Chapter 3 Basic Number Theory

In modern cryptographic systems, the messages are represented by numerical values prior to being encrypted and transmitted. The encryption processes are mathematical operations that turn the input numerical values into output numerical values. Building, analyzing, and attacking these cryptosystems requires mathematical tools. The most important of these is number theory, especially the theory of congruences. This chapter presents the basic tools needed for the rest of the book. More advanced topics such as factoring, discrete logarithms, and elliptic curves, will be treated in later chapters (Chapters 9, 10, and 21, respectively).

3.1 Basic Notions

3.1.1 Divisibility

Number theory is concerned with the properties of the integers. One of the most important is divisibility.

Definition

Let a and b be integers with $a \neq 0$. We say that a **divides** b, if there is an integer k such that $b = ak$. This is denoted by $a|b$. Another way to express this is that b is a multiple of a.

Example

$3|15,\ -15|60,\ 7 \nmid 18$ (does not divide).

The following properties of divisibility are useful.

Proposition

Let a, b, c represent integers.

1. For every $a \neq 0$, $a|0$ and $a|a$. Also, $1|b$ for every b.
2. If $a|b$ and $b|c$, then $a|c$.
3. If $a|b$ and $a|c$, then $a|(sb + tc)$ for all integers s and t.

Proof. Since $0 = a \cdot 0$, we may take $k = 0$ in the definition to obtain $a|0$. Since $a = a \cdot 1$, we take $k = 1$

to prove $a|a$. Since $b = 1 \cdot b,$ we have $1|b$. This proves (1). In (2), there exist k and ℓ such that $b = ak$ and $c = b\ell$. Therefore, $c = (k\ell)a,$ so $a|c$. For (3), write $b = ak_1$ and $c = ak_2$. Then $sb + tc = a(sk_1 + tk_2)$, so $a|sb + tc$.

For example, take $a = 2$ in part (2). Then $2|b$ simply means that b is even. The statement in the proposition says that $c,$ which is a multiple of the even number b, must also be even (that is, a multiple of $a = 2$).

3.1.2 Prime Numbers

A number $p > 1$ whose positive divisors are only 1 and itself is called a **prime number**. The first few primes are $2, 3, 5, 7, 11, 13, 17, \cdots$. An integer $n > 1$ that is not prime is called **composite**, which means that n must be expressible as a product ab of integers with $1 < a, b < n$. A fact, known already to Euclid, is that there are infinitely many prime numbers. A more precise statement is the following, proved in 1896.

Prime Number Theorem

Let $\pi(x)$ be the number of primes less than x. Then

$$\pi(x) \approx \frac{x}{\ln x},$$

in the sense that the ratio $\pi(x)/(x/\ln x) \to 1$ as $x \to \infty$.

We won't prove this here; its proof would lead us too far away from our cryptographic goals. In various applications, we'll need large primes, say of around 300 digits. We can estimate the number of 300-digit primes as follows:

$$\pi\left(10^{300}\right) - \pi\left(10^{299}\right) \approx \frac{10^{300}}{\ln 10^{300}} - \frac{10^{299}}{\ln 10^{299}} \approx 1.4 \times 10^{297}.$$

So there are certainly enough such primes. Later, we'll discuss how to find them.

Prime numbers are the building blocks of the integers. Every positive integer has a unique representation as a product of prime numbers raised to different powers. For example, 504 and 1125 have the following factorizations:

$$504 = 2^3 3^2 7, \qquad 1125 = 3^2 5^3.$$

Moreover, these factorizations are unique, except for reordering the factors. For example, if we factor 504 into primes, then we will always obtain three factors of 2, two factors of 3, and one factor of 7. Anyone who obtains the prime 41 as a factor has made a mistake.

Theorem

Every positive integer is a product of primes. This factorization into primes is unique, up to reordering the factors.

Proof. There is a small technicality that must be dealt with before we begin. When dealing with products, it is convenient to make the convention that an empty product equals 1. This is similar to the convention that $x^0 = 1$. Therefore, the positive integer 1 is a product of primes, namely the empty product. Also, each prime is regarded as a one-factor product of primes.

Suppose there exist positive integers that are not products of primes. Let n be the smallest such integer. Then n cannot be 1 (= the empty product), or a prime (= a one-factor product), so n must be composite. Therefore, $n = ab$ with $1 < a,\ b < n$. Since n is the smallest positive integer that is not a product of primes, both a and b are products of primes. But a product of

primes times a product of primes is a product of primes, so $n = ab$ is a product of primes. This contradiction shows that the set of integers that are not products of primes must be the empty set. Therefore, every positive integer is a product of primes.

The uniqueness of the factorization is more difficult to prove. We need the following very important property of primes.

Lemma

If p is a prime and p divides a product of integers ab, then either $p|a$ or $p|b$. More generally, if a prime p divides a product $ab \cdots z$, then p must divide one of the factors $a, b, \ldots, z$.

For example, when $p = 2$, this says that if a product of two integers is even then one of the two integers must be even. The proof of the lemma will be given at the end of the next section, after we discuss the Extended Euclidean algorithm.

Continuing with the proof of the theorem, suppose that an integer n can be written as a product of primes in two different ways:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t},$$

where $p_1, \ldots, p_s$ and $q_1, \ldots, q_t$ are primes, and the exponents a_i and b_j are nonzero. If a prime occurs in both factorizations, divide both sides by it to obtain a shorter relation. Continuing in this way, we may assume that none of the primes $p_1, \ldots, p_s$ occur among the q_j 's. Take a prime that occurs on the left side, say p_1. Since p_1 divides n, which equals $q_1 q_1 \cdots q_1 q_2 q_2 cdots q_t q_t$, the lemma says that p_1 must divide one of the factors q_j. Since q_j is prime, $p_1 = q_j$. This contradicts the assumption that p_1 does not occur among the q_j's.

Therefore, an integer cannot have two distinct factorizations, as claimed.

3.1.3 Greatest Common Divisor

The **greatest common divisor** of a and b is the largest positive integer dividing both a and b and is denoted by either $gcd(a, b)$ or by (a, b). In this book, we use the first notation. To avoid technicalities, we always assume implicitly that at least one of a and b is nonzero.

Example

$$\gcd\,(6,\ 4) = 2, \qquad \gcd\,(5,\ 7) = 1, \qquad \gcd\,(24,\ 60) = 12.$$

We say that a and b are **relatively prime** if $\gcd(a, b) = 1$. There are two standard ways for finding the gcd:

1. If you can factor a and b into primes, do so. For each prime number, look at the powers that it appears in the factorizations of a and b. Take the smaller of the two. Put these prime powers together to get the gcd. This is easiest to understand by examples:

   $$576 = 2^6 3^2, \quad 135 = 3^3 5, \quad \gcd(576, 135) = 3^2 = 9$$
   $$\gcd(2^5 3^4 7^2, 2^2 5^3 7) = 2^2 3^0 5^0 7^1 = 2^2 7 = 28.$$

   Note that if a prime does not appear in a factorization, then it cannot appear in the gcd.

2. Suppose a and b are large numbers, so it might not be easy to factor them. The gcd can be calculated by a procedure known as the **Euclidean algorithm**. It goes back to what everyone learned in grade school: division with remainder. Before giving a formal description of the algorithm, let's see some examples.

Example

Compute gcd(482, 1180).

SOLUTION

Divide 482 into 1180. The quotient is 2 and the remainder is 216. Now divide the remainder 216 into 482. The quotient is 2 and the remainder is 50. Divide the remainder 50 into the previous remainder 216. The quotient is 4 and the remainder is 16. Continue this process of dividing the most recent remainder into the previous one. The last nonzero remainder is the gcd, which is 2 in this case:

$$\begin{aligned} 1180 &= 2 \cdot 482 + 216 \\ 482 &= 2 \cdot 216 + 50 \\ 216 &= 4 \cdot 50 + 16 \\ 50 &= 3 \cdot 16 + 2 \\ 16 &= 8 \cdot 2 + 0. \end{aligned}$$

Notice how the numbers are shifted:

$$\text{remainder} \rightarrow \text{todivisor} \rightarrow \text{todividend} \rightarrow \text{toignore}.$$

Here is another example:

$$\begin{aligned} 12345 &= 1 \cdot 11111 + 1234 \\ 11111 &= 9 \cdot 1234 + 5 \\ 1234 &= 246 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

Therefore, $\gcd\,(12345, 11111) = 1.$

Using these examples as guidelines, we can now give a more formal description of the **Euclidean algorithm**. Suppose that a is greater than b. If not, switch a and b. The first step is to divide a by $b,$ hence represent a in the form

$$a = q_1 b + r_1.$$

If $r_1 = 0,$ then b divides a and the greatest common divisor is b. If $r_1 \neq 0,$ then continue by representing b in the form

$$b = q_2 r_1 + r_2.$$

Continue in this way until the remainder is zero, giving the following sequence of steps:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \quad \vdots \quad \vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k. \end{aligned}$$

The conclusion is that

$$\gcd\,(a, b) = r_k.$$

There are two important aspects to this algorithm:

1. It does not require factorization of the numbers.
2. It is fast.

For a proof that it actually computes the gcd, see Exercise 59.

3.2 The Extended Euclidean Algorithm

The Euclidean Algorithm computes greatest common divisors quickly, but also, with only slightly more work, yields a very useful fact: $\gcd(a, b)$ can be expressed as a linear combination of a and b. That is, there exist integers x and y such that $\gcd(a, b) = ax + by$. For example,

$$\begin{aligned} 1 &= \gcd(45, 13) = 45 \cdot (-2) + 13 \cdot 7 \\ 7 &= \gcd(259, 119) = 259 \cdot 6 - 119 \cdot 13. \end{aligned}$$

The **Extended Euclidean Algorithm** will tell us how to find x and y. Rather than give a set of equations, we'll show how it works with the two examples we calculated in Subsection 3.1.3.

When we computed $\gcd(12345, 11111)$, we did the following calculation:

$$\begin{aligned} 12345 &= 1 \cdot 11111 + 1234 \\ 11111 &= 9 \cdot 1234 + 5 \\ 1234 &= 246 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1. \end{aligned}$$

For the Extended Euclidean Algorithm, we'll form a table with three columns and explain how they arise as we compute them.

We begin by forming two rows and three columns. The first entries in the rows are the original numbers we started with, namely 12345 and 11111. We will do some calculations so that we always have

$$\text{entry in first column} = 12345x + 11111y,$$

where x and y are integers. The first two lines are trivial: $12345 = 1 \cdot 12345 + 0 \cdot 11111$ and

$11111 = 0 \cdot 12345 + 1 \cdot 11111$:

	x	y
12345	1	0
11111	0	1

The first line in our $\gcd\ (12345,\ \ 11111)$ calculation tells us that $12345 = 1 \cdot 11111 + 1234$. We rewrite this as $1234 = 12345 - 1 \cdot 11111$. Using this, we compute

$$(\text{1st row}) \ - 1 \cdot (\text{2nd row}),$$

yielding the following:

	x	y	
12345	1	0	
11111	0	1	
1234	1	-1	(1st row) $-$ 1·(2nd row).

In effect, we have done the following subtraction:

$$\begin{aligned} 12345 &= 12345(1) + 11111(0) \\ 1111 &= 12345(0) + 11111(1) \\ 1234 &= 12345(0) + 11111(-1). \end{aligned}$$

Therefore, the last line tells us that
$1234 = 12345 \cdot 1 + 11111 \cdot (-1)$.

We now move to the second row of our gcd calculation. This says that $11111 = 9 \cdot 1234 + 5,$ which we rewrite as $5 = 11111 - 9 \cdot 1234$. This tells us to compute (2nd row) -9·(3rd row). We write this as

	x	y	
12345	1	0	
11111	0	1	
1234	1	-1	
5	-9	10	(2nd row) $-9\cdot$(3rd row).

The last line tells us that
$5 = 12345 \cdot (-9) + 11111 \cdot 10.$

The third row of our gcd calculation tells us that
$4 = 1234 - 246 \cdot 5$. This becomes

	x	y	
12345	1	0	
11111	0	1	
1234	1	-1	
5	-9	10	
4	2215	-2461	(3rd row) $- 246\cdot$(4th row).

Finally, we obtain

12345	1	0
11111	0	1
1234	1	-1
5	-9	10
4	2215	-2461

1	−2224	2471	(4th row) − (5th row).

This tells us that
$1 = 12345 \cdot (-2224) + 11111 \cdot 2471.$

Notice that as we proceeded, we were doing the Euclidean Algorithm in the first column. The first entry of each row is a remainder from the gcd calculation, and the entries in the second and third columns allow us to express the number in the first column as a linear combination of 12345 and 11111. The quotients in the Euclidean Algorithm tell us what to multiply a row by before subtracting it from the previous row.

Let's do another example using 482 and 1180 and our previous calculation that $\gcd(1180, 482) = 2$:

	x	y	
1180	1	0	
482	0	1	
216	1	−2	(1st row) − 2·(2nd row)
50	−2	5	(2nd row) − 2·(3rd row)
16	9	−22	(3rd row) − 4·(4th row)
2	−29	71	(4rd row) − 3·(5th row).

The end result is $2 = 1180 \cdot (-29) + 482 \cdot 71.$

To summarize, we state the following.

Theorem

Let a and b be integers with at least one of a, b nonzero. There exist integers x and $y,$ which can be found by the Extended Euclidean Algorithm, such that

$$\gcd(a, b) = ax + by.$$

As a corollary, we deduce the lemma we needed during the proof of the uniqueness of factorization into primes.

Corollary

If p is a prime and p divides a product of integers ab, then either $p|a$ or $p|b$. More generally, if a prime p divides a product $ab \cdots z,$ then p must divide one of the factors $a, b, \ldots, z$.

Proof. First, let's work with the case $p|ab$. If p divides a, we are done. Now assume $p \nmid a$. We claim $p|b$. Since p is prime, $\gcd(a, p) = 1$ or p. Since $p \nmid a,$ the gcd cannot be p. Therefore, $\gcd(a, p) = 1,$ so there exist integers x, y with $ax + py = 1$. Multiply by b to obtain $abx + pby = b$. Since $p|ab$ and $p|p,$ we have $p|abx + pby,$ so $p|b,$ as claimed.

If $p|ab \cdots z,$ then $p|a$ or $p|b \cdots z$. If $p|a,$ we're done. Otherwise, $p|b \cdots z$. We now have a shorter product. Either $p|b,$ in which case we're done, or p divides the product of the remaining factors. Continuing in this way, we eventually find that p divides one of the factors of the product.

The property of primes stated in the corollary holds only for primes. For example, if we know a product ab is divisible by 6, we cannot conclude that a or b is a multiple of 6. The problem is that $6 = 2 \cdot 3,$ and the 2 could be in a while the 3 could be in $b,$ as seen in the example $60 = 4 \cdot 15$. More generally, if $n = ab$ is any composite, then $n|ab$ but $n \nmid a$ and $n \nmid b$. Therefore, the

primes, and 1, are the only integers with the property of the corollary.

3.3 Congruences

One of the most basic and useful notions in number theory is modular arithmetic, or congruences.

Definition

Let a, b, n be integers with $n \neq 0$. We say that

$$a \equiv b \pmod{n}$$

(read: a is **congruent** to b mod n) if $a - b$ is a multiple (positive or negative or zero) of n.

Another formulation is that $a \equiv b \pmod{n}$ if a and b differ by a multiple of n. This can be rewritten as $a = b + nk$ for some integer k (positive or negative).

Example

$$32 \equiv 7 \pmod{5}, \quad -12 \equiv 37 \pmod{7}, \quad 17 \equiv 17 \pmod{13}.$$

Note: Many computer programs regard $17 \pmod{10}$ as equal to the number 7, namely, the remainder obtained when 17 is divided by 10 (often written as $17\%10 = 7$). The notion of congruence we use is closely related. We have that two numbers are congruent mod n if they yield the same remainders when divided by n. For example, $17 \equiv 37 \pmod{10}$ because $17\%10$ and $37\%10$ are equal.

Congruence behaves very much like equality. In fact, the notation for congruence was intentionally chosen to resemble the notation for equality.

Proposition

Let a, b, c, n be integers with $n \neq 0$.

1. $a \equiv 0 \pmod{n}$ if and only if $n|a$.
2. $a \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$.
4. If $a \equiv b$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proof. In (1), $a \equiv 0 \pmod{n}$ means that $a = a - 0$ is a multiple of n, which is the same as $n|a$. In (2), we have $a - a = 0 \cdot n$, so $a \equiv a \pmod{n}$. In (3), if $a \equiv b \pmod{n}$, write $a - b = nk$. Then $b - a = n(-k)$, so $b \equiv a \pmod{n}$. Reversing the roles of a and b gives the reverse implication. For (4), write $a = b + nk$ and $b = c + n\ell$. Then $a - c = n(k + \ell)$, so $a \equiv c \pmod{n}$.

Usually, we have $n > 0$ and we work with the integers mod n, denoted $\mathbf{Z}_n$. These may be regarded as the set $\{0, 1, 2, \ldots, n-1\}$, with addition, subtraction, and multiplication mod n. If a is any integer, we may divide a by n and obtain a remainder in this set:

$$a = nq + r \text{ with } 0 \leq r < n.$$

(This is just division with remainder; q is the quotient and r is the remainder.) Then $a \equiv r \pmod{n}$, so every number a is congruent mod n to some integer r with $0 \leq r < n$.

Proposition

Let a, b, c, d, n be integers with $n \neq 0$, and suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then

$$a + c \equiv b + d, \quad a - c \equiv b - d, \quad ac \equiv bd \pmod{n}.$$

Proof. Write $a = b + nk$ and $c = d + n\ell,$ for integers k and ℓ. Then $a + c = b + d + n(k + \ell),$ so $a + c \equiv b + d \pmod{n}$. The proof that $a - c \equiv b - d$ is similar. For multiplication, we have $ac = bd + n(dk + b\ell + nk\ell),$ so $ac \equiv bd.$

The proposition says you can perform the usual arithmetic operations of addition, subtraction, and multiplication with congruences. You must be careful, however, when trying to perform division, as we'll see.

If we take two numbers and want to multiply them modulo $n,$ we start by multiplying them as integers. If the product is less than $n,$ we stop. If the product is larger than $n - 1,$ we divide by n and take the remainder. Addition and subtraction are done similarly. For example, the integers modulo 6 have the following addition table:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

3.3-1 Full Alternative Text

A table for multiplication mod 6 is

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

3.3-2 Full Alternative Text

Example

Here is an example of how we can do algebra mod n. Consider the following problem: Solve $x + 7 \equiv 3 \pmod{17}$.

SOLUTION

$$x \equiv 3 - 7 \equiv -4 \equiv 13 \pmod{17}.$$

There is nothing wrong with negative answers, but usually we write the final answer as an integer from 0 to $n - 1$ when we are working mod n.

3.3.1 Division

Division is much trickier mod n than it is with rational numbers. The general rule is that you can divide by $a \pmod{n}$ when $\gcd(a, n) = 1$.

Proposition

Let a, b, c, n be integers with $n \neq 0$ and with $\gcd(a, n) = 1$. If $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$. In other words, if a and n are relatively prime, we can divide both sides of the congruence by a.

Proof Since $\gcd(a, n) = 1$, there exist integers x, y such that $ax + ny = 1$. Multiply by $b - c$ to obtain

$$(ab - ac)x + n(b - c)y = b - c.$$

Since $ab - ac$ is a multiple of n, by assumption, and $n(b - c)y$ is also a multiple of n, we find that $b - c$ is a multiple of n. This means that $b \equiv c \pmod{n}$.

Example

Solve: $2x + 7 \equiv 3 \pmod{17}$.

SOLUTION

$2x \equiv 3 - 7 \equiv -4$, so $x \equiv -2 \equiv 15 \pmod{17}$. The division by 2 is allowed since $\gcd(2, 17) = 1$.

Example

Solve: $5x + 6 \equiv 13 \pmod{11}$.

SOLUTION

$5x \equiv 7 \pmod{11}$. Now what do we do? We want to divide by 5, but what does $7/5$ mean mod 11? Note that $7 \equiv 18 \equiv 29 \equiv 40 \equiv \cdots \pmod{11}$. So $5x \equiv 7$ is the same as $5x \equiv 40$. Now we can divide by 5 and obtain $x \equiv 8 \pmod{11}$ as the answer. Note that $7 \equiv 8 \cdot 5 \pmod{11}$, so 8 acts like $7/5$.

The last example can be done another way. Since $5 \cdot 9 \equiv 1 \pmod{11},$ we see that 9 is the multiplicative inverse of $5 \pmod{11}$. Therefore, dividing by 5 can be accomplished by multiplying by 9. If we want to solve $5x \equiv 7 \pmod{11},$ we multiply both sides by 9 and obtain

$$x \equiv 45x \equiv 63 \equiv 8 \pmod{11}.$$

Proposition

Suppose $\gcd(a, n) = 1$. Let s and t be integers such that $as + nt = 1$ (they can be found using the extended Euclidean algorithm). Then $as \equiv 1 \pmod{n},$ so s is the multiplicative inverse for $a \pmod{n}$.

Proof. Since $as - 1 = -nt,$ we see that $as - 1$ is a multiple of n.

Notation: We let $\boldsymbol{a^{-1}}$ denote this $s,$ so a^{-1} satisfies $a^{-1}a \equiv 1 \pmod{n}$.

The extended Euclidean algorithm is fairly efficient for computing the multiplicative inverse of a by the method stated in the proposition.

Example

Solve $11111x \equiv 4 \pmod{12345}$.

SOLUTION

In Section 3.2, from the calculation of $\gcd(12345, 11111)$ we obtained

$$1 = 12345 \cdot (-2224) + 11111 \cdot 2471.$$

This says that

$$11111 \cdot 2471 \equiv 1 \pmod{12345}.$$

Multiplying both sides of the original congruence by 2471 yields

$$x \equiv 9884 \pmod{12345}.$$

In practice, this means that if we are working mod 12345 and we encounter the fraction 4/11111, we can replace it with 9884. This might seem a little strange, but think about what 4/11111 means. It's simply a symbol to represent a quantity that, when multiplied by 11111, yields 4. When we are working mod 12345, the number 9884 also has this property since $11111 \times 9884 \equiv 4 \pmod{12345}$.

Let's summarize some of the discussion:

Finding

$$a^{-1} \pmod{n}$$

1. Use the extended Euclidean algorithm to find integers s and t such that $as + nt = 1$.
2. $a^{-1} \equiv s \pmod{n}$.

Solving

$ax \equiv c \pmod{n}$ **when** $\gcd(a, n) = 1$

(Equivalently, you could be working mod n and encounter a fraction c/a with $\gcd(a, n) = 1$*.)*

1. Use the extended Euclidean algorithm to find integers s and t such that $as + nt = 1$.
2. The solution is $x \equiv cs \pmod{n}$ (equivalently, replace the fraction c/a with $cs \pmod{n}$).

What if

$$\gcd(a, n) > 1?$$

Occasionally we will need to solve congruences of the form $ax \equiv b \pmod{n}$ when $\gcd(a, n) = d > 1$. The procedure is as follows:

1. If d does not divide b, there is no solution.
2. Assume $d|b$. Consider the new congruence

   $$(a/d)x \equiv b/d \pmod{n/d}.$$

   Note that a/d, b/d, n/d are integers and $\gcd(a/d, n/d) = 1$. Solve this congruence by the above procedure to obtain a solution x_0.
3. The solutions of the original congruence $ax \equiv b \pmod{n}$ are

   $$x_0, \quad x_0 + (n/d), \quad x_0 + 2(n/d), \ \ldots, \quad x_0 + (d-1)(n/d) \pmod{n}.$$

Example

Solve $12x \equiv 21 \pmod{39}$.

SOLUTION

$\gcd(12, 39) = 3$, which divides 21. Divide by 3 to obtain the new congruence $4x \equiv 7 \pmod{13}$. A solution $x_0 = 5$ can be obtained by trying a few numbers, or by using the extended Euclidean algorithm. The solutions to the original congruence are $x \equiv 5,\ 18,\ 31 \pmod{39}$.

The preceding congruences contained x to the first power. However, nonlinear congruences are also useful. In several places in this book, we will meet equations of the form

$$x^2 \equiv a \pmod{n}.$$

First, consider $x^2 \equiv 1 \pmod{7}$. The solutions are $x \equiv 1, 6 \pmod{7}$, as we can see by trying the values

$0, 1, 2, \ldots, 6$ for x. In general, when p is an odd prime, $x^2 \equiv 1 \pmod{p}$ has exactly the two solutions $x \equiv \pm 1 \pmod{p}$ (see Exercise 15).

Now consider $x^2 \equiv 1 \pmod{15}$. If we try the numbers $0, 1, 2, \ldots, 14$ for x, we find that $x = 1, 4, 11, 14$ are solutions. For example, $11^2 \equiv 121 \equiv 1 \pmod{15}$. Therefore, a quadratic congruence for a composite modulus can have more than two solutions, in contrast to the fact that a quadratic equation with real numbers, for example, can have at most two solutions. In Section 3.4, we'll discuss this phenomenon. In Chapters 9 (factoring), 18 (flipping coins), and 19 (identification schemes), we'll meet applications of this fact.

3.3.2 Working with Fractions

In many situations, it will be convenient to work with fractions mod n. For example, $1/2 \pmod{12345}$ is easier to write than $6173 \pmod{12345}$ (note that $2 \times 6173 \equiv 1 \pmod{12345}$). The general rule is that a fraction b/a can be used mod n if $\gcd(a, n) = 1$. Of course, it should be remembered that $b/a \pmod{n}$ really means $a^{-1}b \pmod{n}$, where a^{-1} denotes the integer mod n that satisfies $a^{-1}a \equiv 1 \pmod{n}$. But nothing will go wrong if it is treated as a fraction.

Another way to look at this is the following. The symbol "1/2" is simply a symbol with exactly one property: If you multiply 1/2 by 2, you get 1. In all calculations involving the symbol 1/2, this is the only property that is used. When we are working mod 12345, the number 6173 also has this property, since $6173 \times 2 \equiv 1 \pmod{12345}$. Therefore, $1/2 \pmod{12345}$ and $6173 \pmod{12345}$ may be used interchangeably.

Why can't we use fractions with arbitrary denominators? Of course, we cannot use $1/6 \pmod{6}$, since that

would mean dividing by $0 \pmod 6$. But even if we try to work with $1/2 \pmod 6$, we run into trouble. For example, $2 \equiv 8 \pmod 6$, but we cannot multiply both sides by 1/2, since $1 \not\equiv 4 \pmod 6$. The problem is that $\gcd(2, 6) = 2 \neq 1$. Since 2 is a factor of 6, we can think of dividing by 2 as "partially dividing by 0." In any case, it is not allowed.

3.4 The Chinese Remainder Theorem

In many situations, it is useful to break a congruence mod n into a system of congruences mod factors of n. Consider the following example. Suppose we know that a number x satisfies $x \equiv 25 \pmod{42}$. This means that we can write $x = 25 + 42k$ for some integer k. Rewriting 42 as $7 \cdot 6$, we obtain $x = 25 + 7(6k)$, which implies that $x \equiv 25 \equiv 4 \pmod{7}$. Similarly, since $x = 25 + 6(7k)$, we have $x \equiv 25 \equiv 1 \pmod{6}$. Therefore,

$$x \equiv 25 \pmod{42} \quad \Rightarrow \quad \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 1 \pmod{6}. \end{cases}$$

The Chinese remainder theorem shows that this process can be reversed; namely, a system of congruences can be replaced by a single congruence under certain conditions.

Chinese Remainder Theorem

Suppose $\gcd(m, n) = 1$. Given integers a and b, there exists exactly one solution $x \pmod{mn}$ to the simultaneous congruences

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}.$$

Proof. There exist integers s, t such that $ms + nt = 1$. Then $ms \equiv 1 \pmod{n}$ and $nt \equiv 1 \pmod{m}$. Let $x = bms + ant$. Then $x \equiv ant \equiv a \pmod{m}$, and $x \equiv bms \equiv b \pmod{n}$, so a solution x exists. Suppose x_1 is another solution. Then $x \equiv x_1 \pmod{m}$ and $x \equiv x_1 \pmod{n}$, so $x - x_1$ is a multiple of both m and n.

Lemma

Let m, n be integers with $\gcd(m, n) = 1$. If an integer c is a multiple of both m and n, then c is a multiple of mn.

Proof. Let $c = mk = n\ell$. Write $ms + nt = 1$ with integers s, t. Multiply by c to obtain $c = cms + cnt = mn\ell s + mnkt = mn(\ell s + kt)$.

To finish the proof of the theorem, let $c = x - x_1$ in the lemma to find that $x - x_1$ is a multiple of mn. Therefore, $x \equiv x_1 \pmod{mn}$. This means that any two solutions x to the system of congruences are congruent mod mn, as claimed.

Example

Solve $x \equiv 3 \pmod{7}, \quad x \equiv 5 \pmod{15}$.

SOLUTION

$x \equiv 80 \pmod{105}$ (note: $105 = 7 \cdot 15$). Since $80 \equiv 3 \pmod{7}$ and $80 \equiv 5 \pmod{15}$, 80 is a solution. The theorem guarantees that such a solution exists, and says that it is uniquely determined mod the product mn, which is 105 in the present example.

How does one find the solution? One way, which works with small numbers m and n, is to list the numbers congruent to $b \pmod{n}$ until you find one that is congruent to $a \pmod{m}$. For example, the numbers congruent to $5 \pmod{15}$ are

$$5, 20, 35, 50, 65, 80, 95, \ldots.$$

Mod 7, these are $5, 6, 0, 1, 2, 3, 4, \ldots$. Since we want $3 \pmod{7}$, we choose 80.

For slightly larger numbers m and n, making a list would be inefficient. However, the proof of the theorem gives a fast method for finding x:

1. Use the Extended Euclidean algorithm to find s and t with $ms + nt = 1$.
2. Let $x \equiv bms + ant \pmod{mn}$.

Example

Solve $x \equiv 7 \pmod{12345}, \quad x \equiv 3 \pmod{11111}$.

SOLUTION

First, we know from our calculations in Section 3.2 that

$$12345 \cdot (-2224) + 11111 \cdot 2471 = 1,$$

so $s = -2224$ and $t = 2471$. Therefore,
$x \equiv 3 \cdot 12345 \cdot (-2224) + 7 \cdot 11111 \cdot 2471 \equiv 109821127 \pmod{(11111 \cdot 12345)}$.

How do you use the Chinese remainder theorem? The main idea is that if you start with a congruence mod a composite number n, you can break it into simultaneous congruences mod each prime power factor of n, then recombine the resulting information to obtain an answer mod n. The advantage is that often it is easier to analyze congruences mod primes or mod prime powers than to work mod composite numbers.

Suppose you want to solve $x^2 \equiv 1 \pmod{35}$. Note that $35 = 5 \cdot 7$. We have

$$x^2 \equiv 1 \pmod{35} \quad \Leftrightarrow \quad \begin{cases} x^2 \equiv 1 \pmod{7} \\ x^2 \equiv 1 \pmod{5}. \end{cases}$$

Now, $x^2 \equiv 1 \pmod{5}$ has two solutions: $x \equiv \pm 1 \pmod{5}$. Also, $x^2 \equiv 1 \pmod{7}$ has two solutions: $x \equiv \pm 1 \pmod{7}$. We can put these together in four ways:

$$
\begin{array}{rcrlcrcrl}
x &\equiv& 1 &\pmod 5, & x &\equiv& 1 &\pmod 7 & \to & x &\equiv& 1 &\pmod{35},\\
x &\equiv& 1 &\pmod 5, & x &\equiv& -1 &\pmod 7 & \to & x &\equiv& 6 &\pmod{35},\\
x &\equiv& -1 &\pmod 5, & x &\equiv& 1 &\pmod 7 & \to & x &\equiv& 29 &\pmod{35},\\
x &\equiv& -1 &\pmod 5, & x &\equiv& -1 &\pmod 7 & \to & x &\equiv& 34 &\pmod{35}.
\end{array}
$$

So the solutions of $x^2 \equiv 1 \pmod{35}$ are
$x \equiv 1, 6, 29, 34 \pmod{35}$.

In general, if $n = p_1 p_2 \cdots p_r$ is the product of r distinct odd primes, then $x^2 \equiv 1 \pmod n$ has 2^r solutions. This is a consequence of the following.

Chinese Remainder Theorem (General Form)

Let $m_1, \ \ldots\ , m_k$ be integers with $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. Given integers $a_1, \ \ldots\ , \ a_k,$ there exists exactly one solution $x \pmod{m_1 \cdots m_k}$ to the simultaneous congruences

$$
x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \ \ldots\ , \quad x \equiv a_k \pmod{m_k}.
$$

For example, the theorem guarantees there is a solution to the simultaneous congruences

$$
x \equiv 1 \pmod{11}, \qquad x \equiv -1 \pmod{13}, \qquad x \equiv 1 \pmod{17}.
$$

In fact, $x \equiv 1871 \pmod{11 \cdot 13 \cdot 17}$ is the answer.

Exercise 57 gives a method for computing the number x in the theorem.

3.5 Modular Exponentiation

Throughout this book, we will be interested in numbers of the form

$$x^a \pmod{n}.$$

In this and the next couple of sections, we discuss some properties of numbers raised to a power modulo an integer.

Suppose we want to compute $2^{1234} \pmod{789}$. If we first compute 2^{1234}, then reduce mod 789, we'll be working with very large numbers, even though the final answer has only 3 digits. We should therefore perform each multiplication and then calculate the remainder. Calculating the consecutive powers of 2 would require that we perform the modular multiplication 1233 times. This is method is too slow to be practical, especially when the exponent becomes very large. A more efficient way is the following (all congruences are mod 789).

We start with $2^2 \equiv 4 \pmod{789}$ and repeatedly square both sides to obtain the following congruences:

$$\begin{aligned} 2^4 &\equiv 4^2 \equiv 16 \\ 2^8 &\equiv 16^2 \equiv 256 \\ 2^{16} &\equiv 256^2 \equiv 49 \\ 2^{32} &\equiv 34 \\ 2^{64} &\equiv 367 \\ 2^{128} &\equiv 559 \\ 2^{256} &\equiv 37 \\ 2^{512} &\equiv 580 \\ 2^{1024} &\equiv 286. \end{aligned}$$

Since $1234 = 1024 + 128 + 64 + 16 + 2$ (this just means that 1234 equals 10011010010 in binary), we have

$$2^{1234} \equiv 286 \cdot 559 \cdot 367 \cdot 49 \cdot 4 \equiv 481 \pmod{789}.$$

Note that we never needed to work with a number larger than 788^2.

The same method works in general. If we want to compute $a^b \pmod{n}$, we can do it with at most $2 \log_2 (b)$ multiplications mod n, and we never have to work with numbers larger than n^2. This means that exponentiation can be accomplished quickly, and not much memory is needed.

This method is very useful if a, b, n are 100-digit numbers. If we simply computed a^b, then reduced mod n, the computer's memory would overflow: The number a^b has more than 10^{100} digits, which is more digits than there are particles in the universe. However, the computation of $a^b \pmod{n}$ can be accomplished in fewer than 700 steps by the present method, never using a number of more than 200 digits.

Algorithmic versions of this procedure are given in Exercise 56. For more examples, see Examples 8 and 24–30 in the Computer Appendices.

3.6 Fermat's Theorem and Euler's Theorem

Two of the most basic results in number theory are Fermat's and Euler's theorems. Originally admired for their theoretical value, they have more recently proved to have important cryptographic applications and will be used repeatedly throughout this book.

Fermat's Theorem

If p is a prime and p does not divide a, then

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

Proof. Let

$$S = \{1, 2, 3, \ldots, p-1\}.$$

Consider the map $\psi : S \to S$ defined by $\psi(x) = ax \pmod{p}$. For example, when $p = 7$ and $a = 2$, the map ψ takes a number x, multiplies it by 2, then reduces the result mod 7.

We need to check that if $x \in S$, then $\psi(x)$ is actually in S; that is, $\psi(x) \neq 0$. Suppose $\psi(x) = 0$. Then $ax \equiv 0 \pmod{p}$. Since $\gcd(a, p) = 1$, we can divide this congruence by a to obtain $x \equiv 0 \pmod{p}$, so $x \notin S$. This contradiction means that $\psi(x)$ cannot be 0, hence $\psi(x) \in S$. Now suppose there are $x, y \in S$ with $\psi(x) = \psi(y)$. This means $ax \equiv ay \pmod{p}$. Since $\gcd(a, p) = 1$, we can divide this congruence by a to obtain $x \equiv y \pmod{p}$. We conclude that if x, y are distinct elements of S, then $\psi(x)$ and $\psi(y)$ are distinct. Therefore,

$$\psi(1), \psi(2), \psi(3), \ \cdots, \psi(p-1)$$

are distinct elements of S. Since S has only $p-1$ elements, these must be the elements of S written in a some order. It follows that

$$\begin{aligned} & 1 \cdot 2 \cdot 3 \cdots (p-1) \\ \equiv\ & \psi(1) \cdot \psi(2) \cdot \psi(3) \cdots \psi(p-1) \\ \equiv\ & (a \cdot 1)(a \cdot 2)(a \cdot 3) \cdots (a \cdot (p-1)) \\ \equiv\ & a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \pmod{p}. \end{aligned}$$

Since $\gcd(j, p) = 1$ for $j \in S,$ we can divide this congruence by $1, 2, 3, \ \ldots, p-1$. What remains is $1 \equiv a^{p-1} \pmod{p}$.

Example

$2^{10} = 1024 \equiv 1 \pmod{11}$. From this we can evaluate $2^{53} \pmod{11}$: Write $2^{53} = (2^{10})^5 2^3 \equiv 1^5 2^3 \equiv 8 \pmod{11}$. Note that when working mod 11, we are essentially working with the exponents mod 10, not mod 11. In other words, from $53 \equiv 3 \pmod{10},$ we deduce $2^{53} \equiv 2^3 \pmod{11}$.

The example leads us to a very important fact:

Basic Principle

Let p be prime and let a, x, y be integers with $\gcd(a, p) = 1$. If $x \equiv y \pmod{p-1},$ then $a^x \equiv a^y \pmod{p}$. In other words, if you want to work mod $p,$ you should work mod $p-1$ in the exponent.

Proof. Write $x = y + (p-1)k$. Then

$$a^x = a^{y+(p-1)k} = a^y (a^{p-1})^k \equiv a^y 1^k \equiv a^y \pmod{p}.$$

This completes the proof.

In the rest of this book, almost every time you see a congruence mod $p-1$, it will involve numbers that appear in exponents. The Basic Principle that was just stated shows that this translates into an overall congruence mod p. Do not make the (unfortunately, very common) mistake of working mod p in the exponent with the hope that it will yield an overall congruence mod p. It doesn't.

We can often use Fermat's theorem to show that a number is composite, without factoring. For example, let's show that 49 is composite. We use the technique of Section 3.5 to calculate

$$\begin{aligned} 2^2 &\equiv 4 \pmod{49} \\ 2^4 &\equiv 16 \\ 2^8 &\equiv 16^2 \equiv 11 \\ 2^{16} &\equiv 11^2 \equiv 23 \\ 2^{32} &\equiv 23^2 \equiv 39 \\ 2^{48} &\equiv 2^{32}2^{16} \equiv 39 \cdot 23 \equiv 15. \end{aligned}$$

Since

$$2^{48} \not\equiv 1 \pmod{49},$$

we conclude that 49 cannot be prime (otherwise, Fermat's theorem would require that $2^{48} \equiv 1 \pmod{49}$). Note that we showed that a factorization must exist, even though we didn't find the factors.

Usually, if $2^{n-1} \equiv 1 \pmod{n}$, the number n is prime. However, there are exceptions: $561 = 3 \cdot 11 \cdot 17$ is composite but $2^{560} \equiv 1 \pmod{561}$. We can see this as follows: Since $560 \equiv 0 \pmod{2}$, we have $2^{560} \equiv 2^0 \equiv 1 \pmod{3}$. Similarly, since $560 \equiv 0 \pmod{10}$ and $560 \equiv 0 \pmod{16}$, we can conclude that $2^{560} \equiv 1 \pmod{11}$ and $2^{560} \equiv 1 \pmod{17}$. Putting things together via the Chinese remainder theorem, we find that $2^{560} \equiv 1 \pmod{561}$.

Another such exception is $1729 = 7 \cdot 13 \cdot 19$. However, these exceptions are fairly rare in practice. Therefore, if $2^{n-1} \equiv 1 \pmod{n}$, it is quite likely that n is prime. Of course, if $2^{n-1} \not\equiv 1 \pmod{n}$, then n cannot be prime.

Since $2^{n-1} \pmod{n}$ can be evaluated very quickly (see Section 3.5), this gives a way to search for prime numbers. Namely, choose a starting point n_0 and successively test each odd number $n \geq n_0$ to see whether $2^{n-1} \equiv 1 \pmod{n}$. If n fails the test, discard it and proceed to the next n. When an n passes the test, use more sophisticated techniques (see Section 9.3) to test n for primality. The advantage is that this procedure is much faster than trying to factor each n, especially since it eliminates many n quickly. Of course, there are ways to speed up the search, for example, by first eliminating any n that has small prime factors.

For example, suppose we want to find a random 300-digit prime. Choose a random 300-digit odd integer n_0 as a starting point. Successively, for each odd integer $n \geq n_0$, compute $2^{n-1} \pmod{n}$ by the modular exponentiation technique of Section 3.5. If $2^{n-1} \not\equiv 1 \pmod{n}$, Fermat's theorem guarantees that n is not prime. This will probably throw out all the composites encountered. When you find an n with $2^{n-1} \equiv 1 \pmod{n}$, you probably have a prime number. But how many n do we have to examine before finding the prime? The Prime Number Theorem (see Subsection 3.1.2) says that the number of 300-digit primes is approximately 1.4×10^{297}, so approximately 1 out of every 690 numbers is prime. But we are looking only at odd numbers, so we expect to find a prime approximately every 345 steps. Since the modular exponentiations can be done quickly, the whole process takes much less than a second on a laptop computer.

We'll also need the analog of Fermat's theorem for a composite modulus n. Let $\phi(n)$ be the number of integers $1 \leq a \leq n$ such that $\gcd\ (a, n) = 1$. For example, if $n = 10,$ then there are four such integers, namely 1,3,7,9. Therefore, $\phi(10) = 4$. Often ϕ is called **Euler's ϕ-function**.

If p is a prime and $n = p^r,$ then we must remove every pth number in order to get the list of a's with $\gcd\ (a, n) = 1,$ which yields

$$\phi(p^r) = (1 - \frac{1}{p})p^r.$$

In particular,

$$\phi(p) = p - 1.$$

More generally, it can be deduced from the Chinese remainder theorem that for any integer n,

$$\phi(n) = n\prod_{p|n}(1 - \frac{1}{p}),$$

where the product is over the distinct primes p dividing n. When $n = pq$ is the product of two distinct primes, this yields

$$\phi(pq) = (p - 1)(q - 1).$$

Examples

$$\phi(10) = (2 - 1)(5 - 1) = 4,$$

$$\phi(120) = 120(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 32$$

Euler's Theorem

If $\gcd\ (a, n) = 1,$ then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. The proof of this theorem is almost the same as the one given for Fermat's theorem. Let S be the set of integers $1 \leq x \leq n$ with $\gcd\,(x, n) = 1$. Let $\psi : S \to S$ be defined by $\psi(x) \equiv ax \pmod{n}$. As in the proof of Fermat's theorem, the numbers $\psi(x)$ for $x \in S$ are the numbers in S written in some order. Therefore,

$$\prod_{x \in S} x \equiv \prod_{x \in S} \psi(x) \equiv a^{\phi(n)} \prod_{x \in S} x.$$

Dividing out the factors $x \in S,$ we are left with $1 \equiv a^{\phi(n)} \pmod{n}$.

Note that when $n = p$ is prime, Euler's theorem is the same as Fermat's theorem.

Example

What are the last three digits of 7^{803}?

SOLUTION

Knowing the last three digits is the same as working mod 1000. Since $\phi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400,$ we have $7^{803} = \left(7^{400}\right)^2 7^3 \equiv 7^3 \equiv 343 \pmod{1000}$. Therefore, the last three digits are 343.

In this example, we were able to change the exponent 803 to 3 because $803 \equiv 3 \pmod{\phi(1000)}$.

Example

Compute $2^{43210} \pmod{101}$.

SOLUTION

Note that 101 is prime. From Fermat's theorem, we know that $2^{100} \equiv 1 (\mathrm{mod}\, 101)$. Therefore,

$$2^{43210} \equiv (2^{100})^{432} 2^{10} \equiv 1^{432} 2^{10} \equiv 1024 \equiv 14 \pmod{101}.$$

In this case, we were able to change the exponent 43210 to 10 because $43210 \equiv 10 \,(\mathrm{mod}\, 100)$.

To summarize, we state the following, which is a generalization of what we know for primes:

Basic Principle

Let a, n, x, y be integers with $n \geq 1$ and $\gcd\,(a, n) = 1$. If $x \equiv y \,(\mathrm{mod}\, \phi(n)),$ then $a^x \equiv a^y \,(\mathrm{mod}\, n)$. In other words, if you want to work mod n, you should work mod $\phi(n)$ in the exponent.

Proof. Write $x = y + \phi(n)k$. Then

$$a^x = a^{y+\phi(n)k} = a^y (a^{\phi(n)})^k \equiv a^y 1^k \equiv a^y \pmod{n}.$$

This completes the proof.

This extremely important fact will be used repeatedly in the remainder of the book. Review the preceding examples until you are convinced that the exponents mod $400 = \phi(1000)$ and mod 100 are what count (i.e., don't be one of the many people who mistakenly try to work with the exponents mod 1000 and mod 101 in these examples).

3.6.1 Three-Pass Protocol

Alice wishes to transfer a secret key K (or any short message) to Bob via communication on a public channel. The Basic Principle can be used to solve this problem.

First, here is a nonmathematical way to do it. Alice puts K into a box and puts her lock on the box. She sends the locked box to Bob, who puts his lock on the box and sends the box back to Alice. Alice then takes her lock off and sends the box to Bob. Bob takes his lock off, opens the box, and finds K.

Here is the mathematical realization of the method. First, Alice chooses a large prime number p that is large enough to represent the key K. For example, if Alice were trying to send a 56-bit key, she would need a prime number that is at least 56 bits long. However, for security purposes (to make what is known as the discrete log problem hard), she would want to choose a prime significantly longer than 56 bits. Alice publishes p so that Bob (or anyone else) can download it. Bob downloads p. Alice and Bob now do the following:

1. Alice selects a random number a with $\gcd(a, p-1) = 1$ and Bob selects a random number b with $\gcd(b, p-1) = 1$. We will denote by a^{-1} and b^{-1} the inverses of a and b mod $p-1$.
2. Alice sends $K_1 \equiv K^a \pmod{p}$ to Bob.
3. Bob sends $K_2 \equiv K_1^b \pmod{p}$ to Alice.
4. Alice sends $K_3 \equiv K_2^{a^{-1}} \pmod{p}$ to Bob.
5. Bob computes $K \equiv K_3^{b^{-1}} \pmod{p}$.

At the end of this protocol, both Alice and Bob have the key K.

The reason this works is that Bob has computed $K^{aba^{-1}b^{-1}} \pmod{p}$. Since $aa^{-1} \equiv bb^{-1} \equiv 1 \pmod{p-1}$, the Basic Principle implies that $K^{aba^{-1}b^{-1}} \equiv K^1 \equiv K \pmod{p}$.

The procedure is usually attributed to Shamir and to Massey and Omura. One drawback is that it requires multiple communications between Alice and Bob. Also, it

is vulnerable to the intruder-in-the-middle attack (see Chapter 15).

3.7 Primitive Roots

Consider the powers of $3 \pmod 7$:

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1.$$

Note that we obtain all the nonzero congruence classes mod 7 as powers of 3. This means that 3 is a primitive root mod 7 (the term *multiplicative generator* might be better but is not as common). Similarly, every nonzero congruence class mod 13 is a power of 2, so 2 is a primitive root mod 13. However, $3^3 \equiv 1 \pmod{13},$ so the powers of 3 mod 13 repeat much more frequently:

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv 1, \quad 3^4 \equiv 3, \quad 3^5 \equiv 9, \quad 3^6 \equiv 1, \ \ldots,$$

so only 1, 3, 9 are powers of 3. Therefore, 3 is not a primitive root mod 13. The primitive roots mod 13 are 2, 6, 7, 11.

In general, when p is a prime, a **primitive root** mod p is a number whose powers yield every nonzero class mod p. It can be shown that there are $\phi(p-1)$ primitive roots mod p. In particular, there is always at least one. In practice, it is not difficult to find one, at least if the factorization of $p-1$ is known. See Exercise 54.

The following summarizes the main facts we need about primitive roots.

Proposition

Let α be a primitive root for the prime p.

1. Let n be an integer. Then $\alpha^n \equiv 1 \pmod p$ if and only if $n \equiv 0 \pmod{p-1}$.

2. If j and k are integers, then $\alpha^j \equiv \alpha^k \pmod{p}$ if and only if $j \equiv k \pmod{p-1}$.

3. A number β is a primitive root mod p if and only if $p-1$ is the smallest positive integer k such that $\beta^k \equiv 1 \pmod{p}$.

Proof. If $n \equiv 0 \pmod{p-1}$, then $n = (p-1)m$ for some m. Therefore,

$$\alpha^n \equiv (\alpha^m)^{p-1} \equiv 1 \pmod{p}$$

by Fermat's theorem. Conversely, suppose $\alpha^n \equiv 1 \pmod{p}$. We want to show that $p-1$ divides n, so we divide $p-1$ into n and try to show that the remainder is 0. Write

$$n = (p-1)q + r, \quad \text{with } 0 \leq r < p-1$$

(this is just division with quotient q and remainder r). We have

$$1 \equiv \alpha^n \equiv (\alpha^q)^{p-1}\alpha^r \equiv 1 \cdot \alpha^r \equiv \alpha^r \pmod{p}.$$

Suppose $r > 0$. If we consider the powers $\alpha, \alpha^2, \ldots$ of $\alpha \pmod{p}$, then we get back to 1 after r steps. Then

$$\alpha^{r+1} \equiv \alpha, \quad \alpha^{r+2} \equiv \alpha^2, \quad \ldots$$

so the powers of $\alpha \pmod{p}$ yield only the r numbers $\alpha, \alpha^2, \ldots, 1$. Since $r < p-1$, not every number mod p can be a power of α. This contradicts the assumption that α is a primitive root.

The only possibility that remains is that $r = 0$. This means that $n = (p-1)q$, so $p-1$ divides n. This proves part (1).

For part (2), assume that $j \geq k$ (if not, switch j and k). Suppose that $\alpha^j \equiv \alpha^k \pmod{p}$. Dividing both sides by α^k yields $\alpha^{j-k} \equiv 1 \pmod{p}$. By part (1), $j - k \equiv 0 \pmod{p-1}$, so $j \equiv k \pmod{p-1}$. Conversely, if $j \equiv k \pmod{p-1}$, then $j - k \equiv 0 \pmod{p-1}$, so $\alpha^{j-k} \equiv 1 \pmod{p}$, again by part (1). Multiplying by α^k yields the result.

For part (3), if β is a primitive root, then part (1) says that any integer k with $\beta^k \equiv 1 \bmod p$ must be a multiple of $p-1$, so $k = p-1$ is the smallest. Conversely, suppose $k = p-1$ is the smallest. Look at the numbers $1, \beta, \beta^2, \ldots, \beta^{p-2} \pmod{p}$. If two are congruent mod p, say $\beta^i \equiv \beta^j$ with $0 \le i < j \le p-2$, then $\beta^{j-i} \equiv 1 \pmod{p}$ (note: $\beta^{p-1} \equiv 1 \pmod{p}$ implies that $\beta \not\equiv 0 \pmod{p}$, so we can divide by β). Since $0 < j-i < p-1$, this contradicts the assumption that $k = p-1$ is smallest. Therefore, the numbers $1, \beta, \beta^2, \ldots, \beta^{p-2}$ must be distinct mod p. Since there are $p-1$ numbers on this list and there are $p-1$ numbers $1, 2, 3, \ldots, p-1$ mod p, the two lists must be the same, up to order. Therefore, each number on the list $1, 2, 3, \ldots, p-1$ is congruent to a power of β, so β is a primitive root mod p.

Warning: α is a primitive root mod p if and only if $p-1$ is the smallest positive n such that $\alpha^n \equiv 1 \pmod{p}$. If you want to prove that α is a primitive root, it does not suffice to prove that $\alpha^{p-1} \equiv 1 \pmod{p}$. After all, Fermat's theorem says that every α satisfies this, as long as $\alpha \not\equiv 0 \pmod{p}$. To prove that α is a primitive root, you must show that $p-1$ is the *smallest* positive exponent k such that $\alpha^k \equiv 1$.

3.8 Inverting Matrices Mod *n*

Finding the inverse of a matrix mod n can be accomplished by the usual methods for inverting a matrix, as long as we apply the rule given in Section 3.3 for dealing with fractions. The basic fact we need is that a square matrix is invertible mod n if and only if its determinant and n are relatively prime.

We treat only small matrices here, since that is all we need for the examples in this book. In this case, the easiest way is to find the inverse of the matrix is to use rational numbers, then change back to numbers mod n. It is a general fact that the inverse of an integer matrix can always be written as another integer matrix divided by the determinant of the original matrix. Since we are assuming the determinant and n are relatively prime, we can invert the determinant as in Section 3.3.

For example, in the 2×2 case the usual formula is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

so we need to find an inverse for $ad - bc \pmod{n}$.

Example

Suppose we want to invert $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \pmod{11}$. Since $ad - bc = -2,$ we need the inverse of -2 mod 11. Since $5 \times (-2) \equiv 1 \pmod{11},$ we can replace $-1/2$ by 5 and obtain

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} \equiv \frac{-1}{2}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \equiv 5\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \equiv \begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix} \pmod{11}.$$

A quick calculation shows that

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix} = \begin{pmatrix} 23 & 11 \\ 55 & 23 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{11}.$$

Example

Suppose we want the inverse of

$$M = \begin{matrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{matrix} \pmod{11}.$$

The determinant is 2 and the inverse of M in rational numbers is

$$\frac{1}{2} \begin{matrix} 6 & -5 & 1 \\ -6 & 8 & -2 \\ 2 & -3 & 1 \end{matrix}.$$

(For ways to calculate the inverse of a matrix, look at any book on linear algebra.) We can replace 1/2 with 6 mod 11 and obtain

$$M^{-1} \equiv \begin{matrix} 3 & 3 & 6 \\ 8 & 4 & 10 \\ 1 & 4 & 6 \end{matrix} \pmod{11}.$$

Why do we need the determinant and n to be relatively prime? Suppose $MN \equiv I \pmod{n},$ where I is the identity matrix. Then

$$\det(M)\det(N) \equiv \det(MN) \equiv \det(I) \equiv 1 \pmod{n}.$$

Therefore, $\det(M)$ has an inverse mod $n,$ which means that $\det(M)$ and n must be relatively prime.

3.9 Square Roots Mod n

Suppose we are told that $x^2 \equiv 71 \pmod{77}$ has a solution. How do we find one solution, and how do we find all solutions? More generally, consider the problem of finding all solutions of $x^2 \equiv b \pmod{n}$, where $n = pq$ is the product of two primes. We show in the following that this can be done quite easily, once the factorization of n is known. Conversely, if we know all solutions, then it is easy to factor n.

Let's start with the case of square roots mod a prime p. The easiest case is when $p \equiv 3 \pmod{4}$, and this suffices for our purposes. The case when $p \equiv 1 \pmod{4}$ is more difficult. See [Cohen, pp. 31–34] or [KraftW, p. 317].

Proposition

Let $p \equiv 3 \pmod{4}$ be prime and let y be an integer. Let $x \equiv y^{(p+1)/4} \pmod{p}$.

1. If y has a square root mod p, then the square roots of y mod p are $\pm x$.
2. If y has no square root mod p, then $-y$ has a square root mod p, and the square roots of $-y$ are $\pm x$.

Proof. If $y \equiv 0 \pmod{p}$, all the statements are trivial, so assume $y \not\equiv 0 \pmod{p}$. Fermat's theorem says that $y^{p-1} \equiv 1 \pmod{p}$. Therefore,

$$x^4 \equiv y^{p+1} \equiv y^2 y^{p-1} \equiv y^2 \pmod{p}.$$

This implies that $(x^2 + y)(x^2 - y) \equiv 0 \pmod{p}$, so $x^2 \equiv \pm y \pmod{p}$. (See Exercise 13(a).) Therefore, at least one of y and $-y$ is a square mod p. Suppose both y

and $-y$ are squares mod p, say $y \equiv a^2$ and $-y \equiv b^2$. Then $-1 \equiv (a/b)^2$ (work with fractions mod p as in Section 3.3), which means -1 is a square mod p. This is impossible when $p \equiv 3 \pmod 4$ (see Exercise 26). Therefore, exactly one of y and $-y$ has a square root mod p. If y has a square root mod p then $y \equiv x^2$, and the two square roots of y are $\pm x$. If $-y$ has a square root, then $x^2 \equiv -y$.

Example

Let's find the square root of 5 mod 11. Since $(p+1)/4 = 3$, we compute $x \equiv 5^3 \equiv 4 \pmod{11}$. Since $4^2 \equiv 5 \pmod{11}$, the square roots of 5 mod 11 are ± 4.

Now let's try to find a square root of 2 mod 11. Since $(p+1)/4 = 3$, we compute $2^3 \equiv 8 \pmod{11}$. But $8^2 \equiv 9 \equiv -2 \pmod{11}$, so we have found a square root of -2 rather than of 2. This is because 2 has no square root mod 11.

We now consider square roots for a composite modulus. Note that

$$x^2 \equiv 71 \pmod{77}$$

means that

$$x^2 \equiv 71 \equiv 1 \pmod 7 \text{ and } x^2 \equiv 71 \equiv 5 \pmod{11}.$$

Therefore,

$$x \equiv \pm 1 \pmod 7 \text{ and } x \equiv \pm 4 \pmod{11}.$$

The Chinese remainder theorem tells us that a congruence mod 7 and a congruence mod 11 can be recombined into a congruence mod 77. For example, if $x \equiv 1 \pmod 7$ and $x \equiv 4 \pmod{11}$, then

$x \equiv 15 \pmod{77}$. In this way, we can recombine in four ways to get the solutions

$$x \equiv \pm 15, \quad \pm 29 \pmod{77}.$$

Now let's turn things around. Suppose $n = pq$ is the product of two primes and we know the four solutions $x \equiv \pm a, \ \pm b$ of $x^2 \equiv y \pmod{n}$. From the construction just used above, we know that $a \equiv b \pmod{p}$ and $a \equiv -b \pmod{q}$ (or the same congruences with p and q switched). Therefore, $p|(a-b)$ but $q \nmid (a-b)$. This means that $\gcd(a-b, n) = p$, so we have found a nontrivial factor of n (this is essentially the Basic Factorization Principle of Section 9.4).

For example, in the preceding example we know that $15^2 \equiv 29^2 \equiv 71 \pmod{77}$. Therefore, $\gcd(15-29, 77) = 7$ gives a nontrivial factor of 77.

Another example of computing square roots mod n is given in Section 18.1.

Notice that all the operations used above are fast, with the exception of factoring n. In particular, the Chinese remainder theorem calculation can be done quickly. So can the computation of the gcd. The modular exponentiations needed to compute square roots mod p and mod q can be done quickly using successive squaring. Therefore, we can state the following principle:

Suppose $n = pq$ is the product of two primes congruent to 3 mod 4, and suppose y is a number relatively prime to n that has a square root mod n. Then finding the four solutions $x \equiv \pm a, \ \pm b$ to $x^2 \equiv y \pmod{n}$ is computationally equivalent to factoring n.

In other words, if we can find the solutions, then we can easily factor n; conversely, if we can factor n, we can

easily find the solutions. For more on this, see Section 9.4.

Now suppose someone has a machine that can find single square roots mod n. That is, if we give the machine a number y that has a square root mod n, then the machine returns one solution of $x^2 \equiv y \pmod{n}$. We can use this machine to factor n as follows: Choose a random integer $x_1 \pmod{n}$, compute $y \equiv x_1^2 \pmod{n}$, and give the machine y. The machine returns x with $x^2 \equiv y \pmod{n}$. If our choice of x_1 is truly random, then the machine has no way of knowing the value of x_1, hence it does not know whether $x \equiv x_1 \pmod{n}$ or not, even if it knows all four square roots of y. So half of the time, $x \equiv \pm x_1 \pmod{n}$, but half of the time, $x \not\equiv \pm x_1 \pmod{n}$. In the latter case, we compute $\gcd(x - x_1, n)$ and obtain a nontrivial factor of n. Since there is a 50% chance of success for each time we choose x_1, if we choose several random values of x_1, then it is very likely that we will eventually factor n. Therefore, we conclude that any machine that can find single square roots mod n can be used, with high probability, to factor n.

3.10 Legendre and Jacobi Symbols

Suppose we want to determine whether or not $x^2 \equiv a \pmod{p}$ has a solution, where p is prime. If p is small, we could square all of the numbers mod p and see if a is on the list. When p is large, this is impractical. If $p \equiv 3 \pmod{4},$ we can use the technique of the previous section and compute $s \equiv a^{(p+1)/4} \pmod{p}$. If a has a square root, then s is one of them, so we simply have to square s and see if we get a. If not, then a has no square root mod p. The following proposition gives a method for deciding whether a is a square mod p that works for arbitrary odd p.

Proposition

Let p be an odd prime and let a be an integer with $a \not\equiv 0 \pmod{p}$. Then $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. The congruence $x^2 \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Proof. Let $y \equiv a^{(p-1)/2} \pmod{p}$. Then $y^2 \equiv a^{p-1} \equiv 1 \pmod{p},$ by Fermat's theorem. Therefore (Exercise 15), $y \equiv \pm 1 \pmod{p}$.

If $a \equiv x^2,$ then $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$. The hard part is showing the converse. Let α be a primitive root mod p. Then $a \equiv \alpha^j$ for some j. If $a^{(p-1)/2} \equiv 1 \pmod{p},$ then

$$\alpha^{j(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}.$$

By the Proposition of Section 3.7, $j(p-1)/2 \equiv 0 \pmod{p-1}$. This implies that j must

be even: $j = 2k$. Therefore, $a \equiv g^j \equiv (\alpha^k)^2 \pmod{p}$, so a is a square mod p.

The criterion is very easy to implement on a computer, but it can be rather difficult to use by hand. In the following, we introduce the Legendre and Jacobi symbols, which give us an easy way to determine whether or not a number is a square mod p. They also are useful in primality testing (see Section 9.3).

Let p be an odd prime and let $a \not\equiv 0 \pmod{p}$. Define the **Legendre symbol**

$$\left(\frac{a}{p}\right) = \begin{cases} +1 \text{ if } x^2 \equiv a \pmod{p} \text{ has a solution.} \\ -1 \text{ if } x^2 \equiv a \pmod{p} \text{ has no solution.} \end{cases}$$

Some important properties of the Legendre symbol are given in the following.

Proposition

Let p be an odd prime.

1. If $a \equiv b \not\equiv 0 \pmod{p}$, then
$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$
2. If $a \not\equiv 0 \pmod{p}$, then
$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$
3. If $ab \not\equiv 0 \pmod{p}$, then
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$
4. $$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Proof. Part (1) is true because the solutions to $X^2 \equiv a$ are the same as those to $X^2 \equiv b$ when $a \equiv b \pmod{p}$.

Part (2) is the definition of the Legendre symbol combined with the previous proposition.

To prove part (3), we use part (2):

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

Since the left and right ends of this congruence are ± 1 and they are congruent mod the odd prime p, they must be equal. This proves (3).

For part (4), use part (2) with $a = -1$:

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

Again, since the left and right sides of this congruence are ± 1 and they are congruent mod the odd prime p, they must be equal. This proves (4).

Example

Let $p = 11$. The nonzero squares mod 11 are $1, 3, 4, 5, 9$. We have

$$\left(\frac{6}{11}\right)\left(\frac{7}{11}\right) = (-1)(-1) = +1$$

and (use property (1))

$$\left(\frac{42}{11}\right) = \left(\frac{9}{11}\right) = +1.$$

Therefore,

$$\left(\frac{6}{11}\right)\left(\frac{7}{11}\right) = \left(\frac{42}{11}\right).$$

The Jacobi symbol extends the Legendre symbol from primes p to composite odd integers n. One might be tempted to define the symbol to be $+1$ if a is a square mod n and -1 if not. However, this would cause the

important property (3) to fail. For example, 2 is not a square mod 35, and 3 is not a square mod 35 (since they are not squares mod 5), but also the product 6 is not a square mod 35 (since it is not a square mod 7). If Property (3) held, then we would have $(-1)(-1) = -1,$ which is false.

In order to preserve property (3), we define the **Jacobi symbol** as follows. Let n be an odd positive integer and let a be a nonzero integer with $\gcd(a, n) = 1$. Let

$$n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

be the prime factorization of n. Then

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{b_1} \left(\frac{a}{p_2}\right)^{b_2} \cdots \left(\frac{a}{p_r}\right)^{b_r}.$$

The symbols on the right side are the Legendre symbols introduced earlier. Note that if $n = p,$ the right side is simply one Legendre symbol, so the Jacobi symbol reduces to the Legendre symbol.

Example

Let $n = 135 = 3^3 \cdot 5$. Then

$$\left(\frac{2}{135}\right) = \left(\frac{2}{3}\right)^3 \left(\frac{2}{5}\right) = (-1)^3(-1) = +1.$$

Note that 2 is not a square mod 5, hence is not a square mod 135. Therefore, the fact that the Jacobi symbol has the value $+1$ does not imply that 2 is a square mod 135.

The main properties of the Jacobi symbol are given in the following theorem. Parts (1), (2), and (3) can be deduced from those of the Legendre symbol. Parts (4) and (5) are much deeper.

Theorem

Let n be odd.

1. If $a \equiv b \pmod{n}$ and $\gcd(a, n) = 1$, then
$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$
2. If $\gcd(ab, n) = 1$, then
$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$
3. $$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}.$$
4. $$\left(\frac{2}{n}\right) = \begin{cases} +1 \; if \; n \equiv 1 \text{ or } 7 \pmod{8} \\ -1 \; if \; n \equiv 3 \text{ or } 5 \pmod{8}. \end{cases}$$
5. Let m be odd with $\gcd(m, n) = 1$. Then
$$\left(\frac{m}{n}\right) = \begin{array}{l} -\left(\frac{n}{m}\right) if \; m \equiv n \equiv 3 \pmod{4} \\ \\ +\left(\frac{n}{m}\right) otherwise. \end{array}$$

Note that we did not include a statement that $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2}$. This is usually not true for composite n (see Exercise 45). In fact, the Solovay-Strassen primality test (see Section 9.3) is based on this fact.

Part (5) is the famous **law of quadratic reciprocity**, proved by Gauss in 1796. When m and n are primes, it relates the question of whether m is a square mod n to the question of whether n is a square mod m.

A proof of the theorem when m and n are primes can be found in most elementary number theory texts. The extension to composite m and n can be deduced fairly easily from this case. See [Niven et al.], [Rosen], or [KraftW], for example.

When quadratic reciprocity is combined with the other properties of the Jacobi symbol, we obtain a fast way to

evaluate the symbol. Here are two examples.

Example

Let's calculate $\left(\frac{4567}{12345}\right)$:

$$\begin{aligned}
\left(\frac{4567}{12345}\right) &= +\left(\frac{12345}{4567}\right) \quad (\text{by } (5),\ \text{since } 12345 \equiv 1 \pmod 4) \\
&= +\left(\frac{3211}{4567}\right) \quad (\text{by } (1),\ \text{since } 12345 \equiv 3211 \pmod{4567}) \\
&= -\left(\frac{4567}{3211}\right) \quad (\text{by } (5)) \quad = \quad -\left(\frac{1356}{3211}\right) \quad (\text{by } (1)) \\
&= -\left(\frac{2}{3211}\right)^2\left(\frac{339}{3211}\right) \quad (\text{by } (2),\ \text{since } 1356 = 2^2 \cdot 339) \\
&= -\left(\frac{339}{3211}\right) \quad (\text{since } (\pm 1)^2 = 1) \\
&= +\left(\frac{3211}{339}\right) \quad (\text{by } (5)) \quad = \quad +\left(\frac{160}{339}\right) \quad (\text{by } (1)) \\
&= +\left(\frac{2}{339}\right)^5\left(\frac{5}{339}\right) \quad (\text{by } (2),\ \text{since } 160 = 2^5 \cdot 5) \\
&= +(-1)^5\left(\frac{5}{339}\right) \quad (\text{by } (4)) \quad = \quad -\left(\frac{339}{5}\right) \quad (\text{by } (5)) \\
&= -\left(\frac{4}{5}\right) \quad (\text{by } (1)) \quad = \quad -\left(\frac{2}{5}\right)^2 = -1.
\end{aligned}$$

The only factorization needed in the calculation was removing powers of 2, which is easy to do. The fact that the calculations can be done without factoring odd numbers is important in the applications. The fact that the answer is -1 implies that 4567 is not a square mod 12345. However, if the answer had been $+1,$ we could not have deduced whether 4567 is a square or is not a square mod 12345. See Exercise 44.

Example

Let's calculate $\left(\frac{107}{137}\right)$:

$$
\begin{aligned}
\left(\frac{107}{137}\right) &= +\left(\frac{137}{107}\right) \quad \text{(by (5))} \\
&= +\left(\frac{30}{107}\right) \quad \text{(by (1))} \\
&= +\left(\frac{2}{107}\right)\left(\frac{15}{107}\right) \quad \text{(by (2))} \\
&= +(-1)\left(\frac{15}{107}\right) \quad \text{(by (4))} \\
&= +\left(\frac{107}{15}\right) \quad \text{(by (5))} \\
&= +\left(\frac{2}{15}\right) \quad \text{(by (1))} \\
&= +1 \quad \text{(by (5))}.
\end{aligned}
$$

Since 137 is a prime, this says that 107 is a square mod 137. In contrast, during the calculation, we used the fact that $\left(\frac{2}{15}\right) = +1$. This does not mean that 2 is a square mod 15. In fact, 2 is not a square mod 5, so it cannot be a square mod 15. Therefore, although we can interpret the final answer as saying that 107 is a square mod the prime 137, we should not interpret intermediate steps involving composite numbers as saying that a number is a square.

Suppose $n = pq$ is the product of two large primes. If $\left(\frac{a}{n}\right) = -1,$ then we can conclude that a is not a square mod n. What can we conclude if $\left(\frac{a}{n}\right) = +1$? Since

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

there are two possibilities:

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1 \quad \text{or} \quad \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = +1.$$

In the first case, a is not a square mod $p,$ therefore cannot be a square mod pq.

In the second case, a is a square mod p and mod q. The Chinese remainder theorem can be used to combine a square root mod p and a square root mod q to get a square root of a mod n. Therefore, a is a square mod n.

Therefore, if $\left(\frac{a}{n}\right) = +1,$ then a can be either a square or a nonsquare mod n. Deciding which case holds is called the **quadratic residuosity problem**. No fast algorithm is known for solving it. Of course, if we can factor $n,$ then the problem can easily be solved by computing $\left(\frac{a}{p}\right)$.

3.11 Finite Fields

> Note: This section is more advanced than the rest of the chapter. It is included because finite fields are often used in cryptography. In particular, finite fields appear in four places in this book. The finite field $GF(2^8)$ is used in AES (Chapter 8). Finite fields give an explanation of some phenomena that are mentioned in Section 5.2. Finally, finite fields are used in Section 21.4, Chapter 22 and in error correcting codes (Chapter 24).

Many times throughout this book, we work with the integers mod p, where p is a prime. We can add, subtract, and multiply, but what distinguishes working mod p from working mod an arbitrary integer n is that we can divide by any number that is nonzero mod p. For example, if we need to solve $3x \equiv 1 \pmod 5$, then we divide by 3 to obtain $x \equiv 2 \pmod 5$. In contrast, if we want to solve $3x \equiv 1 \pmod 6$, there is no solution since we cannot divide by $3 \pmod 6$. Loosely speaking, a set that has the operations of addition, multiplication, subtraction, and division by nonzero elements is called a field. We also require that the associative, commutative, and distributive laws hold.

Example

The basic examples of fields are the real numbers, the complex numbers, the rational numbers, and the integers mod a prime. The set of all integers is not a field since we sometimes cannot divide and obtain an answer in the set (for example, $4/3$ is not an integer).

Example

Here is a field with four elements. Consider the set

$$GF(4) = \{0, 1, \omega, \omega^2\},$$

with the following laws:

1. $0 + x = x$ for all x.
2. $x + x = 0$ for all x.
3. $1 \cdot x = x$ for all x.
4. $\omega + 1 = \omega^2$.
5. Addition and multiplication are commutative and associative, and the distributive law $x(y + z) = xy + xz$ holds for all x, y, z.

Since

$$\omega^3 = \omega \cdot \omega^2 = \omega \cdot (1 + \omega) = \omega + \omega^2 = \omega + (1 + \omega) = 1,$$

we see that ω^2 is the multiplicative inverse of ω. Therefore, every nonzero element of $GF(4)$ has a multiplicative inverse, and $GF(4)$ is a field with four elements.

In general, a **field** is a set containing elements 0 and 1 (with $1 \neq 0$) and satisfying the following:

1. It has a multiplication and addition satisfying (1), (3), (5) in the preceding list.
2. Every element has an additive inverse (for each x, this means there exists an element $-x$ such that $x + (-x) = 0$).
3. Every nonzero element has a multiplicative inverse.

A field is closed under subtraction. To compute $x - y$, simply compute $x + (-y)$.

The set of 2×2 matrices with real entries is not a field for two reasons. First, the multiplication is not commutative. Second, there are nonzero matrices that do not have inverses (and therefore we cannot divide by them). The set of nonnegative real numbers is not a field. We can add, multiply, and divide, but sometimes when we subtract the answer is not in the set.

For every power p^n of a prime, there is exactly one finite field with p^n elements, and these are the only finite fields. We'll soon show how to construct them, but first let's point out that if $n > 1,$ then the integers mod p^n do not form a field. The congruence $px \equiv 1 \pmod{p^n}$ does not have a solution, so we cannot divide by $p,$ even though $p \not\equiv 0 \pmod{p^n}$. Therefore, we need more complicated constructions to produce fields with p^n elements.

The field with p^n elements is called $GF(p^n)$. The "GF" is for "Galois field," named for the French mathematician Evariste Galois (1811–1832), who did some early work related to fields.

Example, continued

Here is another way to produce the field $GF(4)$. Let $\mathbf{Z}_2[X]$ be the set of polynomials whose coefficients are integers mod 2. For example, $1 + X^3 + X^6$ and X are in this set. Also, the constant polynomials 0 and 1 are in $\mathbf{Z}_2[X]$. We can add, subtract, and multiply in this set, as long as we work with the coefficients mod 2. For example,

$$(X^3 + X + 1)(X + 1) = X^4 + X^3 + X^2 + 1$$

since the term $2X$ disappears mod 2. The important property for our purposes is that we can perform division with remainder, just as with the integers. For example, suppose we divide $X^2 + X + 1$ into $X^4 + X^3 + 1$. We can do this by long division, just as with numbers:

$$\begin{array}{r} X^2 + 1 \\ X^2 + X + 1 \;\overline{)\,X^4 + X^3 + 1} \\ X^4 + X^3 + X^2 \\ \hline X^2 + 1 \\ X^2 + X + 1 \\ \hline X \end{array}$$

In words, what we did was to divide by $X^2 + X + 1$ and obtain the X^2 as the first term of the quotient. Then we multiplied this X^2 times $X^2 + X + 1$ to get $X^4 + X^3 + X^2,$ which we subtracted from $X^4 + X^3 + 1,$ leaving $X^2 + 1$. We divided this $X^2 + 1$ by $X^2 + X + 1$ and obtained the second term of the quotient, namely 1. Multiplying 1 times $X^2 + X + 1$ and subtracting from $X^2 + 1$ left the remainder X. Since the degree of the polynomial X is less than the degree of $X^2 + X + 1,$ we stopped. The quotient was $X^2 + 1$ and the remainder was X:

$$X^4 + X^3 + 1 = (X^2 + 1)(X^2 + X + 1) + X.$$

We can write this as

$$X^4 + X^3 + 1 \equiv X \pmod{X^2 + X + 1}.$$

Whenever we divide by $X^2 + X + 1$ we can obtain a remainder that is either 0 or a polynomial of degree at most 1 (if the remainder had degree 2 or more, we could continue dividing). Therefore, we define $\mathbf{Z}_2[X] \pmod{X^2 + X + 1}$ to be the set

$$\{0, 1, X, X + 1\}$$

of polynomials of degree at most 1, since these are the remainders that we obtain when we divide by $X^2 + X + 1$. Addition, subtraction, and multiplication are done mod $X^2 + X + 1$. This is completely analogous to what happens when we work with integers mod n. In the present situation, we say that two polynomials $f(X)$ and $g(X)$ are congruent mod $X^2 + X + 1,$ written $f(X) \equiv g(X) \pmod{X^2 + X + 1},$ if $f(X)$ and $g(X)$ have the same remainder when divided by $X^2 + X + 1$. Another way of saying this is that $f(X) - g(X)$ is a multiple of $X^2 + X + 1$. This means that there is a polynomial $h(X)$ such that $f(X) - g(X) = (X^2 + X + 1)h(X)$.

Now let's multiply in $\mathbf{Z}_2[X] \pmod{X^2+X+1}$. For example,

$$X \cdot X = X^2 \equiv X+1 \pmod{X^2+X+1}.$$

(It might seem that the right side should be $-X-1$, but recall that we are working with coefficients mod 2, so $+1$ and -1 are the same.) As another example, we have

$$X^3 \equiv X \cdot X^2 \equiv X \cdot (X+1) \equiv X^2 + X \equiv 1 \pmod{X^2+X+1}.$$

It is easy to see that we are working with the set $GF(4)$ from before, with X in place of ω.

Working with $\mathbf{Z}_2[X]$ mod a polynomial can be used to produce finite fields. But we cannot work mod an arbitrary polynomial. The polynomial must be irreducible, which means that it doesn't factor into polynomials of lower degree mod 2. For example, $X^2+1,$ which is irreducible when we are working with real numbers, is not irreducible when the coefficients are taken mod 2 since $X^2+1 = (X+1)(X+1)$ when we are working mod 2. However, X^2+X+1 is irreducible: Suppose it factors mod 2 into polynomials of lower degree. The only possible factors mod 2 are X and $X+1,$ and X^2+X+1 is not a multiple of either of these, even mod 2.

Here is the general procedure for constructing a finite field with p^n elements, where p is prime and $n \geq 1$. We let $\mathbf{Z}_p$ denote the integers mod p.

1. $\mathbf{Z}_p[X]$ is the set of polynomials with coefficients mod p.
2. Choose $P(X)$ to be an irreducible polynomial mod p of degree n.
3. Let $GF(p^n)$ be $\mathbf{Z}_p[X]$ mod $P(X)$. Then $GF(p^n)$ is a field with p^n elements.

The fact that $GF(p^n)$ has p^n elements is easy to see. The possible remainders after dividing by $P(X)$ are the polynomials of the form $a_0 + a_1X + \cdots + a_{n-1}X^{n-1},$ where the coefficients

are integers mod p. There are p choices for each coefficient, hence p^n possible remainders.

For each n, there are irreducible polynomials mod p of degree n, so this construction produces fields with p^n elements for each $n \geq 1$. What happens if we do the same construction for two different polynomials $P_1(X)$ and $P_2(X)$, both of degree n? We obtain two fields, call them $GF(p^n)'$ and $GF(p^n)''$. It is possible to show that these are essentially the same field (the technical term is that the two fields are isomorphic), though this is not obvious since multiplication mod $P_1(X)$ is not the same as multiplication mod $P_2(X)$.

3.11.1 Division

We can easily add, subtract, and multiply polynomials in $\mathbf{Z}_p[X]$, but division is a little more subtle. Let's look at an example. The polynomial $X^8 + X^4 + X^3 + X + 1$ is irreducible in $\mathbf{Z}_2[X]$ (although there are faster methods, one way to show it is irreducible is to divide it by all polynomials of smaller degree in $\mathbf{Z}_2[X]$). Consider the field

$$GF(2^8) = \mathbf{Z}_2[X] \pmod{X^8 + X^4 + X^3 + X + 1}.$$

Since $X^7 + X^6 + X^3 + X + 1$ is not 0, it should have an inverse. The inverse is found using the analog of the extended Euclidean algorithm. First, perform the gcd calculation for
$\gcd\,(X^7 + X^6 + X^3 + X + 1, X^8 + X^4 + X^3 + X + 1)$.
The procedure (remainder $\rightarrow$ divisor $\rightarrow$ dividend $\rightarrow$ ignore) is the same as for integers:

$$\begin{aligned} X^8 + X^4 + X^3 + X + 1 &= (X+1)(X^7 + X^6 + X^3 + X + 1) + (X^6 + X^2 + X) \\ X^7 + X^6 + X^3 + X + 1 &= (X+1)(X^6 + X^2 + X) + 1. \end{aligned}$$

The last remainder is 1, which tells us that the "greatest common divisor" of $X^7 + X^6 + X^3 + X + 1$ and $X^8 + X^4 + X^3 + X + 1$ is 1. Of course, this must be

the case, since $X^8 + X^4 + X^3 + X + 1$ is irreducible, so its only factors are 1 and itself.

Now work the Extended Euclidean algorithm to express 1 as a linear combination of $X^7 + X^6 + X^3 + X + 1$ and $X^8 + X^4 + X^3 + X + 1$:

	x	y	
$X^8 + X^4 + X^3 + X + 1$	1	0	
$X^7 + X^6 + X^3 + X + 1$	0	1	
$X^6 + X^2 + X$	1	$X + 1$	(1st row) $-(X + 1)\cdot$ (2nd row)
1	$X + 1$	X^2	(2nd row) $-(X + 1)\cdot$ (3rd row).

The end result is

$$1 = (X^2)(X^7+X^6+X^3+X+1)+(X+1)(X^8+X^4+X^3+X+1).$$

Reducing mod $X^8 + X^4 + X^3 + X + 1,$ we obtain

$$(X^2)(X^7 + X^6 + X^3 + X + 1) \equiv 1 \pmod{X^8 + X^4 + X^3 + X + 1},$$

which means that X^2 is the multiplicative inverse of $X^7 + X^6 + X^3 + X + 1$. Whenever we need to divide by $X^7 + X^6 + X^3 + X + 1,$ we can instead multiply by X^2. This is the analog of what we did when working with the usual integers mod p.

3.11.2 $GF(2^8)$

In Chapter 8, we discuss AES, which uses $GF(2^8),$ so let's look at this field a little more closely. We'll work mod the irreducible polynomial

$X^8 + X^4 + X^3 + X + 1,$ since that is the one used by AES. However, there are other irreducible polynomials of degree 8, and any one of them would lead to similar calculations. Every element can be represented uniquely as a polynomial

$$b_7X^7 + b_6X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0,$$

where each b_i is 0 or 1. The 8 bits $b_7b_6b_5b_4b_3b_2b_1b_0$ represent a byte, so we can represent the elements of $GF(2^8)$ as 8-bit bytes. For example, the polynomial $X^7 + X^6 + X^3 + X + 1$ becomes 11001011. Addition is the XOR of the bits:

$$\begin{gathered}(X^7 + X^6 + X^3 + X + 1) + (X^4 + X^3 + 1) \\ \to 11001011 \oplus 00011001 = 11010010 \\ \to X^7 + X^6 + X^4 + X.\end{gathered}$$

Multiplication is more subtle and does not have as easy an interpretation. That is because we are working mod the polynomial $X^8 + X^4 + X^3 + X + 1,$ which we can represent by the 9 bits 100011011. First, let's multiply $X^7 + X^6 + X^3 + X + 1$ by X: With polynomials, we calculate

$$\begin{aligned}&(X^7 + X^6 + X^3 + X + 1)(X) = X^8 + X^7 + X^4 + X^2 + X \\ &= (X^7 + X^3 + X^2 + 1) + (X^8 + X^4 + X^3 + X + 1) \\ &\equiv X^7 + X^3 + X^2 + 1 \pmod{X^8 + X^4 + X^3 + X + 1}.\end{aligned}$$

The same operation with bits becomes

$$\begin{array}{lcll}11001011 & \to & 110010110 & \text{(shift left and append a 0)} \\ & \to & 110010110 \oplus 100011011 & \text{(subtract } X^8 + X^4 + X^3 + X + 1) \\ & = & 010001101, & \end{array}$$

which corresponds to the preceding answer. In general, we can multiply by X by the following algorithm:

1. Shift left and append a 0 as the last bit.
2. If the first bit is 0, stop.
3. If the first bit is 1, *XOR* with 100011011.

The reason we stop in step 2 is that if the first bit is 0 then the polynomial still has degree less than 8 after we multiply by X, so it does not need to be reduced. To multiply by higher powers of X, multiply by X several times. For example, multiplication by X^3 can be done with three shifts and at most three *XOR*s. Multiplication by an arbitrary polynomial can be accomplished by multiplying by the various powers of X appearing in that polynomial, then adding (i.e., *XOR*ing) the results.

In summary, we see that the field operations of addition and multiplication in $GF(2^8)$ can be carried out very efficiently. Similar considerations apply to any finite field.

The analogy between the integers mod a prime and polynomials mod an irreducible polynomial is quite remarkable. We summarize in the following.

$$\begin{aligned} \text{integers} &\longleftrightarrow \mathbf{Z}_p[X] \\ \text{prime number } q &\longleftrightarrow \text{irreducible } P(X) \text{ of degree } n \\ \mathbf{Z}_q &\longleftrightarrow \mathbf{Z}_p[X] \pmod{P(X)} \\ \text{field with } q \text{ elements} &\longleftrightarrow \text{field with } p^n \text{ elements} \end{aligned}$$

Let $GF(p^n)^*$ denote the nonzero elements of $GF(p^n)$. This set, which has $p^n - 1$ elements, is closed under multiplication, just as the integers not congruent to 0 mod p are closed under multiplication. It can be shown that there is a generating polynomial $g(X)$ such that every element in $GF(p^n)^*$ can be expressed as a power of $g(X)$. This also means that the smallest exponent k such that $g(X)^k \equiv 1$ is $p^n - 1$. This is the analog of a primitive root for primes. There are $\phi(p^n - 1)$ such generating polynomials, where ϕ is Euler's function. An interesting situation occurs when $p = 2$ and $2^n - 1$ is prime. In this case, every nonzero polynomial $f(X) \neq 1$ in $GF(2^n)$ is a generating polynomial. (*Remark, for those who know some group theory:* The set $GF(2^n)^*$ is a group of prime order in this case, so every element except the identity is a generator.)

The **discrete log problem** mod a prime, which we'll discuss in Chapter 10, has an analog for finite fields; namely, given $h(x)$, find an integer k such that $h(X) = g(X)^k$ in $GF(p^n)$. Finding such a k is believed to be very hard in most situations.

3.11.3 LFSR Sequences

We can now explain a phenomenon that is mentioned in Section 5.2 on LFSR sequences.

Suppose that we have a recurrence relation

$$x_{n+m} \equiv c_0 x_n + c_1 x_{n+1} + \cdots + c_{m-1} x_{n+m-1} \pmod 2.$$

For simplicity, we assume that the associated polynomial

$$P(X) = X^m + c_{m-1}X^{m-1} + c_{m-2}X^{m-2} + \cdots + c_0$$

is irreducible mod 2. Then $\mathbf{Z}_2[X] \pmod{P(X)}$ is the field $GF(2^m)$. We regard $GF(2^m)$ as a vector space over $\mathbf{Z}_2$ with basis $\{1, X, X^2, X^3, \ldots, X^{m-1}\}$. Multiplication by X gives a linear transformation of this vector space. Since

$$\begin{aligned} &X \cdot 1 = X, \quad X \cdot X = X^2, \quad X \cdot X^2 = X^3, \quad \ldots \\ &X \cdot X^{m-1} = X^m \equiv c_0 + c_1 X + \cdots + c_{m-1}X^{m-1}, \end{aligned}$$

multiplication by X is represented by the matrix

$$M_X = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & c_{m-1} \end{pmatrix}.$$

Suppose we know $(x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m-1})$. We compute

$$\begin{aligned} &(x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m-1})\, M_X \\ &= (x_{n+1}, x_{n+2}, x_{n+3}, \ldots, c_0 x_n + \cdots + c_{m-1} x_{n+m-1}) \\ &\equiv (x_{n+1}, x_{n+2}, x_{n+3}, \ldots, x_{n+m}). \end{aligned}$$

Therefore, multiplication by M_X shifts the indices by 1. It follows easily that multiplication on the right by the matrix M_X^j sends $(x_1, x_2, \ \ldots\ , x_m)$ to $(x_{1+j}, x_{2+j}, \ \ldots\ , x_{m+j})$. If $M_X^j \equiv I,$ the identity matrix, this must be the original vector $(x_1, x_2, \ \ldots\ , x_m)$. Since there are $2^m - 1$ nonzero elements in $GF(2^m),$ it follows from Lagrange's theorem in group theory that $X^{2^m-1} \equiv 1,$ which implies that $M_X^{2^m-1} = I$. Therefore, we know that $x_1 \equiv x_{2^m}, \quad x_2 \equiv x_{2^m+1}, \ \ldots.$

For any set of initial values (we'll assume that at least one initial value is nonzero), the sequence will repeat after k terms, where k is the smallest positive integer such that $X^k \equiv 1 \pmod{P(X)}$. It can be shown that k divides $2^m - 1$.

In fact, the period of such a sequence is exactly k. This can be proved as follows, using a few results from linear algebra: Let $v = (x_1, \ \ldots\ , x_m) \neq 0$ be the row vector of initial values. The sequence repeats when $vM_X^j = v$. This means that the nonzero *row* vector v is in the left null space of the matrix $M_X^j - I,$ so $\det\,(M_X^j - I) = 0$. But this means that there is a nonzero *column* vector $w = (a_0, \ \ldots\ , a_{m-1})^T$ in the right null space of $M_X^j - I$. That is, $M_X^j\, w = w$. Since the matrix M_X^j represents the linear transformation given by multiplication by X^j with respect to the basis $\{1, X, \ \ldots\ , X^{m-1}\},$ this can be changed back into a relation among polynomials:

$$X^j(a_0 + a_1X + \cdots + a_{m-1}X^{m-1}) \equiv a_0 + a_1X + \cdots + a_{m-1}X^{m-1} \pmod{P(X)}.$$

But $a_0 + a_1X + \cdots + a_{m-1}X^{m-1} \pmod{P(X)}$ is a nonzero element of the field $GF(2^m),$ so we can divide by this element to get $X^j \equiv 1 \pmod{P(X)}$. Since $j = k$ is the first time this happens, the sequence first repeats after k terms, so it has period k.

As mentioned previously, when $2^m - 1$ is prime, all polynomials (except 0 and 1) are generating polynomials for $GF(2^m)$. In particular, X is a generating polynomial and therefore $k = 2^m - 1$ is the period of the recurrence.

3.12 Continued Fractions

There are many situations where we want to approximate a real number by a rational number. For example, we can approximate $\pi = 3.14159265\ldots$ by $314/100 = 157/50$. But $22/7$ is a slightly better approximation, and it is more efficient in the sense that it uses a smaller denominator than $157/50$. The method of continued fractions is a procedure that yields this type of good approximations. In this section, we summarize some basic facts. For proofs and more details, see, for example, [Hardy-Wright], [Niven et al.], [Rosen], and [KraftW].

An easy way to approximate a real number x is to take the largest integer less than or equal to x. This is often denoted by $[x]$. For example, $[\pi] = 3$. If we want to get a better approximation, we need to look at the remaining fractional part. For $\pi = 3.14159\ldots,$ this is $.14159\ldots$. This looks close to $1/7 = .142857\ldots$. One way to express this is to look at $1/.14159 = 7.06251$. We can approximate this last number by $[7.06251\ldots] = 7$ and therefore conclude that 1/7 is indeed a good approximation for $.14159$ and that $22/7$ is a good approximation for π. Continuing in this manner yields even better approximations. For example, the next step is to compute $1/.06251 = 15.9966$ and then take the greatest integer to get 15 (yes, 16 is closer, but the algorithm corrects for this in the next step). We now have

$$\pi \approx 3 + \cfrac{1}{7 + \cfrac{1}{15}} = \frac{333}{106}.$$

If we continue one more step, we obtain

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1}}} = \frac{355}{113}.$$

This last approximation is very accurate:

$$\pi = 3.14159265\ldots, \text{ and } \qquad 355/113 = 3.14159292\ldots.$$

This procedure works for arbitrary real numbers. Start with a real number x. Let $a_0 = [x]$ and $x_0 = x$. Then (if $x_i \neq a_i$; otherwise, stop) define

$$x_{i+1} = \frac{1}{x_i - a_i}, \qquad a_{i+1} = [x_{i+1}].$$

We obtain the approximations

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}.$$

We have therefore produced a sequence of rational numbers $p_1/q_1, p_2/q_2, \ldots$. It can be shown that each rational number p_k/q_k gives a better approximation to x than any of the preceding rational numbers p_j/q_j with $1 \leq j < k$. Moreover, the following holds.

Theorem

If $\left|x - (r/s)\right| < 1/2s^2$ for integers $r, s,$ then $r/s = p_i/q_i$ for some i.

For example, $|\pi - 22/7| \approx .001 < 1/98$ and $22/7 = p_2/q_2$.

Continued fractions yield a convenient way to recognize rational numbers from their decimal expansions. For example, suppose we encounter the decimal 3.764705882 and we suspect that it is the beginning of the decimal expansion of a rational number with small

denominator. The first few terms of the continued fraction are

$$3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{9803921}}}}.$$

The fact that 9803921 is large indicates that the preceding approximation is quite good, so we calculate

$$3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4}}}=\frac{64}{17}=3.7647058823529\ldots,$$

which agrees with all of the terms of the original 3.764605882. Therefore, $64/17$ is a likely candidate for the answer. Note that if we had included the 9803921, we would have obtained a fraction that also agrees with the original decimal expansion but has a significantly larger denominator.

Now let's apply the procedure to $12345/11111$. We have

$$\frac{12345}{11111}=1+\cfrac{1}{9+\cfrac{1}{246+\cfrac{1}{1+\cfrac{1}{4}}}}.$$

This yields the numbers

$$1,\quad \frac{10}{9},\quad \frac{2461}{2215},\quad \frac{2471}{2224},\quad \frac{12345}{11111}.$$

Note that the numbers 1, 9, 246, 1, 4 are the quotients obtained during the computation of $\gcd(12345, 11111)$ in Subsection 3.1.3 (see Exercise 49).

Calculating the fractions such as

$$\frac{2461}{2215} = 1 + \cfrac{1}{9 + \cfrac{1}{246}}$$

can become tiresome when done in the straightforward way. Fortunately, there is a faster method. Define

$$\begin{array}{lllll} p_{-2} = 0, & p_{-1} & = & 1, \quad q_{-2} = 1, & q_{-1} = 0, \\ & p_{n+1} & = & {}_{n+1}p_n + p_{n-1} & \\ & q_{n+1} & = & a_{n+1}q_n + q_{n-1}. & \end{array}$$

Then

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}.$$

Using these relations, we can compute the partial quotients p_n/q_n from the previous ones, rather than having to start a new computation every time a new a_n is found.

3.13 Exercises

1.
   a. Find integers x and y such that $17x + 101y = 1$.
   b. Find $17^{-1} \pmod{101}$.

2.
   a. Using the identity $x^3 + y^3 = (x + y)(x^2 - xy + y^3)$, factor $2^{333} + 1$ into a product of two integers greater than 1.
   b. Using the congruence $2^2 \equiv 1 \pmod{3}$, deduce that $2^{232} \equiv 1 \pmod{3}$ and show that $2^{333} + 1$ is a multiple of 3.

3.
   a. Solve $7d \equiv 1 \pmod{30}$.
   b. Suppose you write a message as a number $m \pmod{31}$. Encrypt m as $m^7 \pmod{31}$. How would you decrypt? (Hint: Decryption is done by raising the ciphertext to a power mod 31. Fermat's theorem will be useful.)

4. Solve $5x + 2 \equiv 3x - 7 \pmod{31}$.

5.
   a. Find all solutions of $12x \equiv 28 \pmod{236}$.
   b. Find all solutions of $12x \equiv 30 \pmod{236}$.

6.
   a. Find all solutions of $4x \equiv 20 \pmod{50}$.
   b. Find all solutions of $4x \equiv 21 \pmod{50}$.

7.
   a. Let $n \geq 2$. Show that if n is composite then n has a prime factor $p \leq \sqrt{n}$.
   b. Use the Euclidean algorithm to compute $\gcd(30030, 257)$.
   c. Using the result of parts (a) and (b) and the fact that $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, show that 257 is prime. (Remark: This method of computing one gcd, rather than doing several trial divisions (by 2, 3, 5, ...), is often faster for checking whether small primes divide a number.)

8. Compute $\gcd(12345678987654321, 100)$.

9.
    1. Compute $\gcd\,(4883, 4369)$.
    2. Factor 4883 and 4369 into products of primes.

10.
    1. What is $\gcd\,(111, 11)$? Using the Extended Euclidean algorithm, find $11^{-1} \bmod 111$.
    2. What is $\gcd\,(1111, 11)$? Does $11^{-1} \bmod 1111$ exist?
    3. Find $\gcd\,(x, 11),$ where x consists of n repeated 1s. What can you say about $11^{-1} \bmod x$ as a function of n?

11.
    1. Let $F_1 = 1,\ F_2 = 1,\ F_{n+1} = F_n + F_{n-1}$ define the Fibonacci numbers $1, 1, 2, 3, 5, 8, \ldots$. Use the Euclidean algorithm to compute $\gcd\,(F_n, F_{n-1})$ for all $n \geq 1$.
    2. Find $\gcd\,(11111111, 11111)$.
    3. Let $a = 111 \cdots 11$ be formed with F_n repeated 1's and let $b = 111 \cdots 11$ be formed with F_{n-1} repeated 1's. Find $\gcd\,(a, b)$. (Hint: Compare your computations in parts (a) and (b).)

12. Let $n \geq 2$. Show that none of the numbers $n! + 2, n! + 3, n! + 4,\ \ldots\ , n! + n$ are prime.

13.
    1. Let p be prime. Suppose a and b are integers such that $ab \equiv 0 \pmod{p}$. Show that either $a \equiv 0$ or $b \equiv 0 \pmod{p}$.
    2. Show that if a, b, n are integers with $n|ab$ and $\gcd\,(a, n) = 1,$ then $n|b$.

14. Let p be prime.
    1. Show that if $x^2 \equiv 0 \pmod{p},$ then $x \equiv 0 \pmod{p}$.
    2. Show that if $k \geq 2,$ then $x^2 \equiv 0 \pmod{p^k}$ has solutions with $x \not\equiv 0 \pmod{p^k}$.

15. Let $p \geq 3$ be prime. Show that the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$. (Hint: Apply Exercise 13(a) to $(x + 1)(x - 1)$.)

16. Find x with $x \equiv 3 \pmod{5}$ and $x \equiv 9 \pmod{11}$.

17. Suppose $x \equiv 2 \pmod{7}$ and $x \equiv 3 \pmod{10}$. What is x congruent to mod 70?

18. Find x with $2x \equiv 1 \pmod{7}$ and $4x \equiv 2 \pmod{9}$. (Hint: Replace $2x \equiv 1 \pmod{7}$ with $x \equiv a \pmod{7}$ for a suitable a,

and similarly for the second congruence.)

19. A group of people are arranging themselves for a parade. If they line up three to a row, one person is left over. If they line up four to a row, two people are left over, and if they line up five to a row, three people are left over. What is the smallest possible number of people? What is the next smallest number? (Hint: Interpret this problem in terms of the Chinese remainder theorem.)

20. You want to find x such that when you divide x by each of the numbers from 2 to 10, the remainder is 1. The smallest such x is $x = 1$. What is the next smallest x? (The answer is less than 3000.)

21.
    1. Find all four solutions to $x^2 \equiv 133 \pmod{143}$. (Note that $143 = 11 \cdot 13$.)

    2. Find all solutions to $x^2 \equiv 77 \pmod{143}$. (There are only two solutions in this case. This is because $\gcd(77, 143) \neq 1$.)

22. You need to compute $123456789^{65537} \pmod{581859289607}$. A friend offers to help: 1 cent for each multiplication mod 581859289607. Your friend is hoping to get more than $650. Describe how you can have the friend do the computation for less than 25 cents. (Note: $65537 = 2^{16} + 1$ is the most commonly used RSA encryption exponent.)

23. Divide 2^{10203} by 101. What is the remainder?

24. Divide $3^{987654321}$ by 11. What is the remainder?

25. Find the last 2 digits of 123^{562}.

26. Let $p \equiv 3 \pmod{4}$ be prime. Show that $x^2 \equiv -1 \pmod{p}$ has no solutions. (Hint: Suppose x exists. Raise both sides to the power $(p-1)/2$ and use Fermat's theorem. Also, $(-1)^{(p-1)/2} = -1$ because $(p-1)/2$ is odd.)

27. Let p be prime. Show that $a^p \equiv a \pmod{p}$ for all a.

28. Let p be prime and let a and b be integers. Show that $(a+b)^p \equiv a^p + b^p \pmod{p}$.

29.
    1. Evaluate $7^7 \pmod{4}$.

    2. Use part (a) to find the last digit of 7^{7^7}. (Note: a^{b^c} means $a^{(b^c)}$ since the other possible interpretation would be $(a^b)^c = a^{bc}$, which is written more easily without a second exponentiation.) (Hint: Use part (a) and the Basic Principle that follows Euler's Theorem.)

30. You are told that exactly one of the numbers

$$2^{1000}+277, \quad 2^{1000}+291, \quad 2^{1000}+297$$

is prime and you have one minute to figure out which one. Describe calculations you could do (with software such as MATLAB or Mathematica) that would give you a very good chance of figuring out which number is prime? Do not do the calculations. Do not try to factor the numbers. They do not have any prime factors less than 10^9. You may use modular exponentiation, but you may not use commands of the form "IsPrime[n]" or "NextPrime[n]." (See Computer Problem 3 below.)

31.

1. Let $p = 7,\ 13$, or 19. Show that $a^{1728} \equiv 1 \pmod{p}$ for all a with $p \nmid a$.

2. Let $p = 7,\ 13$, or 19. Show that $a^{1729} \equiv a \pmod{p}$ for all a. (Hint: Consider the case $p|a$ separately.)

3. Show that $a^{1729} \equiv a \pmod{1729}$ for all a. Composite numbers n such that $a^n \equiv a \pmod{n}$ for all a are called Carmichael numbers. They are rare (561 is another example), but there are infinitely many of them [Alford et al. 2].

32.

1. Show that $2^{10} \equiv 1 \pmod{11}$ and $2^5 \equiv 1 \pmod{31}$.

2. Show that $2^{340} \equiv 1 \pmod{341}$.

3. Is 341 prime?

33.

1. Let p be prime and let $a \not\equiv 0 \pmod{p}$. Let $b \equiv a^{p-2} \pmod{p}$. Show that $ab \equiv 1 \pmod{p}$.

2. Use the method of part (a) to solve $2x \equiv 1 \pmod{7}$.

34. You are appearing on the Math Superstars Show and, for the final question, you are given a 500-digit number n and are asked to guess whether or not it is prime. You are told that n is either prime or the product of a 200-digit prime and a 300-digit prime. You have one minute, and fortunately you have a computer. How would you make a guess that's very probably correct? Name any theorems that you are using.

35.

1. Compute $\phi(d)$ for all of the divisors of 10 (namely, 1, 2, 5, 10), and find the sum of these $\phi(d)$.

2. Repeat part (a) for all of the divisors of 12.

3. Let $n \geq 1$. Conjecture the value of $\sum \phi(d)$, where the sum is over the divisors of n. (This result is proved in many elementary number theory texts.)

36. Find a number α mod 7 that is a primitive root mod 7 and find a number $\gamma \not\equiv 0 \pmod 7$ that is not a primitive root mod 7. Show that α and γ have the desired properties.

37.
    1. Show that every nonzero congruence class mod 11 is a power of 2, and therefore 2 is a primitive root mod 11.
    2. Note that $2^3 \equiv 8 \pmod{11}$. Find x such that $8^x \equiv 2 \pmod{11}$. (Hint: What is the inverse of $3 \pmod{10}$?)
    3. Show that every nonzero congruence class mod 11 is a power of 8, and therefore 8 is a primitive root mod 11.
    4. Let p be prime and let α be a primitive root mod p. Let $h \equiv \alpha^y \pmod p$ with $\gcd(y, p-1) = 1$. Let $xy \equiv 1 \pmod{p-1}$. Show that $h^x \equiv \alpha \pmod p$.
    5. Let p and h be as in part (d). Show that h is a primitive root mod p. (Remark: Since there are $\phi(p-1)$ possibilities for the exponent x in part (d), this yields all of the $\phi(p-1)$ primitive roots mod p.)
    6. Use the method of part (e) to find all primitive roots for $p = 13$, given that 2 is a primitive root.

38. It is known that 14 is a primitive root for the prime $p = 30000001$. Let $b \equiv 14^{9000000} \pmod p$. (The exponent is $3(p-1)/10$.)
    1. Explain why $b^{10} \equiv 1 \pmod p$.
    2. Explain why $b \not\equiv 1 \pmod p$.

39.
    1. Find the inverse of $\begin{pmatrix} 1 & 1 \\ 6 & 1 \end{pmatrix} \pmod{26}$.
    2. Find all values of $b \pmod{26}$ such that $\begin{pmatrix} 1 & 1 \\ b & 1 \end{pmatrix} \pmod{26}$ is invertible.

40. Find the inverse of $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \pmod 2$.

41. Find all primes p for which $\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod p$ is not invertible.

42.
    1. Use the Legendre symbol to show that $x^2 \equiv 5 \pmod{19}$ has a solution.
    2. Use the method of Section 3.9 to find a solution to $x^2 \equiv 5 \pmod{19}$.

43. Use the Legendre symbol to determine which of the following congruences have solutions (each modulus is prime):

    1. $X^2 \equiv 123 \pmod{401}$
    2. $X^2 \equiv 43 \pmod{179}$
    3. $X^2 \equiv 1093 \pmod{65537}$

44.
    1. Let n be odd and assume $\gcd(a, n) = 1$. Show that if $\left(\frac{a}{n}\right) = -1$, then a is not a square mod n.
    2. Show that $\left(\frac{3}{35}\right) = +1$.
    3. Show that 3 is not a square mod 35.

45. Let $n = 15$. Show that $\left(\frac{2}{n}\right) \not\equiv 2^{(n-1)/2} \pmod{n}$.

46.
    1. Show that $\left(\frac{3}{65537}\right) = -1$.
    2. Show that $3^{(65537-1)/2} \not\equiv 1 \pmod{65537}$.
    3. Use the procedure of Exercise 54 to show that 3 is a primitive root mod 65537. (Remark: The same proof shows that 3 is a primitive root for any prime $p \geq 5$ such that $p - 1$ is a power of 2. However, there are only six known primes with $p - 1$ a power of 2; namely, 2, 3, 5, 17, 257, 65537. They are called *Fermat primes*.)

47.
    1. Show that the only irreducible polynomials in $\mathbf{Z}_2[X]$ of degree at most 2 are X, $X + 1$, and $X^2 + X + 1$.
    2. Show that $X^4 + X + 1$ is irreducible in $\mathbf{Z}_2[X]$. (Hint: If it factors, it must have at least one factor of degree at most 2.)
    3. Show that $X^4 \equiv X + 1$, $X^8 \equiv X^2 + 1$, and $X^{16} \equiv X \pmod{X^4 + X + 1}$.
    4. Show that $X^{15} \equiv 1 \pmod{X^4 + X + 1}$.

48.
    1. Show that $X^2 + 1$ is irreducible in $\mathbf{Z}_3[X]$.
    2. Find the multiplicative inverse of $1 + 2X$ in $\mathbf{Z}_3[X] \pmod{X^2 + 1}$.

49. Show that the quotients in the Euclidean algorithm for $\gcd(a, b)$ are exactly the numbers $a_0, a_1, \ldots$ that appear in the continued

fraction of a/b.

50.

1. Compute several steps of the continued fractions of $\sqrt{3}$ and $\sqrt{7}$. Do you notice any patterns? (It can be shown that the a_i's in the continued fraction of every irrational number of the form $a + b\sqrt{d}$ with a, b, d rational and $d > 0$ eventually become periodic.)

2. For each of $d = 3, 7,$ let n be such that $a_{n+1} = 2a_0$ in the continued fraction of $\sqrt{d}$. Compute p_n and q_n and show that $x = p_n$ and $y = q_n$ give a solution of what is known as Pell's equation: $x^2 - dy^2 = 1$.

3. Use the method of part (b) to solve $x^2 - 19y^2 = 1$.

51. Compute several steps of the continued fraction expansion of e. Do you notice any patterns? (On the other hand, the continued fraction expansion of π seems to be fairly random.)

52. Compute several steps of the continued fraction expansion of $(1 + \sqrt{5})/2$ and compute the corresponding numbers p_n and q_n (defined in Section 3.12). The sequences p_0, p_1, p_2, $\ldots$ and q_1, q_2, $\ldots$ are what famous sequence of numbers?

53. Let a and $n > 1$ be integers with $\gcd(a, n) = 1$. The **order** of a mod n is the smallest positive integer r such that $a^r \equiv 1 \pmod{n}$. We denote $r = \mathrm{ord}_n(a)$.

1. Show that $r \leq \phi(n)$.

2. Show that if $m = rk$ is a multiple of r, then $a^m \equiv 1 \pmod{n}$.

3. Suppose $a^t \equiv 1 \pmod{n}$. Write $t = qr + s$ with $0 \leq s < r$ (this is just division with remainder). Show that $a^s \equiv 1 \pmod{n}$.

4. Using the definition of r and the fact that $0 \leq s < r$, show that $s = 0$ and therefore $r|t$. This, combined with part (b), yields the result that $a^t \equiv 1 \pmod{n}$ if and only if $\mathrm{ord}_n(a)|t$.

5. Show that $\mathrm{ord}_n(a)|\phi(n)$.

54. This exercise will show by example how to use the results of Exercise 53 to prove a number is a primitive root mod a prime p, once we know the factorization of $p - 1$. In particular, we'll show that 7 is a primitive root mod 601. Note that $600 = 2^3 \cdot 3 \cdot 5^2$.

1. Show that if an integer $r < 600$ divides 600, then it divides at least one of 300, 200, 120 (these numbers are 600/2, 600/3, and 600/5).

2. Show that if $\text{ord}_{601}(7) < 600,$ then it divides one of the numbers 300, 200, 120.

3. A calculation shows that

$$7^{300} \equiv 600, \quad 7^{200} \equiv 576, \quad 7^{120} \equiv 423 \pmod{601}.$$

Why can we conclude that $\text{ord}_{601}(7)$ does not divide 300, 200, or 120?

4. Show that 7 is a primitive root mod 601.

5. In general, suppose p is a prime and $p - 1 = q_1^{a_1} \cdots q_s^{a_s}$ is the factorization of $p - 1$ into primes. Describe a procedure to check whether a number α is a primitive root mod p. (Therefore, if we need to find a primitive root mod $p,$ we can simply use this procedure to test the numbers α =2, 3, 5, 6, ... in succession until we find one that is a primitive root.)

55. We want to find an exponent k such that $3^k \equiv 2 \pmod{65537}$.

1. Observe that $2^{32} \equiv 1 \pmod{65537},$ but $2^{16} \not\equiv 1 \pmod{65537}$. It can be shown (Exercise 46) that 3 is a primitive root mod 65537, which implies that $3^n \equiv 1 \pmod{65537}$ if and only if $65536|n$. Use this to show that $2048|k$ but 4096 does not divide k. (Hint: Raise both sides of $3^k \equiv 2$ to the 16th and to the 32nd powers.)

2. Use the result of part (a) to conclude that there are only 16 possible choices for k that need to be considered. Use this information to determine k. This problem shows that if $p - 1$ has a special structure, for example, a power of 2, then this can be used to avoid exhaustive searches. Therefore, such primes are cryptographically weak. See Exercise 12 in Chapter 10 for a reinterpretation of the present problem.

56. 1. Let $x = b_1 b_2 \ldots b_w$ be an integer written in binary (for example, when $x = 1011,$ we have $b_1 = 1, b_2 = 0, b_3 = 1, b_4 = 1$). Let y and n be integers. Perform the following procedure:

    1. Start with $k = 1$ and $s_1 = 1$.

    2. If $b_k = 1,$ let $r_k \equiv s_k y \pmod{n}$. If $b_k = 0,$ let $r_k = s_k$.

    3. Let $s_{k+1} \equiv r_k^2 \pmod{n}$.

    4. If $k = w,$ stop. If $k < w,$ add 1 to k and go to (2).

Show that $r_w \equiv y^x \pmod{n}$.

2. Let $x,\ y,$ and n be positive integers. Show that the following procedure computes $y^x \pmod{n}$.

    1. Start with $a = x$, $b = 1$, $c = y$.
    2. If a is even, let $a = a/2,$ and let $b = b$, $c \equiv c^2 \pmod{n}$.
    3. If a is odd, let $a = a - 1,$ and let $b \equiv bc \pmod{n}$, $c = c$.
    4. If $a \neq 0,$ go to step 2.
    5. Output b.

    (Remark: This algorithm is similar to the one in part (a), but it uses the binary bits of x in reverse order.)

57. Here is how to construct the x guaranteed by the general form of the Chinese remainder theorem. Suppose $m_1,\ \ldots\ , m_k$ are integers with $\gcd\ (m_i, m_j) = 1$ whenever $i \neq j$. Let $a_1,\ \ldots\ , a_k$ be integers. Perform the following procedure:

    1. For $i = 1,\ \ldots\ , k,$ let $z_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$.
    2. For $i = 1,\ \ldots\ , k,$ let $y_i \equiv z_i^{-1} \pmod{m_i}$.
    3. Let $x = a_1 y_1 z_1 + \ \cdots\ + a_k y_k z_k$.

    Show $x \equiv a_i \pmod{m_i}$ for all i.

58. Alice designs a cryptosystem as follows (this system is due to Rabin). She chooses two distinct primes p and q (preferably, both p and q are congruent to 3 mod 4) and keeps them secret. She makes $n = pq$ public. When Bob wants to send Alice a message $m,$ he computes $x \equiv\ m^2 \pmod{n}$ and sends x to Alice. She makes a decryption machine that does the following: When the machine is given a number $x,$ it computes the square roots of $x \bmod\ n$ since it knows p and q. There is usually more than one square root. It chooses one at random, and gives it to Alice. When Alice receives x from Bob, she puts it into her machine. If the output from the machine is a meaningful message, she assumes it is the correct message. If it is not meaningful, she puts x into the machine again. She continues until she gets a meaningful message.

    1. Why should Alice expect to get a meaningful message fairly soon?

2. If Oscar intercepts x (he already knows n), why should it be hard for him to determine the message m?

3. If Eve breaks into Alice's office and thereby is able to try a few chosen-ciphertext attacks on Alice's decryption machine, how can she determine the factorization of n?

59. This exercise shows that the Euclidean algorithm computes the gcd. Let a, b, q_i, r_i be as in Subsection 3.1.3.

    1. Let d be a common divisor of a, b. Show that $d|r_1$, and use this to show that $d|r_2$.

    2. Let d be as in (a). Use induction to show that $d|r_i$ for all i. In particular, $d|r_k$, the last nonzero remainder.

    3. Use induction to show that $r_k|r_i$ for $1 \leq i \leq k$.

    4. Using the facts that $r_k|r_1$ and $r_k|r_2$, show that $r_k|b$ and then $r_k|a$. Therefore, r_k is a common divisor of a, b.

    5. Use (b) to show that $r_k \geq d$ for all common divisors d, and therefore r_k is the greatest common divisor.

60. Let p and q be distinct primes.

    1. Show that among the integers m satisfying $1 \leq m < pq$, there are $q-1$ multiples of p, and there are $p-1$ multiples of q.

    2. Suppose $\gcd(m, pq) > 1$. Show that m is a multiple of p or a multiple of q.

    3. Show that if $1 \leq m < pq$, then m cannot be a multiple of both p and q.

    4. Show that the number of integers m with $1 \leq m < q$ such that $\gcd(m, pq) = 1$ is $pq - 1 - (p-1) - (q-1) = (p-1)(q-1)$. (Remark: This proves the formula that $\phi(pq) = (p-1)(q-1)$.)

61.

    1. Give an example of integers $m \neq n$ with $\gcd(m, n) gt 1$ and integers a, b such that the simultaneous congruences

    $$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}$$

    have no solution.

    2. Give an example of integers $m \neq n$ with $\gcd(m, n) > 1$ and integers $a \neq b$ such that the simultaneous congruences

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}$$

have a solution.

3.14 Computer Problems

1. Evaluate $\gcd(8765, 23485)$.

2.
    1. Find integers x and y with $65537x + 3511y = 1$.
    2. Find integers x and y with $65537x + 3511y = 17$.

3. You are told that exactly one of the numbers

$$2^{1000} + 277, \quad 2^{1000} + 291, \quad 2^{1000} + 297$$

   is prime and you have one minute to figure out which one. They do not have any prime factors less than 10^9. You may use modular exponentiation, but you may not use commands of the form "IsPrime[n]" or "NextPrime[n]." (This makes explicit Exercise 30 above.)

4. Find the last five digits of $3^{1234567}$. (Note: Don't ask the computer to print $3^{1234567}$. It is too large!)

5. Look at the decimal expansion of $e = 2.71828182845904523\ldots$. Find the consecutive digits 71, the consecutive digits 271, and the consecutive digits 4523 form primes. Find the first set of five consecutive digits that form a prime (04523 does not count as a five-digit number).

6. Solve $314x \equiv 271 \pmod{11111}$.

7. Find all solutions to $216x \equiv 66 \pmod{606}$.

8. Find an integer such that when it is divided by 101 the remainder is 17, when it is divided by 201 the remainder is 18, and when it is divided by 301 the remainder is 19.

9. Let $n = 391 = 17 \cdot 23$. Show that $2^{n-1} \not\equiv 1 \pmod{n}$. Find an exponent $j > 0$ such that $2^j \equiv 1 \pmod{n}$.

10. Let $n = 84047 \cdot 65497$. Find x and y with $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$.

11. Let $M = \begin{matrix} 1 & 2 & 4 \\ 1 & 5 & 25 \\ 1 & 14 & 196 \end{matrix}$.
    1. Find the inverse of $M \pmod{101}$.
    2. For which primes p does M not have an inverse mod p?

12. Find the square roots of 26055 mod the prime 34807.

13. Find all square roots of 1522756 mod 2325781.

14. Try to find a square root of 48382 mod the prime 83987, using the method of Section 3.9. Square your answer to see if it is correct. What number did you find the square root of?