CHAPTER 0

Synopsis

The purpose of this book is to give a comprehensive account of the proof of the following theorem, known as Fermat's Last Theorem:

THEOREM 0.1. *Let n be an integer greater than or equal to* 3. *If integers X, Y, and Z satisfy the equation*

$$X^n + Y^n = Z^n, \tag{0.1}$$

then at least one of X, Y, and Z must be 0.

A flow diagram of the proof can be drawn as follows:

$$\begin{array}{rcl} \text{(a solution of (0.1))} & \Longrightarrow & \text{(an elliptic curve)} \\ & \Longrightarrow & \text{(a modular form)} \\ & \Longrightarrow & \text{(contradiction)} \end{array} \tag{0.2}$$

If we try to explain the meaning of this diagram in a few sentences, it goes as follows. Assume there exists a nontrivial solution to the equation (0.1), and we would like to derive a contradiction. To this end, we define an elliptic curve using such a solution. We then show that such an elliptic curve is closely associated with a modular form with certain properties. Finally, we derive a contradiction by showing that such a modular form could not exist.

In this chapter we give a further explanation of the above diagram. As we can easily see, elliptic curves and modular forms play leading roles in the proof. By following the outline of the proof, the reader should familiarize her/himself with these two subjects. We indicate where the details of certain topics are treated in the main text. Skipping some unfamiliar terminology, the reader should grasp the flow of the proof.

0.1. Simple paraphrase

As a matter of fact, we will prove the following theorem which is stronger than Theorem 0.1.

THEOREM 0.2. *Let ℓ be a prime number with $\ell \geq 5$, and let a be an integer with $a \geq 4$. Then, the equation*

$$X^\ell + 2^a Y^\ell = Z^\ell \tag{0.3}$$

has no integer solutions (X, Y, Z) such that all X, Y, and Z are odd.

Let us verify that Theorem 0.1 follows from Theorem 0.2.

PROOF OF THEOREM 0.2 $\Rightarrow$ THEOREM 0.1. First, decomposing n into prime factors, we can see that in order to show Theorem 0.1, it suffices to show the cases where $n = 4$ and where n is a prime number greater than or equal to 3. The case $n = 4$ is nothing but Proposition 1.1 in Chapter 1 of *Number Theory 1*. For the case of $n = 3$, we find a proof in §4.1(b) in Chapter 4 of *Number Theory 1*. Thus, it suffices to show for the case where n is a prime number ℓ with $\ell \geq 5$. The argument is a repetition of the one in §4.4 in Chapter 4 of *Number Theory 1*.

Let n be a prime number $\ell \geq 5$. Assume (0.1) has a nontrivial solution $(X, Y, Z) = (A, B, C)$, and we derive a contradiction to Theorem 0.2. A solution (A, B, C) of (0.1) is called nontrivial if none of A, B, and C is 0. Dividing by their greatest common divisor, we may assume that the greatest common divisor of A, B, and C is 1. Then, considering the residue modulo 2, we see that one of A, B, and C is an even number and the others are odd. We may assume B is even by rearranging A, B, and C as follows, if necessary. If A is even, replace A with B. If C is even, replace the solution (A, B, C) with $(A, -C, -B)$. Now that B is even, let m be the largest integer such that 2^m divides B, and let $B = 2^m B'$. We have $m \geq 1$ and B' is odd. Then, $(X, Y, Z) = (A, B', C)$ is a solution of (0.3) with $a = m\ell$. Since we have $a \geq 5$, and A, B', and C are all odd; this contradicts Theorem 0.2. □

In the case of $n = 3$, equation (0.3) defines an elliptic curve. We proved Theorem 0.1 for $n = 3$ by studying the rational points of this elliptic curve. In the case of $n = 4$, the curve defined by (0.3) is not an elliptic curve. However, in this case too, we prove Theorem 0.1 by studying the rational points of an elliptic curve closely related to this curve. On the other hand, in the case of $n = \ell \geq 5$, we define an elliptic curve using a solution of (0.1), as we will see in the next section. We then prove that such an elliptic curve cannot exist. Unlike the case where $n = 3, 4$, it is not the existence of rational points on

an elliptic curve but the existence of an elliptic curve itself that is the issue in the case of $n = \ell \geq 5$.

0.2. Elliptic curves

The first arrow in the diagram (0.2) is to paraphrase the problem in terms of elliptic curves. We will study elliptic curves in Chapter 1. For those who are interested only in the proof of Theorem 0.1, it is not too inappropriate to think that an elliptic curve is a curve defined by the equation in x and y given by

$$y^2 = x(x - C^\ell)(x - B^\ell). \tag{0.4}$$

Here, B and C are nonzero distinct integers. In terms of elliptic curves, Theorem 0.2 is equivalent to the following.

THEOREM 0.3. *Let $\ell \geq 5$ be a prime number. Then there does not exist an elliptic curve defined over the rational number field* $\mathbf{Q}$ *satisfying the following three conditions:*

(i) *All* 2*-torsion points of E are* $\mathbf{Q}$*-rational.*
(ii) *E is semistable.*
(iii) *The group of ℓ-torsion points $E[\ell]$ is* good *at all odd prime numbers p.*

We will explain the meaning of the terms appearing in Theorem 0.3 in Chapters 1 and 3. Note that the notion of "good at a prime number p", appearing in (iii), is a technical term which will be defined in Definition 3.31.

The equivalence between Theorems 0.2 and 0.3, or in other words, the connection between Fermat's Last Theorem and elliptic curves, is given by Proposition 0.4 below. To put it plainly, if (0.1) or (0.3) had a solution, the elliptic curve constructed from it would have too good a property to exist. Before stating the proposition, we introduce some notation. For distinct nonzero integers m and n, we denote by $E_{n,m}$ the elliptic curve over $\mathbf{Q}$ defined by the equation

$$y^2 = x(x - n)(x - m). \tag{0.5}$$

PROPOSITION 0.4. *Let ℓ be an odd prime number. The following conditions on an elliptic curve E over* $\mathbf{Q}$ *are equivalent:*

(i) *E satisfies all three conditions in Theorem* 0.3*.*

(ii) *E is isomorphic to an elliptic curve $E_{n,m}$ with n and m satisfying the following condition* (0.6).

(0.6) *The integers n and m are nonzero, distinct, and relatively prime. In addition, $n \equiv -1 \bmod 4$, n and $n-m$ are both ℓ-th powers, and m is of the form $2^a b^\ell$ with $a \geq 4$.*

By Proposition 0.4 we can show that Theorems 0.2 and 0.3 are equivalent. Here, we prove the fact that Theorem 0.2 follows from Theorem 0.3 and Proposition 0.4. In fact, the converse is not necessary for the proof of Theorem 0.1.

Proof of Theorem 0.3 + Proposition 0.4 $\Rightarrow$ Theorem 0.2. It suffices to show that a counterexample of Theorem 0.2 gives a counterexample of Theorem 0.3. By Proposition 0.4, if there are integers n and m satisfying (0.6), the elliptic curve $E_{n,m}$ is a counterexample of Theorem 0.3.

Let $\ell \geq 5$ be a prime number, and let $a \geq 4$ be an integer. Suppose (0.3) has a solution $(X, Y, Z) = (A, B, C)$ such that A, B, and C are all odd. From this we would like to find integers n and m satisfying (0.6). Dividing by their greatest common divisor, we may assume that the greatest common divisor of A, B, and C is 1. Notice that $(X, Y, Z) = (-A, -B, -C)$ is again a solution of (0.3) such that all members are odd. Since either C or $-C$ is congruent to -1 modulo 4, we may assume $C \equiv -1 \bmod 4$ by replacing C by $-C$, if necessary.

Let $n = C^\ell$ and $m = 2^a B^\ell$. We show that these satisfy (0.6). Both n and m are nonzero, they are distinct, and they are relatively prime. Since $C \equiv -1 \bmod 4$, we have $n \equiv -1 \bmod 4$. Moreover, both $n = C^\ell$ and $n - m = A^\ell$ are ℓ-th powers, and $m = 2^a B^\ell$ is the product of an ℓ-th power and 2 to the power $a \geq 4$. Thus, n and m satisfy the condition (0.6). This gives a counterexample of Theorem 0.3. □

Question 1. Verify the fact that Theorem 0.3 follows from Theorem 0.2 and Proposition 0.4.

Fermat's Last Theorem (Theorem 0.1) is thus reduced to Theorem 0.3, which is about elliptic curves. We can summarize as follows. Let $n = \ell$ be a prime number greater than or equal to 5. Suppose there exists a nontrivial solution $(X, Y, Z) = (A, B, C)$ to equation (0.1). Rearranging suitably, we may assume A, B, and C are relatively prime, B is even, and $C \equiv -1 \bmod 4$. Then, the elliptic curve E_{C^ℓ, B^ℓ}

defined by $y^2 = x(x - C^\ell)(x - B^\ell)$ gives a counterexample of Theorem 0.3.

The proof of Theorem 0.3 is given by studying the relation between elliptic curves and modular forms. We will see its outline in the following sections.

0.3. Elliptic curves and modular forms

The second arrow in diagram (0.2) is the connection between elliptic curves and modular forms. It is often through this connection to modular forms that a profound arithmetic property of elliptic curves reveal themselves. The proof of Fermat's Last Theorem is an example of this.

We will study modular forms in detail in Chapter 2. Here, we only introduce necessary terminology in order to explain the outline. In Chapter 2, we will define a finite dimensional complex vector space $S(N)_{\mathbf{C}}$ called the space of modular forms of level N for each integer $N \geq 1$. This is a subspace of the space of formal power series $\mathbf{C}[\![q]\!]$. An important property of the space of modular forms is that an endomorphism $T_n : S(N)_{\mathbf{C}} \to S(N)_{\mathbf{C}}$ called the Hecke operator is defined for each positive integer n. Among the most important modular forms are normalized cusp forms that are simultaneous eigenforms of all Hecke operators. Since such a form appears many times, we call it in this book a "primary form" for short. Its formal definition is as follows.

Definition 0.5. A modular form of level N

$$f = \sum_{m=1}^{\infty} a_m(f) q^m \in S(N)_{\mathbf{C}} \tag{0.7}$$

is called a *primary form* if it is nonzero, and it satisfies

$$T_n f = a_n(f) f \tag{0.8}$$

for all integers $n \geq 1$.

A modular form f is determined by the coefficients $a_m(f)$, $m = 1, 2, 3, \ldots$, as in (0.7). As a matter of fact, a primary form can be determined only by the coefficients $a_p(f)$, where $p = 2, 3, 5, 7, \ldots$ are prime numbers. To formulate the connection between elliptic curves and modular forms, we define a sequence $a_p(E)$ for an elliptic curve E. Its precise definition will be given in Chapter 1, but it is roughly as follows.

Let E be an elliptic curve. Consider an equation with integer coefficients that defines E, such as (0.4) for example. Considering this equation modulo p for each prime number p, we obtain an equation with coefficients in the finite field $\mathbf{F}_p$. Except for a finite number of p, this equation defines an elliptic curve over $\mathbf{F}_p$, which we denote by $E_{\mathbf{F}_p}$. Since the set $E_{\mathbf{F}_p}(\mathbf{F}_p)$ of all $\mathbf{F}_p$-valued points of $E_{\mathbf{F}_p}$ is a finite set, we define

$$a_p(E) = p + 1 - \sharp E_{\mathbf{F}_p}(\mathbf{F}_p), \tag{0.9}$$

where $\sharp$ stands for the number of elements.

EXAMPLE 0.6. Let n and m be distinct nonzero integers relatively prime to each other such that

$$n \equiv -1 \bmod 4, \quad m \equiv 0 \bmod 16. \tag{0.10}$$

Let $E = E_{n,m}$. By Proposition 0.4, E is a semistable elliptic curve.

For a prime number p, the equation $y^2 = x(x-n)(x-m)$ with $\mathbf{F}_p$ coefficients defines an elliptic curve over $\mathbf{F}_p$ if and only if p does not divide $nm(n-m)$. For such a prime number p, we have

$$E_{\mathbf{F}_p}(\mathbf{F}_p) = \{(x,y) \in \mathbf{F}_p \times \mathbf{F}_p \mid y^2 = x(x-n)(x-m)\} \cup \{\infty\}. \tag{0.11}$$

$a_p(E)$ equals the difference $A - B$ of the number A (resp. B) of elements $x \neq 0, n, m$ in $\mathbf{F}_p$ such that $x(x-n)(x-m)$ is nonsquare (resp. square). Using the quadratic residue symbol, we have

$$a_p(E) = -\sum_{x \in \mathbf{F}_p, x \neq 0, n, m} \left(\frac{x(x-n)(x-m)}{p} \right).$$

DEFINITION 0.7. An elliptic curve E over the rational number field $\mathbf{Q}$ is *modular* if there exists a primary form $f = \sum_{m=1}^{\infty} a_m(f) q^m$ such that

$$a_p(E) = a_p(f) \tag{0.12}$$

for all but a finite number of prime numbers p.

The contents of this book are, in substance, an account of the proof of Theorem 0.8, or of Theorem 0.13, which is a partial but refined result of it.

THEOREM 0.8. *Any elliptic curve E over the rational number field $\mathbf{Q}$ is modular. In other words, there exists a primary form $f = \sum_{m=1}^{\infty} a_m(f) q^m$ such that $a_p(E) = a_p(f)$ for all but a finite number of prime numbers p.*

This theorem is the second arrow of the diagram (0.2). In this book we explain the proof of Theorem 0.8 in the case where elliptic curve E is semistable. On the one hand, the proof for the general case is much more complicated, on the other hand this special case is already enough to prove Theorem 0.3.

Using Theorem 0.8, we can prove Theorem 0.3 as follows. Suppose an elliptic curve E over $\mathbf{Q}$ satisfies the conditions (i) to (iii) in Theorem 0.3. Then, by Theorem 0.8, there exists a primary form f such that $a_p(E) = a_p(f)$ for all but a finite number of p. Now, it suffices to show that the existence of such a primary form contradicts the conditions (i) to (iii) in Theorem 0.3. This is the last arrow of the diagram (0.2).

0.4. Conductor of an elliptic curve and level of a modular form

Since what the last arrow of the diagram (0.2) means is rather complicated, we will illustrate it using its easier analogue, the case of quadratic number fields.

PROPOSITION 0.9. *There exists no quadratic extension of* $\mathbf{Q}$ *that is unramified at every prime number.*

If we write a quadratic extension in the form $\mathbf{Q}(\sqrt{a})$, it is not so difficult to prove Proposition 0.9 directly. Here, however, we would like to think it as an analogue of Theorem 0.3, and we derive it from the following proposition.

PROPOSITION 0.10. (1) *Any quadratic extension of* $\mathbf{Q}$ *is a subfield of a cyclotomic field.*

(2) *Let N be an integer, and let p be a prime number. Let p^e be the largest power of p that divides N, and let $N = p^e M$. If a subfield K of the cyclotomic field $\mathbf{Q}(\zeta_N)$ is unramified at p, then K is a subfield of $\mathbf{Q}(\zeta_M)$.*

Proposition 0.10 is a part of class field theory. Proposition 0.10(1) and (2) are Theorem 5.10(1) and (3) in Chapter 5 of *Number Theory 2*, respectively. We can derive Proposition 0.9 from Proposition 0.10 as follows.

PROOF OF PROPOSITION 0.10 $\Rightarrow$ PROPOSITION 0.9. Let K be a quadratic extension unramified at all prime numbers. By Proposition 0.10(1), there exists a cyclotomic field $\mathbf{Q}(\zeta_N)$ that contains K as

a subfield. Applying Proposition 0.10(2) for each prime factor of N repeatedly, we conclude that K is a subfield of $\mathbf{Q} = \mathbf{Q}(\zeta_1)$, which is a contradiction. □

We would like to prove Theorem 0.3 using a similar argument. In other words, we would like to replace quadratic extensions by elliptic curves, and cyclotomic fields by modular forms. Proposition 0.10(1) corresponds to Theorem 0.8. Just as quadratic extensions are contained in cyclotomic fields, elliptic curves are associated with modular forms. However, we still do not have a statement corresponding to Proposition 0.10(2), namely, the relation between the conductor of an elliptic curve and the level of a modular form. In the above proof, it is important to know in which cyclotomic field a quadratic field is contained. Similarly, it is important to know what level of modular form an elliptic curve is related to. So, we state a refinement of Definition 0.7.

DEFINITION 0.11. An elliptic curve E over $\mathbf{Q}$ is called *modular of level* N, if there exists a primary form $f = \sum_{m=1}^{\infty} a_m(f)q^m \in S(N)_{\mathbf{C}}$ of level N such that $a_p(E) = a_p(f)$ for any prime number p not dividing N.

To make the story simple, we focus only on semistable elliptic curves in the following. For a semistable elliptic curve, its conductor is defined as the product of all prime numbers at which E has bad reduction. The conductor N is thus square-free.

EXAMPLE 0.12. Let $E = E_{n,m}$ be the semistable elliptic curve in Example 0.6. In this case, the conductor N of E is the product of all the primes dividing $\frac{1}{16}nm(n-m)$.

This is Proposition 1.9(2) in Chapter 1.

We have the following refinement of Theorem 0.8, which describes the relation between the conductor and the level.

THEOREM 0.13. *Let E be a semistable elliptic curve over $\mathbf{Q}$, and let N be the conductor of E. Then, E is modular of level N.*

Unfortunately, this theorem is not enough to prove Theorem 0.3. To the elliptic curve $E = E_{n,m}$ in Example 0.12, there exists a primary form of level N, which leads to no contradiction. In order to derive a contradiction, we use condition (iii) in Theorem 0.3, but we are not ready for it yet. To do so, we use not the equality $a_p(E) = a_p(f)$,

but the congruence relation

$$a_p(E) \equiv a_p(f) \bmod \ell$$

as a condition on f. In fancier terms, we look at not only the elliptic curve E but also at the group of ℓ-torsion points $E[\ell]$ as a representation of the absolute Galois group $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and we study its relation to the modular forms.

0.5. ℓ-torsion points of elliptic curves and modular forms

In order to formulate the relation between the group of ℓ-torsion points of E and the modular forms more precisely, we would like to study modular forms a little more.

In §0.3, we introduced the space $S(N)_{\mathbf{C}}$ of modular forms of level N as a finite dimensional complex vector space. However, it turns out that we can define more naturally a finite dimensional $\mathbf{Q}$-vector space $S(N)_{\mathbf{Q}}$ of modular forms of level N with $\mathbf{Q}$-coefficients. The $\mathbf{C}$-vector space $S(N)_{\mathbf{C}}$ is the extension of coefficients of $S(N)_{\mathbf{Q}}$ to the complex number field. The Hecke operators are also defined as endomorphisms $T_n : S(N)_{\mathbf{Q}} \to S(N)_{\mathbf{Q}}$. If $f = \sum_{m=1}^{\infty} a_m(f)q^m \in S(N)_{\mathbf{C}}$ is a primary form, then each coefficient $a_m(f)$ is an algebraic number, and we can see from this fact that the field $\mathbf{Q}(f) = \mathbf{Q}(a_m(f), m \in \mathbf{N})$ generated by all the coefficients $a_m(f)$, $m = 1, 2, 3, \ldots$, is a finite extension. As a matter of fact, each coefficient $a_m(f)$ is an algebraic integer of $\mathbf{Q}(f)$. These facts will be treated in Chapters 2 and 9.

Once we know that each $a_m(f)$ is an algebraic integer of $\mathbf{Q}(f)$, we can formulate the relation between the group of ℓ-torsion points of E and the modular forms as follows.

Definition 0.14. Let E be an elliptic curve over $\mathbf{Q}$. Suppose ℓ is a prime number such that the group of ℓ-torsion points $E[\ell]$ is irreducible as a representation of the absolute Galois group $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then we say that $E[\ell]$ is modular of level N if there exists a primary form $f = \sum_{m=1}^{\infty} a_m(f)q^m$ of level dividing N and a prime ideal λ of the integer ring of $\mathbf{Q}(f)$ containing ℓ such that

$$a_p(E) \equiv a_p(f) \mod \lambda$$

for all primes p not dividing N.

The terminology appearing in Definition 0.14 will be defined in Chapter 3. If an elliptic curve E is modular of level N, and the subgroup of ℓ-torsion points $E[\ell]$ is irreducible as a $G_{\mathbf{Q}}$-representation,

then $E[\ell]$ is modular of level N. The meaning of the last arrow in (0.2) is the following two theorems.

THEOREM 0.15. *Let E be an elliptic curve over $\mathbf{Q}$, let N be a positive integer, and let ℓ and p be odd prime numbers. Suppose the group of ℓ-torsion points $E[\ell]$ satisfies the following conditions:*

(i) *$E[\ell]$ is irreducible as a $G_{\mathbf{Q}}$-representation.*
(ii) *$E[\ell]$ is modular of level N.*
(iii) *$E[\ell]$ is* good *at p.*

Then, if p divides $N = pM$ once and only once, $E[\ell]$ is modular of level M.

The meaning of these three conditions will be explained in Chapter 3. The bulk of the proof of Theorem 0.15 will be given in Chapter 9. The following theorem gives a sufficient condition for condition (i) in Theorem 0.15.

THEOREM 0.16. *Let E be a semistable elliptic curve over $\mathbf{Q}$, all of whose 2-torsion points are $\mathbf{Q}$-rational. Let ℓ be a prime number with $\ell \geq 5$. Then, the group of ℓ-torsion points $E[\ell]$ is irreducible as a representation of the absolute Galois group $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.*

Theorem 0.16 says that if an elliptic curve over $\mathbf{Q}$ satisfies conditions (i) and (ii) of Theorem 0.3, it also satisfies condition (i) of Theorem 0.15. Unfortunately, we can only show a small part of the proof of Theorem 0.16 in this book.

PROOF OF THEOREMS 0.13, 0.15, AND 0.16 $\Rightarrow$ THEOREM 0.3. Let ℓ be a prime number greater than or equal to 5, and let E be an elliptic curve over $\mathbf{Q}$ satisfying all the conditions (i)–(iii) in Theorem 0.3. First we show that the subgroup of ℓ-torsion points $E[\ell]$ is modular of level 2, and then we derive a contradiction from it.

Let N be the conductor of E. N is a square-free positive integer. We show that E satisfies conditions (i)–(iii) in Theorem 0.15 for all primes p greater than or equal to 3. Since E satisfies conditions (i)–(ii) in Theorem 0.3, E satisfies condition (i) in Theorem 0.15 by Theorem 0.16.

By Theorem 0.13, E is modular of level N, and thus E satisfies condition (ii) in Theorem 0.15. If p is an odd prime number, then p satisfies condition (iii) in Theorem 0.3. This implies that E satisfies condition (iii) in Theorem 0.15.

Since N is square-free, by applying Theorem 0.15 to each odd prime factor p of N repeatedly, we see that the subgroup of ℓ-torsion

points $E[\ell]$ is modular of level 2. However, this contradicts the following facts.

PROPOSITION 0.17. *The spaces of modular forms* $S(1)_{\mathbf{C}}$ *of level* 1 *and* $S(2)_{\mathbf{C}}$ *of level* 2 *are both* 0.

This proposition will be proved in Chapter 2. We now come back to the proof of Theorem 0.3. Since the group of ℓ-torsion points $E[\ell]$ is modular of level 2, there must exist a primary form of the level dividing 2. However, the primary form is nonzero, and this contradicts Proposition 0.17. □

To conclude this chapter, we review the outline of the proof by following the diagram (0.2) again. Suppose the equation (0.1) $X^n + Y^n = Z^n$ has a nontrivial integral solution $(X, Y, Z) = (A, B, C)$. We may assume that n is a prime number $\ell \geq 5$, the greatest common divisor of A, B and C is 1, $C \equiv -1 \mod 4$, and B is even. Consider the elliptic curve E_{C^ℓ, B^ℓ} defined by the equation (0.4) $y^2 = x(x - C^\ell)(x - B^\ell)$. Then, by Theorem 0.13, $E = E_{C^\ell, B^\ell}$ is modular. Furthermore, by Theorems 0.15 and 0.16, the group of ℓ-torsion points $E[\ell]$ is modular of level 2. However there does not exist a nonzero modular form of level 1 or 2, which is a contradiction.

We hope the reader has grasped the outline. We begin to see the details from the next chapter. Let us review what we have to prove. If Theorem 0.3 and Proposition 0.4 hold, then Theorem 0.2 holds, and so does Theorem 0.1. This has been proved in §§0.1–0.2. We also explained in §§0.4–0.5 that Theorem 0.3 follows from Theorems 0.13, 0.15, 0.16, and Proposition 0.17. Therefore, what we really have to show are Propositions 0.4 and 0.17, and Theorems 0.13, 0.15, and 0.16. Proposition 0.4 will be proved in Chapters 1 and 3, and Proposition 0.17 will be proved in Chapter 2. Theorem 0.13 will be reduced to Theorem 3.36 in Chapter 4. The outline of the proof of Theorem 3.36 will be illustrated in Chapter 5. Theorem 0.15 will be dealt with in Chapter 9. We will show a part of the proof of Theorem 0.16 in Chapter 4. The proof of Theorem 0.1 will be reviewed in §4.2 again.

Notation and terminology. $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ represent, as usual, the set of nonnegative integers, the ring of rational integers, the rational number field, the real number field, and the complex number field, respectively. A ring always contains a unit 1, and a ring homomorphism maps 1 to 1. The characteristic of a field K is denoted by $\mathrm{char}(K)$.

If a property for prime numbers holds for all but a finite number of primes, we say that this property holds for almost all primes.