Chapter 3
Number Theory Background

Primes and Divisibility

Even in ancient times, people were fascinated by the idea of divisibility. This book is interested primarily in positive integers, just as Euclid was.

Definition 3.1. A positive integer a is said to be a divisor of another positive integer b if $b=ac$ for some positive integer c. (If a is a divisor of b, we write $a|b$ and say "a divides b," or "b is a multiple of a").
Definition 3.2. If an integer $p>1$ has only 1 and p as divisors, it is called prime (for example 2, 3, 4, 7, and 11 are primes).

Two elementary facts help illuminate the place of primes among the integers. First, if $p_1, p_2, ..., p_n$ are primes, then $N=1+p_1p_2...p_n$ is not divisible by any of $p_1, p_2, ..., p_n$ (the remainder when N is divided by any p_i is 1). Thus either N is prime or N has a prime divisor other than the p_i. Thus,

Theorem 3.3. (Euclid). There are infinitely many primes.

Also, if $n>1$ is not prime (such an integer is called composite), n must have a prime divisor $\leq \sqrt{n}$, since it must have a divisor $\leq \sqrt{n}$ ($n = ab$ implies $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$), and that divisor is either prime a or has a prime divisor $\leq \sqrt{n}$. Thus, one can determine if a number $\leq \sqrt{n}$ is prime by eliminating all multiples of the primes $\leq \sqrt{n}$. This method is known as the Sieve of Eratosthenes (Figure 3.1).

For example, all primes < $169=13^2$ can be determined by crossing out the multiples of 2, 3, 4, 7, and 11. Indeed, given that every even integer > 2 is composite (since divisible by 2) and every integer >5 is composite (since divisible by 5), one need only consider integers with last digit 1, 3, 7, or 9 and cross out the multiples of 3, 7, and 11. That process is illustrated in the animated Figure 3.1.

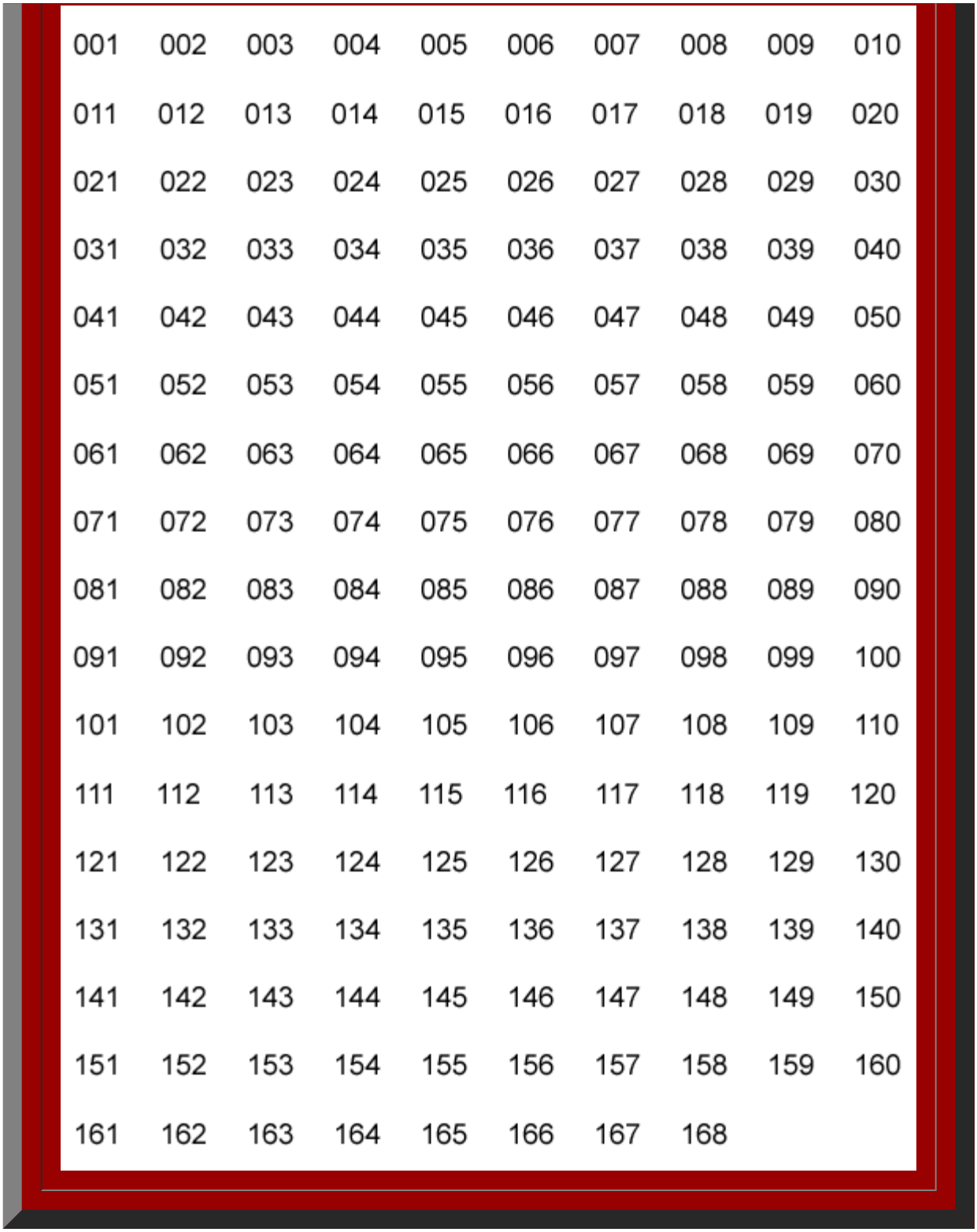

Figure 3.1. Animated Sieve of Eratosthenes. Primes are sifted out that are less than $169 = 13^2$. Thus, only multiples of 2, 3, 5, 7, and 11 need be eliminated. The animation shows the successive elimination of these multiples to reveal the set of all primes less than 169. Click here to see a movie in which the reader can control the animation rate in order to study pattern.

The primes are the building blocks of the integers, since every positive integer can be written uniquely as a product of primes (Fundamental Theorem of Arithmetic). This uniqueness extends only to the primes involved and how many times they are involved; for example, the fact that $12 = 2\cdot2\cdot3 = 2\cdot3\cdot2 = 3\cdot2\cdot2$ does not violate uniqueness. By convention, we say that 1 is a product of no primes. It is the desire for unique

factorization that led to the avoidance of 1 as a prime; obviously, 1 can be included in a factorization of a number as often as desired.

Take a side trip to an application that employs a strategy that is abstractly similar to the method of Eratosthenes. It does so, however, in the urban setting of downtown Ann Arbor, Michigan.

The Euclidean Algorithm

Almost as important as knowing what divisors an integer has is knowing what divisors it shares with other integers. For this allows the consideration of equations relating one integer to another.

Definition 3.4. Let a, b be two positive integers. The greatest common divisor (a, b) of these two integers is the largest positive integer d such that $d|a$ and $d|b$.

> For example $(12, 16) = 4$ since $4|12$ $4|16$, and no greater divisor of 12 (6, 12 are possibilities) is a divisor of 16.

The greatest common divisor is useful in reducing fractions to lowest terms, since if a/b is a fraction $[a/(a,b)]/[b/(a,b)]$ is in lowest terms.

> For example, $12/16 = [12/4]/[16/4] = ¾$.

Definition 3.5. The above definition can be extended to any integer as follows
1. if a and b are integers, neither of which is equal to 0, then $(a, b) = (|a|, |b|)$
2. if $a \neq 0$, then $(a, 0) = |a|$ ((0,0) is not defined).

If the prime factorizations of a and b are readily available, it is easy to find (a, b).

> For example, if $a = 360 = 2^3 \cdot 3^2 \cdot 5$ and $b = 756 = 2^2 \cdot 3^3 \cdot 7$, then $(a,b) = 2^2 \cdot 3^2 = 36$, since the highest power of 2 which is a factor of (a, b) is the lowest power of 2 in the factorizations of a and b (*i.e.* the 2^2 in b).

Unfortunately, it is not always obvious what the prime factorizations of a and b are when the problem of finding (a, b) occurs. A method that is relatively quick and always successful is called the Euclidean Algorithm. It depends on some easy properties of divisibility, familiar from grade school arithmetic and high school algebra.

Suppose a and b are positive integers, $a > b$. Then there are integers q (quotient) and r (remainder) such that $a = bq + r$ and $0 \leq r < b$ (these were first encountered when learning long division in the fourth grade).

> For example, $756 = 360(2) + 36$; in fourth grade terms, if we want to computer 756/360, the quotient is 2, the remainder 36.

This division algorithm is closely related to the idea of greatest common divisor, as the following mini-theorem demonstrates.

Mini-Theorem 3.6. Suppose a, b, r are positive integers with $a = bq + r$, $0 < r < b < a$. Then $(a,b) = (b, r)$.
Proof: It is only necessary to show that a, b, r share exactly the same divisors, since then they certainly have the same GREATEST common divisor.

> 1. First, suppose $n|a$ and $n|b$, say $a = nx$ and $b = ny$. Then $r = a - bq = nx - nyq = n(x - yq)$, so $n|r$.
> 2. Suppose $n|b$ and $n|r$, say $b = ny$ and $r = nz$. Then $a = bq + r = nyq + nz = n(yq + z)$, so $n|a$.

Mini-Fact 3.7. If $a = bq$, then $(a,b) = b$.

These two small facts are all we need to prove the famous

Euclidean Algorithm 3.8. Suppose a, b are positive integers with $a > b$. Suppose further that

$$\begin{aligned} a &= bq_0 + r_1 & 0 &< r_1 < b \\ b &= r_1q_1 + r_2 & 0 &< r_2 < r_1 \\ r_1 &= r_2q_2 + r_3 & 0 &< r_3 < r_2 \\ &\ldots \\ r_{n-1} &= r_nq_n + r_{n+1} & 0 &< r_{n+1} < r_n \\ r_n &= r_{n+1}q_{n+1} \end{aligned}$$

Then $(a, b) = r_{n+1}$, the last non-zero remainder in the process.

Proof: First note that the process defined above is a finite one, since each remainder is smaller than the previous one, with the result that eventually, the integer remainder must become 0. (Computer scientists might be interested in Lamé's Theorem, which proves that this process can take at most $5n$ steps, where n is the number of decimal digits in b.)

By the mini-fact, $(r_n, r_{n+1}) = r_{n+1}$. But, by the mini-theorem, $(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, r_{n+1})$. Therefore, $(a, b) = r_{n+1}$.

For example,

$$\begin{aligned} 756 &= 360(2) + 36 \\ 360 &= 36(10) \end{aligned}$$

so that $(756, 360) = 36$

It is always possible to express (a, b) as $ma + nb$ for some integers m and n. That this is true can be seen from the Euclidean Algorithm as follows:
$(a, b) = r_{n+1} = r_{n-1} - r_nq_n = r_{n-1} - (r_{n-2} - r_{n-1}q_{n-1})q_n = \ldots$.

That is, one can work backwards through the equations until (a, b) is expressed in terms of a and b. But the computations appear quite difficult, and it appears that all the quotients and remainders are needed. But the computation can be done more easily if each remainder is expressed in terms of a and b as the Euclidean Algorithm is carried out. Note that

$$\begin{aligned} a &= 1(a) + 0(b) \\ b &= 0(a) + 1(b) \end{aligned}$$

Then since

$$\begin{aligned} r_1 &= a - bq_0, \\ a &= 1(a) + 0(b) \\ -q_0b &= -q_0(a) - q_0(1)(b) \end{aligned}$$

Subtracting

$$r_1 = a - q_0 b = 1a - q_0 b$$

This process can be continued for each remainder.

In fact, the *a* and *b* can be left understood and only their coefficients kept track of. A detailed example follows.

Example. Find d = (6888, 792), and find m, n such that 6888m + 792n = d.

First computation 6888 = 792(8) + 552.

Notice
6888 = 1(6888) + 0(792)
792 = 0(6888) + 1(792)
552 = 6888 - 8(792) = [1 - 8(0)]6888 + [0 - 8(1)]
(792) = 1(6888) - 8(792)

so we retain the following information

	6888	1	0
	792	0	1
6888 = 792(8) + 552	552	1	-8

noting that 1 - 8(0) = 1 and 0 - 8(1) = -8 so row 3 above is obtained by subtracting 8(row 2) from row 1.

Second computation 792 = 552(1) + 240.

Notice
240 = 792 - 2(552)
= [0 - 1(1)]6888 + [1 - 1(-8)](792) = -1(6888) + 9(792)

so we retain the following information

	6888	1	0
	792	0	1
6888 = 792(8) + 552	552	1	-8
792 = 552(1) + 240	240	-1	9

noting row 4 = row 2 - 1(row 3) since 1 is the quotient in the second computation.

Full computation

	6888	1	0
	792	0	1
6888 = 792(8) + 552	552	1	-8
792 = 552(1) + 240	240	-1	9
552 = 240(2) + 72	72	3	-26
240 = 72(3) + 24	24	-10	87
72 = 24(3)			

In each case, an **arbitrary row** is obtained by subtracting the **quotient times the row above** from **the row two rows above**.
The result: (6888, 792) = 24, 24 = -10(6888) + 87(792).

This example is illustrated in the animation in Figure 3.2.

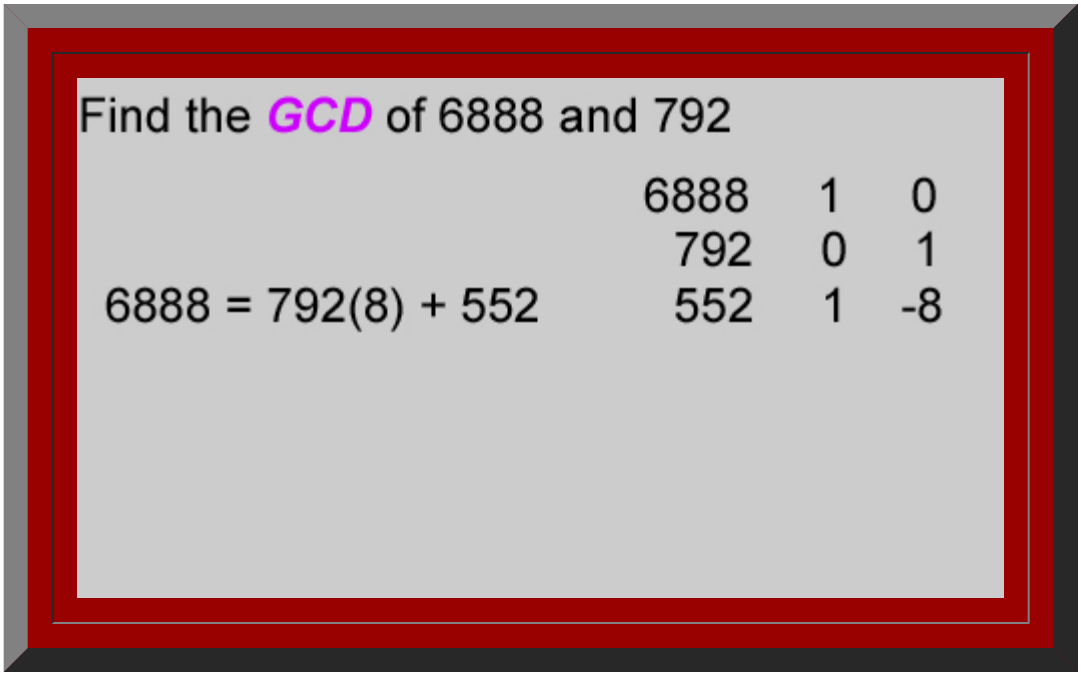

Figure 3.2. Animation of Euclidean Algorithm application. Click here to see a movie in which the reader can control the animation rate in order to study pattern.

The procedure of this section will be of great significance in solving congruences in the next section.

Number-theoretic congruence

One of the most powerful tools of number theory is the notion of congruence, which partitions the integers into finite sets of related integers.

Definition 3.9. Two integers x and y are said to be congruent modulo m (a positive integer) if m is a divisor of $x - y$. This is written $x \equiv y \pmod{m}$.

The most common place the everyday world uses congruence, albeit not consciously, is in telling time. Any time y a multiple of 12 hours after a time x is called by the same time as x.

For example, 60 hours after 3 o'clock, it is once more 3 o'clock, since $60 + 3 \equiv 3$ modulo 12.

Indeed, it is quite common to use a set of small representatives of all the possibilities modulo m. In telling time, 1, 2, ..., 12 are used for all possibilities. Military time uses 0, 1, ..., 23 for the hours in a day modulo 24. Mathematicians usually use 0, 1, ..., m-1 when they want representatives for the classes of numbers which are congruent modulo m, for the following reason.

Theorem 3.10. If $a = mb + r$, $0 \leq r < n$, then $a \equiv r \pmod{m}$.

Proof: $a - r = mb$, so m is a divisor of $a - r$. Thus the natural representative of a number modulo m is its remainder when divided by m.

In fact, any set of m integers, none of which is congruent to any of the others modulo m, is called a complete residue system modulo m. No doubt this name comes from thinking of remainders as residues (what's left over) after division by m. It is easy to create an addition and multiplication for these residues.

Theorem 3.11. Suppose $x \equiv y \pmod m$ and $s \equiv t \pmod m$. Then $x + s \equiv y + t \pmod m$ and $xs \equiv yt \pmod m$.

Proof: Suppose $x - y = am$ and $s - t = bm$. Then $(x + s) - (y + t) = (x - y) + (s - t) = am + bm = (a + b)m$. So $x + s \equiv y + t \pmod m$. Also $xs - yt = (xs - xt) + (xt - yt) = x(s - t) + (x - y)t = xbm + amt = m(xb + at)$ So $xs \equiv yt \pmod m$.

Telling time is an obvious example of the addition part of this theorem. For instance, 5 hours after 9 o'clock comes 2 o'clock, since $9 + 5 \equiv 2 \pmod{12}$.

Linear congruences

The first type of equation to investigate is the linear congruence $ax \equiv b \pmod m$. One needed fact is an easy consequence of the Euclidean Algorithm.

Lemma 3.12. If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Proof: Suppose $bc = ax$. Because $(a, b) = 1$, there are integers m, n such that $1 = ma + nb$. Then $c = cma + cnb = cma + nax = a(cm + nx)$. Thus $a \mid c$.

This allows proof of a limited cancellation theorem. In ordinary algebra, if $ax = ay$, then $x = y$. Such a general theorem is impossible for congruences.

For example, $6(4) \equiv 6(2) \bmod 12$, but 4 is not congruent to 2 mod 12.

However, if $(a, m) = 1$, cancellation is still possible.

Theorem 3.13. If $ax \equiv \pmod m$ and $(a, m) = 1$, then $x \equiv y \pmod m$.

Proof: Since $ax \equiv ay \pmod m$, $a(x - y) \equiv 0 \pmod m$. Thus $m \mid a(x - y)$. But, since $(a, m) = 1$, Lemma 3.12 assures $m \mid (x - y)$. Therefore, $x \equiv y \pmod m$.

This enables a complete analysis of $ax \equiv b \pmod m$ if $(a, m) = 1$.

Theorem 3.14. Suppose $(a, m) = 1$. Then

a) $ax \equiv 1 \pmod m$ has a unique solution $x \equiv t \pmod m$
b) $ax \equiv b \pmod m$ has a unique solution $x \equiv tb \pmod m$.

Proof:

a) Since $(a, m) = 1$, there are integers s, t such that $ms + at = 1$, so $at - 1 = ms$. Therefore $at \equiv 1 \pmod m$. This is the only solution, since by Theorem 3.13 $at \equiv ay \pmod m$ implies $x \equiv y \pmod m$.
b) To solve $ax \equiv b \pmod m$, multiply through by this number t. Therefore $t(ax) \equiv tb \bmod m$. Since $ta \equiv 1 \pmod m$, this gives $x \equiv tb \bmod m$. As before, this solution is unique.

The solution of $ax \equiv 1 \pmod m$ is sometimes called the inverse a^{-1} of a modulo m, analogous to the fact that $a^{-1} = 1/a$ is the multiplicative inverse of a in ordinary arithmetic. Of course, a natural question arises: what happens if $(a, m) \neq 1$. There are two cases: $(a, m) \mid b$ and $(a, m) \nmid b$.

Theorem 3.15. Suppose $d = (a, m) \nmid b$. Then $ax \equiv b \pmod m$ has no solution.

Proof: If $ax \equiv b \pmod m$, then $ax - b = my$ for some integer y. Thus $b = ax - my$. But since $d \mid a$ and $d \mid m$, this means $d \mid b$, contrary to the theorem's hypothesis. (Note: $a = ds$, $m = dt$ means $b = dsn - dty = d(sx - ty)$.)

Theorem 3.16. Suppose $d = (a, m) \mid b$. Then $ax \equiv b \pmod m$ has a unique solution modulo $m \mid d$ and d solutions modulo m.

Proof: Let $b = dr$, $a = ds$, $m = dt$. Then $ax \equiv b \pmod m$ is and only if $ax - b = my$ for some integer y. Substituting for a, b, $cdsx - ds = dty$. Canceling $xs - r = ty$ or $sx \equiv r \pmod t$. By Theorem 3.14, this has a unique solution modulo $t = m/d$. Call this solution A (so $sA \equiv r \pmod t$). Then, A, $A + t$, ..., $A + (d-1)t$ are the d solutions (modulo m). Note that these are all congruent modulo t but incongruent modulo m, and notice that since $sA - r = tB$ for some B

$s(A+kt) - r = t(B+sk)$, $k=0, 1, ..., d-1$
$ds(A+kt) - dr = dt(B+sk)$, $k=0, 1, ..., d-1$
$a(A+kt) - b = m(B+sk)$, $k=0, 1, ..., d-1$
$a(A+kt) \equiv b \pmod m$, $k=0, 1, ..., d-1$

Fermat's Little Theorem and Euler's Theorem

The ability to solve congruences leads to some interesting results.

Theorem 3.17 (Fermat's Little Theorem) Suppose p is a prime, $(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod p$.

Proof: Consider the integers a, $2a$, $3a$, ..., $(p-1)a$. These $p-1$ integers are all incongruent mod p, since by Theorem 3.13 $sa \equiv ta \pmod p$ implies $s \equiv t \pmod p$. Since none of them is divisible by p (by Lemma 3.12, if $p \mid ka$, then $p \mid k$, which is false). Thus these $p - 1$ integers are congruent to the integers 1, 2, ..., $p-1$ in some order. Therefore, $a(2a)...(p-1)a \equiv 1(2)...(p-1) \pmod p$. By Theorem 3.13, cancellation of $2(3)...(p-1)$ gives $a^{p-1} \equiv 1 \pmod p$.

Fermat's Little Theorem can be used to perform some amazing computations. For example, it can be used to compute the remainder when 3^{2460} is divided by 113, certainly a computation unlikely by direct computation. But Theorem 3.17 assures $3^{112} \equiv 1 \pmod{113}$. Simple division gives $2460 = 112(13) + 4$. Therefore $3^{2460} = 3^{112(13)+4} = (3^{112})^{13} 3^4 \equiv 3^4 \equiv 81 \bmod 113$. So the remainder when 3^{2460} is divided by 113 is 81.

The situation of Theorem 3.17 can be generalized.

Definition 3.18. Let m be a positive integer. A complete reduced residue system modulo m is the set of numbers obtained from a complete residue system by removing all the integers which have a factor in common with m.

For example, the integers 1, 2, ..., $p-1$ are a reduced residue system modulo a prime p. Also, the integers 1, 3, 7, 11, 13, 17, 19 for a reduced residue system modulo 20.

Definition 3.19. The Euler ϕ - function (phi-function) $\phi(m)$ (or, phi(m) in subscripts or superscripts) is the number of integers in a complete reduced residue system modulo m.

For example $\phi(p) = p-1$, $\phi(20) = 8$.

The Euler ϕ - function has been studied extensively. The interested reader should consult any of the

numerous number theory texts listed in the references. Fermat's Little Theorem can be generalized as follows:

Theorem 3.20.(Euler's Theorem) Suppose $(a, m) = 1$. Then $a^{\text{phi}(m)} \equiv 1 \pmod{m}$.

Proof: Let $1, x_2, x_3, \ldots, x_{\text{phi}(m)}$ be a reduced residue system modulo m. As in Theorem 3.17, $a, a_2, \ldots, ax_{\text{phi}(m)}$ are all incongruent modulo m; also, since each has no factor in common with m, they form a complete reduced residue system and are congruent to $1, x_2, \ldots, x_{\text{phi}(m)}$ in some order. Therefore $a(ax_2) \ldots (ax_{\text{phi}(m)}) \equiv x_2x_3\ldots x_{\text{phi}(m)} \pmod{m}$, so by cancellation $a^{\text{phi}(m)} \equiv 1 \pmod{m}$.

Again, by way of example, it is easy to compute the remainder when 13^{8059} is divided by 20. By Euler's Theorem, $13^{\text{phi}(20)} = 13^8 \equiv 13^3 \pmod{20}$. But $13^2 = 169 \equiv 9 \pmod{20}$. Therefore $13^3 = 13^2(13) \equiv 9(13) \equiv 117 \equiv 17 \pmod{20}$. Thus the remainder is 17.

Wilson's Theorem and Quadratic Residues

Definition 3.21. Let m be a positive integer, $(a, m) = 1$; a is said to be a quadratic residue modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution.

A great deal of discussion about quadratic residues centers on prime moduli. The case $p = 2$ is not very interesting, since a is a quadratic residue if and only if $a \equiv 1 \pmod{2}$. So odd primes are of the most interest.

Theorem 3.22. Let p be an odd prime. Then the congruence $x^2 \equiv a \pmod{p}$ has either 0 or 2 solutions modulo p.

Proof: If $s^2 \equiv a \pmod{p}$, then $(-s)^2 \equiv a \pmod{p}$, and since p is odd, s and $-s$ are incongruent (mod p). ($s \equiv -s \pmod{p}$ implies $2s \equiv 0 \pmod{p}$.) Thus, if there is one solution, there are two solutions. If t is another solution, then $t^2 \equiv a \equiv s^2 \pmod{p}$. Then $t^2 - s^2 \equiv 0 \pmod{p}$, so $(t - s)(t + s) \equiv 0 \pmod{p}$. Thus p is a divisor of either $t - s$ or $t + s$, so either $t \equiv s \pmod{p}$ or $t \equiv -s \pmod{p}$. So there are no other solutions.

A surprising consequence of this simple fact is

Theorem 3.23 (Wilson's Theorem) If p is a prime, then $(p - 1)! \equiv -1 \pmod{p}$.

Proof: If $p = 2$, this just says $1 \equiv -1 \pmod{2}$, which is true. If p is an odd prime, the congruence $x^2 \equiv 1 \pmod{p}$ has the two solutions $x \equiv 1 \pmod{p}$ and $x \equiv -1 \equiv p - 1 \pmod{p}$. If a is an integer between 2 and $p - 2$, then the congruence $ax \equiv 1 \pmod{p}$ has a unique solution by Theorem 3.14, and that solution is not congruent to a modulo p, or a would satisfy $a^2 \equiv 1 \pmod{p}$, not possible by Theorem 3.22. Thus the integers $2, \ldots, (p - 2)$ can be grouped into $(p-3)/2$ pairs (a_i, a_i^{-1}), $1 \leq i \leq (p-3)/2$ such that for each i, $(a_i, a_i^{-1}) \equiv 1 \pmod{p}$. Thus the product $(p-1)! \equiv 1(p-1)(a_i, a_i^{-1})\ldots(a_k, a_k^{-1}) \equiv p - 1 \equiv -1 \pmod{p}$, where $k = (p-3)/2$.

Quadratic Residues and Euler's Criterion

Suppose p is an odd prime. Clearly $1^2, 2^2, \ldots, ((p - 1)/2)^2$ are all quadratic residues. Further, if $1 \leq x,y \leq (p - 1)/2$, then x^2 and y^2 are incongruent modulo p, since $x^2 \equiv y^2 \pmod{p}$ implies $(x-y)(x+y) \equiv 0 \pmod{p}$; but then either $p|(x-y)$ and $x = y$ or $p|(x+y)$, which is impossible since $2 \leq x+y \leq p - 1$. So there are $(p - 1)/2$ quadratic residues accounted for. But
$(-1)^2, (-2)^2, \ldots, (-(p - 1)/2)^2$ give the same numbers as $1^2, 2^2, \ldots, ((p - 1)/2)^2$; so since $-(p - 1)/2, \ldots, -1, 1, \ldots, (p-1)/2$ is a complete reduced residue system modulo p, there are exactly $(p - 1)/2$ quadratic residues mod p

and hence there are (p -1)/2 quadratic non-residues modulo p.

Definition 3.24 Legendre symbol. The symbol (a/p), called the Legendre symbol, is defined by (a/p) =

1 if a is a quadratic residue mod p
(-1) if a is not a quadratic residue mod p.

Some number theorists write (0/p)=0. Clearly $0^2 \equiv 0 \pmod p$, but quadratic residues are defined to be relatively prime to the modulus.

Now suppose a is a quadratic residue. Then there is an x with $x^2 = a$. But by Fermat's Little Theorem $x^{p-1} \equiv 1 \pmod p$, so $a^{(p-1)/2} = x^2 \equiv 1 \pmod p$. On the other hand, suppose a is not a quadratic residue. Then, if (r, p)=1, the equation $rx \equiv a \pmod p$ has a unique solution $s \pmod p$ by Theorem 3.14, and s is not congruent to $r \pmod p$ (otherwise a would be a quadratic residue). Thus the elements of the set 1, 2, ..., p -1 can be grouped into (p -1)/2 pairs, where the product of each pair is $\equiv a \pmod p$. Thus $a^{(p-1)/2} \equiv 1(2)...(p-1) \equiv -1$ by Wilson's Theorem. Thus we have proved

Theorem 3.25 Euler's Criterion $(a/p) \equiv a^{(p-1)/2} \pmod p$

This enables one to prove some interesting facts about quadratic residues

Theorem 3.26

a) $(a^2/p) = 1$
b) $(a/p)=(b/p)$ if $a \equiv b \pmod p$
c) $((ab)/p) = (a/p)(b/p)$
d) $(-1/p)=(-1)^{(p-1)/2}$

Proof:
a) and b) are obvious, d) is a restatement of Euler's Criterion for a = 1, and c) follows since $(ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2}$

So -1 is a quadratic residue of primes $p \equiv 1 \pmod 4$, since then (p-1)/2 is even but not of primes $p \equiv 3 \pmod 4$, since then (p-1)/2 is odd. The product of quadratic residues is a quadratic residue, but so is the product of quadratic non-residues. The product of a residue and a non-residue is a non-residue.

For example, if p = 7, the quadratic residues are congruent to 1^2, 2^2, $3^2 \pmod 7$; that is congruent to 1, 2, 4. Note that -1 is not a residue. Since 2 and 4 are residues, so is $2(4) \equiv 1 \pmod 7$. Since 3 and 6 are non-residues, $3(6) \equiv 4 \pmod 7$ is a residue. But $4(6) \equiv 5 \pmod 7$, the product of a residue and a non-residue, is a non-residue.

Similarly, for p = 13 the residues are 1, 3, 4, 9, 10, 12 and the non-residues are 2, 5, 6, 7, 8, 11; $-1 \equiv 12 \pmod{13}$ is a residue, $4(9) \equiv 10 \pmod{13}$ is a residue, $5(6) \equiv 4 \pmod{13}$ is a residue, and $4(7) \equiv 2 \pmod{13}$ is a non-residue.

For p=11, the residues are 1, 3, 4, 5, 9; the non-residues 2, 6, 7, 8, 10.

Quadratic Reciprocity

The most famous theorem relating quadratic residues, the Law of Quadratic Reciprocity, was first proved by Gauss.

Theorem 3.27. Gauss's Law of Quadratic Reciprocity.

If p, q are odd primes $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)} = (-1)^{((p-1)(q-1))/4}$

This theorem has been proved many times in many ways. An example illustrates its power. There are many proofs available on the Internet. Take a look at the linked paper to see one contemporary strategy. Compare the proof of Wilson's Theorem in the linked material to the proof of Wilson's Theorem above in order to gain insight into the strategy in the linked paper. Then, consider the example below and then the proof of the Quadratic Reciprocity law that appears in that link. (Click here, if the link at the beginning of this paragraph fails).

$(p/3)(3/p) = (-1)^{(p-1)(3-1)/4} = (-1)^{(p-1)/2} = (-1/p)$
Therefore, $(p/3)(3/p)(3/p) = (-1/p)(3/p) = (-3/p)$
Therefore $(p/3) = (-3/p)$
But $(p/3) = (1/p)=1$ if $p \equiv 1 \pmod 3$ and $(p/3) = (2/3) = -1$. Thus -3 is a quadratic residue of the primes $p \equiv 1 \pmod 3$ but not of the primes $p \equiv 2 \pmod 3$.

Spatial Synthesis: Centrality and Hierarchy, Volume I, Book 1.
Sandra Lach Arlinghaus and William Charles Arlinghaus