Chapter 2
Basic Facts

In this chapter, we lay the foundations for all of the work that will be done in subsequent chapters. Section 2.1 defines the Legendre symbol and verifies its basic properties, proves Euler's criterion, and deduces some corollaries which will be very useful in many situations in which we will find ourselves. Motivated by the solutions of a quadratic congruence modulo a prime which we discussed in Chap. 1, we formulate what we will call the Basic Problem and the Fundamental Problem for Primes in Sect. 2.2. In Sect. 2.3, we state and prove Gauss' Lemma for residues and non-residues and use it to solve the Fundamental Problem for the prime 2.

2.1 The Legendre Symbol, Euler's Criterion, and Other Important Things

In this section, we establish some fundamental facts about residues and non-residues that will be used repeatedly throughout the rest of these notes.

Proposition 2.1 *In every complete system of ordinary residues modulo p, there are exactly $(p-1)/2$ quadratic residues.*

Proof It suffices to prove that in $[1, p-1]$ there are exactly $(p-1)/2$ quadratic residues. Note first that $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ are all incongruent mod p (if $1 \leq i, j < p/2$ and $i^2 \equiv j^2 \bmod p$ then $i \equiv j$ hence $i = j$ or $i \equiv -j$, i.e., $i+j \equiv 0$. But $2 \leq i + j < p$, and so $i + j \equiv 0$ is impossible).

Let $\mathcal{S}$ denote the set of minimal non-negative ordinary residues mod p of $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$. The elements of $\mathcal{S}$ are quadratic residues of p and $|\mathcal{S}| = (p-1)/2$. Suppose that $n \in [1, p-1]$ is a quadratic residue of p. Then there exists $r \in [1, p-1]$ such that $r^2 \equiv n$. Then $(p-r)^2 \equiv r^2 \equiv n$ and

S. Wright, *Quadratic Residues and Non-Residues*, Lecture Notes in Mathematics 2171, DOI 10.1007/978-3-319-45955-4_2

$\{r, p-r\} \cap [1, (p-1)/2] \neq \emptyset$. Hence $n \in \mathcal{S}$, whence $\mathcal{S}$ = the set of quadratic residues of p inside $[1, p-1]$. QED

Remark The proof of Proposition 2.1 provides a way to easily find, at least in principle, the residues of any prime p. Simply calculate the integers $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ and then reduce mod p. The integers that result from this computation are the residues of p inside $[1, p-1]$. This procedure also finds the modular square roots x of a residue r of p, i.e., the solutions to the congruence $x^2 \equiv r \bmod p$. For example, in just a few minutes on a hand-held calculator, one finds that the residues of 17 are 1, 2, 4, 8, 9, 13, 15, and 16, with corresponding modular square roots ± 1, ± 6, ± 2, ± 5, ± 3, ± 8, ± 7, and ± 4, and the residues of 37 are 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, and 36, with corresponding modular square roots ± 1, ± 15, ± 2, ± 9, ± 3, ± 11, ± 14, ± 7, ± 4, ± 13, ± 5, ± 10, ± 8, ± 18, ± 17, ± 12, ± 16, and ± 6. Of course, for large p, this method quickly becomes impractical for the calculation of residues and modular square roots, but see Sect. 4.9 of Chap. 4 for a practical and efficient way to perform these calculations for large values of p.

N.B. In the next proposition, all residues and non-residues are taken with respect to a fixed prime p.

Proposition 2.2

(*i*) *The product of two residues is a residue.*
(*ii*) *The product of a residue and a non-residue is a non-residue.*
(*iii*) *The product of two non-residues is a residue.*

Proof

(*i*) If α, α' are residues then $x^2 \equiv \alpha$, $y^2 \equiv \alpha'$ imply that $(xy)^2 \equiv \alpha\alpha' \bmod p$.
(*ii*) Let α be a fixed residue. The integers $0, \alpha, \ldots, (p-1)\alpha$ are incongruent mod p, hence are a complete system of ordinary residues mod p. If R denotes the set of all residues in $[1, p-1]$ then by Proposition 2.2(*i*), $\{\alpha r : r \in R\}$ is a set of residues of cardinality $(p-1)/2$, hence Proposition 2.1 implies that there are no other residues among $\alpha, 2\alpha, \ldots, (p-1)\alpha$, i.e., if $\beta \in [1, p-1] \setminus R$ then $\alpha\beta$ is a non-residue. Statement (*ii*) is an immediate consequence of this.
(*iii*) Suppose that β is a non-residue. Then $0, \beta, 2\beta, \ldots, (p-1)\beta$ is a complete system of ordinary residues mod p, and by Proposition 2.2(*ii*) and Proposition 2.1, $\{\beta r : r \in R\}$ is a set of non-residues and there are no other non-residues among $\beta, 2\beta, \ldots, (p-1)\beta$. Hence $\beta' \in [1, p-1] \setminus R$ implies that $\beta\beta'$ is a residue. Statement (*iii*) is an immediate consequence of this. QED

The following definition introduces the most important piece of mathematical technology that we will use to study residues and non-residues.

Definition The *Legendre symbol* χ_p *of* p is the function $\chi_p : \mathbb{Z} \to [-1, 1]$ defined by

$$\chi_p(n) = \begin{cases} 0, & \text{if } p \text{ divides } n, \\ 1, & \text{if } \gcd(p, n) = 1 \text{ and } n \text{ is a residue of } p, \\ -1, & \text{if } \gcd(p, n) = 1 \text{ and } n \text{ is a non-residue of } p. \end{cases}$$

The next proposition asserts that χ_p is a completely multiplicative arithmetic function of period p. This fact will play a crucial role in much of our subsequent work.

Proposition 2.3

(*i*) $\chi_p(n) = 0$ *if and only if* p *divides* n, *and if* $m \equiv n \bmod p$ *then* $\chi_p(m) = \chi_p(n)$(χ_p *is of period* p).
(*ii*) *For all* $m, n \in \mathbb{Z}, \chi_p(mn) = \chi_p(m)\chi_p(n)$($\chi_p$ *is completely multiplicative*).

Proof

(*i*) If $m \equiv n \mod p$ then p divides m (respectively, m is a residue/non-residue of p) if and only if p divides n (respectively, n is a residue/non-residue of p). Hence $\chi_p(m) = \chi_p(n)$.
(*ii*) $\chi_p(mn) = 0$ if and only if p divides mn if and only if p divides m or n if and only if $\chi_p(m) = 0$ or $\chi_p(n) = 0$ if and only if $\chi_p(m)\chi_p(n) = 0$.

Because $\chi_p(n^2) = \big(\chi_p(n)\big)^2$, we may assume that $m \neq n$. Then $\chi_p(mn) = 1$ (respectively, $\chi_p(mn) = -1$) if and only if $\gcd(mn, p) = 1$ and mn is a residue (respectively, mn is a non-residue) of p if and only if $\gcd(m, p) = 1 = \gcd(n, p)$ and, by Proposition 2.2, m and n are either both residues or both non-residues of p (respectively, $\{m, n\}$ contains a residue and a non-residue of p) if and only if $\chi_p(m)\chi_p(n) = 1$ (respectively, $\chi_p(m)\chi_p(n) = -1$). QED

Remark on Notation As a consequence of Proposition 2.3, χ_p defines a homomorphism of the group of units in the ring $\mathbb{Z}/p\mathbb{Z}$ into the circle group, i.e., χ_p is a *character* of the group of units. This is the reason why we have chosen the character-theoretic notation $\chi_p(n)$ for the Legendre symbol, instead of the more traditional notation $\left(\frac{n}{p}\right)$. When p is replaced by an arbitrary integer $m \geq 2$, we will have more to say later (see Sect. 4.4 of Chap. 4) about characters on the group of units in the ring $\mathbb{Z}/m\mathbb{Z}$ and their use in what we will study here.

The next result determines the quadratic character of -1.

Theorem 2.4

$$\chi_p(-1) = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4, \\ -1, & \text{if } p \equiv -1 \bmod 4. \end{cases}$$

This theorem is due to Euler [16], who proved it in 1760. It is of considerable importance in the history of number theory because in 1795, the young Gauss (at the ripe old age of 18!) rediscovered it. Gauss was so struck by the beauty and depth of this result that, as he testifies in the preface to *Disquisitiones Arithmeticae* [19], "I concentrated on it all of my efforts in order to understand the principles on which it depended and to obtain a rigorous proof. When I succeeded in this I was so attracted by these questions that I could not let them be." Thus began Gauss' work in number theory that was to revolutionize the subject.

Proof of Theorem 2.4 The proof that we give is Euler's own. It is based on

Theorem 2.5 (Euler's Criterion) *If* $a \in \mathbb{Z}$ *and* $\gcd(a, p) = 1$ *then*

$$\chi_p(a) \equiv a^{(p-1)/2} \bmod p.$$

If we apply Euler's criterion with $a = -1$ then

$$\chi_p(-1) \equiv (-1)^{(p-1)/2} \bmod p.$$

Hence $\chi_p(-1) - (-1)^{(p-1)/2}$ is either 0 or ± 2 and is divisible by p, hence

$$\chi_p(-1) = (-1)^{(p-1)/2},$$

and so $\chi_p(-1) = 1$ (respectively, -1) if and only if $(p-1)/2$ is even (respectively, odd) if and only if $p \equiv 1 \bmod 4$ (respectively, $p \equiv -1 \bmod 4$). This verifies Theorem 2.4.

Proof of Theorem 2.5 This is an interesting application of Wilson's theorem, which asserts that

$$\text{if } q \text{ is a prime then } (q-1)! \equiv -1 \bmod q, \qquad (*)$$

and was in fact first stated by Abu Ali al-Hasan ibn al-Haytham in 1000 AD, over 750 years before it was attributed to John Wilson, whose name it now bears. We will use Wilson's theorem to first prove Theorem 2.5; after that we then verify Wilson's theorem.

Suppose that $\chi_p(a) = 1$, and so $x^2 \equiv a \mod p$ for some $x \in \mathbb{Z}$. Note now that $1 = \gcd(a, p)$ implies that $1 = \gcd(x^2, p)$, and so $1 = \gcd(x, p)$ (p is prime!), hence by Fermat's little theorem,

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \bmod p.$$

Suppose that $\chi_p(a) = -1$, i.e., a is a non-residue. For each $i \in [1, p-1]$, there exists $j \in [1, p-1]$ uniquely determined by i, such that

$$ij \equiv a \bmod p$$

($\mathbb{Z}/p\mathbb{Z}$ is a field) and $i \neq j$ because a is a non-residue. Hence we can group the integers $1, \ldots, p-1$ into $(p-1)/2$ pairs, each pair with a product $\equiv a \mod p$. Multiplying all of these pairs together yields

$$(p-1)! \equiv a^{(p-1)/2} \mod p,$$

and so (∗) implies that

$$-1 \equiv a^{(p-1)/2} \mod p.$$

QED

Proof of Wilson's Theorem The implication (∗) is clearly valid when $q = 2$, so assume that q is odd. Use Proposition 1.2 to find for each integer $a \in [1, q-1]$ an integer $\bar{a} \in [1, p-1]$ such that $a\bar{a} \equiv 1 \mod q$. The integers 1 and $q-1$ are the only integers in $[1, q-1]$ that are their own inverses mod q, hence we may group the integers from 2 through $q-2$ into $(q-3)/2$ pairs with the product of each pair congruent to 1 mod q. Hence

$$2 \cdot 3 \cdots (q-3)(q-2) \equiv 1 \mod q.$$

Multiplication of both sides of this congruence by $q-1$ yields

$$(q-1)! = 1 \cdot 2 \cdots (q-1) \equiv q-1 \equiv -1 \mod q.$$

QED

Remark The converse of Wilson's theorem is also valid.

2.2 The Basic Problem and the Fundamental Problem for a Prime

From our discussion in Chap. 1, if d is the discriminant of $ax^2 + bx + c$ and if neither a nor d is divisible by p then

$$ax^2 + bx + c \equiv 0 \mod p$$

has a solution if and only if d is a residue of p. This motivates what we will call the

Basic Problem If $d \in \mathbb{Z}$, for what primes p is d a quadratic residue of p?

We now present a strategy for solving this problem which employs Proposition 2.3 as the basic tool. Things can be stated precisely and concisely if we use the following

Notation: if $z \in \mathbb{Z}$, let

$$X_{\pm}(z) = \{p : \chi_p(z) = \pm 1\},$$

$$\pi_{\text{odd}}(z)(\text{resp., } \pi_{\text{even}}(z)) = \{q \in \pi(z) : q \text{ has odd (resp., even) multiplicity in } z\}.$$

We point out here how to read the $\pm$ signs. If $\pm$ signs occur simultaneously in different places in an equation, formula, definition, etc., then the $+$ sign is meant to be taken simultaneously in all occurrences of $\pm$ and then the $-$ sign is also to be taken simultaneously in all occurrences of $\pm$. For example, the equation $X_{\pm}(z) = \{p : \chi_p(z) = \pm 1\}$ above asserts that $X_+(z) = \{p : \chi_p(z) = 1\}$ and $X_-(z) = \{p : \chi_p(z) = -1\}$. We follow this convention in the sequel.

Suppose first that $d > 0$, with $\gcd(d, p) = 1$. If $\pi_{\text{odd}}(d) = \emptyset$ then d is a square, so d is trivially a residue of p. Hence assume that $\pi_{\text{odd}}(d) \neq \emptyset$. Proposition 2.3 implies that

$$\chi_p(d) = \prod_{q \in \pi_{\text{odd}}(d)} \chi_p(q).$$

Hence

$$\chi_p(d) = 1 \text{ iff } |\{q \in \pi_{\text{odd}}(d) : \chi_p(q) = -1\}| \text{ is } \textit{even}. \tag{2.1}$$

Let

$$\mathcal{E} = \{E \subseteq \pi_{\text{odd}}(d) : |E| \text{ is even}\}.$$

If $E \in \mathcal{E}$, let R_E denote the set of all p such that

$$\chi_p(q) = \begin{cases} -1, & \text{if } q \in E, \\ 1, & \text{if } q \in \pi_{\text{odd}}(d) \setminus E. \end{cases}$$

Then (2.1) implies that

$$X_+(d) = \Big(\bigcup_{E \in \mathcal{E}} R_E \Big) \setminus \pi_{\text{even}}(d), \tag{2.2}$$

and this union is pairwise disjoint. Moreover

$$R_E = \Big(\bigcap_{q \in E} X_-(q) \Big) \cap \Big(\bigcap_{q \in \pi_{\text{odd}}(d) \setminus E} X_+(q) \Big). \tag{2.3}$$

Suppose next that $d < 0$. Then $d = (-1)(-d)$, hence

$$\chi_p(d) = \prod_{q \in \{-1\} \cup \pi_{\text{odd}}(d)} \chi_p(q). \tag{2.4}$$

If we let

$$\mathcal{E}_{-1} = \{E \subseteq \{-1\} \cup \pi_{\text{odd}}(d) : |E| \text{ is even}\},$$

then by applying (2.4) and an argument similar to the one that yielded (2.2) and (2.3) for $X_+(d)$, $d > 0$, we also deduce that for $d < 0$,

$$X_+(d) = \Big(\bigcup_{E \in \mathcal{E}_{-1}} R_E \Big) \setminus \pi_{\text{even}}(d), \tag{2.5}$$

where

$$R_E = \Big(\bigcap_{q \in E} X_-(q) \Big) \cap \Big(\bigcap_{q \in (\{-1\} \cup \pi_{\text{odd}}(d)) \setminus E} X_+(q) \Big), E \in \mathcal{E}_{-1}. \tag{2.6}$$

In order to show more concretely how this strategy for the solution of the basic problem is implemented, suppose as an example that we wish to determine $X_+(\pm 126)$. First, factor ± 126 as $\pm 2 \cdot 3^2 \cdot 7$. It follows from this factorization that

$$\pi_{\text{odd}}(\pm 126) = \{2, 7\},\ \pi_{\text{even}}(\pm 126) = \{3\},$$

hence

$$\mathcal{E} = \{\emptyset, \{2, 7\}\},\ \mathcal{E}_{-1} = \{\emptyset, \{-1, 2\}, \{-1, 7\}, \{2, 7\}\}.$$

It now follows from (2.2) and (2.3) that

$$\begin{aligned} X_+(126) &= (R_\emptyset \cup R_{\{2,7\}}) \setminus \{3\} \\ &= \Big(\big(X_+(2) \cap X_+(7)\big) \cup \big(X_-(2) \cap X_-(7)\big) \Big) \setminus \{3\}, \end{aligned}$$

and from (2.5) and (2.6) that

$$\begin{aligned} X_+(-126) &= (R_\emptyset \cup R_{\{-1,2\}} \cup R_{\{-1,7\}} \cup R_{\{2,7\}}) \setminus \{3\} \\ &= \Big(\big(X_+(-1) \cap X_+(2) \cap X_+(7)\big) \cup \big(X_-(-1) \cap X_-(2) \cap X_+(7)\big) \\ &\quad \cup \big(X_-(-1) \cap X_+(2) \cap X_-(7)\big) \cup \big(X_+(-1) \\ &\quad \cap X_-(2) \cap X_-(7)\big) \Big) \setminus \{3\}. \end{aligned}$$

In order to finish this calculation of $X_+(\pm 126)$, we must now calculate $X_+(2) \cap X_+(7)$, $X_-(2) \cap X_-(7)$, $X_+(-1) \cap X_+(2) \cap X_+(7)$, $X_-(-1) \cap X_-(2) \cap X_+(7)$, $X_-(-1) \cap X_+(2) \cap X_-(7)$, and $X_+(-1) \cap X_-(2) \cap X_-(7)$, which in turn requires the calculation of $X_\pm(-1)$, $X_\pm(2)$, and $X_\pm(7)$. Theorem 2.4 and formulae (2.2), (2.3), (2.5), and (2.6) hence reduce the solution of the Basic Problem to the solution of the

Fundamental Problem for Primes. If q is *prime*, calculate $X_\pm(q)$.

The Fundamental Problem for odd primes and the Basic Problem will be completely solved in Sects. 4.1 and 4.2 of Chap. 4. The Fundamental Problem for the prime 2 will be completely solved in the next section.

2.3 Gauss' Lemma and the Fundamental Problem for the Prime 2

The next theorem, along with Theorems 2.4 and 2.5, will be used many times in our subsequent work.

Theorem 2.6 $\chi_p(2) = (-1)^{(p^2-1)/8}$.

Theorem 2.6 solves the Fundamental Problem for the prime 2. It is easy to see that $(p^2-1)/8$ is even (odd) if and only if $p \equiv 1$ or 7 mod 8 ($p \equiv 3$ or 5 mod 8). Hence

$$X_+(2) = \{p : p \equiv 1 \text{ or } 7 \bmod 8\},$$
$$X_-(2) = \{p : p \equiv 3 \text{ or } 5 \bmod 8\}.$$

The proof of Theorem 2.6 will use a basic result in the theory of quadratic residues called Gauss' lemma (this lemma was first used by Gauss in his third proof of the Law of Quadratic Reciprocity [20], which proof we will present in Chap. 3). We will first state Gauss' lemma, then use it to prove Theorem 2.6, and then we will prove Gauss' lemma.

Toward that end, then, let $a \in \mathbb{Z}$, $\gcd(a, p) = 1$. Consider the minimal positive ordinary residues mod p of the integers $a, \ldots, \frac{1}{2}(p-1)a$. None of these ordinary residues is $p/2$, as p is odd, and they are all distinct as $\gcd(a, p) = 1$, hence let

$$u_1, \ldots, u_s \text{ be those ordinary residues that are } > p/2,$$
$$v_1, \ldots, v_t \text{ be those ordinary residues that are } < p/2.$$

N.B. $s + t = \frac{1}{2}(p-1)$. We then have

Theorem 2.7 (Gauss' Lemma)

$$\chi_p(a) = (-1)^s.$$

Proof of Theorem 2.6 Let σ be the number of minimal positive ordinary residues mod p of the integers in the set

$$1 \cdot 2, 2 \cdot 2, \ldots, \frac{1}{2}(p-1) \cdot 2 \tag{2.7}$$

that exceed $p/2$. Gauss' lemma implies that

$$\chi_p(2) = (-1)^\sigma.$$

Because each integer in (2.7) is less than $p, \sigma =$ the number of integers in the set (2.7) that exceed $p/2$. An integer $2j, j \in [1, (p-1)/2]$ does not exceed $p/2$ if and only if $1 \le j \le p/4$, hence the number of integers in (2.7) that do not exceed $p/2$ is $[p/4]$, where $[x]$ denotes the greatest integer not exceeding x. Hence

$$\sigma = \frac{p-1}{2} - \left[\frac{p}{4}\right].$$

To prove Theorem 2.6, it hence suffices to prove that

$$\text{for all odd integers } n, \frac{n-1}{2} - \left[\frac{n}{4}\right] \equiv \frac{n^2-1}{8} \bmod 2. \tag{2.8}$$

To see this, note first that the congruence in (2.8) is true for a particular integer n if and only if it is true for $n+8$, because

$$\frac{(n+8)-1}{2} - \left[\frac{n+8}{4}\right] = \frac{n-1}{2} + 4 - \left(\left[\frac{n}{4}\right] + 2\right) \equiv \frac{n-1}{2} - \left[\frac{n}{4}\right] \bmod 2,$$

$$\frac{(n+8)^2-1}{8} = \frac{n^2-1}{8} + 2n + 8 \equiv \frac{n^2-1}{8} \bmod 2.$$

Thus (2.8) holds if and only if it holds for $n = \pm 1, \pm 3$, and it is easy to check that (2.8) holds for these values of n. QED

Proof of Theorem 2.7 Let u_i, v_i be as defined before the statement of Gauss' lemma. We claim that

$$\{p - u_1, \ldots, p - u_s, v_1, \ldots, v_t\} = [1, \frac{1}{2}(p-1)]. \tag{2.9}$$

To see this, note first that if $i \neq j$ then $v_i \neq v_j, u_i \neq u_j$ hence $p-u_i \neq p-u_j$. It is also true that $p-u_i \neq v_j$ for all i,j; otherwise $p \equiv a(k+l) \bmod p$, where $2 \leq k+l \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1$, which is impossible because $\gcd(a,p) = 1$. Hence

$$|\{p-u_1, \ldots, p-u_s, v_1, \ldots, v_t\}| = s+t = \frac{p-1}{2}. \tag{2.10}$$

But $0 < v_i < p/2$ implies that $0 < v_i \leq (p-1)/2$ and $p/2 < u_i < p$, hence $0 < p-u_i \leq (p-1)/2$, and so

$$\{p-u_1, \ldots, p-u_s, v_1, \ldots, v_t\} \subseteq [1, \frac{1}{2}(p-1)]. \tag{2.11}$$

As $|[1, \frac{1}{2}(p-1)]| = \frac{1}{2}(p-1)$, (2.9) follows from (2.10) and (2.11).

It follows from (2.9) that

$$\prod_1^s (p-u_i) \prod_1^t v_i = \Big(\frac{p-1}{2}\Big)!.$$

Because

$$p-u_i \equiv -u_i \bmod p$$

we conclude from the preceding equation that

$$(-1)^s \prod_1^s u_i \prod_1^t v_i \equiv \Big(\frac{p-1}{2}\Big)! \bmod p. \tag{2.12}$$

Because $u_1, \ldots, u_s, v_1, \ldots, v_t$ are the least positive ordinary residues of $a, \ldots, \frac{1}{2}(p-1)a$, it is a consequence of (2.12) that

$$(-1)^s a^{(p-1)/2} \Big(\frac{p-1}{2}\Big)! \equiv \Big(\frac{p-1}{2}\Big)! \bmod p. \tag{2.13}$$

But p and $(\frac{p-1}{2})!$ are relatively prime, and so (2.13) implies that

$$(-1)^s a^{(p-1)/2} \equiv 1 \bmod p$$

i.e.,

$$a^{(p-1)/2} \equiv (-1)^s \bmod p.$$

By Euler's criterion (Theorem 2.5),

$$a^{(p-1)/2} \equiv \chi_p(a) \bmod p,$$

hence

$$\chi_p(a) \equiv (-1)^s \bmod p.$$

It follows that $\chi_p(a) - (-1)^s$ is either 0 or ± 2 and is also divisible by p and so

$$\chi_p(a) = (-1)^s.$$

QED

We now need to solve the Fundamental Problem for odd primes. This will be done in Chap. 4 by using a result which Gauss called the *theorema aureum*, the "golden theorem", of number theory. We will discuss that result extensively in the next chapter.