course, is that the inverse mod p of a is the (congruence class of the) solution m of $ma + np = 1$, which we find by applying the Euclidean algorithm to express $1 = \gcd(a, p)$ in the form $ma + np$.

Likewise, the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ can be solved, as in ordinary algebra, by "completing the square." We find

$$\begin{aligned}
&ax^2 + bx + c \equiv 0 \pmod{p}\\
\Rightarrow\ & a\left(x^2 + \frac{b}{a}x\right) + c \equiv 0 \pmod{p}\\
\Rightarrow\ & a\left(x^2 + \frac{b}{a}x + \frac{b^2}{4a^2}\right) + c - \frac{b^2}{4a} \equiv 0 \pmod{p}\\
\Rightarrow\ & a\left(x + \frac{b}{2a}\right)^2 \equiv \frac{b^2}{4a} - c \pmod{p}\\
\Rightarrow\ & \left(x + \frac{b}{2a}\right)^2 \equiv \frac{b^2 - 4ac}{(2a)^2} \pmod{p}
\end{aligned}$$

by various applications of $+$, $-$, $\times$, and $\div$ mod p. The big difference is in the next step: finding the "square root" mod p, and indeed deciding whether it exists. This turns out to be a deep and interesting problem, to which we shall devote the next few sections of this chapter. It so happens that exactly half the numbers $1, 2, 3, \ldots, p-1$ are squares mod p, but the rule for finding them is quite mysterious and unexpected.

The first step toward finding which numbers are squares mod p is fairly simple, thanks to Lagrange's polynomial theorem (Section 6.4). We can confine attention to odd primes p, because the only numbers mod 2 are 0 and 1, and these are obviously squares for any modulus.

Euler's criterion. *For an odd prime p, $a \not\equiv 0$ is a square* mod p $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Proof The ($\Rightarrow$) direction is an easy consequence of Fermat's little theorem (Section 6.5):

$$\begin{aligned}
a \text{ is a square mod } p \Rightarrow a &\equiv b^2 \pmod{p} \text{ for some } b\\
\Rightarrow a^{\frac{p-1}{2}} &\equiv b^{p-1} \equiv 1 \pmod{p}\\
&\text{by Fermat's little theorem}
\end{aligned}$$

To prove the ($\Leftarrow$) direction we first observe that exactly half of the numbers $1, 2, 3, \ldots, p-1$ are squares mod p because:

- No two of $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are congruent mod p. This is because $i^2 \equiv j^2 \pmod{p}$ implies $(i-j)(i+j) \equiv 0 \pmod{p}$, which is impossible for distinct i and j among $1, 2, 3, \ldots, \frac{p-1}{2}$, because $i \pm j \not\equiv 0 \pmod{p}$.
- $(p-k)^2 \equiv (-k)^2 \equiv k^2 \pmod{p}$. Hence the only values squares can take are the $\frac{p-1}{2}$ distinct values $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

Thus there are $\frac{p-1}{2}$ nonzero squares mod p. By the first part of the proof they are all solutions of $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, and by Lagrange's polynomial theorem there are no other solutions of this congruence. Hence, if a is not a square mod p then $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. □

Squares mod p are often called *quadratic residues* mod p, and nonsquares are called quadratic *nonresidues*. The terminology is borrowed from Latin, where the same word means both "square" and "quadratic," and it seems misleading to use it when "squares mod p" and "nonsquares mod p" are available. A useful notation for saying whether or not a nonzero a is a square mod p is the *Legendre symbol*, $\left(\frac{a}{p}\right)$. This symbol is also called the *quadratic character* of a (mod p), and is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is a nonsquare mod } p \end{cases}$$

The value of -1 for nonsquares actually comes out the proof of Euler's criterion, if one looks closely, leading to the following.

Restatement of Euler's criterion. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Proof $\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem, and $x^2 \equiv 1 \pmod{p}$ has only the two solutions $x = 1$ and $x = -1$ by Lagrange's polynomial theorem. Therefore, the only possible values (mod p) of $a^{\frac{p-1}{2}}$ are 1, which it takes for squares a, and -1, which it necessarily takes for nonsquares a.

Thus $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$, by definition of the Legendre symbol. □

Exercises

There is another proof of Euler's criterion, which is shorter and more enlightening, but dependent on a harder theorem: the existence of primitive roots. A *primitive root* mod p is a number r such that each of $1, 2, 3, \ldots, p-1$ is congruent to a power of r, mod p.

6.7.1. Show that 2 is a primitive root mod 5, but not a primitive root mod 7. Find a primitive root mod 7.

The existence of a primitive root for each prime p was conjectured by Euler and proved by Gauss (1801). All proofs I am aware of use Lagrange's polynomial theorem plus some extra ingenuity, so the existence of primitive roots should probably be regarded as a harder theorem than Euler's criterion. However, it also throws more light on Euler's criterion.

6.7.2. If r is a primitive root mod p, show that the nonzero squares mod p are the even powers of r. Deduce that there are $\frac{p-1}{2}$ nonzero squares mod p.

6.7.3. Deduce the ($\Leftarrow$) direction of Euler's criterion from Exercise 6.7.2.

The existence of primitive roots can also be used to prove analogous theorems about cubes mod p, and so on. These results are not as complete as Euler's criterion for squares, because they depend on p. Here is what we can say about cubes.

6.7.4. If 3 divides $p-1$ and r is a primitive root mod p, show that the nonzero cubes mod p are $1, r^3, r^6, \ldots$. Deduce that a is a cube mod $p \Leftrightarrow a^{\frac{p-1}{3}} \equiv 1 \pmod{p}$.

6.7.5. If 3 does not divide $p-1$, which numbers are cubes mod p?

6.8* The Quadratic Character of -1 and 2

Euler's criterion does not immediately tell us which a are squares modulo a given odd prime p or the moduli p for which a given a is a square. However, it can be used to obtain this information explicitly for the two important values $a = -1$ and $a = 2$.

Quadratic character of -1. *For any odd prime p, -1 is a square* mod $p \Leftrightarrow p = 4n+1$ *for some integer n.*

Proof By Euler's criterion,

$$\begin{aligned} -1 \text{ is a square mod } p &\Leftrightarrow (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p \\ &\Leftrightarrow \frac{p-1}{2} \text{ is even} \\ &\Leftrightarrow p = 4n+1 \text{ for some integer } n. \end{aligned}$$

□

To find the quadratic character of 2 we have the harder job of evaluating $2^{\frac{p-1}{2}}$ mod p. This can be done by manipulating the product $1 \times 2 \times 3 \times \cdots \times (p-1) \pmod p$ into the form

$$\begin{array}{ll} 2^{\frac{p-1}{2}}(-1)^{\frac{p-1}{4}} \times 1 \times 2 \times 3 \times \cdots \times (p-1) & \text{if } \frac{p-1}{2} \text{ is even,} \\ 2^{\frac{p-1}{2}}(-1)^{\frac{p+1}{4}} \times 1 \times 2 \times 3 \times \cdots \times (p-1) & \text{if } \frac{p-1}{2} \text{ is odd.} \end{array}$$

From this we conclude (by canceling $1, 2, 3, \ldots, p-1$) that

$$2^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{p-1}{4}} \pmod p & \text{if } \frac{p-1}{2} \text{ is even} \\ (-1)^{\frac{p+1}{4}} \pmod p & \text{if } \frac{p-1}{2} \text{ is odd.} \end{cases}$$

The manipulation becomes clearer with an accompanying example, say $p = 11$.

In the product,

$$1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10,$$

separate the even and odd factors,

$$(2 \times 4 \times 6 \times 8 \times 10) \times 1 \times 3 \times 5 \times 7 \times 9.$$

Extract 2 from the $(p-1)/2$ even factors,

$$2^5(1 \times 2 \times 3 \times 4 \times 5) \times 1 \times 3 \times 5 \times 7 \times 9$$

so that even factors $> (p-1)/2$ are lost and odd factors $\leq (p-1)/2$ are repeated.

$$2^5(1 \times 2 \times 3 \times 4 \times 5) \times \underline{1} \times \underline{3} \times \underline{5} \times 7 \times 9$$

Give the repeated factors $-$ signs, inserting factors of -1 to compensate,

$$2^5(1 \times 2 \times 3 \times 4 \times 5) \times (-1)^3(-1) \times (-3) \times (-5) \times 7 \times 9.$$

Replace each odd factor $-n$ by $p-n$, which is even and $> (p-1)/2$,

$$2^5(1 \times 2 \times 3 \times 4 \times 5) \times (-1)^3\underline{10} \times \underline{8} \times \underline{6} \times 7 \times 9$$

so that the new product $\equiv$ the old (mod p), and includes all of $1, 2, 3, \ldots, p-1$.

It is clear from this example why the exponent of 2 is $(p-1)/2$, because this is the number of even numbers among $1, 2, 3, \ldots, p-1$. The exponent of -1 is the number of odd numbers $\leq (p-1)/2$, namely, $(p-1)/4$ if $(p-1)/2$ is even, and $(p+1)/4$ if $(p-1)/2$ is odd, hence the result is as claimed.

From the value of $2^{\frac{p-1}{2}}$ mod p we can now deduce an explicit description of the odd prime moduli for which 2 is a square.

Quadratic character of 2. *For any odd prime p, 2 is a square* mod $p \Leftrightarrow p = 8n \pm 1$ *for some integer n.*

Proof By Euler's criterion, 2 is a square mod $p \Leftrightarrow 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, so it suffices to evaluate $2^{\frac{p-1}{2}}$ (using the expression $(-1)^{\frac{p-1}{4}}$ for $\frac{p-1}{2}$ even, and $(-1)^{\frac{p+1}{4}}$ for $\frac{p-1}{2}$ odd) for the possible odd values of p. Apart from $8n \pm 1$, the other odd values are $8n \pm 3$, and we find

$$p = 8n+1 \Rightarrow \frac{p-1}{2} \text{ even} \Rightarrow 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \equiv (-1)^{\frac{8n}{4}} \equiv 1 \pmod{p}$$

$$p = 8n-1 \Rightarrow \frac{p-1}{2} \text{ odd} \Rightarrow 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{4}} \equiv (-1)^{\frac{8n}{4}} \equiv 1 \pmod{p}$$

$$p = 8n+3 \Rightarrow \frac{p-1}{2} \text{ odd} \Rightarrow 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{4}} \equiv (-1)^{\frac{8n+4}{4}} \equiv -1 \pmod{p}$$

$$p = 8n-3 \Rightarrow \frac{p-1}{2} \text{ even} \Rightarrow 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \equiv (-1)^{\frac{8n-4}{4}} \equiv -1 \pmod{p}$$

as required. □

The calculation of $2^{\frac{p-1}{2}}$ mod p may seem like a lucky accident, but there is reason to believe in advance that it will work. By Wilson's theorem, $1 \times 2 \times 3 \times \cdots \times (p-1) \equiv -1 \pmod{p}$, and by Euler's criterion $2^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Therefore, if we can extract the factor $2^{\frac{p-1}{2}}$ from $1 \times 2 \times 3 \times \cdots \times (p-1)$ (which we obviously can, from the even numbers), then the remaining factor must be $\equiv \pm 1 \pmod{p}$.

Exercises

The description of the quadratic character of 2 can be condensed as follows.

6.8.1. Show that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

As suggested earlier, the calculation of $\left(\frac{2}{p}\right)$ from $1 \times 2 \times 3 \times \cdots \times (p-1)$ can be expected to work, so it is mainly a matter of shuffling the factors until we get what we want. A more imaginative calculation of $\left(\frac{2}{p}\right)$, using $i = \sqrt{-1}$ and de Moivre's formula, is given in Scharlau and Opolka (1985). The main steps follow.

6.8.2.* Using the fact that $2 = \frac{(1+i)^2}{i}$ and Euler's criterion, show that

$$\left(\frac{2}{p}\right) \equiv \frac{(1+i)^p}{i^{\frac{p-1}{2}}(1+i)} \equiv \frac{1+i^p}{i^{\frac{p-1}{2}}(1+i)} \pmod{p}.$$

6.8.3.* Using the fact that $i = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$, show that

$$\frac{1+i^p}{i^{\frac{p-1}{2}}(1+i)} = \frac{(1+i^p)i^{-p/2}}{(1+i)i^{-1/2}} = \frac{\cos(p\pi/4)}{\cos(\pi/4)}.$$

6.8.4.* Deduce from Exercises 6.8.2* and 6.8.3* that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases} = (-1)^{\frac{p^2-1}{8}}.$$

6.9* Quadratic Reciprocity

The Euler criterion may be used to find $\left(\frac{q}{p}\right)$ for various fixed primes q, but it is hard to see any general pattern to the results. Legendre discovered the secret: *knowing whether q is a square mod p depends on knowing whether p is a square mod q*. The exact relationship between the primes p and q is expressed by the *law of quadratic reciprocity*, the fundamental theorem about squares modulo odd primes, first proved by Gauss (1801):

For odd primes p and q,

if p and q are both of the form $4n+3$ then

p is a square mod $q \Leftrightarrow q$ is not a square mod p,

otherwise

p is a square mod $q \Leftrightarrow q$ is a square mod p.

The law is usually presented more concisely with the help of the Legendre symbol. When p and q are both of the form $4n+3$, quadratic reciprocity says that $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ have opposite signs, and hence their product is -1. Otherwise, it says that $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ have the same sign and hence their product is 1. All this is captured by the single equation

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

The law of quadratic reciprocity has been proved more often than any other theorem in mathematics except the Pythagorean theorem. However, it is a more difficult theorem, and none of its proofs is completely transparent. One of the shortest was given by George Rousseau (1991). It produces the result like a rabbit out of a hat, but at least the trick can be done with readily available materials: Wilson's theorem and Euler's criterion. Rousseau's proof may be compared with the computation of $\left(\frac{2}{p}\right)$ in Section 6.8*. It is a manipulation of certain products, mod p and mod q, but this time with the Chinese remainder theorem playing a crucial role. To simplify formulas, we use the standard abbreviation $n!$ for $1 \times 2 \times 3 \times \cdots \times n$.

Quadratic reciprocity. *For any odd primes p and q,*

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

Proof Consider the (congruence classes of the) invertible numbers mod pq. By the Chinese remainder theorem, each such number x can be faithfully represented by the pair (x mod p, x mod q). When we multiply such pairs, the first components are multiplied mod p, and the second components are multiplied mod q.

We want to form the product of all such pairs for the invertible x between 1 and $(pq-1)/2$ inclusive. As we know from Section 6.4, the invertible x are those that are multiples of neither p nor q. We form their product mod p by multiplying the nonmultiples of p, then dividing by the multiples of q. The nonmultiples of p form the sequence

$$1, 2, \ldots, p-1; p+1, p+2, \ldots 2p-1; \ldots.$$

Taking these mod p, we get $(q-1)/2$ sequences $1, 2, \ldots, p-1$, followed by the "half sequence" $1, 2, \ldots, (p-1)/2$. By Wilson's theorem, the mod p product of $1, 2, \ldots, p-1$ is -1, hence the mod p product of all nonmultiples of p between 1 and $(pq-1)/2$ is

$$(-1)^{\frac{q-1}{2}}((p-1)/2)!.$$

Now we divide this by the multiples $q, 2q, \ldots, ((p-1)/2)q$ of q between 1 and $(pq-1)/2$. Their product is

$$q^{\frac{p-1}{2}}((p-1)/2)!,$$

so division gives $(-1)^{\frac{q-1}{2}}/q^{\frac{p-1}{2}}$. By Euler's criterion, $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$, which is either 1 or -1, so it makes no difference whether we multiply or divide by it: the mod p product of the invertible x from 1 to $(pq-1)/2$ is $\left(\frac{q}{p}\right)(-1)^{\frac{q-1}{2}}$.

Similarly, the mod q product of the invertible x is $\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}}$. Hence the product of the pairs (x mod p, x mod q) for invertible x from 1 to $(pq-1)/2$ is

$$\left(\left(\frac{q}{p}\right)(-1)^{\frac{q-1}{2}}, \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}}\right). \tag{1}$$

Now we compute the same product in a second way, which allows it to be expressed without Legendre symbols. Equating the two expressions for the product will give a relation between $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$.

The Chinese remainder theorem says that the pairs (x mod p, x mod q) for invertible x from 1 to $pq-1$ are the (a, b) with $1 \le a \le p-1$ and $1 \le b \le q-1$. Also, the pair ($pq - x$ mod p, $pq - x$ mod q), that is, ($-x$ mod p, $-x$ mod q), equals $(-a, -b)$ if (x mod p, x mod q) equals (a, b). It follows that the pairs (x mod p, x mod q) for $1 \le x \le (pq-1)/2$ include (a, b) if and only if they do *not* include $(-a, -b)$.

Thus the product of the (x mod p, x mod q), for the invertible x from 1 to $(pq-1)/2$, is the product (up to a $\pm$ sign) of any set of pairs that includes (a, b) if and only if it does not include $(-a, -b)$. One