such set is

$$(a, b) \qquad \text{for} \quad 1 \le a \le p-1, \quad 1 \le b \le (q-1)/2.$$

And the product of the members of this set is

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

because each value of a, $1 \le a \le p-1$, occurs in $(q-1)/2$ pairs, and each value of b, $1 \le b \le (q-1)/2$, occurs in $p-1$ pairs.

Bearing in mind that the first component is taken mod p, Wilson's theorem gives $(p-1)! \equiv -1 \pmod{p}$, hence the first component $\equiv (-1)^{\frac{q-1}{2}} \pmod{p}$.

The second component is taken mod q, so Wilson's theorem gives

$$\begin{aligned} -1 &\equiv (q-1)! \pmod{q} \\ &\equiv 1 \times 2 \times \cdots \times ((q-1)/2) \\ &\quad \times (-((q-1)/2) \times \cdots \times (-2) \times (-1) \pmod{q} \\ &\equiv ((q-1)/2)!^2 (-1)^{\frac{q-1}{2}} \pmod{q}. \end{aligned}$$

Therefore

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

and hence, raising both sides to the power $\frac{p-1}{2}$, we get the second component

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

Thus the second expression for the product simplifies to

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

Equating (1) and (2) we get either

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

or

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

In either case, the product of the two equations is

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

□

Exercises

Once we know the primes p that are squares modulo an odd prime q we can recognize *all* the squares mod q.

6.9.1. Show that if $P = p_1 p_2 \cdots p_k$ is the prime factorization of P then

$$P \text{ is a square mod } q \quad \Leftrightarrow \quad \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)\cdots\left(\frac{p_k}{q}\right) = 1.$$

This result suggests a natural extension of the Legendre symbol to all numbers $P \not\equiv 0 \pmod{q}$: if $P = p_1 p_2 \cdots p_k$ is the prime factorization of P, let

$$\left(\frac{P}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)\cdots\left(\frac{p_k}{q}\right).$$

6.9.2. Deduce from this definition that the Legendre symbol is *multiplicative*:

$$\left(\frac{PQ}{q}\right) = \left(\frac{P}{q}\right)\left(\frac{Q}{q}\right) \quad \text{for any } P, Q \not\equiv 0 \pmod{q}.$$

Also, of course, $\left(\frac{P}{q}\right)$ depends only on the congruence class of P, mod q, so we can replace P by its remainder on division by q. Using this fact, the multiplicative property, and quadratic reciprocity, the computation of Legendre symbols is greatly simplified.

6.9.3. Justify each step in the following computations.

$$\left(\frac{5}{31}\right) = \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$$\left(\frac{7}{31}\right) = -\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{11}{31}\right) = -\left(\frac{31}{11}\right) = -\left(\frac{9}{11}\right) = -\left(\frac{3}{11}\right)^2 = -1$$

$$\left(\frac{13}{31}\right) = \left(\frac{31}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

6.9.4. Use similar steps to show that $\left(\frac{19}{31}\right) = 1$. What is 19 the square of, mod 31?

To complete our toolkit for recognizing whether P is a square mod q we need a rule for evaluating $\left(\frac{2}{q}\right)$, because any $P > 1$ is a product of odd primes and 2s. This why we worked out $\left(\frac{2}{q}\right)$ in Section 6.8*. (When

$\left(\frac{2}{3}\right)$ came up in Exercise 6.9.3, we were able to evaluate it by inspection, simply because there are so few squares mod 3.) The formula we found,

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

is known as a *supplement* to the law of quadratic reciprocity.

6.10 Discussion

Congruences and Congruence Classes

Gauss (1801) used his notion and notation of congruence to good effect in the *Disquisitiones*. He clarified many known results, such as Fermat's little theorem and Euler's criterion, and he gave the first proofs of results Euler, Lagrange, and Legendre had attacked without success, such as quadratic reciprocity and the existence of primitive roots. He also gave the very neat proof of Wilson's theorem we used in Section 6.5. Flushed with his success, he made the following remarks about the theorem and its history:

> It was first published by Waring and attributed to Wilson: Waring *Meditationes Algebraicae* (3rd ed., Cambridge, 1782, p. 380). But neither of them was able to prove the theorem, and Waring confessed that the demonstration seemed more difficult because no *notation* can be devised to express a prime number. But in our opinion truths of this kind should be drawn from notions rather than notations. (Gauss (1801), article 76.)

He then proceeded to give his proof, with the help of congruence notation of course.

With hindsight, we can see that the congruence *notion* is implicit in many results that were known before Gauss. A simple example is the rule of casting out nines, and more sophisticated examples are Fermat's little theorem and Wilson's theorem. The latter theorem is another of the "universal" theorems, having been discovered at least twice before Wilson. Leibniz stated it in an unpublished paper around 1670, and its first known appearance is in a work of the Arab

mathematician and scientist Abū 'Ali al-Hasan ibn al-Haytham (965–1039). The first known *proof*, however, is the one given by Lagrange in 1771.

The concept of congruence mod n, and particularly Gauss's notation for it, makes such results easier to discover and prove by clearing the page of all multiples of n. Having to write $\ldots \equiv \ldots \pmod{n}$ rather than $\ldots = \ldots$ is a small price to pay for the simplification, because congruences can be manipulated like equations anyway.

Moreover, if numbers are replaced by their congruence classes, as in Section 6.3, then congruence of numbers is replaced by equality of their congruence classes, and hence we can work with equations after all. The price to pay in this case is accepting *classes* as mathematical objects, like numbers.

Congruence classes were introduced by Dedekind in 1857, the year before he proposed the more radical idea of defining real numbers as pairs of sets of rationals. In the 1870s he used sets again to give meaning to other notions that until then had only a ghostly existence—the idea of an "ideal algebraic number" and the idea of a "point on a Riemann surface." His contemporaries found these ideas *too* radical, and it took several decades of exposure before mathematicians accepted sets as mathematical objects and realized that they made life simpler.

Rings, Fields, and Abelian Groups

Like the congruence concept, rings and fields were implicit in number theory long before they became explicit. In fact, it was only around 1900 that the ring concept was recognized at all, partly because it took that long to recognize that ordinary integers and congruence classes had a lot in common. Writing down what they have in common with each other (and with other "integer-like" objects, such as polynomials), mathematicians arrived at what we called the *ring properties* in Section 1.4. The field concept was recognized in a similar way, by writing down the common properties of various sets of objects for which $+, -, \times$, and $\div$ are meaningful—rational numbers, congruence classes mod p, and rational functions, for example.

The power of an abstract concept, like that of a field, is that it allows us to treat some outlandish mathematical objects like old friends. For example, it tells us that polynomials with mod p coefficients behave the same as ordinary polynomials with rational or real coefficients. This is why Lagrange's polynomial theorem is essentially the same as the corresponding theorem about ordinary polynomials; they both depend only on the fact that the coefficients belong to a field.

Another abstraction that number theory pushes into the limelight is the concept of an *abelian group*. This concept is actually simpler, and hence more general, than the concept of ring or field. A ring involves two operations, $+$ and $\times$, but an abelian group involves only one, usually written $+$ but sometimes $\cdot$ or $\times$. If the group operation is written as $+$, the abelian group properties are the ring properties of $+$:

$$\begin{aligned} a+(b+c) &= (a+b)+c && \text{(associative law)} \\ a+b &= b+a && \text{(commutative law)} \\ a+(-a) &= 0 && \text{(inverse property)} \\ a+0 &= a && \text{(identity property).} \end{aligned}$$

To be precise, an abelian group is a set A with an operation $+$, an *identity element* called 0, and for each a in A an *inverse of* a, written $-a$, with the four properties just given. The notation with $+$ as the group operation, 0 as the identity, and $-a$ as the inverse of a is called *additive notation*. Naturally, it is used for groups where the operation is ordinary addition, or something related to it such as addition of congruence classes.

There is also a *multiplicative notation*, in which the group operation is called $\cdot$ or $\times$, the identity is called 1, and the inverse of a is called a^{-1}.

In multiplicative notation, the abelian group properties are

$$\begin{aligned} a\times(b\times c) &= (a\times b)\times c && \text{(associative law)} \\ a\times b &= b\times a && \text{(commutative law)} \\ a\times a^{-1} &= 1 && \text{(inverse property)} \\ a\times 1 &= a && \text{(identity property).} \end{aligned}$$

Multiplicative notation is natural for groups like the nonzero rationals, where $\times$ is ordinary multiplication, or groups with a related "multiplication," like the nonzero congruence classes mod p. The *abelian* property, by the way, is the commutative law. If this property is dropped, we have what is simply called a *group*. Nonabelian groups include the groups of transformations occurring in geometry (see Section 3.8*). Thus the general group concept unifies ideas from both geometry and number theory and helps to explain the deep connections between the two.

The commutative property of abelian groups makes them easier to handle than general groups, so group theory tends to be easier in number theory than geometry. In fact, many of the groups in number theory are of a specially simple type called *cyclic* groups.

In additive notation, a cyclic group C consists of the elements

$$\ldots, -2, -1, 0, 1, 2, \ldots .$$

If C is infinite it is necessarily the integers $\mathbb{Z}$ under ordinary addition. If C is finite, with n elements, it is necessarily $\mathbb{Z}/n\mathbb{Z}$ under addition of congruence classes. In multiplicative notation, a cyclic group looks like

$$\ldots, c^{-2}, c^{-1}, 1, c, c^2, \ldots .$$

for some element c of C. For example, $\{\ldots, 2^{-2}, 2^{-1}, 1, 2, 2^2, \ldots\}$ is an infinite cyclic subgroup of the rationals, $\mathbb{Q}$. The function $f(2^n) = n$ is an isomorphism between this group and $\mathbb{Z}$, a one-to-one correspondence that sends the product $2^m \times 2^n$ to the corresponding sum $m + n$.

An example of a finite cyclic group under $\times$ is $\{1, 2, 3, 4\}$ under mod 5 multiplication. This group also consists of the powers of 2, but now taken mod 5, because

$$\begin{aligned} 1 &\equiv 2^0 \pmod 5 \\ 2 &\equiv 2^1 \pmod 5 \\ 3 &\equiv 2^3 \pmod 5 \\ 4 &\equiv 2^2 \pmod 5. \end{aligned}$$

More generally, $\{1, 2, 3, \ldots, p-1\}$ is a cyclic group under mod p multiplication for any prime p. This far-from-obvious result follows from the existence of primitive roots, mentioned in Section 6.7.

Applied Number Theory

Fermat's little theorem lay buried in the number theory books for more than 300 years before starting a new life as a fundamental tool of espionage and commerce. This transformation from pure to applied (or is it clean to dirty?) was brought about by the discovery of the RSA *public key cryptosystem* in 1977. Named after its authors, Rivest, Shamir, and Adleman, RSA is a simple method for encoding and decoding messages based on Fermat's little theorem.

Like many traditional codes, RSA scrambles and unscrambles a message using a *key*, a long sequence of digits known only to sender and receiver. Its novel feature is that the sender needs to know only part of the key, which can therefore be made public; only the receiver needs to know the whole key. The receiver's key is in fact a pair (p_1, p_2) of large prime numbers (around 100 digits each), while the public key is their product p_1p_2. The theory behind the system is now explained in most number theory textbooks, for example Niven, Zuckerman, and Montgomery (1991).

The reason the product p_1p_2 is effectively "less information" than the pair of factors p_1, p_2 is that there is no known method for factorizing a random product of 100 digit primes in reasonable time. Although p_1 and p_2 can in principle be derived from p_1p_2, in practice they cannot, and RSA remains a secure system as long as factorization remains hard. A lot of money is riding on the assumption that it will *always* be hard. An industry has sprung up supplying easy-to-use RSA systems and accessories, in some cases even offering large primes for sale! In turn, this has stimulated much research on the problems of factorization and prime recognition.

Fermat's little theorem is fundamental to this research, because it gives an easy way to recognize when a number is *not* prime. The argument goes as follows. If p is prime and $1 < a < p$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

by Fermat's little theorem. It follows that a number n is *not* prime if

$$a^{n-1} \not\equiv 1 \pmod{n}$$

for some a between 1 and n. We then call a a *witness* that n is not prime. When n is large, finding a witness is generally much easier

than finding a divisor of n, because $a^{n-1} \bmod n$ can be quickly computed by the repeated squaring method (Exercises 6.2.6 and 6.2.7*), and 2 or 3 is usually a witness. There are rare cases where a witness does not exist, but the method extends to cover these cases without greatly increasing the computing time.

An excellent introduction to these aspects of number theory may be found in Chapter 33 of Cormen, Leiserson, and Rivest (1990). It is particularly interesting to observe that most of the fundamentals of pure number theory are needed: Euclidean algorithm, abelian groups, Euler's phi function, Chinese remainder theorem, and Fermat's little theorem.