity) is empty if and only if $r = 0$.

We saw that points in the set $2E_n(\mathbb{Q}) - 0$ lead to right triangles with rational sides and area n under the correspondence in Proposition 1. It is natural to ask whether all points meeting the conditions in Proposition 2, i.e., corresponding to triangles, are doubles of points. We now prove that the answer is yes. At the same time, we give another verification of Proposition 18 (not relying on the homework problem 2(c) of §I.7).

Proposition 19. *There is a one-to-one correspondence between right triangles with rational sides $X < Y < Z$ and n, and pairs of points $(x, \pm y) \in$*

$2E_n(\mathbb{Q}) - 0$. *The correspondence is*:

$$(x, \pm y) \mapsto \sqrt{x+n} - \sqrt{x-n}, \sqrt{x+n} + \sqrt{x-n}, 2\sqrt{x};$$
$$X, Y, Z \mapsto (Z^2/4, \pm(Y^2 - X^2)Z/8).$$

In light of Proposition 1 of §I.1, Proposition 19 is an immediate consequence of the following general characterization of the doubles of points on elliptic curves.

Proposition 20. *Let E be the elliptic curve* $y^2 = (x - e_1)(x - e_2)(x - e_3)$ *with* $e_1, e_2, e_3 \in \mathbb{Q}$. *Let* $P = (x_0, y_0) \in E(\mathbb{Q}) - 0$. *Then* $P \in 2E(\mathbb{Q}) - 0$ *if and only if* $x_0 - e_1, x_0 - e_2, x_0 - e_3$ *are all squares of rational numbers.*

Proof. We first note that, without loss of generality, we may assume that $x_0 = 0$. To see this, make the change of variables $x' = x - x_0$. By simply translating the geometrical picture for adding points, we see that the point $P' = (0, y_0)$ on the curve E' with equation $y^2 = (x - e_1')(x - e_2')(x - e_3')$, where $e_i' = e_i - x_0$, is in $2E'(\mathbb{Q}) - 0$ if and only if our original P were in $2E(\mathbb{Q}) - 0$. And trivially, the $x_0 - e_i$ are all squares if and only if the $(0 - e_i')$ are. So it suffices to prove the proposition with $x_0 = 0$.

Next, note that if there exists $Q \in E(\mathbb{Q})$ such that $2Q = P$, then there are exactly four such points $Q, Q_1, Q_2, Q_3 \in E(\mathbb{Q})$ with $2Q_i = P$. To obtain Q_i, simply add to Q the point of order two $(e_i, 0) \in E(\mathbb{Q})$ (see Problem 5 in §I.7).

Choose a point $Q = (x, y)$ such that $2Q = P = (0, y_0)$. We want to find conditions for the coordinates of one such Q (and hence all four) to be rational. Now a point Q on the elliptic curve satisfies $2Q = P$ if and only if the tangent line to the curve at Q passes through $-P = (0, -y_0)$. That is, the four possible points Q are obtained geometrically by drawing the four distinct lines emanating from $-P$ which are tangent to the curve.

We readily verify that the coordinates (x, y) are rational if and only if the slope of the line from $-P$ to Q is rational. The "only if" is immediate. Conversely, if this slope m is rational, then the x-coordinate of Q, which is the double root of the cubic $(mx - y_0)^2 = (x - e_1)(x - e_2)(x - e_3)$, must also be rational. (Explicitly, $x = (e_1 + e_2 + e_3 + m^2)/2$.) In this case the y-coordinate of Q is also rational: $y = mx - y_0$. Thus, we want to know when one (and hence all four) slopes of lines from $-P$ which are tangent to E are rational.

A number $m \in \mathbb{C}$ is the slope of a line from $-P$ which is tangent to E if and only if the following equation has a double root:

$$(mx - y_0)^2 = (x - e_1)(x - e_2)(x - e_3) = x^3 + ax^2 + bx + c, \quad (9.1)$$

with

$$a = -e_1 - e_2 - e_3, \qquad b = e_1e_2 + e_1e_3 + e_2e_3, \qquad c = -e_1e_2e_3 = y_0^2, \quad (9.2)$$

w' ` last equality $c = y_0^2$ comes from the fact that $(0, y_0)$ is on the curve

$y^2 = x^3 + ax^2 + bx + c$. Now if we simplify (9.1) and factor out x, our condition becomes: the following quadratic equation has a double root:

$$x^2 + (a - m^2)x + (b + 2my_0) = 0.$$

This is equivalent to saying that its discriminant must vanish, i.e.,

$$(a - m^2)^2 - 4(b + 2my_0) = 0. \tag{9.3}$$

Thus, our task is to determine when one (and hence all four) roots of this quartic polynomial in m are rational.

We want to find a condition in terms of the e_i's (namely, our claim is that an equivalent condition is: $-e_i \in \mathbb{Q}^2$). In (9.3), the a and b are symmetric polynomials in the e_i, but the y_0 is not. However, y_0 is a symmetric polynomial in the $\sqrt{e_i}$. That is, we introduce f_i satisfying $f_i^2 = -e_i$. There are two possible choices for f_i, unless $e_i = 0$. Choose the f_i in any of the possible ways, subject to the condition that $y_0 = f_1 f_2 f_3$. If all of the e_i are nonzero, this means that the sign of f_1 and f_2 are arbitrary, and then the sign of f_3 is chosen so that y_0 and $f_1 f_2 f_3$ are the same square root of $-e_1 e_2 e_3$. If, say, $e_3 = 0$, then either choice can be made for the sign of f_1, f_2, and of course $f_3 = 0$. In all cases there are four possible choices of the f_i's consistent with the requirement that $y_0 = f_1 f_2 f_3$. Once we fix one such choice f_1, f_2, f_3, we can list the four choices as follows (here we're supposing that e_1 and e_2 are nonzero):

$$f_1, f_2, f_3; \qquad f_1, -f_2, -f_3; \qquad -f_1, f_2, -f_3; \qquad -f_1, -f_2, f_3. \tag{9.4}$$

The advantage of going from the e_i's to the f_i's is that now the coefficients of our equation (9.3) are symmetric functions of f_1, f_2, f_3. More precisely, if we set $s_1 = f_1 + f_2 + f_3$, $s_2 = f_1 f_2 + f_1 f_3 + f_2 f_3$, $s_3 = f_1 f_2 f_3$, the elementary symmetric functions, then

$$\begin{aligned} a &= f_1^2 + f_2^2 + f_3^2 = s_1^2 - 2s_2; \\ b &= f_1^2 f_2^2 + f_1^2 f_3^2 + f_2^2 f_3^2 = s_2^2 - 2s_1 s_3; \\ y_0 &= s_3. \end{aligned}$$

Thus, equation (9.3) becomes

$$\begin{aligned} 0 &= (m^2 - s_1^2 + 2s_2)^2 - 4(s_2^2 - 2s_1 s_3 + 2ms_3) \\ &= (m^2 - s_1^2)^2 + 4s_2(m^2 - s_1^2) - 8s_3(m - s_1). \end{aligned} \tag{9.5}$$

We see at a glance that the polynomial in (9.5) is divisible by $m - s_1$, i.e., $m = s_1 = f_1 + f_2 + f_3$ is a root. Since we could have made three other choices for the signs of the f_i, the other roots must correspond to these choices, i.e., the four solutions of equation (9.3) are:

$$\begin{aligned} m_1 &= f_1 + f_2 + f_3, \qquad & m_2 &= f_1 - f_2 - f_3, \\ m_3 &= -f_1 + f_2 - f_3, \qquad & m_4 &= -f_1 - f_2 + f_3. \end{aligned} \tag{9.6}$$

We want to know whether the four values in (9.6) are rational. Clearly, if all of the f_i are rational, then so are the m_i. Conversely, suppose the m_i are rational. Then $f_1 = (m_1 + m_2)/2, f_2 = (m_1 + m_3)/2$, and $f_3 = (m_1 + m_4)/2$ are rational. The conclusion of this string of equivalent conditions is: the coordinates (x, y) of a point Q for which $2Q = P$ are rational if and only if the $f_i = \sqrt{-e_i}$ are rational. This proves Proposition 20. □

Finally, we note that Proposition 20 holds with $\mathbb{Q}$ replaced by any field K not of characteristic 2. Essentially the same proof applies. (We need only take care to use algebraic rather than geometric arguments, for example, when reducing to the case $P = (0, y_0)$.)

Problems

1. Prove that for f odd, any $\mathbb{F}_{p^f}$-point of order 3 on the elliptic curve E_n: $y^2 = x^3 - n^2x$ is actually an $\mathbb{F}_p$-point; prove that there are at most three such points if $p \equiv 3 \pmod 4$; and find a fairly good sufficient condition on p and f which ensures nine $\mathbb{F}_{p^f}$-points of order 3.

2. For each of the following values of q, find the order and type of the group of $\mathbb{F}_q$-points on the elliptic curve $E_1 : y^2 = x^3 - x$. In all cases, find the type directly, if necessary checking how many points have order 3 or 4. Don't "peek" at the later problems.
   (a) All odd primes from 3 to 23.
   (b) 9
   (c) 27
   (d) 71
   (e) 11^3.

3. Find the type of the group of $\mathbb{F}_p$-points on the elliptic curve E_5: $y^2 = x^3 - 25x$ for all odd primes p of good reduction up to 23.

4. Prove that for $a \in \mathbb{Q}$ the equation $y^2 = x^3 - a$ determines an elliptic curve over any field K whose characteristic p does not divide 6 or the numerator or denominator of a; and that it has $q + 1$ $\mathbb{F}_q$-points if $q \equiv 2 \pmod 3$.

5. Prove that there are exactly 3 $\mathbb{F}_q$-points of order 3 on the elliptic curve in Problem 4 if $q \equiv 2 \pmod 3$.

6. For all odd primes p from 5 to 23, find the order and type of the group of $\mathbb{F}_p$-points on the elliptic curve $y^2 = x^3 - 1$.

7. Prove that the torsion subgroup of the group of $\mathbb{Q}$-points on the elliptic curve $y^2 = x^3 - a$ has order at most 6, and that its order is equal to:
   (a) 6 if $a = -b^6$ for some $b \in \mathbb{Q}$;
   (b) 2 if $a = c^3$ for some $c \in \mathbb{Q}$ with c not of the form $-b^2$;
   (c) 3 if either $a = -d^2$ for some $d \in \mathbb{Q}$ with d not of the form b^3, or if $a = 432b^6$ for some $b \in \mathbb{Q}$;
   (d) 1 otherwise.

8. Show that the correspondence constructed in Problem 2 of §I.2 gives a one-to-one correspondence between right triangles as in Proposition 19 and pairs $\pm P$ of