e = RRLRRLR.... Excellent approximations can be found in this way. For example, $\frac{1264}{465} \approx 2.718280$ agrees with e to six decimal places; we obtained this fraction from the first 19 letters of e's Stern-Brocot representation, and the accuracy is about what we would get with 19 bits of e's binary representation.

We can find the infinite representation of an irrational number α by a simple modification of the matrix-free binary search procedure:

$$\textbf{if } \alpha < 1 \textbf{ then } (\text{output(L)};\ \alpha := \alpha/(1-\alpha)) \\ \textbf{else } (\text{output(R)};\ \alpha := \alpha - 1)\ .$$

(These steps are to be repeated infinitely many times, or until we get tired.) If a is rational, the infinite representation obtained in this way is the same as before but with RL^∞ appended at the right of α's (finite) representation. For example, if $\alpha = 1$, we get RLLL . . . , corresponding to the infinite sequence of fractions $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \ldots$, which approach 1 in the limit. This situation is exactly analogous to ordinary binary notation, if we think of L as 0 and R as 1: Just as every real number x in $[0, 1)$ has an infinite binary representation $(.b_1 b_2 b_3 \ldots)_2$ not ending with all 1's, every real number α in $[0, \infty)$ has an infinite Stern-Brocot representation $B_1 B_2 B_3$ . . . not ending with all R's. Thus we have a one-to-one order-preserving correspondence between [0, 1) and [0, co) if we let $0 \leftrightarrow$ L and $1 \leftrightarrow$ R.

There's an intimate relationship between Euclid's algorithm and the Stern-Brocot representations of rationals. Given α = m/n, we get $\lfloor m/n \rfloor$ R's, then $\lfloor n/(m \bmod n) \rfloor$ L's, then $\lfloor (m \bmod n)/(n \bmod (m \bmod n)) \rfloor$ R's, and so on. These numbers m mod n, n mod (m mod n), . . . are just the values examined in Euclid's algorithm. (A little fudging is needed at the end to make sure that there aren't infinitely many R's.) We will explore this relationship further in Chapter 6.

4.6 'MOD': THE CONGRUENCE RELATION

"Numerorum congruentiam hoc *signo,* $\equiv$, in *posterum denotabimus,* modulum ubi opus *erit* in clausulis *adiungentes,* $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$." —*C.* F. Gauss *[115]*

Modular arithmetic is one of the main tools provided by number theory. We got a glimpse of it in Chapter 3 when we used the binary operation 'mod', usually as one operation amidst others in an expression. In this chapter we will use 'mod' also with entire equations, for which a slightly different notation is more convenient:

$$a \equiv b \pmod m \quad \Longleftrightarrow \quad a \bmod m = b \bmod m. \qquad (4.35)$$

For example, $9 \equiv -16 \pmod 5$, because 9 mod 5 = 4 = (-16) mod 5. The formula 'a $\equiv$ b (mod m)' can be read "a is congruent to b modulo m." The definition makes sense when a, b, and m are arbitrary real numbers, but we almost always use it with integers only.

Since x mod m differs from x by a multiple of m, we can understand congruences in another way:

$$a \equiv b \pmod m \iff a - b \text{ is a multiple of } m. \tag{4.36}$$

For if a mod m = b mod m, then the definition of 'mod' in (3.21) tells us that $a - b = a \bmod m + km - (b \bmod m + lm) = (k - l)m$ for some integers k and l. Conversely if $a - b = km$, then a = b if m = 0; otherwise

$$\begin{aligned} a \bmod m = a - \lfloor a/m \rfloor m &= b + km - \lfloor (b + km)/m \rfloor m \\ &= b - \lfloor b/m \rfloor m = b \bmod m. \end{aligned}$$

The characterization of $\equiv$ in (4.36) is often easier to apply than (4.35). For example, we have $8 \equiv 23 \pmod 5$ because $8 - 23 = -15$ is a multiple of 5; we don't have to compute both 8 mod 5 and 23 mod 5.

The congruence sign '$\equiv$' looks conveniently like '=', because congruences are almost like equations. For example, congruence is an *equivalence relation;* that is, it satisfies the reflexive law '$a \equiv a$', the symmetric law '$a \equiv b \Rightarrow b \equiv a$', and the transitive law '$a \equiv b \equiv c \Rightarrow a \equiv c$'. All these properties are easy to prove, because any relation '$\equiv$' that satisfies '$a \equiv b \iff f(a) = f(b)$' for some function f is an equivalence relation. (In our case, f(x) = x mod m.) Moreover, we can add and subtract congruent elements without losing congruence:

"I fee/*fine* today modulo a slight headache."
The Hacker's Dictionary [277]

$$\begin{aligned} a \equiv b \text{ and } c \equiv d &\implies a + c \equiv b + d \pmod m; \\ a \equiv b \text{ and } c \equiv d &\implies a - c \equiv b - d \pmod m. \end{aligned}$$

For if $a - b$ and $c - d$ are both multiples of m, so are $(a + c) - (b + d) = (a - b) + (c - d)$ and $(a - c) - (b - d) = (a - b) - (c - d)$. Incidentally, it isn't necessary to write '(mod m)' once for every appearance of '$\equiv$'; if the modulus is constant, we need to name it only once in order to establish the context. This is one of the great conveniences of congruence notation.

Multiplication works too, provided that we are dealing with integers:

$$a \equiv b \text{ and } c \equiv d \implies ac \equiv bd \pmod m, \quad \text{integers } b,\ c.$$

Proof: $ac - bd = (a - b)c + b(c - d)$. Repeated application of this multiplication property now allows us to take powers:

$$a \equiv b \implies a^n \equiv b^n \pmod m, \quad \text{integers } a,\ b;\ \text{integer } n \geq 0.$$

For example, since $2 \equiv -1 \pmod 3$, we have $2^n \equiv (-1)^n \pmod 3$; this means that $2^n - 1$ is a multiple of 3 if and only if n is even.

Thus, most of the algebraic operations that we customarily do with equations can also be done with congruences. Most, but not all. The operation of division is conspicuously absent. If $ad \equiv bd \pmod m$, we can't always conclude that $a \equiv b$. For example, $3 \cdot 2 \equiv 5 \cdot 2 \pmod 4$, but $3 \not\equiv 5$.

We can salvage the cancellation property for congruences, however, in the common case that d and m are relatively prime:

$$ad \equiv bd \iff a \equiv b \pmod m, \quad \text{integers a, b, d, m and } d \perp m. \tag{4.37}$$

For example, it's legit to conclude from $15 \equiv 35 \pmod m$ that $3 \equiv 7 \pmod m$, unless the modulus m is a multiple of 5.

To prove this property, we use the extended gcd law (4.5) again, finding d' and m' such that $d'd + m'm = 1$. Then if $ad \equiv bd$ we can multiply both sides of the congruence by d', obtaining $ad'd \equiv bd'd$. Since $d'd \equiv 1$, we have $ad'd \equiv a$ and $bd'd \equiv b$; hence $a \equiv b$. This proof shows that the number d' acts almost like l/d when congruences are considered (mod m); therefore we call it the "inverse of d modulo m!'

Another way to apply division to congruences is to divide the modulus as well as the other numbers:

$$ad \equiv bd \pmod{md} \iff a \equiv b \pmod m, \quad \text{for } d \neq 0. \tag{4.38}$$

This law holds for all real a, b, d, and m, because it depends only on the distributive law $(a \bmod m)\, d = ad \bmod md$: We have $a \bmod m = b \bmod m \iff (a \bmod m)d = (b \bmod m)d \iff ad \bmod md = bd \bmod md$. Thus, for example, from $3 \cdot 2 \equiv 5 \cdot 2 \pmod 4$ we conclude that $3 \equiv 5 \pmod 2$.

We can combine (4.37) and (4.38) to get a general law that changes the modulus as little as possible:

$$ad \equiv bd \pmod m \iff a \equiv b \left(\bmod \frac{m}{\gcd(d, m)}\right), \quad \text{integers a, b, d, m.} \tag{4.39}$$

For we can multiply $ad \equiv bd$ by d', where $d'd + m'm = \gcd(d, m)$; this gives the congruence $a \cdot \gcd(d, m) \equiv b \cdot \gcd(d, m) \pmod m$, which can be divided by $\gcd(d, m)$.

Let's look a bit further into this idea of changing the modulus. If we know that $a \equiv b \pmod{100}$, then we also must have $a \equiv b \pmod{10}$, or modulo any divisor of 100. It's stronger to say that $a - b$ is a multiple of 100

than to say that it's a multiple of 10. In general,

$$a \equiv b \pmod{md} \implies a \equiv b \pmod{m}, \text{ integer } d, \qquad (4.40)$$

because any multiple of md is a multiple of m.

Conversely, if we know that $a \equiv b$ with respect to two small moduli, can we conclude that $a \equiv b$ with respect to a larger one? Yes; the rule is *Modulitos?*

$$a \equiv b \pmod{m} \quad \text{and} \quad a \equiv b \pmod{n} \iff a \equiv b \pmod{\operatorname{lcm}(m, n)}, \qquad \text{integers } m, n > 0. \qquad (4.41)$$

For example, if we know that $a \equiv b$ modulo 12 and 18, we can safely conclude that $a \equiv b \pmod{36}$. The reason is that if $a - b$ is a common multiple of m and n, it is a multiple of $\operatorname{lcm}(m, n)$. This follows from the principle of unique factorization.

The special case $m \perp n$ of this law is extremely important, because $\operatorname{lcm}(m, n) = mn$ when m and n are relatively prime. Therefore we will state it explicitly:

$$a \equiv b \pmod{mn} \iff a \equiv b \pmod{m} \text{ and } a \equiv b \pmod{n}, \quad \text{if } m \perp n. \qquad (4.42)$$

For example, $a \equiv b \pmod{100}$ if and only if $a \equiv b \pmod{25}$ and $a \equiv b \pmod{4}$. Saying this another way, if we know $x \bmod 25$ and $x \bmod 4$, then we have enough facts to determine $x \bmod 100$. This is a special case of the *Chinese Remainder Theorem (see* exercise 30), so called because it was discovered by Sun Tsŭ in China, about A.D. 350.

The moduli m and n in (4.42) can be further decomposed into relatively prime factors until every distinct prime has been isolated. Therefore

$$a \equiv b \pmod{m} \iff a \equiv b \pmod{p^{m_p}} \quad \text{for all } p,$$

if the prime factorization (4.11) of m is $\prod_p p^{m_p}$. Congruences modulo powers of primes are the building blocks for all congruences modulo integers.

4.7 INDEPENDENT RESIDUES

One of the important applications of congruences is a *residue number* system, in which an integer x is represented as a sequence of residues (or remainders) with respect to moduli that are prime to each other:

$$\operatorname{Res}(x) = (x \bmod m_1, \ldots, x \bmod m_r), \qquad \text{if } m_j \perp m_k \text{ for } 1 \leqslant j < k \leqslant r.$$

Knowing $x \bmod m_1, \ldots, x \bmod m_r$ doesn't tell us everything about x. But it does allow us to determine $x \bmod m$, where m is the product $m_1 \ldots m_r$.

In practical applications we'll often know that x lies in a certain range; then we'll know everything about x if we know $x \bmod m$ and if m is large enough.

For example, let's look at a small case of a residue number system that has only two moduli, 3 and 5:

x mod 15	cmod3	‹ mod 5
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Each ordered pair (x mod 3, x mod 5) is different, because $x \bmod 3 = y \bmod 3$ and $x \bmod 5 = y \bmod 5$ if and only if $x \bmod 15 = y \bmod 15$.

We can perform addition, subtraction, and multiplication on the two components *independently,* because of the rules of congruences. For example, if we want to multiply $7 = (1,2)$ by $13 = (1,3)$ modulo 15, we calculate $1 \cdot 1 \bmod 3 = 1$ and $2 \cdot 3 \bmod 5 = 1$. The answer is $(1,1) = 1$; hence $7 \cdot 13 \bmod 15$ must equal 1. Sure enough, it does.

This independence principle is useful in computer applications, because different components can be worked on separately (for example, by different computers). If each modulus m_k is a distinct prime p_k, chosen to be slightly less than 2^{31}, then a computer whose basic arithmetic operations handle integers in the range $[-2^{31}\ 2^{31})$ can easily compute sums, differences, and products modulo pk. A set of r such primes makes it possible to add, subtract, and multiply "multiple-precision numbers" of up to almost 31 r bits, and the residue system makes it possible to do this faster than if such large numbers were added, subtracted, or multiplied in other ways.

For example, *the Mersenne prime* $2^{31} - 1$ works well.

We can even do division, in appropriate circumstances. For example, suppose we want to compute the exact value of a large determinant of integers. The result will be an integer D, and bounds on $|D|$ can be given based on the size of its entries. But the only fast ways known for calculating determinants

require division, and this leads to fractions (and loss of accuracy, if we resort to binary approximations). The remedy is to evaluate D mod $p_k = D_k$, for various large primes p_k. We can safely divide modulo p_k unless the divisor happens to be a multiple of pk. That's very unlikely, but if it does happen we can choose another prime. Finally, knowing D_k for sufficiently many primes, we'll have enough information to determine D.

But we haven't explained how to get from a given sequence of residues (x mod $m_1, \ldots,$ x mod m,) back to x mod m. We've shown that this conversion can be done in principle, but the calculations might be so formidable that they might rule out the idea in practice. Fortunately, there is a reasonably simple way to do the job, and we can illustrate it in the situation (x mod 3,x mod 5) shown in our little table. The key idea is to solve the problem in the two cases (1,0) and (0,1); for if (1,0) = a and (0,1) = b, then (x, y) = (ax + by) mod 15, since congruences can be multiplied and added.

In our case a = 10 and b = 6, by inspection of the table; but how could we find a and b when the moduli are huge? In other words, if $m \perp n$, what is a good way to find numbers a and b such that the equations

$$a \bmod m = 1, \quad a \bmod n = 0, \quad b \bmod m = 0, \quad b \bmod n = 1$$

all hold? Once again, (4.5) comes to the rescue: With Euclid's algorithm, we can find m' and n' such that

$$m'm + n'n = 1.$$

Therefore we can take a = n'n and b = m'm, reducing them both mod mn if desired.

Further tricks are needed in order to minimize the calculations when the moduli are large; the details are beyond the scope of this book, but they can be found in [174, page 274]. Conversion from residues to the corresponding original numbers is feasible, but it is sufficiently slow that we save total time only if a sequence of operations can all be done in the residue number system before converting back.

Let's firm up these congruence ideas by trying to solve a little problem: How many solutions are there to the congruence

$$x^2 \equiv 1 \pmod m, \tag{4.43}$$

if we consider two solutions x and x' to be the same when $x \equiv x'$?

According to the general principles explained earlier, we should consider first the case that m is a prime power, p^k, where $k > 0$. Then the congruence $x^2 \equiv 1$ can be written

$$(x-1)(x+1) \equiv 0 \pmod{p^k},$$

so p must divide either $x - 1$ or $x + 1$, or both. But p can't divide both $x - 1$ and $x + 1$ unless $p = 2$; we'll leave that case for later. If $p > 2$, then $p^k \backslash (x - 1)(x + 1) \iff p^k \backslash (x - 1)$ or $p^k \backslash (x + 1)$; so there are exactly two solutions, $x \equiv +1$ and $x \equiv -1$.

The case $p = 2$ is a little different. If $2^k \backslash (x - 1)(x + 1)$ then either $x - 1$ or $x + 1$ is divisible by 2 but not by 4, so the other one must be divisible by 2^{k-1}. This means that we have four solutions when $k \geqslant 3$, namely $x \equiv \pm 1$ and $x \equiv 2^{k-1} \pm 1$. (For example, when $p^k = 8$ the four solutions are $x \equiv 1, 3, 5, 7 \pmod 8$; it's often useful to know that the square of any odd integer has the form $8n + 1$.)

Now $x^2 \equiv 1 \pmod m$ if and only if $x^2 \equiv 1 \pmod{p^{m_p}}$ for all primes p with $m_p > 0$ in the complete factorization of m. Each prime is independent of the others, and there are exactly two possibilities for x mod p^{m_p} except when $p = 2$. Therefore if m has exactly r different prime divisors, the total number of solutions to $x^2 \equiv 1$ is 2^r, except for a correction when m. is even. The exact number in general is

All primes are odd except 2, which is the oddest of all.

$$2^{r+[8\backslash m]+[4\backslash m]-[2\backslash m]} \tag{4.44}$$

For example, there are four "square roots of unity modulo 12," namely 1, 5, 7, and 11. When $m = 15$ the four are those whose residues mod 3 and mod 5 are ± 1, namely $(1, 1), (1, 4), (2, 1)$, and $(2, 4)$ in the residue number system. These solutions are 1, 4, 11, and 14 in the ordinary (decimal) number system.

4.8 ADDITIONAL APPLICATIONS

There's some unfinished business left over from Chapter 3: We wish to prove that the m numbers

$$0 \bmod m,\ n \bmod m,\ 2n \bmod m,\ \ldots\ (m-1)n \bmod m \tag{4.45}$$

consist of precisely d copies of the m/d numbers

$$0,\ d,\ 2d,\ \ldots\ m-d$$

in some order, where $d = \gcd(m, n)$. For example, when $m = 12$ and $n = 8$ we have $d = 4$, and the numbers are 0, 8, 4, 0, 8, 4, 0, 8, 4, 0, 8, 4.

The first part of the proof-to show that we get d copies of the first m/d values-is now trivial. We have

Mathematicians love to say that *things* are trivial.

$$jn \equiv kn \pmod m \iff j(n/d) \equiv k(n/d) \pmod{m/d}$$

by (4.38); hence we get d copies of the values that occur when $0 \leqslant k < m/d$.

Now we must show that those m/d numbers are $\{0, d, 2d, \ldots, m - d\}$ in some order. Let's write $m = m'd$ and $n = n'd$. Then $kn \bmod m = d(kn' \bmod m')$, by the distributive law (3.23); so the values that occur when $0 \leqslant k < m'$ are d times the numbers

$$0 \bmod m',\ n' \bmod m',\ 2n' \bmod m',\ \ldots,\ (m' - 1)n' \bmod m' .$$

But we know that $m' \perp n'$ by (4.27); we've divided out their gcd. Therefore we need only consider the case $d = 1$, namely the case that m and n are relatively prime.

So let's assume that $m \perp n$. In this case it's easy to see that the numbers (4.45) are just $\{0, 1, \ldots, m - 1\}$ in some order, by using the "pigeonhole principle!' This principle states that if m pigeons are put into m pigeonholes, there is an empty hole if and only if there's a hole with more than one pigeon. (Dirichlet's box principle, proved in exercise 3.8, is similar.) We know that the numbers (4.45) are distinct, because

$$jn \equiv kn \pmod m \iff j \equiv k \pmod m$$

when $m \perp n$; this is (4.37). Therefore the m different numbers must fill all the pigeonholes $0, 1, \ldots, m - 1$. Therefore the unfinished business of Chapter 3 is finished.

The proof is complete, but we can prove even more if we use a direct method instead of relying on the indirect pigeonhole argument. If $m \perp n$ and if a value $j \in [0, m)$ is given, we can explicitly compute $k \in [0, m)$ such that $kn \bmod m = j$ by solving the congruence

$$kn \equiv j \pmod m$$

for k. We simply multiply both sides by n', where $m'm + n'n = 1$, to get

$$k \equiv jn' \pmod m ;$$

hence $k = jn' \bmod m$.

We can use the facts just proved to establish an important result discovered by Pierre de Fermat in 1640. Fermat was a great mathematician who contributed to the discovery of calculus and many other parts of mathematics. He left notebooks containing dozens of theorems stated without proof, and each of those theorems has subsequently been verified-except one. The one that remains, now called "Fermat's Last Theorem," states that

$$a^n + b^n \neq c^n \tag{4.46}$$

[EULER]

Euler [93] conjectured that $a^4 + b^4 + c^4 \neq d^4$, but Noam Elkies found infinitely many solutions in August, 1987. Now Roger Frye has done an exhaustive computer search, proving (after about 110 hours on a Connection Machine) that the smallest solution is:

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

for all positive integers a, b, c, and n, when $n > 2$. (Of course there are lots of solutions to the equations $a + b = c$ and $a^2 + b^2 = c^2$.) This conjecture has been verified for all $n \leqslant 150000$ by Tanner and Wagstaff [285].

Fermat's theorem of 1640 is one of the many that turned out to be provable. It's now called Fermat's Little Theorem (or just Fermat's theorem, for short), and it states that

$$n^{p-1} \equiv 1 \pmod{p}, \qquad \text{if } n \perp p. \tag{4.47}$$

Proof: As usual, we assume that p denotes a prime. We know that the $p-1$ numbers $n \bmod p$, $2n \bmod p$, ... $(p-1)n \bmod p$ are the numbers $1, 2, \ldots, p-1$ in some order. Therefore if we multiply them together we get

$$\begin{aligned} &n \cdot (2n) \cdot \ldots \cdot ((p-1)n) \\ &\quad \equiv (n \bmod p) \cdot (2n \bmod p) \cdot \ldots \cdot ((p-1)n \bmod p) \\ &\quad \equiv (p-1)!, \end{aligned}$$

where the congruence is modulo p. This means that

$$(p-1)!\, n^{p-1} \equiv (p-1)! \pmod{p},$$

and we can cancel the $(p-1)!$ since it's not divisible by p. QED.

An alternative form of Fermat's theorem is sometimes more convenient:

$$n^p \equiv n \pmod{p}, \qquad \text{integer } n. \tag{4.48}$$

This congruence holds for all integers n. The proof is easy: If $n \perp p$ we simply multiply (4.47) by n. If not, $p \backslash n$, so $n^p \equiv 0 \equiv n$.

In the same year that he discovered (4.47), Fermat wrote a letter to Mersenne, saying he suspected that the number

$$f_n = 2^{2^n} + 1$$

". *laquelle* proposition, si *elle* est vraie, est de *très grand usage.*"
-P. de Fermat [97]

would turn out to be prime for all $n \geqslant 0$. He knew that the first five cases gave primes:

$$2^1+1 = 3;\ 2^2+1 = 5;\ 2^4+1 = 17;\ 2^8+1 = 257;\ 2^{16}+1 = 65537;$$

but he couldn't see how to prove that the next case, $2^{32} + 1 = 4294967297$, would be prime.

It's interesting to note that Fermat could have proved that $2^{32} + 1$ is not prime, using his own recently discovered theorem, if he had taken time to perform a few dozen multiplications: We can set $n = 3$ in (4.47), deducing that

$$3^{2^{32}} \equiv 1 \pmod{2^{32}+1}, \qquad \text{if } 2^{32}+1 \text{ is prime.}$$

And it's possible to test this relation by hand, beginning with 3 and squaring 32 times, keeping only the remainders mod $2^{32} + 1$. First we have $3^2 = 9$, then $3^{2^2} = 81$, then $3^{2^3} = 6561$, and so on until we reach

$$3^{2^{32}} \equiv 3029026160 \pmod{2^{32} + 1} .$$

If this is Fermat's Little Theorem, the other one was last but not least.

The result isn't 1, so $2^{32} + 1$ isn't prime. This method of disproof gives us no clue about what the factors might be, but it does prove that factors exist. (They are 641 and 6700417.)

If $3^{2^{32}}$ had turned out to be 1, modulo $2^{32} + 1$, the calculation wouldn't have proved that $2^{32} + 1$ is prime; it just wouldn't have disproved it. But exercise 47 discusses a converse to Fermat's theorem by which we can prove that large prime numbers are prime, without doing an enormous amount of laborious arithmetic.

We proved Fermat's theorem by cancelling $(p - 1)!$ from both sides of a congruence. It turns out that $(p - 1)!$ is always congruent to -1, modulo p; this is part of a classical result known as Wilson's theorem:

$$(n - 1)! \equiv -1 \pmod{n} \iff n \text{ is prime}, \quad \text{if } n > 1. \tag{4.49}$$

One half of this theorem is trivial: If $n > 1$ is not prime, it has a prime divisor p that appears as a factor of $(n - 1)!$, so $(n - 1)!$ cannot be congruent to -1. (If $(n - 1)!$ were congruent to -1 modulo n, it would also be congruent to -1 modulo p, but it isn't.)

The other half of Wilson's theorem states that $(p - 1)! \equiv -1 \pmod{p}$. We can prove this half by pairing up numbers with their inverses mod p. If $n \perp p$, we know that there exists n' such that

$$n'n \equiv 1 \pmod{p};$$

here n' is the inverse of n, and n is also the inverse of n'. Any two inverses of n must be congruent to each other, since $nn' \equiv nn''$ implies $n' \equiv n''$.

If p is *prime, is* p' *prime prime?*

Now suppose we pair up each number between 1 and p-1 with its inverse. Since the product of a number and its inverse is congruent to 1, the product of all the numbers in all pairs of inverses is also congruent to 1; so it seems that $(p - 1)!$ is congruent to 1. Let's check, say for p = 5. We get 4! = 24; but this is congruent to 4, not 1, modulo 5. Oops- what went wrong? Let's take a closer look at the inverses:

$$1' = 1, \quad 2' = 3, \quad 3' = 2, \quad 4' = 4.$$

Ah so; 2 and 3 pair up but 1 and 4 don't-they're their own inverses.

To resurrect our analysis we must determine which numbers are their own inverses. If x is its own inverse, then $x^2 \equiv 1 \pmod{p}$; and we have

already proved that this congruence has exactly two roots when $p > 2$. (If $p = 2$ it's obvious that $(p-1)! \equiv -1$, so we needn't worry about that case.) The roots are 1 and $p-1$, and the other numbers (between 1 and $p-1$) pair up; hence

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1,$$

as desired.

Unfortunately, we can't compute factorials efficiently, so Wilson's theorem is of no use as a practical test for primality. It's just a theorem.

4.9 PHI AND MU

How many of the integers $\{0, 1, \ldots, m-1\}$ are relatively prime to m? This is an important quantity called $\varphi(m)$, the "totient" of m (so named by J. J. Sylvester [284], a British mathematician who liked to invent new words). We have $\varphi(1) = 1$, $\varphi(p) = p-1$, and $\varphi(m) < m-1$ for all composite numbers m.

The φ function is called Euler's totient *function*, because Euler was the first person to study it. Euler discovered, for example, that Fermat's theorem (4.47) can be generalized to nonprime moduli in the following way:

"Si fuerit N ad x numerus *primus* et n numerus *partium* ad N *primarum, tum* potestas x^n *unitate minuta semper per numerum* N *erit divisibilis."*
—*L.* Euler *[89]*

$$n^{\varphi(m)} \equiv 1 \pmod{m}, \qquad \text{if } n \perp m. \tag{4.50}$$

(Exercise 32 asks for a proof of Euler's theorem.)

If m is a prime power p^k, it's easy to compute $\varphi(m)$, because $n \perp p^k \iff p \nmid n$. The multiples of p in $\{0, 1, \ldots, p^k - 1\}$ are $\{0, p, 2p, \ldots, p^k - p\}$; hence there are p^{k-1} of them, and $\varphi(p^k)$ counts what is left:

$$\varphi(p^k) = p^k - p^{k-1}$$

Notice that this formula properly gives $\varphi(p) = p-1$ when $k = 1$.

If $m > 1$ is not a prime power, we can write $m = m_1 m_2$ where $m_1 \perp m_2$. Then the numbers $0 \leqslant n < m$ can be represented in a residue number system as $(n \bmod m_1, n \bmod m_2)$. We have

$$n \perp m \iff n \bmod m_1 \perp m_1 \text{ and } n \bmod m_2 \perp m_2$$

by (4.30) and (4.4). Hence, n mod m is "good" if and only if n mod m_1 and n mod m_2 are both "good," if we consider relative primality to be a virtue. The total number of good values modulo m can now be computed, recursively: It is $\varphi(m_1)\varphi(m_2)$, because there are $\varphi(m_1)$ good ways to choose the first component n mod m_1 and $\varphi(m_2)$ good ways to choose the second component n mod m_2 in the residue representation.