IWANAMI SERIES IN MODERN MATHEMATICS

Translations of
MATHEMATICAL
MONOGRAPHS

Volume 186

Number Theory 1

Fermat's Dream

Kazuya Kato
Nobushige Kurokawa
Takeshi Saito

American Mathematical Society

Selected Titles in This Series

186 **Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito,** Number theory 1: Fermat's dream, 2000

185 **Kenji Ueno,** Algebraic Geometry 1: From algebraic varieties to schemes, 1999

184 **A. V. Mel'nikov,** Financial markets, 1999

183 **Hajime Sato,** Algebraic topology: an intuitive approach, 1999

182 **I. S. Krasil'shchik and A. M. Vinogradov, Editors,** Symmetries and conservation laws for differential equations of mathematical physics, 1999

181 **Ya. G. Berkovich and E. M. Zhmud',** Characters of finite groups. Part 2, 1999

180 **A. A. Milyutin and N. P. Osmolovskii,** Calculus of variations and optimal control, 1998

179 **V. E. Voskresenskiĭ,** Algebraic groups and their birational invariants, 1998

178 **Mitsuo Morimoto,** Analytic functionals on the sphere, 1998

177 **Satoru Igari,** Real analysis—with an introduction to wavelet theory, 1998

176 **L. M. Lerman and Ya. L. Umanskiy,** Four-dimensional integrable Hamiltonian systems with simple singular points (topological aspects), 1998

175 **S. K. Godunov,** Modern aspects of linear algebra, 1998

174 **Ya-Zhe Chen and Lan-Cheng Wu,** Second order elliptic equations and elliptic systems, 1998

173 **Yu. A. Davydov, M. A. Lifshits, and N. V. Smorodina,** Local properties of distributions of stochastic functionals, 1998

172 **Ya. G. Berkovich and E. M. Zhmud',** Characters of finite groups. Part 1, 1998

171 **E. M. Landis,** Second order equations of elliptic and parabolic type, 1998

170 **Viktor Prasolov and Yuri Solovyev,** Elliptic functions and elliptic integrals, 1997

169 **S. K. Godunov,** Ordinary differential equations with constant coefficient, 1997

168 **Junjiro Noguchi,** Introduction to complex analysis, 1998

167 **Masaya Yamaguti, Masayoshi Hata, and Jun Kigami,** Mathematics of fractals, 1997

166 **Kenji Ueno,** An introduction to algebraic geometry, 1997

165 **V. V. Ishkhanov, B. B. Lur'e, and D. K. Faddeev,** The embedding problem in Galois theory, 1997

164 **E. I. Gordon,** Nonstandard methods in commutative harmonic analysis, 1997

163 **A. Ya. Dorogovtsev, D. S. Silvestrov, A. V. Skorokhod, and M. I. Yadrenko,** Probability theory: Collection of problems, 1997

162 **M. V. Boldin, G. I. Simonova, and Yu. N. Tyurin,** Sign-based methods in linear statistical models, 1997

(Continued in the back of this publication)

This page intentionally left blank

Number Theory 1
Fermat's Dream

This page intentionally left blank

IWANAMI SERIES IN MODERN MATHEMATICS

Translations of
MATHEMATICAL MONOGRAPHS

10.1090/mmono/186

Volume 186

Number Theory 1
Fermat's Dream

Kazuya Kato
Nobushige Kurokawa
Takeshi Saito

Translated by
Masato Kuwata

American Mathematical Society
Providence, Rhode Island

数論1

SŪRON (Number Theory 1)

by Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito

Originally published in Japanese
by Iwanami Shoten, Publishers, Tokyo, 1996

Translated from the Japanese by Masato Kuwata

The translation of the original book into English has been partially supported
by the Japan Association for Mathematical Sciences.

2000 *Mathematics Subject Classification.* Primary 11-XX, 14-XX.

Library of Congress Cataloging-in-Publication Data

Kato, K. (Kazuya)
[Sūron. English]
Number theory / Kazuya Kato, Nobushige Kurokawa, Takeshi Saito.
p. cm. — (Translations of mathematical monographs, ISSN 0065-9282 ; v. 186) (Iwanami series in modern mathematics)
Includes index.
Contents: v. 1. Fermat's dream
ISBN 0-8218-0863-X (v. 1. : acid-free)
1. Number theory I. Kurokawa, Nobushige, 1952– . II. Saitō, Takeshi, 1961– . III. Title. IV. Series. V. Series: Iwanami series in modern mathematics.
QA241.K36513 1999
512′.7–dc21 99-33556
CIP

10 9 8 7 6 5 4 3 2 05 04 03 02 01 00

Contents

Preface

This book was written in 1996, two hundred years after 1796, which was a very fruitful year for the great Gauss, who made many fundamental contributions to modern number theory. Gauss was in his late teens at the time. On March 30 he discovered a method of construction of a regular 17-gon. On April 8 he proved the quadratic reciprocity law (see §2.2 in this volume), which he himself called a gem. On May 31 he conjectured what would later be called "the prime number theorem" concerning the distribution of prime numbers. On July 10 he proved that any natural number can be expressed as a sum of at most three triangular numbers (see §0.5). On October 1 he obtained a result on the number of solutions for an equation with coefficients in a finite field, which had a great impact on mathematics in later eras. All these contributions are discussed in these volumes, *Number Theory 1, 2, 3.*

One, two, three, four... as naive as it is, the world of numbers encompasses many wonders that fascinated young Gauss. A discovery in one epoch induces a more profound discovery by the following generation. A hundred years later, in 1896, the prime number theorem was proved. After some 120 years, the quadratic reciprocity law had grown into the class field theory. After 150 years, André Weil, who had examined Gauss's result of October 1, proposed the so-called Weil conjectures. These conjectures influenced a great deal of algebraic geometry in the twentieth century. The brilliance of the gems polished by Gauss has increased through the efforts of the mathematicians of following generations. It is said that there is no unexplored place on the earth any longer, but the world of numbers is still full of mysteries. That makes us think of the profoundness and richness of nature.

Wandering naively in the wonderland of numbers, we would like to describe in this book the intricate world of numbers that modern

number theory has discoverd. We will be very happy if the reader discovers the wonders of numbers and the grandeur of nature.

Kazuya Kato, Nobushige Kurokawa, Takeshi Saito

Preface to the English Edition

The authors hope that the readers enjoy the wonderful world of modern number theory through the book.

Our special thanks are due to Dr. Masato Kuwata, who not only translated the Japanese edition into English but also suggested many improvements on the text so that the present English edition is more readable than the original Japanese edition.

This page intentionally left blank

Objectives and Outline of these Books

In these books, *Number Theory 1, 2, 3*, we introduce core theories in modern number theory, such as class field theory, Iwasawa theory, the theory of modular forms, etc. The structure of this book is as follows.

The starting point of number theory is astonishment at the wonders of numbers. The work of Fermat, who is considered to be a founding father of modern number theory, illustrates very well the wonder of numbers. We first discuss the work of Fermat on number theory in the introduction to *Number Theory 1*. The reader will learn how mathematicians of later eras little by little found a fascinating world behind each fact discovered by Fermat. In *Number Theory 1* we study some important topics in modern number theory, such as elliptic curves (Chapter 1), p-adic numbers (Chapter 2), the ζ-function (Chapter 3), and number fields (Chapter 4). These chapters are more or less independent; the material in the earlier chapters is not necessary to understand each succeeding chapter. Chapters 2 and 3 may be easier to read than Chapter 1. The reader should not hesitate to skip parts that are difficult to understand.

Number Theory 2 is devoted to class field theory. We also study the ζ-function once again. In *Number Theory 3* we explain Iwasawa theory and the theory of modular forms, before coming back to elliptic curves once again.

These books are part of the series *Fundamentals of Modern Mathematics*, but we were not satisfied with the introduction of fundamentals. We tried to include today's developments in number theory. For example, we included some important theories developed in recent years, such as the arithemetic theory of elliptic curves, which is part of arithmetic algebraic geometry, and Iwasawa theory, to which we did not find an introduction elsewhere. We hope that we convey the best of modern number theory.

We wanted to include more topics, but we had to omit many of them due to the limitation on the number of pages. We regret that we could not mention Diophantine approximations and transcendental number theory, both of which are seeing new developments in recent years.

Prerequisites to *Number Theory 1* are the fundamentals of groups, rings and fields. In *Number Theory 2* we recommend that the reader be familiar with Galois theory.

The reader is advised to write down simple and easy examples on scratch paper. Just as astronomical observations are indispensable to the study of astronomy, it is indispensable to observe the numbers in order to study number theory. The wonders are there to be discovered. Also, number theory has a long history, which teaches us interesting lessons. We advise you to take an interest in the history of mathematics.

Notation

Throughout the book we use the following symbols:

$\mathbb{Z}$ the set of all integers
$\mathbb{Q}$ the set of all rational numbers
$\mathbb{R}$ the set of all real numbers
$\mathbb{C}$ the set of all complex numbers

A ring is always assumed to have an identity element (written 1), and a homomorphism of rings is assumed to send 1 to 1.

If A is a ring, $A^\times$ denotes the group of invertible elements of A. In particular, if A is a field, $A^\times$ is the multiplicative group consisting of all the nonzero elements of A.

This page intentionally left blank

This page intentionally left blank

Answers to Questions

In what follows we write $\mathrm{ord}_p(a)$ to indicate which power of the prime number p divides the integer a (see §1.3 and §2.4).

Chapter 1

1.1. Suppose that a is the square of a rational number r. For any prime number p we have $\mathrm{ord}_p(a) = 2\,\mathrm{ord}_p(r)$. Since $\mathrm{ord}_p(a) \geq 0$, we have $\mathrm{ord}_p(r) \geq 0$. The number r is an integer since we have $\mathrm{ord}_p(r) \geq 0$ for all prime numbers p.

1.2. Suppose that p is a prime factor of a_i. By hypothesis we have $\mathrm{ord}_p(a_j) = 0$ for all j different from i. Thus, we have $\mathrm{ord}_p(a_1 \cdots a_r) = \mathrm{ord}_p(a_i)$. On the other hand, since $a_1 \ldots a_r$ is a k-th power, $\mathrm{ord}_p(a_1 \cdots a_r)$ is a multiple of k. Thus, for any prime number p, $\mathrm{ord}_p(a_i)$ is a multiple of k. This implies that a_i is the product of integers of the form p^{km} (m is a natural number), and thus a_i is a k-th power.

1.3. Let (x, y) be the coordinates of the nonzero element P in $E(K)$. Then, the coordinates of $-P$ are $(x, -y)$. The condition $2P = O$ is equivalent to the condition $P = -P$. Thus, it is equivalent to $y = -y$, i.e., $y = 0$. If K is an algebraically closed field, there are three nonzero elements P in $E(K)$ whose y-coordinate is 0. Therefore, $\{P \in E(K) \mid 2P = O\}$ is a group of order 4. Since twice of every element in the group $E(K)$ is O, we see that $E(K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

1.4. The first part is easy. As for the second part, take $A = \mathbb{Q}$. Then, we have $A/2A = \{0\}$, but A is not finitely generated.

Chapter 2

2.1. For example, $\left(\frac{11}{5}, \frac{2}{5}\right)$. This is the point of intersection between the circle and the line with slope -3 passing through $(2, 1)$.

2.2. It suffices to find a rational point on the circle $x^2 + y^2 = 1$ that is very close to the rational point $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$. The slope of the line joining $(-1, 0)$ and $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$ is $\sqrt{2} - 1 = 0.414\cdots$, while the slope of the line joining $(-1, 0)$ and $\left(\frac{119}{169}, \frac{120}{169}\right)$ is $\frac{5}{12} = 0.416\cdots$, as we have seen in the text. Thus, it suffices to take the line passing through $(0, -1)$ whose slope is 0.415 and to find the other point of intersection with the circle. A calculation shows that the coordinate of the other point of intersection is given by $\left(\frac{33111}{46889}, \frac{33200}{46889}\right)$, and we see that

$$33111^2 + 33200^2 = 46889^2.$$

2.3. $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right)$.

2.4. Factor m as $m = l_1 \cdots l_k \cdot r$, where $l_1, \ldots, l_k$ are odd prime numbers and $r \in \{\pm 2^n \mid n \geq 0\}$. If m is odd, we have $r \in \{\pm 1\}$, and

$$\begin{aligned}\left(\frac{m}{p}\right) &= \left(\frac{l_1}{p}\right)\cdots\left(\frac{l_k}{p}\right)\left(\frac{\pm 1}{p}\right) \\ &= \left(\frac{p}{l_1}\right)\cdots\left(\frac{p}{l_k}\right) \times (\text{number determined by } p \bmod 4).\end{aligned}$$

Similarly, if m is even, we have

$$\left(\frac{m}{p}\right) = \left(\frac{p}{l_1}\right)\cdots\left(\frac{p}{l_k}\right) \times (\text{number determined by } p \bmod 8).$$

2.5. The fact that the circle $\frac{15}{36}x^2 - \frac{1}{36}y^2 = 1$ does not have a rational point can be seen from the fact that $\left(\frac{15}{36}, -\frac{1}{36}\right)_p = (15, -1)_p = -1$ if $p = 2$ or $p = 3$.

2.6. $\operatorname{ord}_p\left(\sum_{i=0}^{n} c^i - \frac{1}{1-c}\right) = \operatorname{ord}_p\left(-\frac{c^{n+1}}{1-c}\right) \geq n + 1$.

2.7. The equation (2.9) is equivalent to $\sum_{i=0}^{\infty} 6 \times (-5)^i = 1$ (5-addically). The latter shows that we have $\sum_{i=0}^{m} 6 \times (-5)^i \equiv 1 \bmod 5^n$ when m is sufficiently large.

2.8. We have $\frac{1}{4} = \frac{1}{1+3} = 1 - 3 + 3^2 - 3^3 + 3^4 - 3^5 + 3^6 - \cdots = 61 - 3^5 + 3^6 - \cdots$. Therefore, 61 is the inverse of $\frac{1}{4}$.

2.9. If N is a natural number greater than 1, then the N-adic expansion of a real number α is to express α as

$$\alpha = \sum_{n=m}^{\infty} a_n N^{-n}, \quad a_n \in \{0, 1, \ldots, N-1\}.$$

On the other hand, the p-adic expansion of a p-adic number is of the form $\sum_{n=m}^{\infty} a_n p^n$. The difference is that in the p-adic expansion of a real number, the terms p^n with negative n may appear infinitely many times and the terms p^n with positive n appear only finitely many times, whereas in the p-adic expansion of a p-adic number the terms p^n with negative n may

appear only finitely many times and the terms p^n with positive n appear infinitely many times.

2.10. The existence of a square root of a follows from Proposition 2.18 and the fact that ± 1 are squares in $\mathbb{F}_5$.

2.11. If $p \neq 2$, it follows from Proposition 2.18 that

$$\mathbb{Q}_p \text{ has a square root of } -1 \iff \mathbb{F}_p \text{ has a square root of } -1.$$

If $p = 2$, it follows from Proposition 2.18 and the fact $-1 \not\equiv 1 \bmod 8$ that $\mathbb{Q}_2$ does not have a square root of -1.

2.12. It follows from field theory that any quadratic extension of a field K of characteristic different from 2 is of the form $K(\sqrt{a})$, $(a \in K, \sqrt{a} \notin K)$, and

$$K(\sqrt{a}) = K(\sqrt{b}) \iff ab^{-1} \text{ is a square in } K.$$

Thus, the correspondence that associates $a \bmod (K^\times)^2$ $(a \in K, \sqrt{a} \notin K)$ to $K(\sqrt{a})$ is a one-to-one correspondence between the quadratic extensions of K and the elements of $K^\times/(K^\times)^2$ different from the identity. If $p \neq 2$, then the order of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ is 4 (Proposition 2.19(1)). Thus, the number of quadratic extensions of $\mathbb{Q}_p$ is $4-1=3$. Furthermore, the group $\mathbb{Q}_5^\times/(\mathbb{Q}_5^\times)^2$ consists of classes of 1, 2, 5 and 10, and thus $\mathbb{Q}_5(\sqrt{2})$, $\mathbb{Q}_5(\sqrt{5})$ and $\mathbb{Q}_5(\sqrt{10})$ are all the quadratic extensions of $\mathbb{Q}_5$.

Chapter 3

3.1. By Proposition 3.3(1) we have

$$h_1(i) = -\frac{1}{2} \cdot \frac{1}{2\pi i} \sum_{n \in \mathbb{Z}} \left(\frac{1}{i+n} + \frac{1}{i-n} \right) = \frac{1}{2\pi} \sum_{n \in \mathbb{Z}} \frac{1}{n^2+1}.$$

On the other hand, we have $h_1(i) = -\frac{1}{2i} \cdot \frac{(e^{-\pi}+e^{\pi})/2}{(e^{-\pi}-e^{\pi})/2i}$.

3.2. Use the formula

$$\frac{1}{(n^2+1)^2} = -\frac{1}{4(i+n)^2} - \frac{1}{4(i-n)^2} - \frac{1}{4i} \left(\frac{1}{i+n} + \frac{1}{i-n} \right).$$

3.3. The image of χ is the set of all the n-th roots of unity $\{\zeta_n^r \mid 1 \leq r \leq n\}$ for some $n \geq 2$. Let k be the order of the kernel of χ. For each r satisfying $1 \leq r \leq n$, χ takes the value ζ_n^r on k different elements in G. Thus, $\sum_{a \in G} \chi(a) = \sum_{r=1}^{n} k \cdot \zeta_n^r = 0$.

3.4. We have

$$\begin{aligned}\zeta\left(s,\frac{5}{2}\right) &= 2^s\left(\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{9^s}+\cdots\right)\\ &= 2^s\left(\left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right)-\left(\sum_{n=1}^{\infty}\frac{1}{(2n)^s}\right)-1-\frac{1}{3^s}\right)\\ &= 2^s\zeta(s)-\zeta(s)-2^s-\left(\frac{2}{3}\right)^s.\end{aligned}$$

Thus, we have

$$\begin{aligned}\lim_{s\to 1}\left(-\zeta\left(s,\frac{5}{2}\right)+\zeta(s)\right) &= \lim_{s\to 1}(2-2^s)\zeta(s)+2+\frac{2}{3}\\ &= \lim_{s\to 1}\frac{2-2^s}{s-1}(s-1)\zeta(s)+2+\frac{2}{3}\\ &= \frac{8}{3}-2\log(2).\end{aligned}$$

Here, we used $\lim_{s\to 1}(s-1)\zeta(s)=1$ (Proposition 3.15(2)) to prove the last equality.

3.5. By Proposition 3.24(1), a prime factor of the denominator of $\zeta(m)$ satisfies $m\equiv 1 \bmod p-1$. Since $p-1$ divides $1-m$, we have $p-1\leq 1-m$. Hence $p\leq 2-m$.

Chapter 4

4.1. Factor the equation as $x^3=(y+i)(y-i)$, and use a similar argument as in Proposition 0.11 to obtain

$$y+i=(a+bi)^3,\quad a,b\in\mathbb{Z}.$$

Comparing the imaginary parts of both sides, we obtain $1=3a^2b-b^3=(3a^2-b^2)b$. Thus, we have $b=\pm 1$. The rest is easy.

4.2. Factor the equation as $x^3=(y+\sqrt{-11})(y-\sqrt{-11})$, and use a similar argument as in Proposition 0.10 to obtain

$$y+\sqrt{-11}=\left(a+b\frac{1+\sqrt{-11}}{2}\right)^3,\quad a,b\in\mathbb{Z}.$$

(Here, we used the fact that the only common prime factors of $y+\sqrt{-11}$ and $y-\sqrt{-11}$ are $\pm\sqrt{-11}$ and ± 2.) Comparing the imaginary parts of both sides, we obtain $1=3\left(a+\frac{b}{2}\right)^2\frac{b}{2}-11\left(\frac{b}{2}\right)^3$. From this we obtain $(3a^2+3ab-2b^2)b=2$. Thus, we have $b\in\{\pm 1,\pm 2\}$. The rest is easy.

4.3. Let m be an integer that is not divisible by any square except for 1. Let $K = \mathbb{Q}(\sqrt{m})$, $\alpha = x + y\sqrt{m}$ $(x, y \in \mathbb{Q})$ and $\alpha' = x - y\sqrt{m}$.

(i) First we show that $\alpha \in O_K$ is equivalent to the fact that the rational numbers $\alpha + \alpha' = 2x$ and $\alpha\alpha' = x^2 - my^2$ both belong $\mathbb{Z}$. If $\alpha \in O_K$, then by replacing α by α' in the equation $\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$ $(n \geq 1,\ c_1, \ldots, c_n \in \mathbb{Z})$, we see that $\alpha' \in O_K$. Therefore, we have $\alpha + \alpha'$, $\alpha\alpha' \in O_K$. Thus, these numbers belong to $O_K \cap \mathbb{Q} = \mathbb{Z}$. Conversely, if we have $\alpha + \alpha'$, $\alpha\alpha' \in \mathbb{Z}$, then α satisfies the equation $\alpha^2 + c_1\alpha + c_2 = 0$ with $c_1 = -(\alpha + \alpha')$ and $c_2 = \alpha\alpha'$. This implies that α belongs to O_K.

(ii) By (i) it suffices to show the following: For $x, y \in \mathbb{Q}$

$$2x,\ x^2 - my^2 \in \mathbb{Z} \iff x, y \in \mathbb{Z},$$

if $m \equiv 2, 3 \bmod 4$, and

$$2x,\ x^2 - my^2 \in \mathbb{Z} \iff 2x, 2y \in \mathbb{Z} \text{ and } x - y \in \mathbb{Z},$$

if $m \equiv 1 \bmod 4$.

(iii) Show first that if $x, y \in \mathbb{Q}$ satisfies $2x,\ x^2 - my^2 \in \mathbb{Z}$, then we have $2y \in \mathbb{Z}$. If l is an odd prime number, it follows from $\mathrm{ord}_l(x) \geq 0$ and $x^2 - my^2 \in \mathbb{Z}$ that $\mathrm{ord}_l(m) + 2\,\mathrm{ord}_l(y) \geq 0$. Since $\mathrm{ord}_l(m) \leq 1$, we have $2\,\mathrm{ord}_l(y) \geq -1$. Thus we have $\mathrm{ord}_l(y) \geq 0$. Since $\mathrm{ord}_2(x) \geq -1$ and $x^2 - my^2 \in \mathbb{Z}$, we have $\mathrm{ord}_2(m) + 2\,\mathrm{ord}_2(y) \geq -2$. Since $\mathrm{ord}_2(m) \leq 1$, we have $2\,\mathrm{ord}_2(y) \geq -3$. Thus, we have $\mathrm{ord}_2(y) \geq -1$. Summing it all up, we see that $2y \in \mathbb{Z}$.

(iv) To show the equivalence in (ii), we may assume $2x, 2y \in \mathbb{Z}$ because of (iii). Suppose $2x = u$ and $2y = v$ $(u, v \in \mathbb{Z})$. If $m \equiv 2, 3 \bmod 4$, it suffices to show

$$u^2 - mv^2 \equiv 0 \mod 4 \iff u \equiv v \equiv 0 \mod 2,$$

and if $m \equiv 1 \bmod 4$, it suffices to show

$$u^2 - mv^2 \equiv 0 \mod 4 \iff u \equiv v \mod 2.$$

These are easy to show.

4.4. Similar to the proof or Proposition 4.1(5).

4.5. The answers are 1, 2, 2 and 2, respectively. As an example, we treat the case $\mathbb{Q}(\sqrt{-2})$. We have $w_K = 2$ and $N = 8$, and $\chi : (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}^\times$ is given by

$$\chi(1 \bmod 8) = \chi(3 \bmod 8) = 1, \quad \chi(5 \bmod 8) = \chi(7 \bmod 8) = -1.$$

By Corollary 4.29 we have $h_K = -\frac{2}{2\times 8}\sum_{a=1}^{8} \chi(a)a = -\frac{2}{16}(1+3-5-7) = 1$.

This page intentionally left blank

Answers to Exercises

Chapter 0

0.1. Suppose that the n-th root of 5 is a rational number and that it factors as $\pm p_1^{e_1} \cdots p_r^{e_r}$ ($p_1, \ldots, p_r$ distinct primes, e_i integers satisfying $e_i \neq 0$). Taking the n-th power, we have $5 = p_1^{ne_1} \cdots p_r^{ne_r}$. This is a contradiction to the uniqueness of prime factorization since $n \geq 2$.

0.2. If $\sqrt{2} + \sqrt{3}$ is a rational number, so is $5 + 2\sqrt{6}$. Thus, $\sqrt{6}$ is a rational number. But we can show that $\sqrt{6}$ is an irrational number by a similar method as Exercise 0.1.

0.3. $29 = 2^2 + 5^2$, $37 = 1^2 + 6^2$, $41 = 4^2 + 5^2$, $53 = 2^2 + 7^2$.

0.4. Combining factorizations $5 = (2+i)(2-i)$ and $13 = (3+2i)(3-2i)$, we have

$$\begin{aligned} 65^2 &= \big((2+i)(3+2i)\big)^2\big((2-i)(3-2i)\big)^2 \\ &= (-33+56i)(-33-56i) = 33^2 + 56^2, \\ 65^2 &= \big((2+i)(3-2i)\big)^2\big((2-i)(3+2i)\big)^2 \\ &= (63-16i)(63+16i) = 63^2 + 16^2. \end{aligned}$$

0.5. If x and y satisfy $x^2 - 2y^2 = 1$, then we have $\left(\frac{x}{y} - \sqrt{2}\right)\left(\frac{x}{y} + \sqrt{2}\right) = \frac{1}{y^2}$. Thus, we have $0 < \frac{x}{y} - \sqrt{2} < \frac{1}{\sqrt{2}y^2}$. This shows that $\frac{x}{y}$ becomes closer to $\sqrt{2}$ as y gets bigger.

0.6. It suffices to show that infinitely many pairs of natural numbers (x, y) satisfy $\frac{1}{2}y(y+1) = x^2$. Rewrite this equation as

$$(2y+1)^2 - 2(2x)^2 = 1.$$

For $n \geq 1$, define a_n and b_n by $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$. We have

$$a_n^2 - 2b_n^2 = (a_n + b_n\sqrt{2})(a_n - b_n\sqrt{2}) = (1+\sqrt{2})^n(1-\sqrt{2})^n = (-1)^n.$$

By expanding $(1+\sqrt{2})^n$, we see that $a_n = 1 + (\text{even number})$ and $b_n = n + (\text{even number})$. Thus, if we take an even number as n, then we have

$a_n^2 - 2b_n^2 = 1$ with a_n odd and b_n even. If we set $y = \frac{a_n - 1}{2}$ and $x = \frac{b_n}{2}$, then we have $(2y+1)^2 - 2(2x)^2 = 1$.

Chapter 1

1.1. Answer: The set in question consists of nine points O, $(0, \pm 1)$, $(-\sqrt[3]{4}, \pm\sqrt{-3})$, $(-\sqrt[3]{4}\zeta_3, \pm\sqrt{-3})$ and $(-\sqrt[3]{4}\zeta_3^2, \pm\sqrt{-3})$, where ζ_3 is a primitive cube root of unity.

The method of finding these points: First, we see that $3P = O$ is equivalent to $2P = -P$. In general, if we denote by $x(P)$ the x-coordinate of $P \in E(\mathbb{C})$, $P \neq O$, then we have

$$x(P) = x(Q) \Longleftrightarrow Q = \pm P$$

for any $P, Q \in E(\mathbb{C})$. Thus, we have

$$3P = O,\ P \neq O \iff x(2P) = x(P) \text{ and } P \neq O.$$

For any point P in $E(\mathbb{C})$ satisfying $2P \neq O$ we have $x(2P) = \frac{x(P)^4 - 8x(P)}{4(x(P)^3+1)}$ (§1.2(1.4)). Therefore, $x(2P) = x(P)$ if and only if $x(P) = 0, -\sqrt[3]{4}, -\sqrt[3]{4}\zeta_3$ or $-\sqrt[3]{4}\zeta_3^2$.

1.2. Let m and n be relatively prime integers and let

$$A = |(m^3 + 32n^3)m| \quad \text{and} \quad B = |4(m^3 - 4n^3)n|.$$

Denote by D the greatest common divisor of A and B. In order to show the inequality in question, it suffices to show that D is a divisor of 144. For, if that is the case and if the x-coordinate of P is given by $\frac{m}{n}$ $(n \neq 0)$ in lowest terms, then we have

$$\begin{aligned} H(x\text{-coordinate of } 2P) &= H\left(\frac{A}{B}\right) = \frac{1}{D}\max(A, B) \\ &\geq \frac{1}{D}\max(m, n)^4 = \frac{1}{D}H(x\text{-coordinate of } P)^4. \end{aligned}$$

Let p be a prime number. We have $\mathrm{ord}_p(D) = \min(\mathrm{ord}_p(A), \mathrm{ord}_p(B))$ (since ord_p indicates how many times p divides the number). If p is a prime factor of D, then p does not divide n (since if it does, p does not divide m, and thus p does not divide $m^3 + 32n^3$ and A). If p is a prime factor of D and $p \neq 2$, then p does not divide m (since if $p \neq 2$ and p divides m, then p does not divide B). Thus, if p is a prime factor of D and $p \neq 2$, then we have

$$\begin{aligned} \mathrm{ord}_p(D) &= \min\big(\mathrm{ord}_p(m^3 + 32n^3),\ \mathrm{ord}_p(m^3 - 4n^3)\big) \\ &\leq \mathrm{ord}_p\big((m^3 + 32n^3) - (m^3 - 4n^3)\big) \\ &= \mathrm{ord}_p(36n^3) = \mathrm{ord}_p(36). \end{aligned}$$

Hence, we have $p = 3$ and $\mathrm{ord}_3(D) \leq 2$.

Next, we consider $\mathrm{ord}_2(D)$. If m is odd, then $\mathrm{ord}_2(A) = 0$. If m is even, then $\mathrm{ord}_2(m^3 - 4n^3) = 2$ since n is even. Hence we have $\mathrm{ord}_2(B) = 4$. Therefore, D is a divisor of $2^4 \times 3^2 = 144$, and thus the inequality in question is proved.

If $r \geq 6$, then we have the inequality $\frac{1}{144}r^4 > r$. If a rational point P on the elliptic curve in question satisfies $H(x\text{-coordinate of } P) \geq 6$, then we have $H(x\text{-coordinate of } P) > H(x\text{-coordinate of } 2P)$. Then the height of the x-coordinate of P, $2P$, $4P$, $8P$, $16P, \ldots$ are all different. Thus, these points are all distinct. This means there are infinitely many rational points on this elliptic curve. (To be more precise, we can show the following. If integers m and n satisfy $m \not\equiv 0 \bmod 3$ or $n \not\equiv 0 \bmod 3$, then $m^3 - 4n^3 \not\equiv 0 \bmod 9$. This can be done by checking all the possibilities of $0 \leq m \leq 8$, $0 \leq n \leq 8$. Thus we see that D is a divisor of $2^4 \times 3 = 48$ and that

$$48 \cdot H(x\text{-coordinate of } 2P) \geq H(x\text{-coordinate of } P)^4.$$

If $r \geq 4$, then $\frac{1}{48}r^4 > r$. Thus, if $P = (5, 11)$, then the x-coordinates of $P, 2P, 4P, 8P, \ldots$ all have different heights. This implies that we see the existence of infinitely many rational points as soon as we find one rational point $(5, 11)$.)

1.3. Since for $(x, y) \in X$ we have

$$\left(\frac{x-y}{x+y}\right)^2 + \frac{1}{3} = \frac{4}{3} \cdot \frac{x^2 - xy + y^2}{(x+y)^2} = \frac{4k}{3} \cdot \frac{1}{(x+y)^3},$$

we have $\left(\frac{1}{x+y}, \frac{x-y}{x+y}\right) \in Y$. This map is bijective since the map $Y \to X$ given by $(x, y) \mapsto \left(\frac{y+1}{2x}, \frac{1-y}{x}\right)$ is the inverse. (We omit the proof of the fact that we have $\left(\frac{y+1}{2x}, \frac{1-y}{x}\right) \in X$ for $(x, y) \in Y$ and that the compositions $X \to Y \to X$ and $Y \to X \to Y$ are both identities.)

1.4. The inverse is given by $(x, y) \mapsto \left(\frac{y}{2x}, \frac{x}{4} + \frac{k}{x}\right)$.

1.5. We omit the proof of 1.5 since each verification is straightforward, as was the case with 1.3 and 1.4.

1.6. (i) Answer: $(x, y) = (0, 0), (2, \pm 4)$. Reason: If $(x, y) \neq (0, 0)$ is a rational point on the curve $y^2 = x^3 + 4x$, then by considering the case $k = -1$ in Question 1.5, we see that $g(x, y) = \left(\frac{x}{4} - \frac{1}{x}, \frac{y}{8}\left(1 - \frac{4}{x^2}\right)\right)$ is a rational point on the curve $y^2 = x^3 - x$. From Proposition 1.2 we know that this point is one of $(0, 0), (\pm 1, 0)$. Therefore, we have $\frac{y}{8}\left(1 - \frac{4}{x^2}\right) = 0$. Hence $y = 0$ or $x = \pm 2$.

(ii) Answer: $(x, y) = (\pm 1, 0)$. Reason: If (x, y) is a rational point on the curve $y^2 = x^4 - 1$, then by considering the case $k = -1$ in 1.4 and 1.5, the image of (x, y) by the map $X \to Y \xrightarrow{g} E(K)$ given by $(x, y) \mapsto (x^2, xy)$ is a rational point on the curve $y^2 = x^3 - x$. Thus, we obtain $xy = 0$.

(iii) Answer: $(x, y) = (0, \pm 2)$. Reason: Just as (ii), we see that if (x, y) is a rational point on the curve $y^2 = x^4 + 4$, then (x^2, xy) is a rational point on the curve $y^2 = x^3 + 4x$. Thus, it follows from (i) that (x^2, xy) equals one of $(0, 0), (2, \pm 4)$.

Chapter 2

2.1. For example, $\frac{2^n}{2^n+1}$ converges to 1 in $\mathbb{R}$, but it converges to 0 in $\mathbb{Q}_2$. The sequence $\frac{2^n}{2^n+3^n}$ converges to 1 in $\mathbb{Q}_3$ (since $3^n \to 0$), but it converges to 1 in $\mathbb{Q}_2$.

2.2. Let f be an element of $\mathrm{Hom}\left(\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}, \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}\right)$. For any $n \geq 1$ we denote by f_n the restriction of f to $\left(\frac{1}{p^n}\mathbb{Z}\right)/\mathbb{Z}$. The image of the map $f_n : \left(\frac{1}{p^n}\mathbb{Z}\right)/\mathbb{Z} \to \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$ is contained in the kernel $\left(\frac{1}{p^n}\mathbb{Z}\right)/\mathbb{Z}$ of the multiplication-by-p^n map of $\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$ (since every element of the subgroup $\left(\frac{1}{p^n}\mathbb{Z}\right)/\mathbb{Z}$ becomes 0 if it is multiplied by p^n). Thus, f_n is a homomorphism from $\left(\frac{1}{p^n}\mathbb{Z}\right)/\mathbb{Z}$ to $\left(\frac{1}{p^n}\mathbb{Z}\right)/\mathbb{Z}$, and it coincides with the multiplication-by-a_n map of $\mathbb{Z}/p^n\mathbb{Z}$ for some element a_n. Thus, we obtain a ring homomorphism

$$\varphi : \mathrm{Hom}\left(\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}, \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}\right) \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}; \quad \varphi(f) = (a_n)_{n\geq 1}.$$

Conversely, we can find a ring homomorphism

$$\psi : \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \to \mathrm{Hom}\left(\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}, \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}\right)$$

as follows. Let $(a_n)_{n\geq 1} \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. For $x \in \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$ there exists a positive integer n such that $x \in \left(\frac{1}{p^n}\mathbb{Z}\right)/\mathbb{Z}$ since $\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z} = \bigcup_{n\geq 1}\left(\frac{1}{p^n}\mathbb{Z}\right)/\mathbb{Z}$. We obtain a homomorphism $f \in \mathrm{Hom}\left(\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}, \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}\right)$ by defining $f(x) = a_n x$. Define $\psi((a_n)_{n\geq 1}) = f$. It is easy to check that $\psi \circ \varphi$ and $\varphi \circ \psi$ are the identities of $\mathrm{Hom}\left(\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}, \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}\right)$ and $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, respectively. Hence, we have

$$\mathrm{Hom}\left(\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}, \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}\right) \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p\,.$$

2.3. For $n \neq 0$ define $k = \mathrm{ord}_3(n)$. From Proposition 2.14(4) we see the following. Since 4 belongs to $1 + 3\mathbb{Z}_3$, but not to $1 + 9\mathbb{Z}_3$, $\log(4)$ belongs to $3\mathbb{Z}_3$, but not to $9\mathbb{Z}_3$. Thus, $n\log(4)$ belongs to $3^{k+1}\mathbb{Z}_3$, but not to $3^{k+2}\mathbb{Z}_3$. Thus, $4^n = \exp(n\log(4))$ belongs to $1 + 3^{k+1}\mathbb{Z}_3$, but not to

$1+3^{k+2}\mathbb{Z}_3$. Thus 4^n-1 belongs to $3^{k+1}\mathbb{Z}_3$, but not to $3^{k+2}\mathbb{Z}_3$. Hence, we have $\mathrm{ord}_3(4^n-1)=k+1$.

2.4. First, (1) follows from Proposition 2.18 and the fact that for an odd prime number p we have

$$\left(\frac{-2}{p}\right)=1 \iff p\equiv 1,3 \mod 8.$$

Next, the equation $x^2+y^2=-2$ in (2) can be written as $-\frac{1}{2}x^2-\frac{1}{2}y^2=1$. The necessary and sufficient condition for the existence of $x,y\in\mathbb{Q}_p$ satisfying the equation is $\left(-\frac{1}{2},-\frac{1}{2}\right)_p=1$ by Proposition 2.20. But, if $p\neq 2$, we have $\left(-\frac{1}{2},-\frac{1}{2}\right)_p=1, \left(-\frac{1}{2},-\frac{1}{2}\right)_2=-1$. In order to show (3), it suffices to show the existence of elements x, y and z in $\mathbb{Q}_2$ satisfying $x^2+y^2+z^2=-2$ (since if $p\neq 2$, a solution of $x^2+y^2=-2$ satisfies $x^2+y^2+0^2=-2$). In $\mathbb{Q}_2$, 14 is very close to -2, and we have $1^2+2^2+3^2=14$. Since $\frac{14}{-2}=-7\equiv 1 \mod 8$, it follows from Proposition 2.18 that there exists $a\in\mathbb{Q}_2^\times$ such that $a^2=\frac{14}{-2}$. Thus, we have $-2=\frac{14}{a^2}=\left(\frac{1}{a}\right)^2+\left(\frac{2}{a}\right)^2+\left(\frac{3}{a}\right)^2$.

Chapter 3

3.1. (1) Consider the Dirichlet character $\chi:(\mathbb{Z}/8\mathbb{Z})^\times\to\mathbb{C}^\times$ given by $\chi(1 \mod 8)=\chi(3 \mod 8)=1$ and $\chi(5 \mod 8)=\chi(7 \mod 8)=-1$. Then (1) is to find $L(1,\chi)$. Since $\chi(-1)=-1$, it follows from Theorem 3.4 that

$$L(1,\chi)=-\frac{2\pi i}{8}\cdot\frac{1}{2}\cdot(h_1(\zeta_8)+h_1(\zeta_8^3)-h_1(\zeta_8^5)-h_1(\zeta_8^7))=\frac{\pi}{2\sqrt{2}}.$$

(2) Consider the Dirichlet character $\chi:(\mathbb{Z}/8\mathbb{Z})^\times\to\mathbb{C}^\times$ given by $\chi(1 \mod 8)=\chi(7 \mod 8)=1$, $\chi(3 \mod 8)=\chi(5 \mod 8)=-1$. Then (2) is to find $L(2,\chi)$. Since $\chi(-1)=1$, it follows from Theorem 3.4 that

$$L(2,\chi)=\left(-\frac{2\pi i}{8}\right)^2\cdot\frac{1}{2}\cdot(h_2(\zeta_8)-h_2(\zeta_8^3)-h_2(\zeta_8^5)+h_2(\zeta_8^7))=\frac{\sqrt{2}}{16}\pi^2.$$

3.2. (1) $(1-2^{1-s})\zeta(s)=\sum_{n=1}^\infty\frac{1}{n^s}-2\sum_{n=1}^\infty\frac{1}{(2n)^s}=1-\frac{1}{2^s}+\frac{1}{3^s}-\frac{1}{4^s}+\frac{1}{5^s}-\frac{1}{6^s}+\cdots$.

(2) $\lim_{s\to 1+0}(s-1)\zeta(s)=\lim_{s\to 1+0}\frac{s-1}{1-2^{1-s}}\cdot\left(1-\frac{1}{2^s}+\frac{1}{3^s}-\frac{1}{4^s}+\cdots\right)=\frac{1}{\log 2}\cdot\log 2=1$.

3.3. By calculating $s_1-s_3-s_5+s_7$, we have

$$-\log\left(\frac{(1-\zeta_8)(1-\zeta_8^7)}{(1-\zeta_8^3)(1-\zeta_8^5)}\right)=(\zeta_8-\zeta_8^3-\zeta_8^5+\zeta_8^7)L(1,\chi),$$

where χ is the same character as the one in Exercise 3.1(2). We have

$$-\log\left(\frac{1}{(1+\sqrt{2})^2}\right)=2\sqrt{2}L(1,\chi).$$

Hence, $L(1,\chi) = \frac{1}{\sqrt{2}}\log(1+\sqrt{2})$.

3.4. We omit the proof of absolute convergence, and we explain the analytic continuation and the values at nonpositive integers. For simplicity, we denote the sum over $n_1,\dots,n_k \geq 0$ just by $\sum$. We have

$$\begin{aligned}\Gamma(s)\zeta(s,x;c_1,\cdots,c_k) &= \int_0^\infty e^{-t}t^s\frac{dt}{t}\cdot\sum\frac{1}{(x+c_1n_1+\cdots+c_kn_k)^s}\\ &= \int_0^\infty\sum e^{-(x+c_1n_1+\cdots+c_kn_k)u}u^s\frac{du}{u}\\ &= \int_0^\infty\frac{e^{-xu}}{(1-e^{-c_1u})\cdot\cdots\cdot(1-e^{-c_ku})}u^s\frac{du}{u}.\end{aligned}$$

Let $a>0$. Divide the integral $\int_0^\infty = \int_0^a + \int_a^\infty$. Since e^{-xu} approaches very rapidly as u goes to ∞, the part $\int_a^\infty$ can be analytically continued to the entire plane as a holomorphic function in s. Take a small enough that $1-e^{-c_iu}\,(1\leq i\leq k)$ does not have a zero in $0<|u|\leq a$. Then, in $0<u\leq a$ we have

$$c_1\cdots c_k\cdot\frac{e^{-xu}}{(1-e^{-c_1u})\cdot\cdots\cdot(1-e^{-c_ku})} = u^{-k}\sum_{n=0}^\infty A_nu^n,$$

where A_n is a polynomial in $x,c_1,\dots,c_k$ with $\mathbb{Q}$ coefficients. Thus, we have

$$c_1\cdots c_k\cdot\int_0^a = \sum_{n=0}^\infty A_n\cdot\frac{a^{s+n-k}}{s+n-k}.$$

Therefore, $\zeta(s,x;c_1,\dots,c_k)$ may be analytically continued to the entire plane and we see that it is holomorphic outside $1,2,\dots,k$. If m is a negative integer or 0, then we have

$$\begin{aligned}&c_1\cdots c_k\cdot\zeta(m;x,c_1,\dots,c_k)\\ &\qquad = \lim_{s\to m}\frac{1}{\Gamma(s)}\cdot A_{k-m}\cdot\frac{a^{s-m}}{s-m} = A_{k-m}\cdot(-1)^m\cdot|m|!.\end{aligned}$$

Chapter 4

4.1. Since $x^2+xy+2y^2 = \left(x+y\frac{1+\sqrt{-7}}{2}\right)\left(x+y\frac{1-\sqrt{-7}}{2}\right)$, we have

$$\text{(i)} \iff \text{There exists } \alpha\in\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \text{ such that } p=\alpha\overline{\alpha}.$$

Using a similar argument to the proofs of Propositions 0.2, 0.3 and 0.4 in §4.1, we have

$$\text{The above condition} \iff \left(\frac{-7}{p}\right)=1 \iff p\equiv 1,2,4 \mod 7,$$

if $p\neq 2,7$.

4.2. If (ii) is satisfied, then we have $n = m^2 \prod_{j=1}^{r} p_j$, where m is a natural number, $r \geq 0$, and p_j is a prime number congruent to 1 modulo 4 or $p_j = 2$. We have $p_j = \alpha_j \overline{\alpha}_j$, $\alpha_j \in \mathbb{Z}[\sqrt{-1}]$. Writing $m \prod_{j=1}^{r} \alpha_j$ as β and putting $\beta = x + yi$ $(x, y \in \mathbb{Z})$, we have $n = \beta\overline{\beta} = x^2 + y^2$.

If (ii) is not satisfied, then there exists a prime number $p \equiv 3 \bmod 4$ such that $\mathrm{ord}_p(n)$ is odd. Since $(-1, n)_p = \left(\frac{-1}{p}\right) = -1$, we see that there do not exist $x, y \in \mathbb{Q}$ such that $n = x^2 + y^2$.

4.3. Put $p = \alpha\overline{\alpha}$ (α is a prime element of $\mathbb{Z}[i]$), and put $\alpha^{2n} = x + yi$. Then we have $p^{2n} = \alpha^{2n}\overline{\alpha}^{2n} = x^2 + y^2$. Because of the unique prime factorization property we have $x \neq 0$, $y \neq 0$. Thus, p^n is the hypotenuse of the right triangle formed by x, y and p^n. Since α^{2n} is not divisible p, the greatest common divisor of the three sides is 1. We show that this is the only triangle up to congruence. Suppose that $p^{2n} = x^2 + y^2$ with x, y natural numbers. We have $p^{2n} = (x + yi)(x - yi)$. Consider the prime factorization of both sides, we see that $x+yi = \alpha^r\overline{\alpha}^s\beta$, $x-yi = \alpha^s\overline{\alpha}^r\overline{\beta}$, $r \geq 0$, $s \geq 0$, $r + s = 2n$, $\beta \in \{\pm 1, \pm i\}$. If $r \neq 0$, $s \neq 0$, $x + yi$ is divisible by p, and thus x, y, p^n are all divisible by p. If $r = 0$ or $s = 0$, we have $x + yi = \alpha^{2n}\beta$ or $x + yi = \overline{\alpha}^{2n}\beta$. Each gives a triangle equivalent to the one we obtained above.

4.4. Using the notation of Proposition 4.27, we see that $(2, 1) \in P_3'$ is the element in P_3' whose y-coordinate is the smallest. The assertion now follows from Proposition 4.27.

4.5. By Theorem A.2 in Appendix A, $\prod_{\mathfrak{p}} \mathfrak{p}^{c_{\mathfrak{p}}}$ is the largest fractional ideal in A contained in both $\mathfrak{a}$ and $\mathfrak{b}$, and $\mathfrak{a} \cap \mathfrak{b}$ has the same property. Similarly, $\prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}}$ is the smallest fractional ideal in A containing both $\mathfrak{a}$ and $\mathfrak{b}$, and $\mathfrak{a} + \mathfrak{b}$ has the same property.

4.6. We have $x^3 = (y + 2\sqrt{-5})(y - 2\sqrt{-5})$. We show that $y + 2\sqrt{-5}$ is a cube in $\mathbb{Z}[\sqrt{-5}]$. A prime ideal that contains both $(y + 2\sqrt{-5})$ and $(y-2\sqrt{-5})$ contains the element $(y+2\sqrt{-5})-(y-2\sqrt{-5}) = 4\sqrt{-5}$. We can show that the prime factorization of (2) is $(2) = \mathfrak{a}^2$, where $\mathfrak{a} = (2, 1+\sqrt{-5})$, and $(\sqrt{-5})$ is a prime ideal. Thus, we have

$$(y + 2\sqrt{-5}) = \mathfrak{a}^m(\sqrt{-5})^n\mathfrak{b}, \quad (y - 2\sqrt{-5}) = \mathfrak{a}^m(\sqrt{-5})^n\mathfrak{c}, \quad m \geq 0, \ n \geq 0,$$

where $\mathfrak{a}$, $(\sqrt{-5})$, $\mathfrak{b}$ and $\mathfrak{c}$ are pairwise relatively prime ideals. From $(x)^3 = \mathfrak{a}^{2m}(\sqrt{-5})^{2n}\mathfrak{b}\mathfrak{c}$ we see that m and n are multiples of 3, and that $\mathfrak{b}$ and $\mathfrak{c}$ are cubes. Thus, $(y + 2\sqrt{-5})$ is the cube of an idea $\mathfrak{d}$. This means that the cube of $\mathfrak{d}$ is a principal ideal. But, since the class number is not divisible by 3, $\mathfrak{d}$ itself is a principal ideal by a similar argument as the one used in §4.4. Put $\mathfrak{d} = (\alpha)$, $\alpha \in \mathbb{Z}[\sqrt{-5}]$. From $(y + 2\sqrt{-5}) = (\alpha^3)$, we see that $y + 2\sqrt{-5} = \pm\alpha^3 = (\pm\alpha)^3$. Hence, $y + 2\sqrt{-5}$ is a cube in $\mathbb{Z}[\sqrt{-5}]$; i.e.,

$$y + 2\sqrt{-5} = (a + b\sqrt{-5})^3, \quad a, b \in \mathbb{Z}[\sqrt{-5}].$$

Thus, we have $y = a^3 - 15ab^2$ and $2 = 3a^2b - 5b^3 = (3a^2 - 5b^2)b$. The latter shows that $b = \pm 1, \pm 2$. The rest is easy.

Index

Selected Titles in This Series

(*Continued from the front of this publication*

161 **Michael Blank,** Discreteness and continuity in problems of chaotic dynamics, 1997

160 **V. G. Osmolovskiĭ,** Linear and nonlinear perturbations of the operator div, 1997

159 **S. Ya. Khavinson,** Best approximation by linear superpositions (approximate nomography), 1997

158 **Hideki Omori,** Infinite-dimensional Lie groups, 1997

157 **V. B. Kolmanovskiĭ and L. E. Shaĭkhet,** Control of systems with aftereffect, 1996

156 **V. N. Shevchenko,** Qualitative topics in integer linear programming, 1997

155 **Yu. Safarov and D. Vassiliev,** The asymptotic distribution of eigenvalues of partial differential operators, 1997

154 **V. V. Prasolov and A. B. Sossinsky,** Knots, links, braids and 3-manifolds. An introduction to the new invariants in low-dimensional topology, 1997

153 **S. Kh. Aranson, G. R. Belitsky, and E. V. Zhuzhoma,** Introductio to the qualitative theory of dynamical systems on surfaces, 1996

152 **R. S. Ismagilov,** Representations of infinite-dimensional groups, 1996

151 **S. Yu. Slavyanov,** Asymptotic solutions of the one-dimensional Schrödinger equation, 1996

150 **B. Ya. Levin,** Lectures on entire functions, 1996

149 **Takashi Sakai,** Riemannian geometry, 1996

148 **Vladimir I. Piterbarg,** Asymptotic methods in the theory of Gaussian processes and fields, 1996

147 **S. G. Gindikin and L. R. Volevich,** Mixed problem for partial differential equations with quasihomogeneous principal part, 1996

146 **L. Ya. Adrianova,** Introduction to linear systems of differential equations, 1995

145 **A. N. Andrianov and V. G. Zhuravlev,** Modular forms and Hecke operators, 1995

144 **O. V. Troshkin,** Nontraditional methods in mathematical hydrodynamics, 1995

143 **V. A. Malyshev and R. A. Minlos,** Linear infinite-particle operators, 1995

142 **N. V. Krylov,** Introduction to the theory of diffusion processes, 1995

141 **A. A. Davydov,** Qualitative theory of control systems, 1994

140 **Aizik I. Volpert, Vitaly A. Volpert, and Vladimir A. Volpert,** Traveling wave solutions of parabolic systems, 1994

ISBN 0-8218-0863-X

9 780821 808634

MMONO/186