7 Quadratic Residues

In this chapter, we will consider the general question of whether an integer a has a square root mod (n), and if so, how many there are and how one can find them. One of the main applications of this is to the solution of quadratic congruences, but we will also deduce a proof that there are infinitely many primes $p \equiv 1 \bmod (4)$, and we will give a useful primality test for Fermat numbers.

7.1 Quadratic congruences

To provide some motivation for what follows, we first briefly consider quadratic congruences. Just as in the case of quadratic equations, solving quadratic congruences can be reduced to the problem of finding square roots. Consider the formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

for the roots of a quadratic equation $ax^2 + bx + c = 0$, where a, b and c are real or complex numbers. If we want this to apply to the case where $a, b, c \in \mathbb{Z}_n$, we will clearly need $2a$ to be a unit mod (n), so that we can divide by $2a$. Let us therefore assume, for the moment, that n is odd and that $a \in U_n$. Then $4a \in U_n$, so the quadratic equation is equivalent to

$$4a^2x^2 + 4abx + 4ac = 0\,.$$

Now we know that

$$(2ax+b)^2 = 4a^2x^2 + 4abx + b^2\,,$$

so we can write the equation in the form

$$(2ax+b)^2 = b^2 - 4ac\,.$$

If we can find all the square roots s of $b^2 - 4ac$ in $\mathbb{Z}_n$, we can then find all the solutions $x \in \mathbb{Z}_n$ of the quadratic equation in the form $2ax + b = s$, or equivalently $x = (-b+s)/2a$. In looking for square roots in $\mathbb{Z}_n$, however, we should be prepared for surprises (if that is not a contradiction): for instance, in $\mathbb{Z}_{15}$ the elements 1 and 4 each have four square roots (namely $\pm 1, \pm 4$ and $\pm 2, \pm 7$ respectively), while the other units have none.

Exercise 7.1

Find all the solutions in $\mathbb{Z}_{15}$ of the congruence $x^2 - 3x + 2 \equiv 0 \bmod (15)$.

Exercise 7.2

What square roots do the elements 5 and 16 have in $\mathbb{Z}_{21}$? Hence find all solutions of the congruences $x^2 + 3x + 1 \equiv 0 \bmod (21)$ and $x^2 + 2x - 3 \equiv 0 \bmod (21)$.

7.2 The group of quadratic residues

Definition

An element $a \in U_n$ is a *quadratic residue* mod (n) if $a = s^2$ for some $s \in U_n$; the set of such quadratic residues is denoted by Q_n. For small n one can determine Q_n simply by squaring all the elements $s \in U_n$.

Example 7.1

$Q_7 = \{1, 2, 4\} \subset U_7$, while $Q_8 = \{1\} \subset U_8$.

Exercise 7.3

Find Q_n for each $n \leq 12$.

We now determine how many square roots an element $a \in Q_n$ can have.

Lemma 7.1

Let k denote the number of distinct primes dividing n. If $a \in Q_n$, then the number N of elements $t \in U_n$ such that $t^2 = a$ is given by

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \bmod (8), \\ 2^{k-1} & \text{if } n \equiv 2 \bmod (4), \\ 2^k & \text{otherwise.} \end{cases}$$

Proof. If $a \in Q_n$ then $s^2 = a$ for some $s \in U_n$. Any element $t \in U_n$ has the form $t = sx$ for some unique $x \in U_n$, and we have $t^2 = a$ if and only if $x^2 = 1$ in U_n. Thus N is the number of solutions of $x^2 = 1$ in U_n, and Example 3.18 gives the required formula for N. □

Comment

The number N of square roots depends only on n, and not on the element $a \in Q_n$. Moreover, if we have one square root s of a, then we can find all its other square roots $t = sx$ by finding all solutions of $x^2 = 1$, using the method of Example 3.18.

Exercise 7.4

Show that $|Q_n| = \phi(n)/N$, where N is given by Lemma 7.1.

Exercise 7.5

Find the elements of Q_{60}, together with their square roots.

Lemma 7.2

Q_n is a subgroup of U_n.

Proof

We need to show that Q_n contains the identity element of U_n, and is closed under taking products and inverses. Firstly, $1 \in Q_n$ since $1 = 1^2$ with $1 \in U_n$. If $a, b \in Q_n$ then $a = s^2$ and $b = t^2$ for some $s, t \in U_n$, so $ab = (st)^2$ with $st \in U_n$, giving $ab \in Q_n$. Finally, if $a \in Q_n$ then $a = s^2$ for some $s \in U_n$; since a and s

are units mod (n) they have inverses a^{-1} and s^{-1} in U_n, and $a^{-1} = (s^{-1})^2$ so that $a^{-1} \in Q_n$. □

Algebraic comment

The function $\theta : U_n \to Q_n$, given by $\theta(s) = s^2$, is a homomorphism of groups, since $\theta(st) = (st)^2 = s^2t^2 = \theta(s)\theta(t)$ for all $s, t \in U_n$. It is onto, by definition of Q_n, and its kernel K (the set of elements $x \in U_n$ such that $\theta(x) = 1$) is the subgroup of U_n consisting of the N solutions of $x^2 = 1$. For each $a \in Q_n$, the N square roots of a form a coset $\theta^{-1}(a)$ of K in U_n. For instance, the square roots of the elements $1, 2, 4$ of Q_7 form the cosets $\{\pm1\}, \{\pm3\}, \{\pm2\}$ of $K = \{\pm1\}$ in U_7.

In the special cases where U_n is cyclic (see Theorem 6.11), we have a simple description of Q_n:

Lemma 7.3

Let $n > 2$, and suppose that there is a primitive root g mod (n); then Q_n is a cyclic group of order $\phi(n)/2$, generated by g^2, consisting of the even powers of g.

Proof

Since $n > 2$, Exercise 5.7 implies that $\phi(n)$ is even. The elements $a \in U_n$ are the powers g^i for $i = 1, \ldots, \phi(n)$, with $g^{\phi(n)} = 1$. If i is even, then $a = g^i = (g^{i/2})^2 \in Q_n$. Conversely, if $a \in Q_n$ then $a = (g^j)^2$ for some j, so $i \equiv 2j$ mod $(\phi(n))$ for some j; since $\phi(n)$ is even, this implies that i is even. Thus Q_n consists of the even powers of g, so it is the cyclic group of order $\phi(n)/2$ generated by g^2. □

Warning

We need the condition $n > 2$ to ensure that the cyclic group U_n has even order. In any cyclic group of *odd* order m, every element is a square and can be written as an even power of a generator g: for each i we have $g^i = g^{i+m}$, with one of i and $i + m$ even, so g^i is a square.

Example 7.2

If $n = 7$ then we can take $g = 3$ as a primitive root. The powers of g in U_7 are $g = 3$, $g^2 = 2$, $g^3 = 6$, $g^4 = 4$, $g^5 = 5$ and $g^6 = 1$; of these, the quadratic residues $a = 1, 2$ and 4 correspond to the even powers of g. Thus Q_7 is the cyclic group of order 3 generated by $g^2 = 2$.

Exercise 7.6

Use a primitive root to find the elements of Q_{25}.

7.3 The Legendre symbol

We now consider the problem of determining whether or not a given element $a \in U_n$ is a quadratic residue. Unfortunately, Lemma 7.3 is not very effective here: U_n is not always cyclic, and even when it is, it can be difficult to find a primitive root g and then express a as a power of g (see Chapter 6). We therefore need more powerful techniques. Quadratic residues are easiest to determine in the case of prime moduli; the case $n = 2$ is trivial, so we assume for the time being that n is an odd prime p. The following piece of notation greatly simplifies the problem of determining the elements of Q_p:

Definition

For an odd prime p, the *Legendre symbol* of any integer a is

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a, \\ 1 & \text{if } a \in Q_p, \\ -1 & \text{if } a \in U_p \setminus Q_p. \end{cases}$$

Clearly this depends only on the congruence class of a mod (p), so we can regard it as being defined either on $\mathbb{Z}$ or on $\mathbb{Z}_p$.

Example 7.3

Let $p = 7$. Then as in Example 7.2 we have

$$\left(\frac{a}{7}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \bmod (7), \\ 1 & \text{if } a \equiv 1, 2 \text{ or } 4 \bmod (7), \\ -1 & \text{if } a \equiv 3, 5 \text{ or } 6 \bmod (7). \end{cases}$$

Recall that by Corollary 6.6 there is a primitive root g mod (p), so that each $a \in U_p$ has the form g^i for some i. This justifies the next result:

Corollary 7.4

If p is an odd prime, and g is a primitive root mod (p), then

$$\left(\frac{g^i}{p}\right) = (-1)^i.$$

Proof

Both $(\frac{g^i}{p})$ and $(-1)^i$ are equal to ± 1, and Lemma 7.3 shows that $(\frac{g^i}{p}) = 1$ if and only if i is even, which is also the condition for $(-1)^i$ to be 1. □

The next result is very useful for calculations with the Legendre symbol:

Theorem 7.5

If p is an odd prime, then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

for all integers a and b.

Proof

If p divides a or b then each side is equal to 0, so we may assume that $a, b \in U_p$. If we put $a = g^i$ and $b = g^j$ for some primitive root $g \in U_p$, so that $ab = g^{i+j}$, then Corollary 7.4 gives

$$\left(\frac{ab}{p}\right) = (-1)^{i+j} = (-1)^i(-1)^j = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Example 7.4

Let $p = 17$. Then $-1 \equiv 4^2$, so $(\frac{-1}{17}) = 1$ and hence Theorem 7.5 gives $(\frac{a}{17}) = (\frac{-a}{17})$ for all $a \in U_{17}$, that is, $a \in Q_{17}$ if and only if $-a \in Q_{17}$. For instance, $13 \in Q_{17}$ since $-13 \equiv 2^2 \in Q_{17}$.

Warning

The values of $(\frac{-a}{p})$ and $-(\frac{a}{p})$ may well be different: for instance, $(\frac{-1}{17}) = 1$ but $-(\frac{1}{17}) = -1$.

There is an obvious extension of Theorem 7.5: for all integers $a_1, \ldots, a_k$ we have

$$\left(\frac{a_1 \ldots a_k}{p}\right) = \left(\frac{a_1}{p}\right) \ldots \left(\frac{a_k}{p}\right).$$

Exercise 7.7

By factorising 28, show that $-1 \in Q_{29}$.

In algebraic terms, Theorem 7.5 states that the function $U_p \rightarrow \{\pm 1\}$, which sends each unit a to $(\frac{a}{p})$, is a group-homomorphism; its kernel is Q_p. The next result is known as *Euler's criterion*:

Theorem 7.6

If p is an odd prime, then for all integers a we have

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

(This is slightly more effective than Corollary 7.4 for determining quadratic residues, since one is not required to find a primitive root, but it can nevertheless be a little tedious to compute $a^{(p-1)/2} \bmod (p)$.)

Proof

The result is trivial if p divides a, so we may assume that $a \in U_p$. Thus $a = g^i$ for some primitive root $g \in U_p$. Define $h = g^{(p-1)/2}$. Then $h^2 = g^{p-1} = 1$ in U_p, so $h = \pm 1$ (either apply Lagrange's Theorem (Theorem 4.1) to the polynomial $x^2 - 1$, or note that p divides $h^2 - 1 = (h-1)(h+1)$). Since g has order $p - 1 > (p-1)/2$ we cannot have $h = 1$, so $h = -1$. Then using Corollary 7.4 we have

$$a^{(p-1)/2} = \left(g^i\right)^{(p-1)/2} = \left(g^{(p-1)/2}\right)^i = h^i = (-1)^i = \left(\frac{g^i}{p}\right) = \left(\frac{a}{p}\right)$$

in $\mathbb{Z}_p$, which proves the result. □

Example 7.5

Let $p = 23$ and $a = 5$. To determine whether $5 \in Q_{23}$ we need to compute 5^{11} mod (23). Now $5^2 \equiv 2$, so $5^{11} \equiv 2^5.5 \equiv 9.5 \equiv -1$. Thus $(\frac{5}{23}) = -1$ and so $5 \notin Q_{23}$.

Exercise 7.8

Determine whether 3 and 5 are quadratic residues mod (29).

Corollary 7.7

Let p be an odd prime. Then $-1 \in Q_p$ if and only if $p \equiv 1$ mod (4).

Proof

If we take $a = -1$ in Theorem 7.6, we see that

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \bmod (p),$$

so $-1 \in Q_p$ if and only if $(p-1)/2$ is even, that is, $p \equiv 1$ mod (4). □

Example 7.6

We have $-1 = 2^2$ in $\mathbb{Z}_5$ and $-1 = 5^2$ in $\mathbb{Z}_{13}$, but -1 is not a square in $\mathbb{Z}_3$ or $\mathbb{Z}_7$.

We showed in Theorem 2.9 that there are infinitely many primes $p \equiv 3$ mod (4). We can now fulfil the promise made then to prove the same result for primes $p \equiv 1$ mod (4).

Corollary 7.8

There are infinitely many primes $p \equiv 1$ mod (4).

Proof

If there are only finitely many primes $p \equiv 1$ mod (4), say $p_1, \ldots, p_k$, then define $m = (2p_1 \ldots p_k)^2 + 1$. Being odd, m must be divisible by some odd prime p. Then $(2p_1 \ldots p_k)^2 \equiv -1$ mod (p), so $-1 \in Q_p$, and hence $p \equiv 1$ mod (4) by Corollary 7.7. By our hypothesis, this implies that $p = p_i$ for some $i = 1, \ldots, k$, so p divides $m-(2p_1\dots p_k)^2=1$, which is impossible. Hence there must be infinitely many primes $p\equiv 1 \bmod (4)$. □

In order to state the next result we need some more notation. If we use the set $\{\pm1,\pm2,\dots,\pm(p-1)/2\}$ as a reduced set of residues mod (p), then we can partition U_p into two subsets

$$P=\{1,2,\dots,(p-1)/2\}\subset U_p \quad\text{and}\quad N=\{-1,-2,\dots,-(p-1)/2\}\subset U_p\,,$$

represented as shown by positive and negative integers. For each $a\in U_p$ we define

$$aP=\{ax \mid x\in P\}=\{a,2a,\dots,(p-1)a/2\}\subset U_p\,.$$

Thus $N=(-1)P$, for example.

A more effective test for quadratic residues is given by *Gauss's Lemma:*

Theorem 7.9

If p is an odd prime and $a\in U_p$, then $(\frac{a}{p})=(-1)^\mu$ where $\mu=|aP\cap N|$.

Before proving this, let us consider an example:

Example 7.7

Let $p=19$, so $P=\{1,2,\dots,9\}$, and let $a=11$. If we multiply each element of P by 11 mod (19), and then represent it by an element of $P\cup N$, we get

$$aP=11P=\{-8,3,-5,6,-2,9,1,-7,4\}\,.$$

This contains four elements of N (the terms with minus signs), so $\mu=4$, which is even; thus $(\frac{11}{19})=1$, so $11\in Q_{19}$. In fact, $11\equiv 7^2 \bmod (19)$.

Proof (Proof of Theorem 7.9.)

If x and y are distinct elements of P then $ax\not\equiv\pm ay$ in U_p: for if $ax\equiv\pm ay$ in $\mathbb{Z}$ then $p\mid a(x\mp y)$, so $p\mid(x\mp y)$, which is impossible since x and y are distinct elements of $\{1,2,\ \dots\ ,(p-1)/2\}$. This means that the elements of aP lie in distinct sets

$$\{\pm1\},\ \{\pm2\},\ \dots\ ,\{\pm(p-1)/2\}\,.$$

There are $(p-1)/2$ such sets, and there are $(p-1)/2$ elements of aP, so each set contains exactly one element of aP; thus

$$aP=\{\varepsilon_i i \mid i=1,2,\ \dots\ ,(p-1)/2\}$$

where each $\varepsilon_i = \pm 1$. Note that $\varepsilon_i = 1$ if $\varepsilon_i i \in P$, and $\varepsilon_i = -1$ if $\varepsilon_i i \in N$. Since aP is contained in the abelian group U_p, we can multiply all its elements together in any order, and get the same result, so

$$\begin{aligned} a^{(p-1)/2}((p-1)/2)! &= (\prod_i \varepsilon_i).((p-1)/2)! \\ &= (-1)^{\mu}.((p-1)/2)! \end{aligned}$$

in U_p, where $\mu = |aP \cap N|$ is the number of i such that $\varepsilon_i = -1$. Cancelling the unit $((p-1)/2)!$, we see that $a^{(p-1)/2} = (-1)^{\mu}$ in U_p, so that

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

in $\mathbb{Z}$. Now Euler's criterion (Theorem 7.6) gives

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

so

$$\left(\frac{a}{p}\right) \equiv (-1)^{\mu} \bmod (p)\,.$$

Both sides of this congruence are equal to ± 1, so they must be equal to each other since $p > 2$. □

Exercise 7.9

Apply Gauss's Lemma to Exercise 7.8 ($p = 29$ and $a = 3, 5$). Does 10 belong to Q_{29}?

Corollary 7.10

If p is an odd prime then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}\,;$$

thus $2 \in Q_p$ if and only if $p \equiv \pm 1 \bmod (8)$.

Proof

Putting $a = 2$ in Gauss's Lemma, we get

$$aP = 2P = \{2, 4, 6, \ldots, p-1\}\,.$$

First suppose that $p \equiv 1 \bmod (4)$. Then

$$2P = \{2, 4, \ldots, (p-1)/2, (p+3)/2, \ldots, p-1\}$$

with the first $(p-1)/4$ elements $2, 4, \ldots, (p-1)/2$ in P, and the remaining $(p-1)/4$ elements $(p+3)/2, \ldots, p-1$ in N. Thus $\mu = |2P \cap N| = (p-1)/4$, so Gauss's Lemma gives

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/4} = \left((-1)^{(p-1)/4}\right)^{(p+1)/2} = (-1)^{(p^2-1)/8},$$

where we have used the fact that $(p+1)/2$ is odd. Now suppose that $p \equiv -1 \bmod (4)$. Then

$$2P = \{2, 4, \ldots, (p-3)/2, (p+1)/2, \ldots, p-1\}$$

with the first $(p-3)/4$ elements $2, 4, \ldots, (p-3)/2$ in P, and the remaining $(p+1)/4$ elements $(p+1)/2, \ldots, p-1$ in N. Thus $\mu = (p+1)/4$ and hence

$$\left(\frac{2}{p}\right) = (-1)^{(p+1)/4} = \left((-1)^{(p+1)/4}\right)^{(p-1)/2} = (-1)^{(p^2-1)/8},$$

where we have now used the fact that $(p-1)/2$ is odd.

This proves the first part of the theorem, and for the second part we have

$$\begin{aligned} 2 \in Q_p \quad &\Longleftrightarrow \quad \left(\frac{2}{p}\right) = +1 \\ &\Longleftrightarrow \quad (p^2-1)/8 \text{ is even} \\ &\Longleftrightarrow \quad 16 | p^2 - 1 \\ &\Longleftrightarrow \quad 16 | (p-1)(p+1) \\ &\Longleftrightarrow \quad 8 | p-1 \text{ or } 8 | p+1 \\ &\Longleftrightarrow \quad p \equiv \pm 1 \bmod (8), \end{aligned}$$

completing the proof. □

Example 7.8

2 is a quadratic residue mod (p) for $p = 7, 17, 23, 31, \ldots$, with square roots $\pm 3, \pm 6, \pm 5, \pm 8, \ldots$; however, 2 is not a quadratic residue mod (p) for $p = 3, 5, 11, 13, \ldots$.

Exercise 7.10

For which primes p is $-2 \in Q_p$?

7.4 Quadratic reciprocity

To determine whether or not an integer a is a quadratic residue mod (p), we need to evaluate $(\frac{a}{p})$; by Theorem 7.5, $(\frac{a}{p})$ is the product of the Legendre symbols $(\frac{q}{p})$ where q ranges over the primes dividing a (with repetitions, as necessary). It is therefore sufficient to evaluate $(\frac{q}{p})$ for each prime q. We have just dealt with the case $q = 2$, so we can assume that q is an odd prime. If we calculate $(\frac{q}{p})$ for small primes p and q (for instance by Gauss's Lemma) we get the following table, with rows and columns indexed by the values of p and q respectively:

	$q =$ 3	5	7	11	13	17	19
$p =$ 3	0	−1	1	−1	1	−1	1
5	−1	0	−1	1	−1	−1	1
7	−1	−1	0	1	−1	−1	−1
11	1	1	−1	0	−1	−1	−1
13	1	−1	−1	−1	0	1	−1
17	−1	−1	−1	−1	1	0	1
19	−1	1	1	1	−1	1	0

Values of the Legendre symbol $(\frac{q}{p})$ for odd primes $p, q \leq 19$

We notice that the table is nearly symmetric, that is, $(\frac{q}{p}) = (\frac{p}{q})$ for most p and q, the exceptions occuring when p and q are distinct primes congruent to 3 mod (4). This is a general result, called the *Law of Quadratic Reciprocity*, conjectured by Euler in 1783. Legendre gave several incomplete proofs, but in 1795 Gauss (aged 18) discovered the law for himself and provided the first correct proof. This is one of the central theorems of number theory, and many different proofs have subsequently been published.

Theorem 7.11

If p and q are distinct odd primes, then

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

except when $p \equiv q \equiv 3$ mod (4), in which case

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Comment

An equivalent form of this is the elegant result, due to Legendre, that

$$\left(\frac{q}{p}\right).\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$$

for all distinct odd primes p and q.

Before proving this theorem, let us look at some applications.

Example 7.9

Is $83 \in Q_{103}$? Since 83 and 103 are distinct odd primes, we have

$$\begin{aligned}
\left(\frac{83}{103}\right) &= -\left(\frac{103}{83}\right) && \text{(by Theorem 7.11, since } 83 \equiv 103 \equiv 3 \bmod (4))\\
&= -\left(\frac{20}{83}\right) && \text{(since } 103 \equiv 20 \bmod (83))\\
&= -\left(\frac{2}{83}\right)^2\left(\frac{5}{83}\right) && \text{(by Theorem 7.5, since } 20 = 2^2.5)\\
&= -\left(\frac{5}{83}\right) && \text{(since } \left(\frac{2}{83}\right) = \pm 1)\\
&= -\left(\frac{83}{5}\right) && \text{(by Theorem 7.11)}\\
&= -\left(\frac{3}{5}\right) && \text{(since } 83 \equiv 3 \bmod (5))\\
&= -\left(\frac{5}{3}\right) && \text{(by Theorem 7.11)}\\
&= -\left(\frac{2}{3}\right) && \text{(since } 5 \equiv 2 \bmod (3))\\
&= 1, && \text{(since } 2 \notin Q_3)
\end{aligned}$$

so that $83 \in Q_{103}$. (In fact $83 \equiv 17^2 \bmod (103)$.)

Exercise 7.11

Is 219 a quadratic residue mod (383)?

Example 7.10

For which primes p is $3 \in Q_p$? Since $3 \in Q_2$ and $3 \notin Q_3$, we may assume that $p > 3$. If $p \equiv 1 \bmod (4)$ then the Law of Quadratic Reciprocity gives

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \bmod (3), \text{ that is, if } p \equiv 1 \bmod (12),\\ -1 & \text{if } p \equiv 2 \bmod (3), \text{ that is, if } p \equiv 5 \bmod (12).\end{cases}$$

If $p \equiv 3 \bmod (4)$ then it gives

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} -1 & \text{if } p \equiv 1 \bmod (3), \text{ that is, if } p \equiv 7 \bmod (12), \\ +1 & \text{if } p \equiv 2 \bmod (3), \text{ that is, if } p \equiv 11 \bmod (12). \end{cases}$$

Putting these results together, we see that $3 \in Q_p$ if and only if $p = 2$ or $p \equiv \pm 1 \bmod (12)$.

Exercise 7.12

For each of the following integers a, determine the primes p for which $a \in Q_p$: $a = -3, 5, 6, 7, 10, 169$.

Example 7.10 leads to *Pepin's test* for primality of Fermat numbers (see Chapter 2). Pepin proved this in 1877, and in recent years it has been implemented on computers to show that several Fermat numbers are composite.

Corollary 7.12

If $n \geq 1$, then the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if

$$3^{(F_n - 1)/2} \equiv -1 \bmod (F_n).$$

Proof

It is easily seen that $F_n \equiv 5 \bmod (12)$, so if F_n is a prime p then $3 \notin Q_p$ by Example 7.10; then Euler's criterion gives $3^{(p-1)/2} \equiv -1 \bmod (p)$, as required. For the converse, suppose that $3^{(F_n-1)/2} \equiv -1 \bmod (F_n)$; then squaring, we get $3^{F_n - 1} \equiv 1 \bmod (F_n)$ and hence $3^{F_n-1} \equiv 1 \bmod (p)$ for any prime p dividing F_n. As an element of the group U_p, 3 therefore has order m dividing $F_n - 1 = 2^{2^n}$, so $m = 2^i$ for some $i \leq 2^n$. Now

$$3^{2^{2^n - 1}} = 3^{(F_n - 1)/2} \equiv -1 \not\equiv 1 \bmod (p)$$

(since p is odd, because F_n is), so $i = 2^n$ and $m = 2^{2^n} = F_n - 1$. However, $m \leq |U_p| = p - 1$ by definition of m, so $F_n \leq p$ and hence $F_n = p$, showing that F_n is prime. □

Comment

This proof shows that 3 is a primitive root for any Fermat prime p, since 3 has order $p - 1$ as an element of U_p.

Example 7.11

Let $n = 2$, so that $F_n = 17$. Then $3^{(F_n-1)/2} = 3^8 = (3^4)^2 \equiv (-4)^2 \equiv -1$ mod (17), confirming that 17 is prime.

Exercise 7.13

Use Pepin's test to show that $F_3 = 257$ is prime.

Proof (Proof of Theorem 7.11.)

There are many proofs, none of them entirely straightforward. Perhaps the neatest is that due to Eisenstein, using trigonometric functions, given in Serre (1973), but it is so slick that it doesn't really explain why the result should be true. The following proof is a little longer, but it is fairly elementary and somewhat more illuminating.

Let $P = \{1, 2, \ldots, (p-1)/2\} \subset U_p$ and $N = (-1)P$ as before, and similarly let $Q = \{1, 2, \ldots, (q-1)/2\} \subset U_q$. If we put $a = q$ in Gauss's Lemma, then

$$\left(\frac{q}{p}\right) = (-1)^{\mu}$$

where $\mu = |qP \cap N|$ is the number of elements $x \in P$ such that $qx \equiv n \bmod (p)$ for some $n \in N$; this congruence is equivalent to $qx - py \in N$ for some integer y, that is,

$$-\frac{p}{2} < qx - py < 0$$

for some integer y. We now look for the possible values of y satisfying this condition.

Given any $x \in P$, the values of $qx - py$ for $y \in \mathbb{Z}$ differ by multiples of p, so $-p/2 < qx - py < 0$ for at most one integer y. If such an integer y exists, then

$$0 < \frac{qx}{p} < y < \frac{qx}{p} + \frac{1}{2}.$$

Now $x \leq (p-1)/2$, so

$$y < \frac{qx}{p} + \frac{1}{2} \leq \frac{q(p-1)}{2p} + \frac{1}{2} < \frac{q+1}{2}.$$

Thus y is an integer strictly between 0 and $(q+1)/2$, so $y \in \{1, 2, \ldots, (q-1)/2\} = Q$. We have therefore shown that μ is the number of pairs $(x, y) \in P \times Q$ such that

$$-\frac{p}{2} < qx - py < 0.$$

Interchanging the roles of p and q, we also have

$$\left(\frac{p}{q}\right) = (-1)^{\nu}$$

where ν is the number of pairs $(y, x) \in Q \times P$ such that $-q/2 < py - qx < 0$, or equivalently the number of pairs $(x, y) \in P \times Q$ such that

$$0 < qx - py < \frac{q}{2}.$$

It follows that

$$\left(\frac{q}{p}\right).\left(\frac{p}{q}\right) = (-1)^{\mu+\nu},$$

where $\mu + \nu$ is the number of pairs $(x, y) \in P \times Q$ such that

$$-\frac{p}{2} < qx - py < 0 \quad \text{or} \quad 0 < qx - py < \frac{q}{2}.$$

There are no pairs $(x, y) \in P \times Q$ satisfying $qx - py = 0$, since p and q are coprime, so this condition can be simplified to

$$-\frac{p}{2} < qx - py < \frac{q}{2}.$$

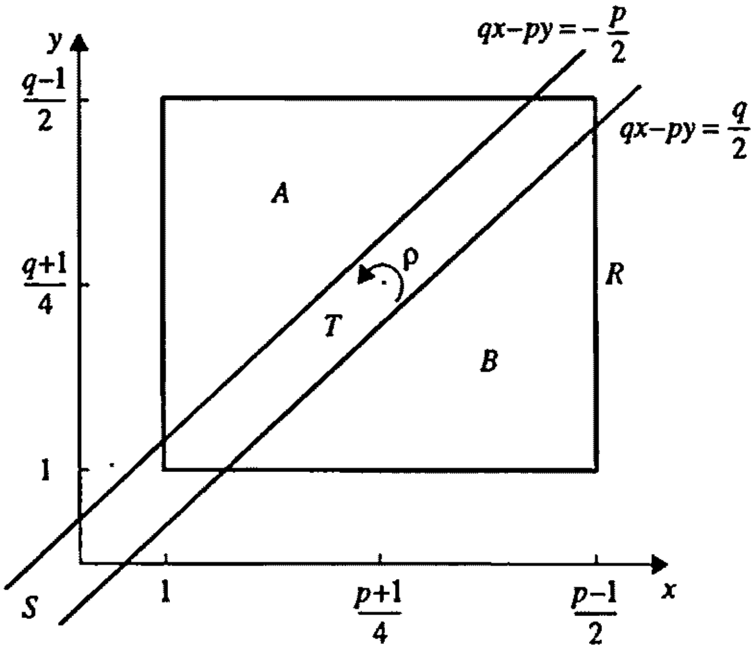

Figure 7.1. The proof of Theorem 7.11.

Figure 7.1 shows $P \times Q$ as the set of integer points (x, y) (points with integer coordinates) in the rectangle R in the xy-plane given by

$$1 \leq x \leq \frac{p-1}{2}, \quad 1 \leq y \leq \frac{q-1}{2}.$$

The inequalities $-p/2 < qx - py < q/2$ define the strip S between the two parallel straight lines $qx - py = -p/2$ and $qx - py = q/2$, so $\mu + \nu$ is the number of integer points in the region $T = R \cap S$. Now the number of integer points $(x, y) \in R$ is $|P \times Q| = |P|.|Q| = (p-1)(q-1)/4$, so

$$\mu + \nu = \frac{(p-1)(q-1)}{4} - (\alpha + \beta)$$

where α and β are the numbers of integer points in the subsets A and B of R above and below S. If we can show that $\alpha = \beta$, then $\mu + \nu \equiv (p-1)(q-1)/4 \bmod (2)$, and hence

$$\left(\frac{q}{p}\right).\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$$

as required.

We prove that $\alpha = \beta$ by using the half-turn of R about its midpoint $((p+1)/4, (q+1)/4)$ to pair off the integer points in A and B. This half-turn is the rotation ρ given by

$$\rho(x, y) = (x', y') = \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right),$$

a formula which shows that ρ sends integer points to integer points. Moreover, it is straightforward to check that $qx - py < -p/2$ if and only if $qx' - py' > q/2$, so $\rho(A) = B$ and $\rho(B) = A$. Thus ρ induces the required bijection between the integer points in A and B, so $\alpha = \beta$ and the proof is complete. □

7.5 Quadratic residues for prime-power moduli

Having dealt with quadratic residues for prime moduli, we now consider prime-power moduli, dealing with the odd case first.

Theorem 7.13

Let p be an odd prime, let $e \geq 1$, and let $a \in \mathbb{Z}$. Then $a \in Q_{p^e}$ if and only if $a \in Q_p$.

Proof

We know from Theorem 6.7 that there is a primitive root g mod (p^e), so by applying Lemma 7.3 with $n = p^e$ we see that Q_{p^e} consists of the even powers of g. Now g, regarded as an element of U_p, is also a primitive root mod (p), and by applying Lemma 7.3 with $n = p$ we know that Q_p also consists of the even powers of g. Thus $a \in Q_{p^e}$ if and only if $a \in Q_p$. □

For odd primes p, we can find square roots in U_{p^e} for $e \geq 2$ by applying the iterative method in Chapter 4, Section 3 to the polynomial $f(x) = x^2 - a$: we use a square root of a mod (p^i) to find the square roots mod (p^{i+1}). Suppose that $a \in Q_p$, and r is a square root of a mod (p^i) for some $i \geq 1$; thus $r^2 \equiv a$ mod (p^i), say $r^2 = a + p^i q$. If we put $s = r + p^i k$, where k is as yet unknown, then $s^2 = r^2 + 2rp^i k + p^{2i}k^2 \equiv a + (q + 2rk)p^i$ mod (p^{i+1}), since $2i \geq i+1$. Now $\gcd(2r, p) = 1$, so we can choose k to satisfy the linear congruence $q + 2rk \equiv 0$ mod (p), giving $s^2 \equiv a$ mod (p^{i+1}) as required. By Lemma 7.1, an element $a \in Q_{p^{i+1}}$ has just two square roots in $U_{p^{i+1}}$ for odd p, so these must be $\pm s$. It follows that if we have a square root for a in U_p, then we can iterate this process to find its square roots in U_{p^e} for all e.

Example 7.12

Let us take $a = 6$ and $p^e = 5^2$. In U_5 we have $a = 1 = 1^2$, so we can take $r = 1$ as a square root mod (5). Then $r^2 = 1 = 6 + 5.(-1)$, so $q = -1$ and we need to solve the linear congruence $-1 + 2k \equiv 0$ mod (5). This has solution $k \equiv 3$ mod (5), so we take $s = r + p^i k = 1 + 5.3 = 16$, and the square roots of 6 in $\mathbb{Z}_{5^2}$ are given by ± 16, or equivalently ± 9 mod (5^2). If we want the square roots of 6 in $\mathbb{Z}_{5^3}$ we repeat the process: we can take $r = 9$ as a square root mod (5^2), with $r^2 = 81 = 6 + 5^2.3$, so $q = 3$; solving $3 + 18k \equiv 0$ mod (5) we have $k \equiv -1$, so $s = 9 + 5^2.(-1) = -16$, giving square roots ± 16 mod (5^3).

Exercise 7.14

Find the square roots of 6 mod (5^4).

Exercise 7.15

Find the square roots of -3 mod (7^2) and mod (7^3).

It should not be a surprise to learn that the situation for $p = 2$ is similar but slightly more complicated:

Theorem 7.14

Let a be an odd integer. Then

(a) $a \in Q_2$;

(b) $a \in Q_4$ if and only if $a \equiv 1$ mod (4);

(c) if $e \geq 3$, then $a \in Q_{2^e}$ if and only if $a \equiv 1$ mod (8).

Proof

Parts (a) and (b) are obvious: squaring the elements of $U_2 = \{1\} \subset \mathbb{Z}_2$ and of $U_4 = \{1, 3\} \subset \mathbb{Z}_4$, we see that $Q_2 = \{1\}$ and $Q_4 = \{1\}$. For part (c) we use Theorem 6.10, which states that the elements of U_{2^e} all have the form $\pm 5^i$ for some i; squaring, we see that the quadratic residues are the even powers of 5. Since $5^2 \equiv 1 \bmod (8)$, these are all represented by integers $a \equiv 1 \bmod (8)$. Now both the even powers of 5 and the elements $a \equiv 1 \bmod (8)$ account for exactly one quarter of the classes in Q_{2^e}; since the first set is contained in the second, these two sets are equal. □

Example 7.13

$Q_8 = \{1\}$, $Q_{16} = \{1, 9\}$, $Q_{32} = \{1, 9, 17, 25\}$, and so on.

One can find square roots in Q_{2^e} by adapting the iterative algorithm given earlier for odd prime-powers. Suppose that $a \in Q_{2^i}$ for some $i \geq 3$, say $r^2 = a + 2^i q$. If we put $s = r + 2^{i-1}k$, then $s^2 = r^2 + 2^i rk + 2^{2(i-1)}k^2 \equiv a + (q + rk)2^i \bmod (2^{i+1})$, since $2(i-1) \geq i + 1$. Now r is odd, so we can choose $k = 0$ or 1 to make $q + rk$ even, giving $s^2 \equiv a \bmod(2^{i+1})$. Thus s is a square root of a in $U_{2^{i+1}}$. By Lemma 7.1 there are four square roots of a in $U_{2^{i+1}}$, and these have the form $t = sx$, where $x = \pm 1$ or $2^i \pm 1$ is a square root of 1. Since $a \equiv 1 \bmod (8)$, we can start with a square root $r = 1$ for a in U_{2^3}, and then by iterating this process we can find the square roots of a in U_{2^e} for any e.

Example 7.14

Let us find the square roots of $a = 17 \bmod (2^5)$; these exist since $17 \equiv 1 \bmod (8)$. First we find a square root mod (2^4). Taking $r = 1$ we have $r^2 = 1^2 = 17 + 2^3.(-2)$, so $q = -2$; taking $k = 0$ makes $q + rk = -2$ even, so $s = r + 2^2 k = 1$ is a square root of 17 mod (2^4). (This is obvious, but it is worth illustrating the process first in a simple case.) Now we repeat this process, using $r = 1$ as a square root mod (2^4) to find a square root s mod (2^5). We have $r^2 = 1 = 17 + 2^4.(-1)$, so now $q = -1$; taking $k = 1$ makes $q + rk = 0$ even, so $s = r + 2^3 k = 9$ is a square root of 17 mod (2^5). The remaining square roots t are found by multiplying $s = 9$ by -1 and by $2^4 \pm 1 = \pm 15$, so we have $\pm 7, \pm 9$ as the complete set of square roots of 17 mod (2^5).

Exercise 7.16

Find the square roots of 41 mod (2^6).

7.6 Quadratic residues for arbitrary moduli

The following result allows us to combine our characterisations of Q_{p^e} for different prime-powers:

Theorem 7.15

Let $n = n_1 n_2 \ldots n_k$, where the integers n_i are mutually coprime. Then $a \in Q_n$ if and only if $a \in Q_{n_i}$ for each i.

Proof

If $a \in Q_n$ then $a \equiv s^2 \bmod (n)$ for some $s \in U_n$. Clearly $a \equiv s^2 \bmod (n_i)$ for each i, with s coprime to n_i, so $a \in Q_{n_i}$. Conversely, if $a \in Q_{n_i}$ for each i then there exist elements $s_i \in U_{n_i}$ such that $a \equiv s_i^2 \bmod (n_i)$. By the Chinese Remainder Theorem (Theorem 3.10) there is an element $s \in \mathbb{Z}_n$ such that $s \equiv s_i \bmod (n_i)$ for all i. Then $s^2 \equiv s_i^2 \equiv a \bmod (n_i)$ for all i, and hence $s^2 \equiv a \bmod (n)$ since the moduli n_i are coprime, so $a \in Q_n$. □

This result can be expressed in algebraic terms as giving a direct product decomposition

$$Q_n \cong Q_{n_1} \times \cdots \times Q_{n_k} .$$

This is analogous to the decomposition $U_n \cong U_{n_1} \times \cdots \times U_{n_k}$ given in Theorem 6.13, and indeed it can be deduced directly from it by noting that an element of U_n is a square if and only if its component in each factor U_{n_i} is a square.

We can now answer the question of whether $a \in Q_n$ for arbitrary moduli n:

Theorem 7.16

Let $a \in U_n$. Then $a \in Q_n$ if and only if

(1) $a \in Q_p$ for each odd prime p dividing n, and

(2) $a \equiv 1 \bmod (4)$ if $2^2 \,\|\, n$, and $a \equiv 1 \bmod (8)$ if $2^3 \mid n$.

(Note that condition (2) is relevant only when n is divisible by 4; in all other cases we can ignore it.)

Proof

By Theorem 7.15, $a \in Q_n$ if and only if $a \in Q_{p^e}$ for each prime-power p^e in the factorisation of n. For odd primes p this is equivalent to $a \in Q_p$, by

Theorem 7.13, giving condition (1); for $p = 2$ it is equivalent to condition (2), by Theorem 7.14. □

Example 7.15

Let $n = 144 = 2^4.3^2$. An element $a \in U_{144}$ is a quadratic residue if and only if $a \in Q_3$ and $a \equiv 1 \bmod (8)$; since $Q_3 = \{1\} \subset \mathbb{Z}_3$, this is equivalent to $a \equiv 1 \bmod (24)$, so $Q_{144} = \{1, 25, 49, 73, 97, 121\} \subset U_{144}$. Any $a \in Q_{144}$ must have $N = 8$ square roots, by Lemma 7.1. To find these, we first find its four square roots mod (2^4) and its two square roots mod (3^2) by the methods described in Section 7.5, and then we use the Chinese Remainder Theorem to convert each of these eight pairs of roots into a square root mod (144). For instance, let $a = 73$; then $a \equiv 9 \bmod (2^4)$, with square roots $s \equiv \pm 3, \pm 5 \bmod (2^4)$, and similarly $a \equiv 1 \bmod (3^2)$, with square roots $s \equiv \pm 1 \bmod (3^2)$; solving these eight pairs of simultaneous congruences for s, we get the square roots $s \equiv \pm 19, \pm 35, \pm 37, \pm 53 \bmod (144)$.

Exercise 7.17

Find the square roots of 49 mod (144).

Exercise 7.18

Find the square roots of 25 mod (168).

Example 7.16

As an application of the results in this chapter, let us return to Example 3.8. We claimed there (without proof) that if

$$f(x) = (x^2 - 13)(x^2 - 17)(x^2 - 221),$$

then for each integer $n \geq 1$ there is a solution $x \in \mathbb{Z}$ of the congruence $f(x) \equiv 0 \bmod (n)$. (This is despite the fact that the equation $f(x) = 0$ clearly has no integer solutions.) To prove this, it is sufficient by the Chinese Remainder Theorem to show that for each prime-power p^e there is a solution of $f(x) \equiv 0 \bmod (p^e)$, and for this, it is sufficient to show that at least one of 13, 17 and 221 is a quadratic residue mod (p^e). If $p = 2$, then since $17 \equiv 1 \bmod (8)$ we have $17 \in Q_{2^e}$ for all e by Theorem 7.14. If $p = 13$, then since $17 \equiv 2^2 \bmod (13)$ we have $17 \in Q_{13}$, and hence $17 \in Q_{13^e}$ for all e by Theorem 7.13. If $p = 17$, then a similar argument based on $13 \equiv 8^2 \bmod (17)$ gives $13 \in Q_{17^e}$ for all e.

Finally, if $p \neq 2, 13$ or 17, then since $221 = 13 \times 17$ we have

$$\left(\frac{221}{p}\right) = \left(\frac{13}{p}\right)\left(\frac{17}{p}\right)$$

by Theorem 7.5, with each of these three terms equal to ± 1; at least one of them must therefore be equal to 1, so at least one of 13, 17 or 221 must be in Q_p and hence in Q_{p^e} for all e by Theorem 7.13.

Exercise 7.19

Show that the polynomial $g(x) = (x^2 - 5)(x^2 - 41)(x^2 - 205)$ has no integer roots, but the congruence $g(x) \equiv 0$ has a solution mod (n) for every integer $n \geq 1$.

7.7 Supplementary exercises

Exercise 7.20

Show that, for each $r \geq 1$, there are infinitely many primes $p \equiv 1$ mod (2^r).

Exercise 7.21

For which values of n is -1 a quadratic residue mod (n)?

Exercise 7.22

Show that if q and r are distinct primes, with $q \equiv r \equiv 1$ mod (4) and $(\frac{q}{r}) = 1$, then the polynomial $h(x) = (x^2 - q)(x^2 - r)(x^2 - qr)$ has no integer roots, but the congruence $h(x) \equiv 0$ has a solution mod (n) for every integer $n \geq 1$.

Exercise 7.23

Show that if $n > 2$ then a quadratic residue mod (n) cannot also be a primitive root mod (n).

Exercise 7.24

Show that if p is a Fermat prime F_n, then each element of U_p is either a primitive root or a quadratic residue, but not both. Show that the Fermat primes are the only primes with this property.

Exercise 7.25

Is 43 a quadratic residue mod (923)?

Exercise 7.26

Find the square roots of 7 mod (513).

Exercise 7.27

Show that $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$ for each odd prime p. Show that $\sum_{a\in Q_p} a \equiv 0$ mod (p) for each prime $p > 3$.