Appendix A

Number Theory

Basic results

Let n be a positive integer and let $\mathbf{Z}_n$ be the set of integers mod n. It is a group with respect to addition. We can represent the elements of $\mathbf{Z}_n$ by the numbers $0, 1, 2, \ldots, n-1$. Let

$$\mathbf{Z}_n^\times = \{a \,|\, 1 \le a \le n,\ \gcd(a,n) = 1\}.$$

Then $\mathbf{Z}_n^\times$ is a group with respect to multiplication mod n.

Let $a \in \mathbf{Z}_n^\times$. The **order of** a **mod** n is the smallest integer $k > 0$ such that $a^k \equiv 1 \pmod{n}$. The order of a mod n divides $\phi(n)$, where ϕ is the Euler ϕ-function.

Let p be a prime and let $a \in \mathbf{Z}_p^\times$. The order of a mod p divides $p-1$. A **primitive root** mod p is an integer g such that the order of g mod p equals $p-1$. If g is a primitive root mod p, then every integer is congruent mod p to 0 or to a power of g. For example, 3 is a primitive root mod 7 and

$$\{1, 3, 9, 27, 81, 243\} \equiv \{1, 3, 2, 6, 4, 5\} \pmod{7}.$$

There are $\phi(p-1)$ primitive roots mod p. In particular, a primitive root mod p always exists, so $\mathbf{Z}_p^\times$ is a cyclic group.

There is an easy criterion for deciding whether g is a primitive root mod p, assuming we know the factorization of $p-1$: If $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all primes $q | p-1$, then g is a primitive root mod p. This can be proved by noting that if g is not a primitive root, then its order is a proper divisor of $p-1$, hence divides $(p-1)/q$ for some prime q.

One way to find a primitive root for p, assuming the factorization of $p-1$ is known, is simply to test the numbers 2, 3, 5, 6, ... successively until a primitive root is found. Since there are many primitive roots, one should be found fairly quickly in most cases.

A very useful result in number theory is the following.

THEOREM A.1 (Chinese Remainder Theorem)
Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ when $i \neq j$. Let $a_1, a_2, \ldots, a_r$ be integers. Then there exists an x such that

$$x \equiv a_i \pmod{n_i} \quad \text{for all } i.$$

The integer x is uniquely determined mod $n_1 n_2 \cdots n_r$.

For example, let $n_1 = 4$, $n_2 = 3$, $n_3 = 5$ and let $a_1 = 1$, $a_2 = 2$, $a_3 = 3$. Then $x = 53$ is a solution to the simultaneous congruences

$$x \equiv 1 \pmod 4, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5,$$

and any solution x satisfies $x \equiv 53 \pmod{60}$.

Another way to state the Chinese Remainder Theorem is to say that if $\gcd(n_i, n_j) = 1$ for $i \neq j$, then

$$\mathbf{Z}_{n_1 n_2 \cdots n_r} \simeq \mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_r}$$

(see Appendix B for the definition of $\oplus$). This is an isomorphism of additive groups. It is also an isomorphism of rings.

p-adic numbers

Let p be a prime number and let x be a nonzero rational number. Write

$$x = p^r \frac{a}{b},$$

where a, b are integers such that $p \nmid ab$. Then r is called the **p-adic valuation** of x and is denoted by

$$r = v_p(x).$$

Define $v_p(0) = \infty$. (The p-adic valuation is discussed in more detail in Sections 5.4 and 8.1.) The **p-adic absolute value** of x is defined to be

$$|x|_p = p^{-r}.$$

Define $|0|_p = 0$.

For example,

$$\left|\frac{12}{35}\right|_2 = \frac{1}{4}, \quad \left|\frac{11}{250}\right|_5 = 125, \quad \left|\frac{1}{2} - 41\right|_3 = \frac{1}{81}.$$

The last example says that $1/2$ and 41 are close 3-adically. Note that two integers are close p-adically if and only if they are congruent mod a large power of p.

The **p-adic integers** are most easily regarded as sums of the form

$$\sum_{n=0}^{\infty} a_n p^n, \quad a_n \in \{0, 1, 2, \ldots, p-1\}.$$

Such infinite sums do not converge in the real numbers, but they do make sense with the p-adic absolute value since $|a_n p^n|_p \to 0$ as $n \to \infty$.

Arithmetic operations are carried out just as with finite sums. For example, in the 3-adic integers,

$$\begin{aligned}(1 + 2 \cdot 3 + 0 \cdot 3^2 + \cdots) + (1 + 2 \cdot 3 + 1 \cdot 3^2 + \cdots) &= 2 + 4 \cdot 3 + 1 \cdot 3^2 + \cdots \\ &= 2 + 1 \cdot 3 + 2 \cdot 3^2 + \cdots\end{aligned}$$

(where we wrote $4 = 1 + 3$ and regrouped, or "carried," to obtain the last expression). If

$$x = a_k p^k + a_{k+1} p^{k+1} + \cdots$$

with $a_k \neq 0$, then

$$-x = (p - a_k) p^k + (p - 1 - a_{k+1}) p^{k+1} + (p - 1 - a_{k+2}) p^{k+2} + \cdots \quad \text{(A.1)}$$

(use the fact that $p^{k+1} + (p-1)p^{k+1} + (p-1)p^{k+2} + \cdots = 0$ because the sum telescopes, so all the terms cancel). Therefore, p-adic integers have additive inverses. It is not hard to show that the p-adic integers form a ring.

Any rational number with denominator not divisible by p is a p-adic integer. For example, in the 3-adics,

$$\frac{1}{2} = \frac{-1}{1-3} = -(1 + 3 + 3^2 + \cdots) = 2 + 3 + 3^2 + \cdots,$$

where we used (A.1) for the last equality. In fact, it can be shown that if $x = \sum_{n=0}^{\infty} a_n p^n$ is a p-adic integer with $a_0 \neq 0$, then $1/x$ is a p-adic integer.

The **p-adic rationals**, which we denote by $\mathbf{Q}_p$, are sums of the form

$$y = \sum_{n=m}^{\infty} a_n p^n, \quad \text{(A.2)}$$

with m positive or negative or zero and with $a_n \in \{0, 1, \ldots, p-1\}$. If $y \in \mathbf{Q}_p$, then $p^k y$ is a p-adic integer for some integer k. The p-adic rationals form a field, and every rational number lies in $\mathbf{Q}_p$. If $a_m \neq 0$ in (A.2), then we define

$$v_p(y) = m, \quad |y|_p = p^{-m}.$$

This agrees with the definitions of the p-adic valuation and absolute value defined above when y is a rational number.

Another way to look at p-adic integers is the following. Consider sequences of integers $x_1, x_2, \ldots$ such that

$$x_m \equiv x_{m+1} \pmod{p^m} \quad \text{(A.3)}$$

for all $m \geq 1$. Since $x_m \equiv x_k \pmod{p^m}$ for all $k \geq m$, the base p expansions for all x_k with $k \geq m$ must agree through the p^{m-1} term. Therefore, the sequence of integers x_m determines an expression of the form

$$\sum_{n=0}^{\infty} a_n p^n,$$

where

$$x_m \equiv \sum_{n=0}^{m-1} a_n p^n \pmod{p^m}$$

for all m. In other words, the sequence of integers determines a p-adic integer. Conversely, the partial sums of a p-adic integer determine a sequence of integers satisfying (A.3).

Let's use these ideas to show that -1 is a square in the 5-adic integers. Let $x_1 = 2$, so

$$x_1^2 \equiv -1 \pmod{5}.$$

Suppose we have defined x_m such that

$$x_m^2 \equiv -1 \pmod{5^m}.$$

Let $x_{m+1} = x_m + b5^m$, where

$$b \equiv \frac{-1 - x_m^2}{2 \cdot 5^m x_m} \pmod{5}.$$

Note that $x_m^2 \equiv -1 \pmod{5^m}$ implies that the right side of this last congruence is defined mod 5. A quick calculation shows that

$$x_{m+1}^2 \equiv -1 \pmod{5^{m+1}}.$$

Since (A.3) is satisfied, there is a 5-adic integer x with $x \equiv x_m \pmod{5^m}$ for all m. Moreover,

$$x^2 \equiv -1 \pmod{5^m}$$

for all m. This implies that $x^2 = -1$.

In general, this procedure leads to the following very useful result.

THEOREM A.2 (Hensel's Lemma)
Let $f(X)$ be a polynomial with coefficients that are p-adic integers and suppose x_1 is an integer such that

$$f(x_1) \equiv 0 \pmod{p}.$$

If

$$f'(x_1) \not\equiv 0 \pmod{p},$$

then there exists a p-adic integer x with $x \equiv x_1 \pmod{p}$ *and*

$$f(x) = 0.$$

COROLLARY A.3
Let p be an odd prime and suppose b is a p-adic integer that is a nonzero square mod p. Then b is the square of a p-adic integer.

The corollary can be proved by exactly the same method that was used to prove that -1 is a square in the 5-adic integers. The corollary can also be deduced from the theorem as follows. Define $f(X) = X^2 - b$ and let $x_1^2 \equiv b \pmod{p}$. Then $f(x_1) \equiv 0 \pmod{p}$ and

$$f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$$

since p is odd and $x_1 \not\equiv 0$ by assumption. Hensel's Lemma shows that there is a p-adic integer x with $f(x) = 0$. This means that $x^2 = b$, as desired.

When $p = 2$, the corollary is not true. For example, 5 is a square mod 2 but is not a square mod 8, hence is not a 2-adic square. However, the inductive procedure used above yields the following:

PROPOSITION A.4
If b is a 2-adic integer such that $b \equiv 1 \pmod{8}$ *then b is the square of a 2-adic integer.*

Appendix B

Groups

Basic definitions

Since most of the groups in this book are additive abelian groups, we'll use additive notation for the group operations in this appendix. Therefore, a group G has a binary operation $+$ that is associative. There is an additive identity that we'll call 0 satisfying

$$0 + g = g + 0 = g$$

for all $g \in G$. Each $g \in G$ is assumed to have an additive inverse $-g$ satisfying

$$(-g) + g = g + (-g) = 0.$$

If n is a positive integer, we let

$$ng = g + g + \cdots + g \quad (n \text{ summands}).$$

If $n < 0$, we let $ng = -(|n|g) = -(g + \cdots + g)$.

Almost all of the groups in this book are abelian, which means that $g + h = h + g$ for all $g, h \in G$.

If G is a finite group, the **order** of G is the number of elements in G. The **order of an element** $g \in G$ is the smallest integer $k > 0$ such that $kg = 0$. If k is the order of g, then

$$ig = jg \iff i \equiv j \pmod{k}.$$

The basic result about orders is the following.

THEOREM B.1 (Lagrange's Theorem)
Let G be a finite group.

1. *Let H be a subgroup of G. Then the order of H divides the order of G.*
2. *Let $g \in G$. Then the order of g divides the order of G.*

The ratio $\#G/\#H$ is called the **index** of H in G. More generally, the index of a (possibly infinite) subgroup H in a group G is the smallest number n of elements such that we can write G as a union of translates of G by elements $g_i \in G$:

$$G = \cup_{i=1}^{n} (g_i + H).$$

For example, $\mathbf{Z} = (0 + 3\mathbf{Z}) \cup (1 + 3\mathbf{Z}) \cup (2 + 3\mathbf{Z})$, so the index of $3\mathbf{Z}$ in $\mathbf{Z}$ is 3.

A **cyclic** group is a group isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$ for some n. These groups have the property that they can be generated by one element. For example, $\mathbf{Z}_4$ is generated by 1, and it is also generated by 3 since $\{0, 3, 3 + 3, 3 + 3 + 3\}$ is all of $\mathbf{Z}_4$. The following result says that the converse of Lagrange's theorem holds for finite cyclic groups.

THEOREM B.2
Let G be a finite cyclic group of order n. Let $d > 0$ divide n.

1. *G has a unique subgroup of order d.*
2. *G has d elements of order dividing d, and G has $\phi(d)$ elements of order exactly d (where $\phi(d)$ is Euler's ϕ-function).*

For example, $\mathbf{Z}_6$ contains the subgroup $\{0, 2, 4\}$ of order 3. The elements $2, 4 \in \mathbf{Z}_6$ have order 3.

The **direct sum** of two groups G_1 and G_2 is defined to be the set of ordered pairs formed from elements of G_1 and G_2:

$$G_1 \oplus G_2 = \{(g_1, g_2) \,|\, g_1 \in G_1,\ g_2 \in G_2\}.$$

Ordered pairs can be added componentwise:

$$(g_1, g_2) + (h_1, h_2) = (g_1 + h_1, g_2 + h_2).$$

This makes $G_1 \oplus G_2$ into a group with $(0, 0)$ as the identity element. A similar definition holds for the direct sum of more than two groups. We write G^r for the direct sum of r copies of G. In particular, $\mathbf{Z}^r$ denotes the set of r-tuples of integers, which is a group under addition.

Structure theorems

Two groups, G_1 and G_2, are said to be **isomorphic** if there exists a bijection $\psi : G_1 \to G_2$ such that $\psi(gh) = \psi(g)\psi(h)$ for all $g, h \in G_1$ (note that the multiplication gh is in G_1 while the multiplication $\psi(g)\psi(h)$ takes place in G_2).

THEOREM B.3

A finite abelian group is isomorphic to a group of the form

$$\mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_s}$$

with $n_i | n_{i+1}$ for $i = 1, 2, \ldots, s-1$. The integers n_i are uniquely determined by G.

An abelian group G is called **finitely generated** if there is a finite set $\{g_1, g_2, \ldots, g_k\}$ contained in G such that every element of G can be written (not necessarily uniquely) in the form

$$m_1 g_1 + \cdots + m_k g_k$$

with $m_i \in \mathbf{Z}$.

THEOREM B.4

A finitely generated abelian group is isomorphic to a group of the form

$$\mathbf{Z}^r \oplus \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_s}$$

with $r \geq 0$ and with $n_i | n_{i+1}$ for $i = 1, 2, \ldots, s-1$. The integers r and n_i are uniquely determined by G.

The subgroup of G isomorphic to

$$\mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_s}$$

is called the **torsion subgroup** of G. The integer r is called the **rank** of G.

This theorem can be used to prove the following.

THEOREM B.5

Let $G_1 \subseteq G_2 \subseteq G_3$ be groups and assume that, for some integer r, both G_1 and G_2 are isomorphic to $\mathbf{Z}^r$. Then G_2 is isomorphic to $\mathbf{Z}^r$.

For example, $G_1 = 12\mathbf{Z}$, $G_2 = 6\mathbf{Z}$, and $G_3 = \mathbf{Z}$, each of which is isomorphic as a group to $\mathbf{Z}$, satisfy the theorem. This theorem is used in the text when G_1 and G_3 are lattices in $\mathbf{C}$. Then G_1 and G_3 are isomorphic to $\mathbf{Z}^2$. If $G_1 \subseteq G_2 \subseteq G_3$, then $G_2 \simeq \mathbf{Z}^2$, so there exist ω_1, ω_2 such that $G_2 = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$. Since G_1 is a lattice, it contains two vectors that are linearly independent over $\mathbf{R}$. Since $G_1 \subseteq G_2$, this implies that ω_1 and ω_2 are linearly independent over $\mathbf{R}$. Therefore, G_2 is a lattice.

Homomorphisms

Let G_1, G_2 be groups. A **homomorphism** from G_1 to G_2 is a map $\psi : G_1 \to G_2$ such that $\psi(g+h) = \psi(g) + \psi(h)$ for all $g, h \in G_1$. In other words, the map takes sums in G_1 to the corresponding sums in G_2. The **kernel** of ψ is

$$\text{Ker } \psi = \{g \in G_1 \mid \psi(g) = 0\}.$$

The image of ψ is denoted $\psi(G_1)$, which is a subgroup of G_2. The main result we need is the following.

THEOREM B.6

Assume G_1 is a finite group and $\psi : G_1 \to G_2$ is a homomorphism. Then

$$\#G_1 = (\#\text{Ker } \psi)\,(\#\psi(G_1))\,.$$

In fact, in terms of quotient groups, $G_1/\text{Ker } \psi \simeq \psi(G_1)$.

Appendix C

Fields

Let K be a field. There is a ring homomorphism $\psi : \mathbf{Z} \to K$ that sends $1 \in \mathbf{Z}$ to $1 \in K$. If ψ is injective, then we say that K has **characteristic** 0. Otherwise, there is a smallest positive integer p such that $\psi(p) = 0$. In this case, we say that K has **characteristic** p. If p factors as ab with $1 < a \leq b < p$, then $\psi(a)\psi(b) = \psi(p) = 0$, so $\psi(a) = 0$ or $\psi(b) = 0$, contradicting the minimality of p. Therefore, p is prime.

When K has characteristic 0, the field $\mathbf{Q}$ of rational numbers is contained in K. When K has characteristic p, the field $\mathbf{F}_p$ of integers mod p is contained in K.

Let K and L be fields with $K \subseteq L$. If $\alpha \in L$, we say that α is **algebraic** over K if there exists a nonconstant polynomial

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with $a_0, \ldots, a_{n-1} \in K$ such that $f(\alpha) = 0$. We say that L is an **algebraic** over K, or that L is an **algebraic extension** of K, if every element of L is algebraic over K. An **algebraic closure** of a field K is a field $\overline{K}$ containing K such that

1. $\overline{K}$ is algebraic over K.

2. Every nonconstant polynomial $g(X)$ with coefficients in $\overline{K}$ has a root in $\overline{K}$ (this means that $\overline{K}$ is algebraically closed).

If $g(X)$ has degree n and has a root $\alpha \in \overline{K}$, then we can write $g(X) = (X - \alpha)g_1(X)$ with $g_1(X)$ of degree $n - 1$. By induction, we see that $g(X)$ has exactly n roots (counting multiplicity) in $\overline{K}$.

It can be shown that every field K has an algebraic closure, and that any two algebraic closures of K are isomorphic. Throughout the book, we implicitly assume that a particular algebraic closure of a field K has been chosen, and we refer to it as the algebraic closure of K.

When $K = \mathbf{Q}$, the algebraic closure $\overline{\mathbf{Q}}$ is the set of complex numbers that are algebraic over $\mathbf{Q}$. When $K = \mathbf{C}$, the algebraic closure is $\mathbf{C}$ itself, since the fundamental theorem of algebra states that $\mathbf{C}$ is algebraically closed.

Finite fields

Let p be a prime. The integers mod p form a field $\mathbf{F}_p$ with p elements. It can be shown that the number of elements in a finite field is a power of a prime, and for each power p^n of a prime p, there is a unique (up to isomorphism) field with p^n elements. (*Note:* The ring $\mathbf{Z}_{p^n}$ is not a field when $n \geq 2$ since p does not have a multiplicative inverse; in fact, p is a zero divisor since $p \cdot p^{n-1} \equiv 0 \pmod{p^n}$.) In this book, the field with p^n elements is denoted $\mathbf{F}_{p^n}$. Another notation that appears often in the literature is $GF(p^n)$. It can be shown that

$$\mathbf{F}_{p^m} \subseteq \mathbf{F}_{p^n} \quad \Longleftrightarrow \quad m|n.$$

The algebraic closure of $\mathbf{F}_p$ can be shown to be

$$\overline{\mathbf{F}}_p = \bigcup_{n \geq 1} \mathbf{F}_{p^n}.$$

THEOREM C.1
Let $\overline{\mathbf{F}}_p$ be the algebraic closure of $\mathbf{F}_p$ and let $q = p^n$. Then

$$\mathbf{F}_q = \{\alpha \in \overline{\mathbf{F}}_p \,|\, \alpha^q = \alpha\}.$$

PROOF The group $\mathbf{F}_q^\times$ of nonzero elements of $\mathbf{F}_q$ forms a group of order $q-1$, so $\alpha^{q-1} = 1$ when $0 \neq \alpha \in \mathbf{F}_q$. Therefore, $\alpha^q = \alpha$ for all $\alpha \in \mathbf{F}_q$.

Recall that a polynomial $g(X)$ has multiple roots if and only if $g(X)$ and $g'(X)$ have a common root. Since

$$\frac{d}{dX}(X^q - X) = qX^{q-1} - 1 = -1$$

(since $q = p^n = 0$ in $\mathbf{F}_p$), the polynomial $X^q - X$ has no multiple roots. Therefore, there are q distinct $\alpha \in \overline{\mathbf{F}}_p$ such that $\alpha^q = \alpha$.

Since both sets in the statement of the theorem have q elements and one is contained in the other, they are equal. ∎

Define the q-th power **Frobenius automorphism** ϕ_q of $\overline{\mathbf{F}}_q$ by the formula

$$\phi_q(x) = x^q \quad \text{for all } x \in \overline{\mathbf{F}}_q.$$

PROPOSITION C.2
Let q be a power of the prime p.

1. $\overline{\mathbf{F}}_q = \overline{\mathbf{F}}_p$.

2. *ϕ_q is an automorphism of $\overline{\mathbf{F}}_q$. In particular,*

$$\phi_q(x+y) = \phi_q(x) + \phi_q(y), \qquad \phi_q(xy) = \phi_q(x)\phi_q(y)$$

for all $x, y \in \overline{\mathbf{F}}_q$.

3. *Let $\alpha \in \overline{\mathbf{F}}_q$. Then*

$$\alpha \in \mathbf{F}_{q^n} \iff \phi_q^n(\alpha) = \alpha.$$

PROOF Part (1) is a special case of a more general fact: If $K \subseteq L$ and every element of L is algebraic over K, then $\overline{L} = \overline{K}$. This can be proved as follows. If α is algebraic over L and L is algebraic over K, then a basic property of algebraicity is that α is then algebraic over K. Therefore, $\overline{L}$ is algebraic over K and is algebraically closed. Therefore, it is an algebraic closure of K.

Part (3) is just a restatement of Theorem C.1, with q^n in place of q.

We now prove part (2). If $1 \leq j \leq p-1$, the binomial coefficient $\binom{p}{j}$ has a factor of p in its numerator that is not canceled by the denominator, so

$$\binom{p}{j} \equiv 0 \pmod{p}.$$

Therefore,

$$\begin{aligned}(x+y)^p &= x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + y^p \\ &= x^p + y^p\end{aligned}$$

since we are working in characteristic p. An easy induction yields that

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}$$

for all $x, y \in \overline{\mathbf{F}}_p$. This implies that $\phi_q(x+y) = \phi_q(x) + \phi_q(y)$. The fact that $\phi_q(xy) = \phi_q(x)\phi_q(y)$ is clear. This proves that ϕ_q is a homomorphism of fields. Since a homomorphism of fields is automatically injective (see the discussion preceding Proposition C.5), it remains to prove that ϕ_q is surjective. If $\alpha \in \overline{\mathbf{F}}_p$, then $\alpha \in \mathbf{F}_{q^n}$ for some n, so $\phi_q^n(\alpha) = \alpha$. Therefore, α is in the image of ϕ_q, so ϕ_q is surjective. Therefore, ϕ_q is an automorphism. ∎

In Appendix A, it was pointed out that $\mathbf{F}_p^\times = \mathbf{Z}_p^\times$ is a cyclic group, generated by a primitive root. More generally, it can be shown that $\mathbf{F}_q^\times$ is a cyclic group. A useful consequence is the following.

PROPOSITION C.3

Let m be a positive integer with $p \nmid m$ and let μ_m be the group of mth roots of unity. Then

$$\mu_m \subseteq \mathbf{F}_q^\times \iff m | q-1.$$

PROOF By Lagrange's theorem (see Appendix B), if $\mu_m \subseteq \mathbf{F}_q^\times$, then $m|q-1$. Conversely, suppose $m|q-1$. Since $\mathbf{F}_q^\times$ is cyclic of order $q-1$, it has a subgroup of order m (see Appendix B). By Lagrange's theorem, the elements of this subgroup must satisfy $x^m = 1$, hence they must be the m elements of μ_m. ∎

Let $\mathbf{F}_q \subseteq \mathbf{F}_{q^n}$ be finite fields. We can regard $\mathbf{F}_{q^n}$ as a vector space of dimension n over $\mathbf{F}_q$. This means that there is a basis $\{\beta_1, \ldots, \beta_n\}$ of elements of $\mathbf{F}_{q^n}$ such that every element of $\mathbf{F}_{q^n}$ has a unique expression of the form

$$a_1\beta_1 + \cdots + a_n\beta_n$$

with $a_1, \ldots, a_n \in \mathbf{F}_q$. The next result says that it is possible to choose a basis of a particularly nice form, sometimes called a **normal basis**.

PROPOSITION C.4
There exists $\beta \in \mathbf{F}_{q^n}$ such that

$$\{\beta, \phi_q(\beta), \ldots, \phi_q^{n-1}(\beta)\}$$

is a basis of $\mathbf{F}_{q^n}$ as a vector space over $\mathbf{F}_q$.

An advantage of a normal basis is that the qth power map becomes a shift operator on the coordinates: Let

$$x = a_1\beta + a_2\phi_q(\beta) + \cdots + a_n\phi_q^{n-1}(\beta),$$

with $a_i \in \mathbf{F}_q$. Then $a_i^q = a_i$ and $\phi_q^n(\beta) = \beta$, so

$$\begin{aligned} x^q &= a_1\beta^q + a_2\phi_q(\beta^q) + \cdots + a_n\phi_q^{n-1}(\beta^q) \\ &= a_n\phi_q^n(\beta) + a_1\phi_q(\beta) + \cdots + a_{n-1}\phi_q^{n-1}(\beta) \\ &= a_n\beta + a_1\phi_q(\beta) + \cdots + a_{n-1}\phi_q^{n-1}(\beta). \end{aligned}$$

Therefore, if x has coordinates $(a_1, \ldots, a_n)$ with respect to the normal basis, then x^q has coordinates $(a_n, a_1, \ldots, a_{n-1})$. Therefore, the computation of qth powers is very fast and requires no calculation in $\mathbf{F}_{q^n}$. This has great computational advantages.

Embeddings and automorphisms

Let K be a field of characteristic 0, so $\mathbf{Q} \subseteq K$. An element $\alpha \in K$ is called **transcendental** if it is not the root of any nonzero polynomial with

rational coefficients, that is, if it is not algebraic over $\mathbf{Q}$. A set of elements $S = \{\alpha_i\} \subseteq K$ (with i running through some (possibly infinite) index set I) is called **algebraically dependent** if there are n distinct elements $\alpha_1, \ldots, \alpha_n$ of S, for some $n \geq 1$, and a nonzero polynomial $f(X_1, \ldots, X_n)$ with rational coefficients such that $f(\alpha_1, \ldots, \alpha_n) = 0$. The set S is called **algebraically independent** if it is not algebraically dependent. This means that there is no polynomial relation among the elements of S. A maximal algebraically independent subset of K is called a **transcendence basis** of K. The **transcendence degree** of K over $\mathbf{Q}$ is the cardinality of a transcendence basis (the cardinality is independent of the choice of transcendence basis). If every element of K is algebraic over $\mathbf{Q}$, then the transcendence degree is 0. The transcendence degree of $\mathbf{C}$ over $\mathbf{Q}$ is infinite, in fact, uncountably infinite.

Let K be a field of characteristic 0, and choose a transcendence basis S. Let F be the field generated by $\mathbf{Q}$ and the elements of S. The maximality of S implies that every element of K is algebraic over F. Therefore, K can be obtained by starting with $\mathbf{Q}$, adjoining algebraically independent transcendental elements, then making an algebraic extension.

Let K and L be fields and let $f : K \to L$ be a homomorphism of fields. We always assume f maps $1 \in K$ to $1 \in L$. Then f is injective. One way to see this is to note that if $0 \neq x \in K$, then $1 = f(x)f(x^{-1}) = f(x)f(x)^{-1}$; since $f(x)$ has a multiplicative inverse, it cannot be 0.

The following result is very useful. It is proved using Zorn's Lemma (see [71]).

PROPOSITION C.5

Let K and L be fields. Assume that L is algebraically closed and that there is a field homomorphism

$$f : K \longrightarrow L.$$

Then there is a homomorphism $\tilde{f} : \overline{K} \to L$ such that $\tilde{f}$ restricted to K is f.

Proposition C.5 has the following nice consequence.

COROLLARY C.6

Let K be a field of characteristic 0. Assume that K has finite transcendence degree over $\mathbf{Q}$. Then there is a homomorphism $K \to \mathbf{C}$. Therefore, K can be regarded as a subfield of $\mathbf{C}$.

PROOF Choose a transcendence basis $S = \{\alpha_1, \ldots, \alpha_n\}$ of K and let F be the field generated by $\mathbf{Q}$ and S. Since $\mathbf{C}$ has uncountable transcendence degree over $\mathbf{Q}$, we can choose n algebraically independent elements $\tau_1, \ldots, \tau_n \in \mathbf{C}$. Define $f : F \to \mathbf{C}$ by making f the identity map on $\mathbf{Q}$ and setting $f(\alpha_j) = \tau_j$ for all j. The proposition says that f can be extended to $\tilde{f} : \overline{F} \to \mathbf{C}$. Since K is an algebraic extension of F, we have $K \subseteq \overline{F}$. Restricting $\tilde{f}$ to K yields

the desired homomorphism from $K \to \mathbf{C}$. Since a homomorphism of fields is injective, K is isomorphic to its image under this homomorphism. Therefore, K is isomorphic to a subfield of $\mathbf{C}$. ∎

The proposition also holds, with a similar proof, if the transcendence degree of K is at most the cardinality of the real numbers, which is the cardinality of a transcendence basis of $\mathbf{C}$.

If $\alpha \in \mathbf{C}$ is algebraic over $\mathbf{Q}$, then $f(\alpha) = 0$ for some nonzero polynomial with rational coefficients. Let $\mathrm{Aut}(\mathbf{C})$ be the set of field automorphisms of $\mathbf{C}$ and let $\sigma \in \mathrm{Aut}(\mathbf{C})$. Then $\sigma(1) = 1$, from which it follows that σ is the identity on $\mathbf{Q}$. Therefore,

$$0 = \sigma(f(\alpha)) = f(\sigma(\alpha)),$$

so $\sigma(\alpha)$ is one of the finitely many roots of $f(X)$. The next result gives a converse to this fact.

PROPOSITION C.7

Let $\alpha \in \mathbf{C}$. If the set

$$\{\sigma(\alpha) \,|\, \sigma \in Aut(\mathbf{C})\},$$

where σ runs through all automorphisms of $\mathbf{C}$, is finite, then α is algebraic over $\mathbf{Q}$.

PROOF Suppose α is transcendental. There is a transcendence basis S of $\mathbf{C}$ with $\alpha \in S$. Then $\mathbf{C}$ is algebraic over the field F generated by $\mathbf{Q}$ and S.

The map

$$\begin{aligned} \sigma :\ & F \longrightarrow F \\ & \alpha \longmapsto \alpha + 1 \\ & \beta \longmapsto \beta \quad \text{when } \beta \in S,\ \beta \neq \alpha \end{aligned}$$

defines an automorphism of F. By Proposition C.5, σ can be extended to a map $\tilde{\sigma} : \mathbf{C} \to \mathbf{C}$. We want to show that $\tilde{\sigma}$ is an automorphism, which means that we must show that $\tilde{\sigma}$ is surjective. Let $y \in \mathbf{C}$. Since y is algebraic over F, there is a nonzero polynomial $g(X)$ with coefficients in F such that $g(y) = 0$. Let $g^{\sigma^{-1}}$ denote the result of applying σ^{-1} to all of the coefficients of g (note that we know σ^{-1} exists on F because we already know that σ is an automorphism of F). For any root r of $g^{\sigma^{-1}}$, we have

$$0 = \tilde{\sigma}\left(g^{\sigma^{-1}}(r)\right) = g(\tilde{\sigma}(r)).$$

Therefore, $\tilde{\sigma}$ maps the roots of $g^{\sigma^{-1}}$ to roots of g. Since the two polynomials have the same number of roots, $\tilde{\sigma}$ gives a bijection between the two sets of

roots. In particular, $\tilde{\sigma}(r) = y$ for some r. Therefore, y is in the image of $\tilde{\sigma}$. This proves that $\tilde{\sigma}$ is surjective, so $\tilde{\sigma}$ is an automorphism of $\mathbf{C}$.

Since

$$\tilde{\sigma}^j(\alpha) = \alpha + j,$$

the set of images of α under automorphisms of $\mathbf{C}$ is infinite, in contradiction to our assumption. Therefore, α cannot be transcendental, hence must be algebraic. ∎

REMARK C.8 In Proposition C.7, the assumption that the set is finite can be changed to assuming that the set is countable, with essentially the same proof. Namely, if α is transcendental, then, for any $\gamma \in S$, there is an automorphism σ satisfying $\sigma(\alpha) = \alpha + \gamma$. The fact that S is uncountable yields the result. ∎

Appendix D

Computer Packages

There are several computer algebra packages available that do calculations on elliptic curves. In this appendix, we give a brief introduction to three of the major packages. Rather than give explanations of the structure of these packages, we simply include some examples of some computations that can be performed with them. The reader should consult the documentation that is available online or with the packages to see numerous other possibilities.

D.1 Pari

Pari/GP is a free computer algebra system for number theory calculations. It can be downloaded from `http://pari.math.u-bordeaux.fr/`.

Here is a transcript of a session, with commentary.

```
                GP/PARI CALCULATOR Version 2.3.0 (released)
              i686 running linux (ix86 kernel) 32-bit version
         compiled:  Aug 16 2007, gcc-3.4.4 20050721 (Red Hat 3.4.4-2)
        (readline v4.3 enabled [was v5.0 in Configure], extended help
                                  available)
                    Copyright (C) 2000-2006 The PARI Group

PARI/GP is free software, covered by the GNU General Public
License, and comes WITHOUT ANY WARRANTY WHATSOEVER.
Type ?  for help, \q to quit.  Type ?12 for how to get moral
(and possibly technical) support.
parisize = 4000000, primelimit = 500000
```

First, we need to enter and initialize an elliptic curve. Let $[a_1, a_2, a_3, a_4, a_6]$ be the coefficients for the curve in generalized Weierstrass form. Start with the curve of Example 9.3: $E_1 : y^2 = x^3 - 58347x + 3954150$.

```
?  e1=ellinit([0,0,0,-58347,3954150])
%1 = [0, 0, 0, -58347, 3954150, 0, -116694, 15816600,
```

```
-3404372409, 2800656, -3416385600, 5958184124547072,
10091699281/2737152, [195.15478718479016072394976 45,
75.000000000000000000000000000, -270.15478718479016072394976 45],
0.19860246926874753552600421 88, 0.15671326754771459826130478 83*I,
-6.85589981198857494406354470 5, -21.22835194662770142565252843*I,
0.03112364190214999895971387115]
```

The output contains several parameters for the curve (type `?ellinit` to see an explanation). For example, the periods $\omega_1 = i0.156713\ldots$ and $\omega_2 = 0.198602\ldots$ are entries. The j-invariant is the 13th entry:

```
?  e1[13]
%2 = 10091699281/2737152
```

Here is the curve $E_2 : y^2 = x^3 + 73$:

```
?  e2=ellinit([0,0,0,0,73])
%3 = [0, 0, 0, 0, 73, 0, 0, 292, 0, 0, -63072, -2302128, 0,
[-4.17933919638123189205637 6349, 2.08966959819061594602818 8174
+ 3.61941391509818767453045 5654*I, 2.08966959819061594602818 8174
-3.61941391509818767453045 5654*I], 2.05765170800492375625105 5780,
-1.02882585400246187812552 7890+0.59399288375756798111001 34634*I,
-2.64446994189243655339512 5300, 1.32223497094621827669756 2650
-2.29017814922320837143138 8983*I, 1.22223047180652989043161 4914]
```

We can add the points $(2, 9)$ and $(3, 10)$, which lie on the curve:

```
?  elladd(e2,[2,9],[3,10])
%4 = [-4, -3]
```

We can compute the 3rd multiple of $(2, 9)$:

```
?  ellpow(e2,[2,9],3)
%5 = [5111/625, -389016/15625]
```

The torsion subgroup of the Mordell-Weil group can be computed:

```
?  elltors(e1)
%6 = [10, [10], [[3, 1944]]]
?  elltors(e2)
%7 = [1, [], []]
```

The first output says that the torsion subgroup of $E_1(\mathbf{Q})$ has order 10, it is cyclic of order 10, and it is generated by the point $(3, 1944)$. The second output says that the torsion subgroup of $E_2(\mathbf{Q})$ is trivial.

The number of points on an elliptic curve mod a prime p has the form $p + 1 - a_p$. The value of a_{13} for E_1 is computed as follows:

```
?  ellap(e1,13)
%8 = 4
```

Therefore, there are $13 + 1 - 4 = 10$ points on E_1 mod 13.

We can also compute with curves mod p. Let's consider $E_3 : y^2 = x^3 + 10x + 5 \pmod{13}$ (this is the reduction of E_1 mod 13):

```
?  e3=ellinit([0,0,0,Mod(10,13),Mod(5,13)])
%9 = [0, 0, 0, Mod(10, 13), Mod(5, 13), 0, Mod(7, 13),
Mod(7, 13), Mod(4, 13), Mod(1, 13), Mod(9, 13), Mod(2, 13),
Mod(7, 13), 0, 0, 0, 0, 0, 0]
```

Multiples of points can be computed as before:

```
?  ellpow(e3,[Mod(3,13),Mod(7,13)],10)
%10 = [0]
?  ellpow(e3,[Mod(3,13),Mod(7,13)],5)
%11 = [Mod(10, 13), Mod(0, 13)]
```

The first output means that the 10th multiple of the point is ∞.

The height pairing can be computed. For example, on E_2 the pairing $\langle (2,9),(3,10)\rangle$ from Example 8.11 is computed as follows:

```
?  ellbil(e2,[2,9],[3,10])
%12 = -0.97704341280383824411625933747
```

Pari works with the complex functions associated to an elliptic curve. For example, the value of $j((1+\sqrt{-171})/2)$ (see the beginning of Section 10.4) is computed as follows:

```
?  ellj((1+sqrt(-171))/2)
%13 = -694282057876536664.0122886865 + 0.00000000003565219231*I
```

We know the value should be real. To increase the precision to 60 digits, type:

```
?  \p 60
realprecision = 67 significant digits (60 digits displayed)
```

Now, retype the previous command:

```
?  ellj((1+sqrt(-171))/2)
%14 = -694282057876536664.012288686708307426044367453641244662629851 - 7.05609883 E-49*I
```

The imaginary part of the answer is less than 10^{-48}.

To find other functions that are available, type `?`. To find the functions that relate to elliptic curves, type `?5`. To find how to use a command, for example `elladd`, type

```
?elladd
elladd(e,z1,z2):  sum of the points z1 and z2 on elliptic
curve e.
```

To quit, type

```
?  \q
Goodbye!
```

D.2 Magma

Magma is a large computer algebra package. It requires a license to use. It is available on some institutional computers. For general information, see `http://magma.maths.usyd.edu.au/magma/`.

The following is the transcript of a session, with commentary.

The session starts:

```
Magma V2.11-14 Thu Nov 1 2007 15:48:04 [Seed = 3635786414]
Type ?  for help.  Type <Ctrl>-D to quit.
```

Let's enter the elliptic curve $E_1 : y^2 = x^3 - 58447x + 3954150$ of Example 9.3. The vector represents the coefficients $[a_1, a_2, a_3, a_4, a_6]$ in generalized Weierstrass form. Unless otherwise specified, the curve is over the rational numbers.

```
> E1:= EllipticCurve( [ 0, 0, 0, -58347, 3954150 ]);
```

Note that the line needs to end with a semicolon. To find out what E_1 is:

```
> E1;
Elliptic Curve defined by y^2 = x^3 - 58347*x + 3954150 over
Rational Field
```

Let's also define $E_2 : y^2 = x^3 + 73$. Here we use the shortened form of the coefficient vector $[a_4, a_6]$ corresponding to (nongeneralized) Weierstrass form.

```
> E2:= EllipticCurve( [ 0, 73 ]);
```

Let's add the points $(2, 9)$ and $(3, 10)$ on E_2. The notation `E2![2,9]` specifies that $[2, 9]$ lives on E_2, rather than in some other set.

```
> E2![2,9] + E2![3, 10];
(-4 :  -3 :  1)
```

Note that the answer is in projective coordinates. We could have done the computation with one or both points in projective coordinates. For example:

```
> E2![2,9] + E2![3, 10, 1];
(-4 :  -3 :  1)
```

The identity element of $E2$ is

```
> E2!0;
(0 :  1 :  0)
```

We can also define a point using `:=`

```
> S:= E2![2,9] + E2![3, 10];
```

To find out what S is:

```
> S;
(-4 :  -3 :  1)
```

The computer remembers that S lies on E_2, so we can add it to another point on E_2:

```
> S + E2![2, 9];
(6 :  -17 :  1)
```

To find the 3rd multiple of the point $(2, 9)$ on E_2:

```
> 3*E2![2,9];
(5111/625 :  -389016/15625 :  1)
```

To find the torsion subgroup of $E_1(\mathbf{Q})$:

```
> TorsionSubgroup(E1);
Abelian Group isomorphic to Z/10
Defined on 1 generator
Relations:
  10*$.1 = 0
```

Note that we obtained only an abstract group, not the points. To get the points, we define a group G and an isomorphism f from G to the set of points:

```
> G, f:= TorsionSubgroup(E1);
```

To obtain the first element of G, type:

```
> f(G.1);
(3 :  1944 :  1)
```

This is a torsion point in $E_1(\mathbf{Q})$.

Let's reduce E_1 mod 13. Define F to be the field with 13 elements and E_3 to be E_1 mod 13:

```
> F:= GF(13);
> E3:= ChangeRing( E1, F );
> E3; Elliptic Curve defined by y^2 = x^3 +10*x + 5 over GF(13)
```

The last command was not needed. It simply identified the nature of E_3. We also could have defined a curve over $\mathbf{F}_{13}$. The command `F!10` puts 10 into $\mathbf{F}_{13}$, which forces everything else, for example 5, to be in $\mathbf{F}_{13}$:

```
> E4:= EllipticCurve( [F!10, 5]);
> E4;
Elliptic Curve defined by y^2 = x^3 +10*x + 5 over GF(13)
> E3 eq E4;
true
```

The last command asked whether E_3 is the same as E_4. The answer was yes.

We can find out how many points there are in $E_3(\mathbf{F}_{13})$, or we can list all the points:

```
> #E3;
10
> Points(E3);
{@ (0 :  1 :  0), (1 :  4 :  1), (1 :  9 :  1), (3 :  6 :  1),
(3 :  7 :  1), (8 :  5 :  1), (8 :  8 :  1), (10 :  0 :  1),
```

```
(11 :  4 :  1), (11 :  9 :  1) @}
```

The @'s in the last output specifies that the entries are a set indexed by positive integers.

Let's compute the Weil pairing $e_3((0,3),(5,1))$ on the curve $E_5 : y^2 = x^2+2$ over $\mathbf{F}_7$, as in Example 11.5.

```
> E5:= EllipticCurve([0, GF(7)!2]);
> WeilPairing( E5![0,3], E5![5,1], 3);
4
```

The answer is 4, which is a cube root of unity in $\mathbf{F}_7$. Note that this is the inverse of the Weil pairing used elsewhere in this book (cf. Remark 11.11).

We can compute the Mordell-Weil group $E_2(\mathbf{Q})$:

```
> MordellWeilGroup(E2);
Abelian Group isomorphic to Z + Z
Defined on 2 generators (free)
> Generators(E2);
[ (2 :  9 :  1), (-4 :  3 :  1) ]
```

To find a command that computes, for example, Mordell-Weil groups, type `?MordellWeil` or `?Mordell` to get an example or a list of examples.

To quit Magma, type

```
<Ctrl>D
```

For much more on Magma, go to

`http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`

For elliptic curves, click on the *Arithmetic Geometry* link.

D.3 SAGE

Sage is an open source computer algebra package that can be downloaded for free from `www.sagemath.org/`. For general information, see the web site, which also contains a tutorial and documentation.

The following is the transcript of a session, with commentary.

The session starts:

```
Linux sage 2.6.17-12-386 #2 Sun Sep 23 22:54:19 UTC 2007 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in
the individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

| SAGE Version 2.8.8.1, Release Date:  2007-10-21              |
```

```
| Type notebook() for the GUI, and license() for information.  |
```

Let's enter the elliptic curve $E_1 : y^2 = x^3 - 58447x + 3954150$ of Example 9.3. The vector represents the coefficients $[a_1, a_2, a_3, a_4, a_6]$ in generalized Weierstrass form. Unless otherwise specified, the curve is over the rational numbers.

```
sage:  E1 = EllipticCurve([ 0, 0, 0, -58347, 3954150 ])
```

To find out what E_1 is:

```
sage:  E1
Elliptic Curve defined by y^2 = x^3 - 58347*x + 3954150 over
Rational Field
```

Let's also define $E_2 : y^2 = x^3 + 73$. Here we use the shortened form of the coefficient vector $[a_4, a_6]$ corresponding to (nongeneralized) Weierstrass form.

```
sage:  E2 = EllipticCurve([ 0, 73 ]);
```

Let's add the points $(2, 9)$ and $(3, 10)$ on E_2:

```
sage:  E2([2,9]) + E2([3, 10])
(-4 :  -3 :  1)
```

Note that the answer is in projective coordinates. We could have done the computation with one or both points in projective coordinates. For example:

```
sage:  E2([2,9]) + E2([3, 10, 1])
(-4 :  -3 :  1)
```

The identity element of E_2 is

```
sage:  E2(0)
(0 :  1 :  0)
```

We can also define a point:

```
sage:  S = E2([2,9]) + E2([3, 10])
```

To find out what S is:

```
sage:  S
(-4 :  -3 :  1)
```

The computer remembers that S lies on E_2, so we can add it to another point on E_2:

```
sage:  S + E2([2, 9])
(6 :  -17 :  1)
```

To find the 3rd multiple of the point $(2, 9)$ on E_2:

```
sage:  3*E2([2,9])
(5111/625 :  -389016/15625 :  1)
```

To find the torsion subgroup of $E_1(\mathbf{Q})$:

```
sage:  E1.torsion_subgroup()
Torsion Subgroup isomorphic to Multiplicative Abelian Group
```

```
isomorphic to C10 associated to the Elliptic Curve defined by
y^2= x^3- 58347*x + 3954150 over Rational Field
```

C10 denotes the cyclic group of order 10. To get a generator:

```
sage:  E1.torsion_subgroup().gen()
(3 :  1944 :  1)
```

The number of points on an elliptic curve mod a prime p has the form $p + 1 - a_p$. The value of a_{13} for E_1 is computed as follows:

```
sage:  E1.ap(13)
4
```

Therefore, there are $13 + 1 - 4 = 10$ points on E_1 mod 13.

Let's reduce E_1 mod 13:

```
sage:  E3 = E2.change_ring(GF(13))
sage:  E3
Elliptic Curve defined by y^2 = x^3 +10*x + 5
over Finite Field of size 13
```

The last command was not needed. It simply identified the nature of E_3. We also could have defined a curve over $\mathbf{F}_{13}$.

```
sage:  E4 = EllipticCurve(GF(13), [10, 5])
sage:  E4
Elliptic Curve defined by y^2 = x^3 +10*x + 5
over Finite Field of size 13
sage:  E3 is E4
True
```

The last command asked whether E_3 is the same as E_4. The answer was yes.

We can find out how many points there are in $E_3(\mathbf{F}_{13})$, or we can list all the points:

```
sage:  E3.cardinality()
10
sage:  E3.points()
[(0 :  1 :  0),
(11 :  4 :  1),
(8 :  5 :  1),
(1 :  4 :  1),
(10 :  0 :  1),
(1 :  9 :  1),
(3 :  6 :  1),
(8 :  8 :  1),
(11 :  9 :  1),
(3 :  7 :  1)]
```

Consider the curve $E_5 : y^2 = x^3 - 1$ over $\mathbf{F}_{229}$, as in Example 4.10. We can compute its group structure:

```
sage:  EllipticCurve(GF(229),[0,-1]).abelian_group()
(Multiplicative Abelian Group isomorphic to C42 x C6,
((62 :  25 :  1), (113 :  14 :  1)))
```

Therefore, $E_5(\mathbf{F}_{229}) \simeq \mathbf{Z}_{42} \oplus \mathbf{Z}_6$, and it has the listed generators.

Let's compute the rank and generators of the Mordell-Weil group $E_2(\mathbf{Q})$:

```
sage:  E2.rank()
2
sage:  E2.gens()
[(-4 :  3 :  1),(2:  9 :  1)]
```

The generators are the generators of the nontorsion part. The command does not yield generators of the torsion subgroup. For these, use the command `E.torsion_subgroup().gen()` used previously.

To find the periods ω_1 and ω_2 of E_1:

```
sage:  E1.period_lattice.0
0.19860246926874753552600421 88...
sage:  E1.period_lattice.1
0.15671326754771459826130478 83...*I
```

The j-invariant of E_1 is

```
sage:  E1.j_invariant()
10091699281/2737152
```

To find a list of commands that start with a given string of letters, type those letters and then press the "Tab" key:

```
sage:  Ell ('Tab')
Ellipsis                 EllipticCurve_from_c4c6
EllipticCurve            EllipticCurve_from_cubic
```

To find out about the command `EllipticCurve`, type

```
sage:  EllipticCurve?
```

The output is a description with some examples.

For more on SAGE, go to `http://www.sagemath.org`.