志村五郎(Goro Shimura)

Springer
Monographs in
Mathematics

Arithmetic of Quadratic Forms

二次型算术

Springer

世界图书出版公司
www.wpcbj.com.cn

Goro Shimura

Arithmetic of Quadratic Forms

Springer

图书在版编目（CIP）数据

二次型算术 = Arithmetic of Quadratic Forms : 英文 /（美）志村五郎著 .— 影印本 .— 北京：世界图书出版公司北京公司，2016.5
ISBN 978-7-5192-1478-4

Ⅰ .①二…　Ⅱ .①志…　Ⅲ .①二次型数论—英文　Ⅳ .①O156.5

中国版本图书馆 CIP 数据核字（2016）第 119617 号

著　　者：志村五郎（Goro Shimura）
责任编辑：刘　慧　高　蓉
装帧设计：任志远

出版发行：世界图书出版公司北京公司
地　　址：北京市东城区朝内大街 137 号
邮　　编：100010
电　　话：010-64038355（发行）　64015580（客服）　64033507（总编室）
网　　址：http://www.wpcbj.com.cn
邮　　箱：wpcbjst@vip.163.com
销　　售：新华书店
印　　刷：三河市国英印务有限公司
开　　本：711mm × 1245mm　1/24
印　　张：10.5
字　　数：201 千
版　　次：2016 年 7 月第 1 版　　2016 年 7 月第 1 次印刷
版权登记：01-2015-7530
定　　价：39.00 元

Springer Monographs in Mathematics

For further volumes:
http://www.springer.com/series/3733

Goro Shimura
Department of Mathematics
Princeton University
Princeton, NJ 08544
USA
goro@math.princeton.edu

ISSN 1439-7382
ISBN 978-1-4419-1731-7		e-ISBN 978-1-4419-1732-4
DOI 10.1007/978-1-4419-1732-4

Library of Congress Control Number: 2010927446

Mathematics Subject Classification (2010): 11D09, 11E08, 11E12, 11E41, 11Rxx, 11Sxx, 17C20

Reprint from English language edition:
Arithmetic of Quadratic Forms
by Goro Shimura
Copyright © 2010, Springer Science+Business Media LLC

This reprint has been authorized by Springer Science & Business Media for distribution in China Mainland only and not for export therefrom.

PREFACE

This book can be divided into two parts. The first part is preliminary and consists of algebraic number theory and the theory of semisimple algebras. The raison d'être of the book is in the second part, and so let us first explain the contents of the second part.

There are two principal topics:

(A) Classification of quadratic forms;
(B) Quadratic Diophantine equations.

Topic (A) can be further divided into two types of theories:

(a1) Classification over an algebraic number field;
(a2) Classification over the ring of algebraic integers.

To classify a quadratic form φ over an algebraic number field F, almost all previous authors followed the methods of Helmut Hasse. Namely, one first takes φ in the diagonal form and associates an invariant to it at each prime spot of F, using the diagonal entries. A superior method was introduced by Martin Eichler in 1952, but strangely it was almost completely ignored, until I resurrected it in one of my recent papers. We associate an invariant to φ at each prime spot, which is the same as Eichler's, but we define it in a different and more direct way, using Clifford algebras. In Sections 27 and 28 we give an exposition of this theory. At some point we need the Hasse norm theorem for a quadratic extension of a number field, which is included in class field theory. We prove it when the base field is the rational number field to make the book self-contained in that case.

The advantage of our method is that it enables us to discuss (a2) in a clear-cut way. The main problem is to determine the genera of quadratic forms with integer coefficients that have given local invariants. A quaratic form of n variables with integer coefficients can be given in the form $\varphi[x] = \sum_{i,\,j=1}^{n} c_{ij}x_ix_j$ with a symmetric matrix (c_{ij}) such that c_{ii} and $2c_{ij}$ are integers for every i and j. If the matrix represents a *symmetric* form with integer coefficients, then c_{ij} is an integer for every $(i,\ j)$. Thus there are two types of classification theories over the ring of integers: one for quadratic forms and the other for symmetric forms. In fact, the former is easier than the latter. There were several previous results in the unimodular case, but there were few, if any, investigations in the general case. We will determine the genera of quadratic or symmetric forms over the integers that are *reduced* in the sense that they cannot be represented by other quadratic or symmetric forms nontrivially. This class of forms contains forms with square-free discriminant.

We devote Section 32 to strong approximation in an indefinite orthogonal group of more than two variables, and as applications we determine the *classes* instead of the *genera* of indefinite reduced forms.

The origin of Topic (a2) is the investigation of Gauss concerning primitive representations of an integer as a sum of three squares. In our book of 2004 we gave a framework in which we could discuss similar problems for an arbitrary quadratic form of more than two variables over the integers. In Chapter VII we present an easier and more accessible version of the theory. Though Gauss treated sums of three squares, he did not state any general principle; he merely explained the technique by which he could solve his problems. In fact, we state results as two types of formulas for a quadratic form, which can be specialized in two different ways to what Gauss was doing. Without going into details here we refer the reader to Section 34 in which a historical perspective is given. Our first main theorem of quadratic Diophantine equations is given in Section 35, from which we derive the two formulas in Section 37.

Let us now come to the first part of the book in which we give preliminaries that are necessary for the main part concerning quadratic forms. Assuming that the reader is familiar with basic algebra, we develop algebraic number theory and also the theory of semisimple algebras more or less in standard ways, and even in old-fashioned ways, whenever we think that is the easiest and most suitable for beginners. In fact, almost all of the material in this part have been taken from the notes of my lectures at Princeton University. However, we have tried a few new approaches and included some theorems that cannot be found in ordinary textbooks. For instance, our formulation and proof of the quadratic reciprocity law in a generalized form do not seem to be well-known; the same may be said about the last theorem of Section 10, which is essentially strong approximation in a special linear group. In the same spirit, we add the classical theory of genera as the last section of the book.

We could have made the whole book self-contained by including an easy part of class field theory, but in order to keep the book a reasonable length, we chose a compromised plan. Namely, we prove basic theorems in local class field theory only in some special cases, and the Hilbert reciprocity law only over the rational number field. However, we at least state the main theorems with an arbitrary number field as the base field, so that the reader who knows class field theory can learn the arithmetic theory of quadratic forms with no further references.

To conclude the preface, it is my great pleasure to express my deepest thanks to my friends Koji Doi, Tomokazu Kashio, Kaoru Okada, and Hiroyuki Yoshida, who kindly read earlier versions of the first two-thirds of the book and contributed many invaluable comments.

Princeton
May, 2009

Goro Shimura

NOTATION AND TERMINOLOGY

In this book we assume that the reader is familiar with basic facts on groups, rings, and the theory of field extensions up to Galois theory. We write $X \subset Y$ for two sets X and Y if X is a subset of Y, including the case $X = Y$, and denote by $\#X$ or $\#\{X\}$ the number of elements of X when it is finite. Following the standard convention, we do not call 0 of the ring $A = \{0\}$ an identity element. Thus, whenever we speak of an identity element of a ring A, we assume that $A \neq \{0\}$. For submodules B and C of a ring A we denote by BC the set of all finite sums $\sum_i b_i c_i$ with $b_i \in B$ and $c_i \in C$.

The symbols **Z**, **Q**, **R**, and **C** will mean as usual the ring of integers and the fields of rational numbers, real numbers, and complex numbers, respectively. In addition, we put

$$\mathbf{T} = \bigl\{\, z \in \mathbf{C} \bigm| |z| = 1 \,\bigr\},$$

and denote by **H** the Hamilton quaternion algebra; see §20.2. Given an associative ring A with identity element and an A-module X, we denote by $A^\times$ the group of all invertible elements of A, and by X_n^m the A-module of all $m \times n$-matrices with entries in X; we put $X^m = X_1^m$ for simplicity. For an element y of X_1^m or X_m^1 we denote by y_i the i-th entry of y. The zero element of A_n^m is denoted by 0_n^m or simply by 0. When we view A_n^n as a ring, we usually denote it by $M_n(A)$. We denote the identity element of $M_n(A)$ by 1_n or simply by 1. The transpose, determinant, and trace of a matrix x are denoted by ${}^t x$, $\det(x)$, and $\mathrm{tr}(x)$. We put $GL_n(A) = M_n(A)^\times$, and

$$SL_n(A) = \bigl\{\alpha \in GL_n(A) \bigm| \det(\alpha) = 1\bigr\}$$

if A is commutative. For square matrices $x_1, \ldots, x_r$, $\mathrm{diag}[x_1, \ldots, x_r]$ denotes the square matrix with $x_1, \ldots, x_r$ in the diagonal blocks and 0 in all other blocks.

For a group G we denote by $[G:1]$ the order of G, and for a subgroup H of G we denote by $[G:H]$ the index of H in G. For a vector space V over a field F we denote by $[V:F]$ the dimension of V over F and by $\mathrm{End}_F(V)$ the ring of all F-linear endomorphisms of V; we put then $GL_F(V) = \mathrm{End}_F(V)^\times$ and $SL_F(V) = \bigl\{\alpha \in GL_F(V) \bigm| \det(\alpha) = 1\bigr\}$. The distinction of $[V:F]$ from $[G:H]$ will be clear from the context. If K is a field containing F, then $[K:F]$ is the degree of the extension K of F. When F is clear from the context, we also write $GL(V)$, $SL(V)$, and $\dim(V)$ for $GL_F(V)$, $SL_F(V)$, and $[V:F]$.

A polynomial in one variable with coefficients in a field is called **monic** if the leading coefficient is 1. Given a square matrix ξ with entries in a field F, by the **minimal** (or **minimum**) polynomial of ξ over F we understand a monic polynomial that generates $\bigl\{\varphi \in F[x] \bigm| \varphi(\xi) = 0\bigr\}$, where x is an indeterminate. We use the same terminology for an element ξ of an algebraic extension of F.

CONTENTS

CHAPTER I

THE QUADRATIC RECIPROCITY LAW

1. Elementary facts

1.1. In this section we recall several well-known elementary facts, mostly without proof. We give the proof for some of them. An ideal I of a commutative ring R is called a **prime ideal** if R/I has no zero divisors; I is called **principal** if $I = \alpha R$ with some $\alpha \in R$. An integral domain (that is, a commutative ring with identity element that has no zero divisors) R is called a **principal ideal domain** if every ideal of R is principal. It is known that for a field F and an indeterminate x the polynomial ring $F[x]$ is a principal ideal domain. Also, the ring $\mathbf{Z}$ is a principal ideal domain. An integral domain is called a **unique factorization domain** if every principal ideal I of R different from $\{0\}$ can be written uniquely in the form $I = P_1^{e_1} \cdots P_r^{e_r}$ with prime ideals P_i that are principal and $0 < e_i \in \mathbf{Z}$.

Theorem 1.2. (i) *Let R be a unique factorization domain. Then the polynomial ring $R[x]$ is a unique factorization domain. If s is a prime element of R (that is, $s \notin R^\times$ and if $s = gh$ with $g, h \in R$, then $g \in R^\times$ or $h \in R^\times$), then sR is a prime ideal of R. Conversely, every prime ideal of R that is principal and different from $\{0\}$ is of the form sR with a prime element s of R.*

(ii) Let R be a principal ideal domain. Then R is a unique factorization domain, and every prime ideal P of R different from $\{0\}$ is a maximal ideal, that is, R/P is a field.

Theorem 1.3. *Let R be a commutative ring with identity element, and let $X_1, \ldots, X_r$ be ideals of R such that $X_i + X_j = R$ if $i \neq j$. Then*

$$R/(X_1 \cdots X_r) \cong R/X_1 \oplus \cdots \oplus R/X_r. \tag{1.1}$$

PROOF. We first prove the case $r = 2$. Define a map $f : R \to R/X_1 \oplus R/X_2$ by

$$f(x) = \bigl(x \pmod{X_1},\, x \pmod{X_2}\bigr).$$

Clearly f is a ring-homomorphism and $\mathrm{Ker}(f) = X_1 \cap X_2$. Now $X_1 \cap X_2 = (X_1 \cap X_2)(X_1 + X_2) \subset X_1X_2 \subset X_1 \cap X_2$, and so $X_1X_2 = X_1 \cap X_2$. Take

G. Shimura, *Arithmetic of Quadratic Forms*, Springer Monographs in Mathematics,
DOI 10.1007/978-1-4419-1732-4_1, © Springer Science+Business Media, LLC 2010

$s \in X_1$ and $t \in X_2$ so that $s + t = 1$. Given $a, b \in R$, put $c = at + bs$. Then $c - a = a(t-1) + bs = (b-a)s \in X_1$, and similarly $c - b \in X_2$. Thus $f(c) = \bigl(a \pmod{X_1}, b \pmod{X_2}\bigr)$, which means that f is surjective. Therefore $R/(X_1X_2) = R/\mathrm{Ker}(f) \cong R/X_1 \oplus R/X_2$, which proves the case $r = 2$. Now suppose $Z + X = Z + Y = R$ for ideals X, Y, and Z of R. Then $R = (Z+X)(Z+Y) = Z + XZ + ZY + XY = Z + XY$, since $XZ + ZY \subset Z$. Taking Z to be X_r and repeating the same argument, we obtain $X_r + X_1 \cdots X_{r-1} = R$, and so $R/(X_1 \cdots X_r) \cong R/(X_1 \cdots X_{r-1}) \oplus R/X_r$. Applying induction to $R/(X_1 \cdots X_{r-1})$, we can complete the proof.

Every infinite cyclic group is isomorphic to $\mathbf{Z}$; every finite cyclic group is isomorphic to $\mathbf{Z}/m\mathbf{Z}$. Now the basic theorem on abelian groups can be stated as follows.

Theorem 1.4. *Every finitely generated abelian group is the direct product of finitely many cyclic groups of finite or infinite order. In particular, every finite abelian group is isomorphic to a direct sum of the form* $\sum_{m\in M} \mathbf{Z}/m\mathbf{Z}$ *with a finite set* M *of positive integers.*

Theorem 1.5. *If* F *is a field, every finite subgroup of* $F^\times$ *is cyclic. In particular,* $F^\times$ *is a cyclic group if* F *is a finite field.*

PROOF. Let G be a finite subgroup of $F^\times$. Then by Theorem 1.4, G is isomorphic to $\sum_{i=1}^{r} \mathbf{Z}/n_i\mathbf{Z}$ with positive integers n_i. We may assume that $r > 1$ and $n_i > 1$ for every i, since G is cyclic otherwise. Suppose n_1 and n_2 are divisible by a prime number p. Then $(\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z})$ has p^2 elements y such that $py = 0$. These elements y correspond to p^2 elements x of G such that $x^p = 1$. Since F is a field, the equation $X^p = 1$ can have at most p solutions in F, a contradiction. Thus n_1 and n_2 are relatively prime, and more generally, $n_1, \ldots, n_r$ are relatively prime. By (1.1), G is isomorphic to $\mathbf{Z}/(n_1 \cdots n_r\mathbf{Z})$, which is cyclic. This proves our theorem.

For example, $(\mathbf{Z}/p\mathbf{Z})^\times$ is a cyclic group of order $p - 1$.

Lemma 1.6. *Let* f *be a homomorphism of a finite group* G *into* $\mathbf{C}^\times$. *Then*

$$\sum_{x\in G} f(x) = \begin{cases} [G:1] & \textit{if } f \textit{ is trivial,} \\ 0 & \textit{if } f \textit{ is nontrivial.} \end{cases}$$

PROOF. Assuming f to be nontrivial, take $y \in G$ such that $f(y) \neq 1$, and observe that $\sum_{x\in G} f(x) = \sum_{x\in G} f(yx) = f(y)\sum_{x\in G} f(x)$, and hence $\sum_{x\in G} f(x) = 0$. Our formula for trivial f is trivial.

For example, let ζ be a primitive m-th root of unity with $1 < m \in \mathbf{Z}$ and let $r \in \mathbf{Z}$. Then taking $f(x) = \zeta^{rx}$, from Lemma 1.6 we obtain

$$\sum_{a=0}^{m-1} \zeta^{ra} = \begin{cases} m & \textit{if} \quad r \in m\mathbf{Z}, \\ 0 & \textit{if} \quad r \notin m\mathbf{Z}. \end{cases} \tag{1.2}$$

Lemma 1.7. *Let R be a commutative ring with identity element. Suppose $R = A_1 \oplus \cdots \oplus A_r = B_1 \oplus \cdots \oplus B_s$ with subrings A_i and B_j that are indecomposable.* (Here a ring X is called **indecomposable** if X cannot be written in the form $X = Y \oplus Z$ with subrings Y and Z that are different from $\{0\}$.) *Then the A_i are the same as the B_j as a whole.*

PROOF. Clearly A_i and B_j are ideals of R. Let $1_R = e_1 + \cdots + e_r$ with $e_i \in A_i$. Then we can easily show that $B_1 = B_1e_1 \oplus \cdots \oplus B_1e_r$. The indecomposability of B_1 implies that $B_1 = B_1e_k$ for exactly one k. Changing the order of the A_i, we may assume that $B_1 = B_1e_1$; then $B_1 \subset A_1$. Exchanging $\{A_i\}$ and $\{B_j\}$, we have $A_1 \subset B_j$ for some j. Clearly $j = 1$, and so $A_1 = B_1$. Repeating the same argument, we eventually obtain the desired conclusion.

Lemma 1.8. *Let K be a separable quadratic extension of a field F, and ρ the nontrivial automorphism of K over F. Then*

$$\{y \in K^\times \mid yy^\rho = 1\} = \{x/x^\rho \mid x \in K^\times\}.$$

PROOF. If $y = x/x^\rho$, then clearly $yy^\rho = 1$. Thus our task is to show that if $y \in K^\times$ and $yy^\rho = 1$, then $y = x/x^\rho$ with some $x \in K^\times$. Suppose $y = -1$. If the characteristic of F is 2, then $y = 1$ and there is no problem. If the characteristic is not 2, then $K = F(x)$ with x such that $x^2 \in F^\times$. Then $x^\rho = -x$, and so $-1 = x/x^\rho$. Suppose $y \neq -1$; put $x = y + 1$. Then $x \neq 0$ and $yx^\rho = 1 + y = x$, and so $y = x/x^\rho$ as expected.

1.9. Finite fields. In this subsection we recall some basic facts on finite fields. A field with a finite number of elements is called a **finite field.** For every prime number p the ring $\mathbf{Z}/p\mathbf{Z}$ is a finite field with p elements. We denote this field by $\mathbf{F}(p)$. Every finite field is a finite algebraic extension of $\mathbf{F}(p)$ for some p, and vice versa. Let us fix a prime number p and an algebraic closure of $\mathbf{F}(p)$, and denote it by $\mathbf{F}(p^\infty)$. For every positive integer n the field $\mathbf{F}(p^\infty)$ contains exactly one algebraic extension of $\mathbf{F}(p)$ of degree n. It has p^n elements, and we denote it by $\mathbf{F}(p^n)$. Put $q = p^n$ with a fixed n. Then $x^q = x$ for every $x \in \mathbf{F}(q)$, and in particular $x^{q-1} = 1$ for every $x \in \mathbf{F}(q)^\times$. By Theorem 1.5, $\mathbf{F}(q)^\times$ is a cyclic group of order $q-1$. For another positive integer m we have $\mathbf{F}(p^n) \subset \mathbf{F}(p^m)$ if and only if $m = \ell n$ with $0 < \ell \in \mathbf{Z}$, in which case $\mathbf{F}(p^m)$ is a cyclic extension (that is, a Galois extension whose Galois group is cyclic) of $\mathbf{F}(p^n)$ of degree ℓ. The Galois group consists of the maps $x \mapsto x^{q^a}$ for $0 \le a < \ell$, where $q = p^n$. Write $k = \mathbf{F}(p^n)$ and $h = \mathbf{F}(p^m)$. Then the maps $\mathrm{Tr}_{h/k} : h \to k$ and $N_{h/k} : h^\times \to k^\times$ are surjective. Indeed, the surjectivity of the trace map is true for every separable extension. As for the norm map, we have $N_{h/k}(x) = x^r$ with $r = \sum_{a=0}^{\ell-1} q^a = (q^\ell - 1)/(q-1) = [h^\times : k^\times]$, and we obtain the desired surjectivity.

2. Structure of $(\mathbf{Z}/m\mathbf{Z})^\times$

2.1. If $m_1, \ldots, m_r$ are relatively prime positive integers > 1, then from (1.1) we obtain $\mathbf{Z}/(m_1 \cdots m_r\mathbf{Z}) \cong \mathbf{Z}/m_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/m_r\mathbf{Z}$, and so

$$(\mathbf{Z}/(m_1 \cdots m_r\mathbf{Z}))^\times \cong (\mathbf{Z}/m_1\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/m_r\mathbf{Z})^\times. \tag{2.1}$$

In particular, if $m = p_1^{e_1} \cdots p_r^{e_r}$ is the prime decomposition of a positive integer $m > 1$, then

$$(\mathbf{Z}/m\mathbf{Z})^\times \cong (\mathbf{Z}/p_1^{e_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_r^{e_r}\mathbf{Z})^\times. \tag{2.1a}$$

Therefore the structure of $(\mathbf{Z}/m\mathbf{Z})^\times$ for $1 < m \in \mathbf{Z}$ can be reduced to the case where m is a prime power. The order of the group $(\mathbf{Z}/m\mathbf{Z})^\times$ is traditionally denoted by $\varphi(m)$. In addition we put $\varphi(1) = 1$. This φ is called **Euler's function**. Observe that $\varphi(m)$ equals the number of integers a prime to m such that $0 < a \leq m$. From (2.1) we obtain

$$\varphi(m_1 \cdots m_k) = \varphi(m_1) \cdots \varphi(m_k) \text{ if the } m_i \text{ are as in (2.1).} \tag{2.2}$$

We easily see that

$$\varphi(p^n) = p^{n-1}(p-1) \text{ if } p \text{ is a prime number and } 0 < n \in \mathbf{Z}. \tag{2.3}$$

Lemma 2.2. *Let p be an odd prime number and b an integer prime to p. Then for $0 \leq e \in \mathbf{Z}$ we have $(1+bp)^{p^e} = 1 + cp^{e+1}$ with an integer c prime to p.*

Proof. We prove this by induction on e. Since $\binom{p}{k}$ is divisible by p if $1 < k < p$, by the binomial theorem we have $(1+bp^e)^p = 1 + bp^{e+1} + dp^f$ with $d \in \mathbf{Z}$ and $f > e+1$, and so $(1+bp^e)^p = 1 + b'p^{e+1}$ with an integer b' prime to p. This proves the case $e = 1$ of our lemma. Assuming our lemma for the exponent p^e, we have $(1+bp)^{p^{e+1}} = \left((1+bp)^{p^e}\right)^p = (1+cp^{e+1})^p = 1 + c'p^{e+2}$ with an integer c' prime to p, and we can complete the proof.

Notice that this lemma is false if $p = 2$. Indeed, $(1+2)^2 = 1 + 2 \cdot 2^2$.

Theorem 2.3. *If p is an odd prime number, then $(\mathbf{Z}/p^n\mathbf{Z})^\times$ is a cyclic group for every $n \in \mathbf{Z}, > 0$.*

Proof. Take an integer r that represents a generator of $(\mathbf{Z}/p\mathbf{Z})^\times$; then $r^{p-1} = 1 + bp$ with $b \in \mathbf{Z}$. Choosing r suitably, we may assume that $p \nmid b$. Indeed, if $p|b$, take $r+p$ instead of r. Since $(r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + p^2s$ with $s \in \mathbf{Z}$, we have $(r+p)^{p-1} = 1 + pt$ with $t = b - r^{p-2} + p(s + r^{p-2})$, which is prime to p as desired. Thus assuming b to be prime to p, let g be the order of the class of $r \pmod{p^n}$ in $(\mathbf{Z}/p^n\mathbf{Z})^\times$. Then $g|p^{n-1}(p-1)$, and also $(p-1)|g$, as r generates $(\mathbf{Z}/p\mathbf{Z})^\times$. Thus $g=(p-1)p^a$ with $0 \leq a \leq n-1$. Then by Lemma 2.2, $r^g=(1+bp)^{p^a}=1+cp^{a+1}$ with an integer c prime to p. Since $r^g-1 \in p^n\mathbf{Z}$, we see that $a+1 \geq n$, and so $a=n-1$, which means that $r \pmod{p^n}$ has order $(p-1)p^{n-1}$. This proves our theorem.

Any integer that represents a generator of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ is called a **primitive root modulo** p^n.

As for the case $p=2$, we first note that $(\mathbf{Z}/2\mathbf{Z})^\times$ is trivial and $(\mathbf{Z}/4\mathbf{Z})^\times$ is of order 2, and so they are cyclic. If $a=4k \pm 1$ with $k \in \mathbf{Z}$, then $a^2=1 \pm 8k+16k^2$, and so $a^2-1 \in 8\mathbf{Z}$ for every odd integer a. Thus $(\mathbf{Z}/8\mathbf{Z})^\times$ has no element of order 4, and so it is not cyclic.

Theorem 2.4. *Let $3 \leq n \in \mathbf{Z}$. For $2 \leq \nu \leq n$ let H_ν denote the subgroup of $(\mathbf{Z}/2^n\mathbf{Z})^\times$ consisting of all $\alpha \pmod{2^n}$ such that $\alpha-1 \in 2^\nu\mathbf{Z}$. Then H_ν is cyclic of order $2^{n-\nu}$ and $(\mathbf{Z}/2^n\mathbf{Z})^\times=\{\pm 1\} \times H_2$.*

PROOF. The order of $(\mathbf{Z}/2^n\mathbf{Z})^\times$ is 2^{n-1}, and so the order of any element of $(\mathbf{Z}/2^n\mathbf{Z})^\times$ is a power of 2. By induction on m we can prove that $(1+2^\nu)^{2^m}=1+2^{m+\nu}k$ with an odd integer k for $0 \leq m \in \mathbf{Z}$. Therefore $1+2^\nu$ is of order $2^{n-\nu}$ in this group. Since every odd integer α satisfies either $\alpha-1 \in 4\mathbf{Z}$ or $\alpha+1 \in 4\mathbf{Z}$, we obtain $(\mathbf{Z}/2^n\mathbf{Z})^\times=\{\pm 1\} \times H_2$. Clearly $\{1\}=H_n \subsetneqq \cdots \subsetneqq H_2$ and H_ν has an element of order $2^{n-\nu}$. Therefore H_ν is cyclic of order $2^{n-\nu}$. This completes the proof.

3. The quadratic reciprocity law

3.0. Here is a problem that motivates our investigation in this section. We consider a congruence $f(x) \equiv 0 \pmod{m}$, where $f(x)$ is a polynomial with coefficients in $\mathbf{Z}$ and m is a positive integer; we ask whether it has a solution x in $\mathbf{Z}$. If m is fixed, then we can answer the question by computing $f(x)$ for $0 \leq x < m$. If we vary m, the question becomes more interesting. For example, we can ask: *For what kind of prime numbers p does the congruence*

$$5x^2 \equiv 3 \pmod{p} \tag{3.0}$$

have a solution x in $\mathbf{Z}$? We will give an answer in §3.8 after developing a general theory.

3.1. Let p be an odd prime number. Then $(\mathbf{Z}/p\mathbf{Z})^\times$ is a cyclic group of order $p-1$, and $p-1$ is even. Therefore $(\mathbf{Z}/p\mathbf{Z})^\times$ has a unique subgroup R of order $(p-1)/2$, and so we have a homomorphism λ of $(\mathbf{Z}/p\mathbf{Z})^\times$ onto $\{\pm 1\}$ such that $\mathrm{Ker}(\lambda)=R$. We then define a symbol $\left(\dfrac{b}{p}\right)$ for $b \in \mathbf{Z}$ by

$$\left(\frac{b}{p}\right) = \begin{cases} \lambda\big(b \pmod p\big) & \textit{if} \quad p\nmid b, \\ 0 & \textit{if} \quad p \mid b. \end{cases}$$

This is called the **quadratic residue symbol.** Clearly

$$\left(\frac{bc}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{c}{p}\right) \quad \text{for} \quad b, c \in \mathbf{Z}.$$

To explain the nature of this symbol, let r be a primitive root modulo p. Then R is generated by $r^2 \pmod p$. If b is an integer prime to p, then $b \equiv r^a \pmod p$ with $0 \le a \in \mathbf{Z}$. Since $\left(\frac{r}{p}\right) = \lambda\big(r \pmod p\big) = -1$, we have $\left(\frac{b}{p}\right) = (-1)^a$, and we easily see that

$$\begin{aligned} \left(\frac{b}{p}\right) = 1 &\iff \bar{b} \in R \iff a \in 2\mathbf{Z} \\ &\iff b \equiv x^2 \pmod p \text{ for some } x \in \mathbf{Z} \text{ prime to } p, \\ \left(\frac{b}{p}\right) = -1 &\iff \bar{b} \notin R \iff a \notin 2\mathbf{Z} \\ &\iff b \not\equiv x^2 \pmod p \text{ for every } x \in \mathbf{Z}, \end{aligned}$$

where $\bar{b}$ denotes the class of b modulo $p\mathbf{Z}$. We call an integer b a **quadratic residue modulo** p if $\left(\frac{b}{p}\right) = 1$ and a **quadratic nonresidue modulo** p if $\left(\frac{b}{p}\right) = -1$.

Theorem 3.2. *For odd prime numbers* p *and* q *we have:*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p \quad \textit{for every} \quad a \in \mathbf{Z}, \tag{3.1}$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \tag{3.2}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if} \quad p \equiv \pm 1 \pmod 8, \\ -1 & \textit{if} \quad p \equiv \pm 3 \pmod 8, \end{cases} \tag{3.3}$$

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \quad \textit{if } p \ne q. \tag{3.4}$$

The last equality is called **the quadratic reciprocity law.**

Proof. The first congruence is clear if $p \mid a$. Let $a \equiv r^m \pmod p$ with a primitive root r modulo p. Then $r^{(p-1)/2} \equiv -1 \pmod p$, and so $a^{(p-1)/2} \equiv \big(r^{(p-1)/2}\big)^m \equiv (-1)^m \pmod p$, which proves (3.1). Taking $a = -1$, we obtain (3.2). We will derive the last two relations in §3.5 as special cases of Theorem 3.4 below.

Formula (3.4) can be written also