Graduate Texts in Mathematics

Jean-Pierre Serre

A Course in Arithmetic

算术教程

Springer

世界图书出版公司
www.wpcbj.com.cn

J.-P. Serre

A Course in Arithmetic

Springer

图书在版编目（CIP）数据

算术教程＝A Course in Arithmetic：英文/（法）赛瑞著．—北京：世界图书出版公司北京公司，2009.8

ISBN 978-7-5100-0535-0

Ⅰ．算… Ⅱ．赛… Ⅲ．算术—教材—英文 Ⅳ．0121

中国版本图书馆 CIP 数据核字（2009）第 127343 号

书　　名：	A Course in Arithmetic
作　　者：	J.-P. Serre
中 译 名：	算术教程
责任编辑：	高蓉
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街 137 号　100010）
联系电话：	010-64021602，010-64015659
电子信箱：	kjb@wpcbj.com.cn
开　　本：	24 开
印　　张：	5.5
版　　次：	2009 年 08 月
版权登记：	图字：01-2009-1053
书　　号：	978-7-5100-0535-0/O·751　　**定　　价：** 19.00 元

世界图书出版公司北京公司已获得 Springer 授权在中国大陆独家重印发行

Graduate Texts in Mathematics 7

Editorial Board
S. Axler F.W. Gehring K.A. Ribet

Springer
New York
Berlin
Heidelberg
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces. 2nd ed.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.
62 KARGAPOLOV/MERLZJAKOV. Fundamentals of the Theory of Groups.
63 BOLLOBAS. Graph Theory.
64 EDWARDS. Fourier Series. Vol. I 2nd ed.
65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
66 WATERHOUSE. Introduction to Affine Group Schemes.
67 SERRE. Local Fields.
68 WEIDMANN. Linear Operators in Hilbert Spaces.
69 LANG. Cyclotomic Fields II.

此为试读，需要完整PDF请访问：www.ertongbook.com
(continued after index)

Preface

This book is divided into two parts.

The first one is purely algebraic. Its objective is the classification of quadratic forms over the field of rational numbers (Hasse-Minkowski theorem). It is achieved in Chapter IV. The first three chapters contain some preliminaries: quadratic reciprocity law, p-adic fields, Hilbert symbols. Chapter V applies the preceding results to integral quadratic forms of discriminant ± 1. These forms occur in various questions: modular functions, differential topology, finite groups.

The second part (Chapters VI and VII) uses "analytic" methods (holomorphic functions). Chapter VI gives the proof of the "theorem on arithmetic progressions" due to Dirichlet; this theorem is used at a critical point in the first part (Chapter III, no. 2.2). Chapter VII deals with modular forms, and in particular, with theta functions. Some of the quadratic forms of Chapter V reappear here.

The two parts correspond to lectures given in 1962 and 1964 to second year students at the Ecole Normale Supérieure. A redaction of these lectures in the form of duplicated notes, was made by J.-J. Sansuc (Chapters I–IV) and J.-P. Ramis and G. Ruget (Chapters VI–VII). They were very useful to me; I extend here my gratitude to their authors.

J.-P. Serre

A Course in Arithmetic

Table of Contents

Part I

Algebraic Methods

此为试读，需要完整PDF请访问：www.ertongbook.com

Chapter I

Finite Fields

All fields considered below are supposed commutative.

§1. *Generalities*

1.1. *Finite fields*

Let K be a field. The image of $\mathbf{Z}$ in K is an integral domain, hence isomorphic to $\mathbf{Z}$ or to $\mathbf{Z}/p\mathbf{Z}$, where p is prime; its field of fractions is isomorphic to $\mathbf{Q}$ or to $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$. In the first case, one says that K is of *characteristic zero*; in the second case, that K is of *characteristic p*.

The characteristic of K is denoted by char(K). If char(K) $= p \neq 0$, p is also the smallest integer $n > 0$ such that $n.1 = 0$.

Lemma.—*If* char(K) $= p$, *the map* $\sigma: x \mapsto x^p$ *is an isomorphism of* K *onto one of its subfields* K^p.

We have $\sigma(xy) = \sigma(x)\sigma(y)$. Moreover, the binomial coefficient $\binom{p}{k}$ is congruent to 0 (mod p) if $0 < k < p$. From this it follows that

$$\sigma(x+y) = \sigma(x)+\sigma(y);$$

hence σ is a homomorphism. Furthermore, σ is clearly injective.

Theorem 1.—i) *The characteristic of a finite field* K *is a prime number* $p \neq 0$; *if* $f = [K:\mathbf{F}_p]$, *the number of elements of* K *is* $q = p^f$.

ii) *Let* p *be a prime number and let* $q = p^f (f \geqq 1)$ *be a power of* p. *Let* Ω *be an algebraically closed field of characteristic* p. *There exists a unique subfield* $\mathbf{F}_q$ *of* Ω *which has* q *elements. It is the set of roots of the polynomial* $X^q - X$.

iii) *All finite fields with* $q = p^f$ *elements are isomorphic to* $\mathbf{F}_q$.

If K is finite, it does not contain the field $\mathbf{Q}$. Hence its characteristic is a prime number p. If f is the degree of the extension $K/\mathbf{F}_p$, it is clear that Card(K) $= p^f$, and i) follows.

On the other hand, if Ω is algebraically closed of characteristic p, the above lemma shows that the map $x \mapsto x^q$ (where $q = p^f$, $f \geqq 1$) is an automorphism of Ω; indeed, this map is the $f-$th iterate of the automorphism $\sigma: x \mapsto x^p$ (note that σ is surjective since Ω is algebraically closed). Therefore, the elements $x \in \Omega$ invariant by $x \mapsto x^q$ form a subfield $\mathbf{F}_q$ of Ω. The derivative of the polynomial $X^q - X$ is

$$qX^{q-1} - 1 = p.p^{f-1}X^{q-1} - 1 = -1$$

and is not zero. This implies (since Ω is algebraically closed) that $X^q - X$ has q distinct roots, hence $\mathrm{Card}(\mathbf{F}_q) = q$. Conversely, if K is a subfield of Ω with q elements, the multiplicative group K^* of nonzero elements in K has $q-1$ elements. Then $x^{q-1} = 1$ if $x \in K^*$ and $x^q = x$ if $x \in K$. This proves that K is contained in $\mathbf{F}_q$. Since $\mathrm{Card}(K) = \mathrm{Card}(\mathbf{F}_q)$ we have $K = \mathbf{F}_q$ which completes the proof of ii).

Assertion iii) follows from ii) and from the fact that all fields with p^f elements can be embedded in Ω since Ω is algebraically closed.

1.2. *The multiplicative group of a finite field*

Let p be a prime number, let f be an integer $\geqq 1$, and let $q = p^f$.

Theorem 2.—*The multiplicative group $\mathbf{F}_q^*$ of a finite field $\mathbf{F}_q$ is cyclic of order $q-1$.*

Proof. If d is an integer $\geqq 1$, recall that $\phi(d)$ denotes the *Euler ϕ-function*, i.e. the number of integers x with $1 \leqq x \leqq d$ which are prime to d (in other words, whose image in $\mathbf{Z}/d\mathbf{Z}$ is a generator of this group). It is clear that the number of generators of a cyclic group of order d is $\phi(d)$.

Lemma 1.—*If n is an integer $\geqq 1$, then $n = \sum_{d|n} \phi(d)$.* (Recall that the notation $d|n$ means that d divides n).

If d divides n, let C_d be the unique subgroup of $\mathbf{Z}/n\mathbf{Z}$ of order d, and let Φ_d be the set of generators of C_d. Since all elements of $\mathbf{Z}/n\mathbf{Z}$ generate one of the C_d, the group $\mathbf{Z}/n\mathbf{Z}$ is the disjoint union of the Φ_d and we have

$$n = \mathrm{Card}(\mathbf{Z}/n\mathbf{Z}) = \sum_{d|n} \mathrm{Card}(\Phi_d) = \sum_{d|n} \phi(d).$$

Lemma 2.—*Let H be a finite group of order n. Suppose that, for all divisors d of n, the set of $x \in H$ such that $x^d = 1$ has at most d elements. Then H is cyclic.*

Let d be a divisor of n. If there exists $x \in H$ of order d, the subgroup $(x) = \{1, x, \ldots, x^{d-1}\}$ generated by x is cyclic of order d; in view of the hypothesis, all elements $y \in H$ such that $y^d = 1$ belong to (x). In particular, all elements of H of order d are generators of (x) and these are in number $\phi(d)$. Hence, the number of elements of H of order d is 0 or $\phi(d)$. If it were zero for a value of d, the formula $n = \sum_{d|n} \phi(d)$ would show that the number of elements in H is $<n$, contrary to hypothesis. In particular, there exists an element $x \in H$ of order n and H coincides with the cyclic group (x).

Theorem 2 follows from lemma 2 applied to $H = \mathbf{F}_q^*$ and $n = q-1$; it is indeed obvious that the equation $x^d = 1$, which has degree d, has at most d solutions in $\mathbf{F}_q$.

Remark. The above proof shows more generally that all finite subgroups of the multiplicative group of a field are cyclic.

§2. *Equations over a finite field*

Let q be a power of a prime number p, and let K be a field with q elements.

2.1. *Power sums*

Lemma.—*Let u be an integer $\geqq 0$. The sum $S(X^u) = \sum_{x \in K} x^u$ is equal to -1 if u is $\geqq 1$ and divisible by $q-1$; it is equal to 0 otherwise.*

(We agree that $x^u = 1$ if $u = 0$ *even if* $x = 0$.)

If $u = 0$, all the terms of the sum are equal to 1; hence $S(X^u) = q.1 = 0$ because K is of characteristic p.

If u is $\geqq 1$ and divisible by $q-1$, we have $0^u = 0$ and $x^u = 1$ if $x \neq 0$. Hence $S(X^u) = (q-1).1 = -1$.

Finally, if u is $\geqq 1$ and not divisible by $q-1$, the fact that K^* is cyclic of order $q-1$(th. 2) shows that there exists $y \in K^*$ such that $y^u \neq 1$. One has:

$$S(X^u) = \sum_{x \in K^*} x^u = \sum_{x \in K^*} y^u x^u = y^u S(X^u)$$

and $(1-y^u)S(X^u) = 0$ which implies that $S(X^u) = 0$.

(*Variant*—Use the fact that, if $d \geqq 2$ is prime to p, the sum of the d-th roots of unity is zero.)

2.2. *Chevalley theorem*

Theorem 3 (Chevalley – Warning).—*Let $f_\alpha \in K[X_1, \ldots, X_n]$ be polynomials in n variables such that $\sum_\alpha \deg f_\alpha < n$, and let V be the set of their common zeros in K^n. One has*

$$\mathrm{Card}(V) \equiv 0 \pmod p.$$

Put $P = \prod_\alpha (1 - f_\alpha^{q-1})$ and let $x \in K^n$. If $x \in V$, all the $f_\alpha(x)$ are zero and $P(x) = 1$; if $x \notin V$, one of the $f_\alpha(x)$ is nonzero and $f_\alpha(x)^{q-1} = 1$, hence $P(x) = 0$. Thus P is the *characteristic function* of V. If, for every polynomial f, we put $S(f) = \sum_{x \in K^n} f(x)$, we have

$$\mathrm{Card}(V) \equiv S(P) \pmod p$$

and we are reduced to showing that $S(P) = 0$.

Now the hypothesis $\sum \deg f_\alpha < n$ implies that $\deg P < n(q-1)$; thus P is a linear combination of monomials $X^u = X_1^{u_1} \ldots X_n^{u_n}$ with $\sum u_i < n(q-1)$. It suffices to prove that, for such a monomial X^u, we have $S(X^u) = 0$, and this follows from the lemma since at least one u_i is $< q-1$.

Corollary 1.— *If $\sum \deg f_\alpha < n$ and if the f_α have no constant term, then the f_α have a nontrivial common zero.*

Indeed, if V were reduced to $\{0\}$, Card(V) would not be divisible by p.

Corollary 1 applies notably when the f_α are *homogeneous*. In particular:

Corollary 2.—*All quadratic forms in at least 3 variables over K have a non trivial zero.*

(In geometric language: every conic over a finite field has a rational point.)

§3. *Quadratic reciprocity law*

3.1. *Squares in $\mathbf{F}_q$*

Let q be a power of a prime number p.

Theorem 4.—(a) *If $p = 2$, then all elements of $\mathbf{F}_q$ are squares.*

(b) *If $p \neq 2$, then the squares of $\mathbf{F}_q^*$ form a subgroup of index 2 in $\mathbf{F}_q^*$; this subgroup is the kernel of the homomorphism $x \mapsto x^{(q-1)/2}$ with values in $\{\pm 1\}$.*

(In other terms, one has an exact sequence:

$$1 \to \mathbf{F}_q^{*2} \to \mathbf{F}_q^* \to \{\pm 1\} \to 1.)$$

Case (a) follows from the fact that $x \mapsto x^2$ is an automorphism of $\mathbf{F}_q$.

In case (b), let Ω be an algebraic closure of $\mathbf{F}_q$; if $x \in \mathbf{F}_q^*$, let $y \in \Omega$ be such that $y^2 = x$. We have:

$$y^{q-1} = x^{(q-1)/2} = \pm 1 \text{ since } x^{q-1} = 1.$$

For x to be a square in $\mathbf{F}_q$ it is necessary and sufficient that y belongs to $\mathbf{F}_q^*$, i.e. $y^{q-1} = 1$. Hence $\mathbf{F}_q^{*2}$ is the kernel of $x \mapsto x^{(q-1)/2}$. Moreover, since $\mathbf{F}_q^*$ is cyclic of order $q-1$, the index of $\mathbf{F}_q^{*2}$ is equal to 2.

3.2. *Legendre symbol (elementary case)*

Definition.—*Let p be a prime number $\neq 2$, and let $x \in \mathbf{F}_p^*$. The Legendre symbol of x, denoted by $\left(\frac{x}{p}\right)$, is the integer $x^{(p-1)/2} = \pm 1$.*

It is convenient to extend $\left(\frac{x}{p}\right)$ to all of $\mathbf{F}_p$ by putting $\left(\frac{0}{p}\right) = 0$. Moreover, if $x \in \mathbf{Z}$ has for image $x' \in \mathbf{F}_p$, one writes $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$.

We have $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$: The Legendre symbol is a "character" (cf. chap. VI, §1). As seen in theorem 4, $\left(\frac{x}{p}\right) = 1$ is equivalent to $x \in \mathbf{F}_p^{*2}$; if $x \in \mathbf{F}_p^*$ has y as a square root in an algebraic closure of $\mathbf{F}_p$, then $\left(\frac{x}{p}\right) = y^{p-1}$.

Computation of $\left(\frac{x}{p}\right)$ *for* $x = 1, -1, 2$:

If n is an *odd* integer, let $\varepsilon(n)$ and $\omega(n)$ be the elements of $\mathbf{Z}/2\mathbf{Z}$ defined by:

$$\varepsilon(n) \equiv \frac{n-1}{2} \pmod 2 = \begin{cases} 0 \text{ if } n \equiv 1 \pmod 4 \\ 1 \text{ if } n \equiv -1 \pmod 4 \end{cases}$$

$$\omega(n) \equiv \frac{n^2-1}{8} \pmod 2 = \begin{cases} 0 \text{ if } n \equiv \pm 1 \pmod 8 \\ 1 \text{ if } n \equiv \pm 5 \pmod 8 \end{cases}$$

[The function ε is a homomorphism of the multiplicative group $(\mathbf{Z}/4\mathbf{Z})^*$ onto $\mathbf{Z}/2\mathbf{Z}$; similarly, ω is a homomorphism of $(\mathbf{Z}/8\mathbf{Z})^*$ onto $\mathbf{Z}/2\mathbf{Z}$.]

Theorem 5.—*The following formulas hold*:

i) $\left(\frac{1}{p}\right) = 1$

ii) $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$

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

Only the last deserves a proof. If α denotes a primitive 8th root of unity in an algebraic closure Ω of $\mathbf{F}_p$, the element $y = \alpha+\alpha^{-1}$ verifies $y^2 = 2$ (from $\alpha^4 = -1$ it follows that $\alpha^2+\alpha^{-2} = 0$). We have

$$y^p = \alpha^p+\alpha^{-p}.$$

If $p \equiv \pm 1 \pmod 8$, this implies $y^p = y$, thus $\left(\frac{2}{p}\right) = y^{p-1} = 1$. If $p \equiv \pm 5 \pmod 8$, one finds $y^p = \alpha^5+\alpha^{-5} = -(\alpha+\alpha^{-1}) = -y$. (This again follows from $\alpha^4 = -1$.) We deduce from this that $y^{p-1} = -1$, whence iii) follows.

Remark. Theorem 5 can be expressed in the following way:

-1 is a square (mod p) if and only if $p \equiv 1 \pmod 4$.

2 is a square (mod p) if and only if $p \equiv \pm 1 \pmod 8$.

3.3 *Quadratic reciprocity law*

Let l and p be two distinct prime numbers different from 2.

Theorem 6 (Gauss).— $\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\varepsilon(l)\varepsilon(p)}$.

Let Ω be an algebraic closure of $\mathbf{F}_p$, and let $w \in \Omega$ be a primitive l-th root of unity. If $x \in \mathbf{F}_l$, the element w^x is well defined since $w^l = 1$. Thus we are able to form the "Gauss sum":

$$y = \sum_{x \in \mathbf{F}_l} \left(\frac{x}{l}\right) w^x.$$

Lemma 1.—$y^2 = (-1)^{\varepsilon(l)} l$.

(By abuse of notation l denotes also the image of l in the field $\mathbf{F}_p$.)

We have

$$y^2 = \sum_{x,z}\left(\frac{xz}{l}\right) w^{x+z} = \sum_{u\in \mathbf{F}_l} w^u\left(\sum_{t\in\mathbf{F}_l}\left(\frac{t(u-t)}{l}\right)\right).$$

Now if $t \neq 0$:

$$\left(\frac{t(u-t)}{l}\right) = \left(\frac{-t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right) = (-1)^{\varepsilon(l)}\left(\frac{1-ut^{-1}}{l}\right),$$

and

$$(-1)^{\varepsilon(l)}y^2 = \sum_{u\in\mathbf{F}_l} C_u w^u,$$

where

$$C_u = \sum_{t\in\mathbf{F}_l^*}\left(\frac{1-ut^{-1}}{l}\right).$$

If $u = 0$, $C_0 = \sum_{t\in\mathbf{F}_l^*}\left(\frac{1}{l}\right) = l-1$; otherwise $s = 1-ut^{-1}$ runs over $\mathbf{F}_l - \{1\}$, and we have

$$C_u = \sum_{s\in\mathbf{F}_l}\left(\frac{s}{l}\right) - \left(\frac{1}{l}\right) = -\left(\frac{1}{l}\right) = -1,$$

since in $\mathbf{F}_l^*$ there are as many squares as non squares. Hence $\sum_{u\in\mathbf{F}_l} C_u w^u = l-1-\sum_{u\in\mathbf{F}_l^*} w^u = l$, which proves the lemma.

Lemma 2.—$y^{p-1} = \left(\frac{p}{l}\right)$

Since Ω is of characteristic p, we have

$$y^p = \sum_{x\in\mathbf{F}_l}\left(\frac{x}{p}\right) w^{xp} = \sum_{z\in\mathbf{F}_l}\left(\frac{zp^{-1}}{l}\right) w^z = \left(\frac{p^{-1}}{l}\right) y = \left(\frac{p}{l}\right) y;$$

hence $y^{p-1} = \left(\frac{p}{l}\right)$.

Theorem 6 is now immediate. Indeed, by lemmas 1 and 2,

$$\left(\frac{(-1)^{\varepsilon(l)}l}{p}\right) = y^{p-1} = \left(\frac{p}{l}\right)$$

and the second part of th. 5 proves that

$$\left(\frac{(-1)^{\varepsilon(l)}}{p}\right) = (-1)^{\varepsilon(l)\varepsilon(p)}.$$

Translation.—Write lRp if l is a square (mod p) (that is to say, if l is a "*quadratic residue*" modulo p) and lNp otherwise. Theorem 6 means that

$$lRp \Leftrightarrow pRl \quad \text{if } p \text{ or } l \equiv 1 \pmod 4$$

$$lRp \Leftrightarrow pNl \quad \text{if } p \text{ and } l \equiv -1 \pmod 4.$$

此为试读，需要完整PDF请访问：www.ertongbook.com