Chapter 1

Congruences and the Quotient Ring of the Integers mod *n*

Monitor to Tegan: "Their language is the language of numbers and they have no need to smile."
Monitor to the Doctor: "Yes, Doctor, you were right. Our numbers were holding the fabric of the universe together."
Dr. Who in Logopolis

Congruences

In this first section, we review a little elementary number theory. We consider congruences mod n and the ring $\mathbb{Z}/n\mathbb{Z}$. We assume that the reader is familiar with some notions from elementary number theory, for example, divisibility of integers and unique factorization into primes. For more information, see Hua [1982], Ireland and Rosen [1982], Rosen [1993], or Stark [1978]. Some references for algebra are Dornhoff and Hohn [1971], Gallian [1990], Gilbert [1976], and Herstein [1964].

Definition. Suppose that n is a positive integer. Then for any integers a, b we say *a is congruent to b modulo n*, written

$$\begin{aligned} a \equiv b \pmod{n} &\Leftrightarrow n \text{ divides } (a-b) \\ &\Leftrightarrow a-b \in n\mathbb{Z} = \text{the ideal of integer multiplies of } n \\ &\Leftrightarrow a \text{ and } b \text{ have the same remainder upon division by } n. \end{aligned} \tag{1}$$

Gauss introduced the congruence notation [in *Disquisitiones Arithmeticae*, 1799]. Consider two integers to be the same if they are congruent modulo n. We will fix n throughout this paragraph. The elements of the quotient ring $\mathbb{Z}/n\mathbb{Z}$ are defined to be the equivalence classes you get upon making this identification. Thus $\mathbb{Z}/n\mathbb{Z}$ is in 1-1 correspondence with the set $\{0, 1, 2, \ldots, n-1\}$. Note

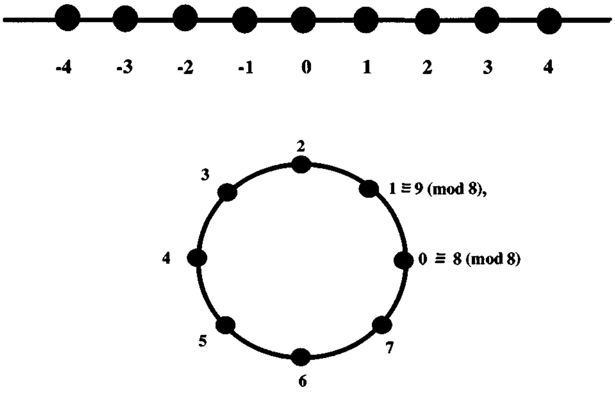

Figure I.2. Rolling up the line of integers into a finite circle.

that here we identify 0 with n. Thus we are taking the integers usually thought of as in a line and rolling that line up into a circle. See Figure I.2.

So we may view $\mathbb{Z}/n\mathbb{Z}$ as the finite circle. Note that we can use other sets of representatives for $\mathbb{Z}/n\mathbb{Z}$ (e.g., $\{1, 2, \ldots, n\}$). In fact we can replace any number j by $j + an$ for some $a \in \mathbb{Z}$.

Define addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ by using + and × in $\mathbb{Z}$ and then taking the remainder of the result upon division by n. Since $\mathbb{Z}/n\mathbb{Z}$ is finite, it is easy to write tables for addition and multiplication. The entry in the ith row and jth column stands for $i + j$ (mod 7) in the addition table (Table I.1) and $i * j$ (mod 7) in the multiplication table (Table I.2).

Exercise. Complete Tables I.1 and I.2. Then the tables for $\mathbb{Z}/12\mathbb{Z}$.

Clearly the addition tables are pretty predictable. Each row is obtained from the one above it by moving everything over 1 and then moving the stuff hanging out at the end back to the beginning.

Table I.1. *Addition mod 7*

+ mod 7	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3					0		
4				0			
5			0				
6		0					

Table I.2. *Multiplication mod 7*

$*$ mod 7	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3			5		
4	0	4		5			
5	0	5	3				
6	0	6					

It is not hard to see that $\mathbb{Z}/n\mathbb{Z}$ forms a commutative group under addition. It is closed under $+$ and $-$, contains 0, and $+$ is associative and commutative. In fact, it is a cyclic group generated by 1, since any element $a \pmod n$ is a sum of a ones.

Moreover, there is a way to visualize this additive group $G = \mathbb{Z}/n\mathbb{Z}$ as the *Cayley graph* obtained as follows. Let $S = \{1, -1 \pmod n\}$. This is a set of generators of G. Take the vertices of the graph to be the elements of G. Draw an edge between two vertices v and w if $w \equiv v+s \pmod n$, $s \equiv \pm 1 \pmod n$. For $n = 8$, we get the graph shown in Fig. I.3, which is just the finite circle graph.

Cayley graphs should actually be directed graphs having edges labeled with the appropriate generator of the group. Since we are taking a symmetric set S of generators of G (i.e., $s \in S$ implies $-s \in S$), we will leave off the directions and draw only one edge between each pair of vertices. We will say more about Cayley graphs in Chapter 3 and elsewhere. References for Cayley graphs are Biggs [1974], Bollobás [1979], and Gallian [1990]. There are connections with finite-state machines or automata [see Dornhoff and Hohn, 1978].

The main application of congruences that we will consider is to Fourier analysis. Replace the real line $\mathbb{R}$ or the circle $\mathbb{T} \cong \mathbb{R}/\mathbb{Z}$ with the finite circle.

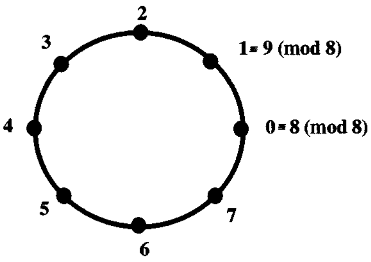

Figure I.3. Cayley graph for additive group $\mathbb{Z}/8\mathbb{Z}$ with generating set $S = \{\pm 1 \pmod 8\}$.

Then the usual Fourier transform or Fourier series can be approximated with the finite Fourier transform.

Of course congruences have numerous applications in computing, error-correcting codes, and cryptography. See Rosen [1993], Schroeder [1986], Knuth [1981], and Szabó and Tanaka [1967]. We will discuss some of these applications later.

What about the multiplication table for $\mathbb{Z}/7\mathbb{Z}$? If you leave out 0 (mod 7), you have a group under multiplication usually denoted $(\mathbb{Z}/7\mathbb{Z})^*$. To see this, you need to see that every $x \not\equiv 0 \pmod 7$ has an inverse $y \pmod 7$ so that $xy \equiv 1 \pmod 7$. For example, $5x \equiv 1 \pmod 7$ has the solution $x \equiv 3 \pmod 7$. So 3 behaves like $1/5$ modulo 7. We say that $\mathbb{Z}/7\mathbb{Z}$ is a field because you can divide by nonzero elements. Here zero means the equivalence class of integers divisible by 7.

By contrast $\mathbb{Z}/12\mathbb{Z}$ is not a field. It is only a ring. For example, $2x \equiv 1 \pmod{12}$ has no solution in integers x. So you cannot divide by 2 in $\mathbb{Z}/12\mathbb{Z}$. A ring is a set in which you can add, subtract, and multiply, but not necessarily divide, with the usual laws of algebra holding. We leave it to you to consider the abstract concepts of ring and field as in Dornhoff and Hohn [1978], Gallian [1990], Gilbert [1976], and Herstein [1964].

Note that if we want to be strictly legal, we should show that our definition of equivalence classes of integers mod n makes sense. That means we should show that

$$a \equiv b \pmod n \quad \text{and} \quad c \equiv d \pmod n$$

implies

$$a + c \equiv b + d \pmod n \quad \text{and} \quad a * c \equiv b * d \pmod n.$$

This is left as an exercise.

Theorem 1. $\mathbb{Z}/n\mathbb{Z}$ is a field, that is, closed under addition, subtraction, multiplication, and division by nonzero elements if and only if n is a prime.

Proof.

$$n = \text{prime} \quad \text{implies} \quad \mathbb{Z}/n\mathbb{Z} = \text{field}.$$

We have to show that if n is prime, we can divide by nonzero elements of $\mathbb{Z}/n\mathbb{Z}$. Suppose that $a \not\equiv 0 \pmod n$. This implies that the greatest common divisor[†] $(a, n) = 1$. But one knows (see the exercise below) that then there are

[†] Here "greatest common divisor" or g.c.d.(a, n) means the largest positive integer dividing both a and n.

integers x and y so that

$$1 = xa + yn.$$

This implies that $ax \equiv 1 \pmod{n}$, that is, that $x \pmod{n}$ is the reciprocal of $a \pmod{n}$.

Exercise.

a) Obtain a constructive proof for the existence of integers x, y such that

$$\text{g.c.d.}(a, n) = xa + yn,$$

using the euclidean algorithm. You can find this in most elementary number theory books (for example, K. Rosen [1993]).

b) Obtain an existence proof for the x, y in Part a using the facts that

$$I = \{ax + ny \mid x, y \in \mathbb{Z}\}$$

is an ideal in the ring $\mathbb{Z}$ and that all ideals in $\mathbb{Z}$ are principal, that is, of the form $d\mathbb{Z}$, for some $d > 0$ which is the least positive element in I. In this case, $d = \text{g.c.d.}(a, n)$. This sort of proof occurs in I. Herstein [1964, p. 18].

$$\mathbb{Z}/n\mathbb{Z} = \text{field} \quad \text{implies} \quad n = \text{prime}.$$

Now we have to show that if n is not a prime then there are integers $a \not\equiv 0 \pmod{n}$ such that the equation $ax \equiv 1 \pmod{n}$ has no solution in integers x. This is easy. If n is not prime, then $n = ab$ with $1 < a, b < n$. Suppose that $ax \equiv 1 \pmod{n}$ has a solution. Then $ax - 1 = abq$, for some $q \in \mathbb{Z}$ and $1 = ax - abq = a(x - bq)$. This says a divides 1, which is impossible. ■

So $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements (also called $\mathbb{F}_p$) if p is a prime. Any finite field has $q = p^r$ elements for some prime p and some positive integer r. See Dornhoff and Hohn [1978], Gallian [1990], Gilbert [1976], Herstein [1964], or Small [1991]. One way to prove this is to show that a finite field must contain some $\mathbb{Z}/p\mathbb{Z}$ as a subfield and then that it is a finite-dimensional vector space over this subfield. See Chapter 3.

The example $\mathbb{Z}/n\mathbb{Z}$ of a quotient ring should be compared with the example of quotient rings formed from $\mathbb{Q}[x]$ = the ring of polynomials with rational coefficients and indeterminate x. The fields $\mathbb{Q}[x]/f(x)\mathbb{Q}[x]$, for $f(x)$ an irreducible polynomial, give all the field extensions of $\mathbb{Q}$ of finite degree. See Herstein [1964].

We could also replace the field of rationals here with a finite field and obtain any finite field as a quotient of polynomial rings over $\mathbb{F}_p$.

Our next task is to consider the structure of a ring like $\mathbb{Z}/12\mathbb{Z}$. This comes out of something called the Chinese remainder theorem, which dates back to Sun Tsu, in the first century A.D. It has numerous computer applications, for example, in writing programs to multiply large integers. First we define the *direct sum of two rings* R and S by

$$R \oplus S = \{(r, s) \,|\, r \in R, s \in S\}. \tag{2}$$

Then define addition and multiplication of vectors componentwise:

$$\begin{aligned}(r, s) + (t, v) &= (r + t, s + v),\\ (r, s) * (t, v) &= (r * t, s * v).\end{aligned}$$

The result is that $R \oplus S$ is also a ring. You can similarly define the direct sum of any number of rings.

Theorem 2 ***(The Chinese Remainder Theorem).*** Suppose that the moduli m_1, $\ldots, m_r$ are pairwise relatively prime, that is, g.c.d.$(m_i, m_j) = 1$ for $i \neq j$. Let $m = m_1 m_2 \cdots m_r$. Then we have the following ring isomorphism:

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}).$$

Proof. The isomorphism T is defined by

$$T(x \bmod m) = (x \bmod m_1, \ldots, x \bmod m_r).$$

Exercise. Check that T is indeed a ring isomorphism, that is, T is a 1-1, onto map that preserves $+$ and $*$. Note that since both sides of the isomorphism have the same number of elements, it suffices (by the pigeon hole principle[†]) to show that the map is either 1-1 or onto. See Dornhoff and Hohn [1978, p. 12]. The easiest is 1-1. You must also check that T is well defined. ■

Note that this is not the proof from the year 1. That proof shows that the map is onto. In fact, there is a song that explains the ancient construction. See Hua

[†] The pigeonhole principle says if you have a set S of n pigeons and a set T of n pigeonholes and a function $f : S \to T$, if f is 1-1, no pigeons can go to the same pigeonhole and so the map must be onto. Similarly if f is onto, it must be 1-1.

[1982, p. 30]:

> Three people walking together, 'tis rare that one be seventy,
> Five cherry blossom trees, twenty one branches bearing flowers,
> Seven disciples reunite for the half-moon,
> Take away (multiple of) one hundred and five and you shall know.

Here the problem is to solve the simultaneous congruences:

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{5}, \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

The meaning of the song is: Multiply by 70 the remainder of x when divided by 3, multiply by 21 the remainder of x when divided by 5, and multiply by 15 (the number of days in half a Chinese month) the remainder of x when divided by 7. Add the three results together and then subtract a multiple of 105 and you get the smallest solution, 23:

$$2 \times 70 + 3 \times 21 + 2 \times 15 = 233 = 23 + 2 \times 105.$$

Where did 70 come from? It is a multiple of 5 and 7 which is congruent to 1 mod 3. Similarly 21 is a multiple of 3 and 7 which is congruent to 1 mod 5. And 15 is a multiple of 3 and 5 that is congruent to 1 mod 7.

It is possible to use the Chinese remainder theorem to add and multiply large integers. See Knuth [1981], Richards [1980], Rosen [1993], or Schroeder [1986], for example. Winograd showed in 1965 how the Chinese remainder theorem could help to do rapid addition (see Dornhoff and Hohn [1978, Sections 5.11 and 5.12]).

Suppose you have a really stupid computer that can only handle the numbers from 1 to 15. You can use the Chinese remainder theorem with moduli 3 and 5. Then each number from 1 to 15 has a place in the rectangle shown in Table I.3.

Table I.3. $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$

	1	2	3	4	5
1	1	7	13	4	10
2	11	2	8	14	5
3	6	12	3	9	15

Table I.4. *How to create Table I.3. Move numbers up a multiple of 3 and left a multiple of 5 places*

	1	2	3	4	5	1	2	3	4	5
1	1									
2		2								
3			3							
1				4						
2					5					
3						6				
1							7			
2								8		
3									9	
1										10
2										
3										

Note that you can fill in the boxes as follows. Make the big table as shown in Table I.4 and move the numbers up a multiple of 3 and left a multiple of 5 places.

Note. This encoding is useful because it behaves well with respect to $+$ and $\times$. So you can multiply numbers ≤ 15 by multiplying much smaller numbers that are ≤ 5. See Knuth [1981, Vol. II, pp. 268–301] for a discussion of how fast we can multiply.

We can use the Chinese remainder theorem to find another visualization of $\mathbb{Z}/15\mathbb{Z}$. Instead of a finite circle or cycle graph, we can consider the product of two finite cycle graphs, which is a finite torus graph. See Figure I.4 for a picture of a continuous torus obtained by rolling up a square piece of material. A finite torus is shown in Figure I.5.

Question. Why are the following rings of order 2^n all different:

$$\mathbb{Z}/2^n\mathbb{Z}, \ (\mathbb{Z}/2\mathbb{Z})^n, \ \mathbb{F}_{2^n}?$$

The additive group of the ring on the left is cyclic $\mathbb{Z}/2^n\mathbb{Z} = \langle 1 \pmod{2^n} \rangle$. See the Cast of Characters or formula (5) in the next section where you have to replace g^n with ng. In the additive groups of the other two rings every nonzero element has order 2, meaning that $2x = 0$ for all $x \neq 0$. The ring on the right

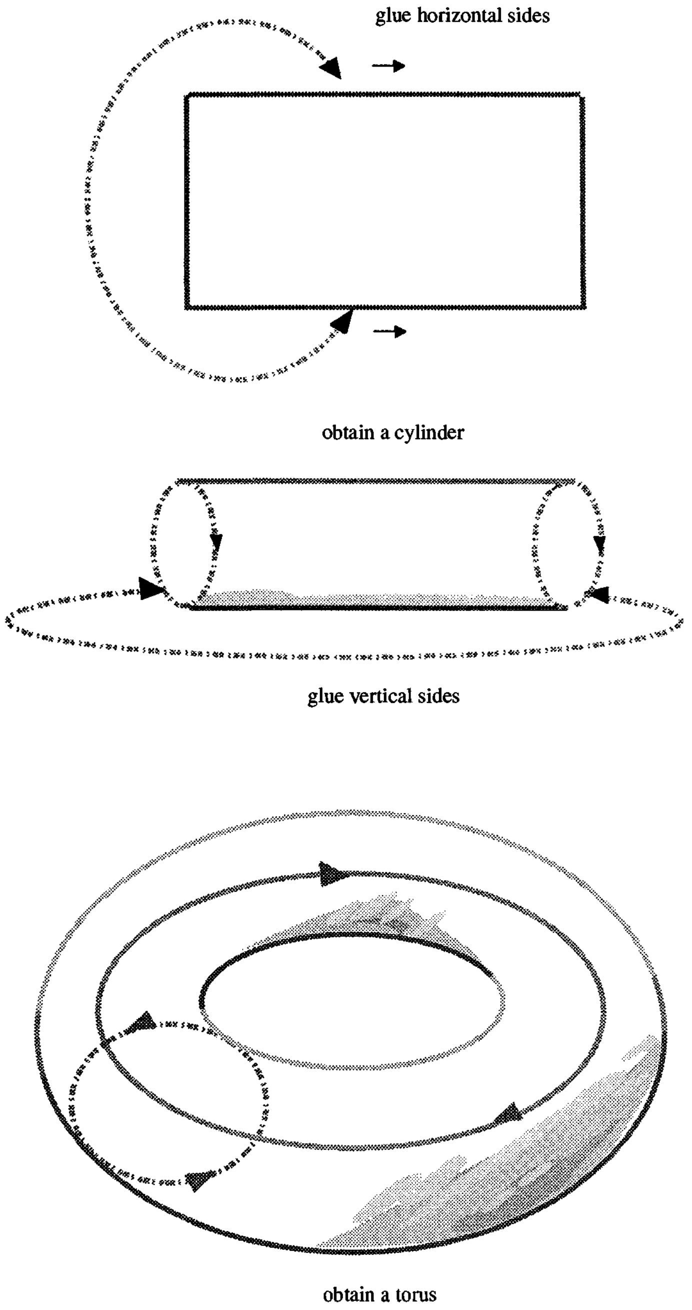

Figure I.4. Continuous torus or doughnut formed from rolling up a rectangle.

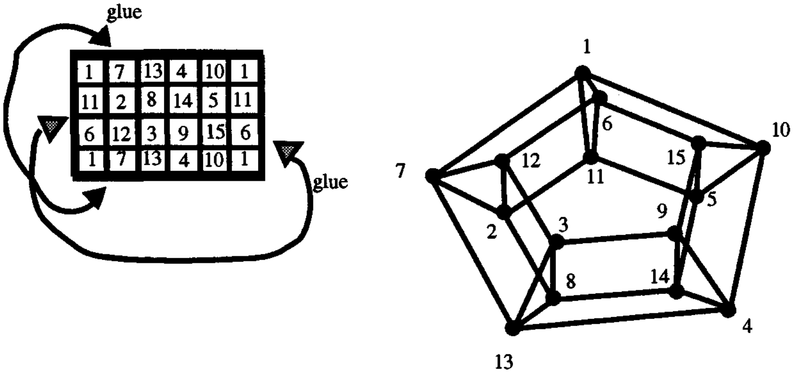

Figure I.5. Finite torus formed from a Cayley graph of $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

is a field and thus has no zero divisors $ab = 0$ with a and b not zero. But the other two rings have zero divisors.

Invertible Elements (for Multiplication) or Units of the Ring $\mathbb{Z}/n\mathbb{Z}$ – Euler's Phi Function

We study the multiplicative group of integers a (mod n) with g.c.d.$(a, n) = 1$.

Definition. The group of *units* of the ring $\mathbb{Z}/n\mathbb{Z}$ is

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^* &= \{a \pmod{n} \mid \text{g.c.d. } (a, n) = 1\} \\ &= \{a \pmod{n} \mid ax \equiv 1 \pmod{n} \text{ has a solution } x \in \mathbb{Z}\}.\end{aligned} \tag{3}$$

Exercise.

a) Prove the last equality. You need to use the property of the greatest common divisor that we used in the proof of Theorem 1.
b) Prove that $(\mathbb{Z}/n\mathbb{Z})^*$ is a group under multiplication.

Examples. We have the following multiplicative groups: $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, 3, \ldots, p-1\}$ for any prime p.

$$(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}, (\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}.$$

Definition. Euler's phi function is

$$\phi(n) = \text{the order of the group } (\mathbb{Z}/n\mathbb{Z})^*. \tag{4}$$

Table I.5. *Euler's phi function*

n	1	2	3	4	5	6	7	8	9	10	11
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10

Examples. See Table I.5.

Exercise. Compute $\phi(n)$ for $12 \leq n \leq 30$. You might want to wait until we have proved a few more facts about Euler's phi function.

Theorem 3. ***Facts about Euler's Phi Function.***

1. If p is a prime, $\phi(p^n) = p^n - p^{n-1}$.
2. If g.c.d. $(n, m) = 1$, then $\phi(nm) = \phi(n)\phi(m)$. This makes the Euler phi function a *multiplicative function*.
3. $$\phi(m) = m \prod_{\substack{p \mid m \\ p = \text{prime}}} \left(1 - \frac{1}{p}\right).$$
4. Suppose x is an integer with g.c.d. $(x, n) = 1$. Then
$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof.

1. By the definitions $\phi(p^n)$ is the number of integers a between 0 and $p^n - 1$ such that g.c.d.$(a, p) = 1$. Equivalently, we can count the numbers a between 0 and $p^n - 1$ such that p divides a and subtract this from p^n. The numbers a with p dividing a such that $0 \leq a \leq p^n - 1$ are
$$0 \cdot p, 1 \cdot p, 2 \cdot p, \ldots, (p^{n-1} - 1) \cdot p.$$
There are p^{n-1} numbers on this list. Thus there are $p^n - p^{n-1}$ elements in $(\mathbb{Z}/p^n\mathbb{Z})^*$.
2. This is really the Chinese remainder theorem. Since
$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z}),$$
we see that $x \pmod{mn}$ is invertible if and only if $x \pmod{n}$ and $x \pmod{m}$ is invertible.
3. We leave the proof of this formula as an exercise.

4. This is a special case of Lagrange's theorem in group theory. See Gallian [1990] or Herstein [1964], for example. If G is a group with r elements, then $x^r =$ the identity of the group, for any $x \in G$. There is another proof of fact 4 to be found in most elementary number theory books (a proof which works for any finite abelian group). In fact, the word "group" seems to be on the censored list for most of these number theory books. ■

Corollary. ***Fermat's Little Theorem.*** Suppose that p is a prime. Then for all $a \in \mathbb{Z}$, we have

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

If p does not divide a, then

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

History

Fermat stated this in 1640 and Euler generalized it in 1760. A special case of Fermat's theorem is that if p is a prime then p divides $2^p - 2$. The ancient Chinese knew this and also believed that the converse was true. They were wrong since, for example, 341 divides $2^{341} - 2$, even though $341 = 11 \cdot 31$. Today a composite integer n such that n divides $2^n - 2$ is called a *pseudoprime* (base 2). The first two pseudoprimes are 341 and 561. There are infinitely many pseudoprimes base 2. See Rosen [1993, p. 193].

There are, in fact, composite numbers n called *Carmichael numbers* such that n divides $b^n - b$ for all b. They are named after the American mathematician who discovered their properties in 1904. In fact 561 is a Carmichael number. Recently (see Cipra [1993, Vol. I]) W. R. Alford, A. Granville, and C. Pomerance have shown that there are infinitely many Carmichael numbers.

Exercise. Show that $\sum_{\substack{0<d \\ d\mid n}} \phi(d) = n$. Here $d|n$ means d divides n, that is, $n = dc$ for some integer c.

Hint. You can use the fact that both sides of the inequality are multiplicative.

Notes. Property 2 makes phi a multiplicative function. There are lots of other multiplicative functions, for example,

$$\sigma_k(n) = \sum_{\substack{0<d \\ d|n}} d^k.$$

Our goal for the moment is to study the structure of the multiplicative groups $(\mathbb{Z}/n\mathbb{Z})^*$ more closely. The simplest groups are the cyclic groups (e.g., the *additive* group $\mathbb{Z}/n\mathbb{Z}$).

Primitive Roots

Definition. A (multiplicative) group G is said to be *cyclic* with *generator* g if every element $x \in G$ has the form $x = g^n$, for some integer n. Write

$$\langle g \rangle = G = \{g^n \mid n \in \mathbb{Z}\}. \tag{5}$$

If the group G is additive we must replace g^n with ng. If G is a finite cyclic group with d elements, then it is easy to see that G is isomorphic to the additive group of $\mathbb{Z}/d\mathbb{Z}$.

Exercise. Prove the last statement. The map $T: G \to \mathbb{Z}/d\mathbb{Z}$ is defined by $T(g^n) = n \pmod{d}$. You need to show that this map is well defined, 1-1, and onto and carries multiplication in G to addition in $\mathbb{Z}/d\mathbb{Z}$.

Definition. The *order* of an element g in a finite group G is the number of elements in (or order of) the subgroup $\langle g \rangle$ generated by g.

Question. When is $(\mathbb{Z}/n\mathbb{Z})^*$ cyclic? When this happens, a generator $g \pmod{n}$ of $(\mathbb{Z}/n\mathbb{Z})^*$ is called a *primitive root modulo n*.
Answer. $(\mathbb{Z}/n\mathbb{Z})^*$ is a cyclic group if and only if $n = 2, 4, p^m, 2p^m$, for odd primes p.

We will content ourselves with proving that $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic for prime p. You might try to do the rest for some nontrivial exercises.

Example 1. The number 2 is not a primitive root for $p = 7$ since $2^3 \equiv 1 \pmod{7}$. However, 3 is a primitive root, since

$$3^2 \equiv 2,\ \ 3^3 \equiv 6,\ \ 3^4 \equiv 4,\ \ 3^5 \equiv 5,\ \ 3^6 \equiv 1 \pmod{7}.$$

A Mathematica Remark. Mathematica has a function called PowerMod $[a, b, n]$ which gives $a^b \pmod{n}$. It is much better to use PowerMod than to write Mod $[a\hat{\ }b, n]$. Why?

Example 2. By the Chinese remainder theorem,

$$(\mathbb{Z}/12\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \oplus (\mathbb{Z}/4\mathbb{Z})^*.$$

So every element of $(\mathbb{Z}/12\mathbb{Z})^*$ has order 2. So there can be no primitive root modulo 12. That is, $(\mathbb{Z}/12\mathbb{Z})^*$ is *not* a cyclic group.

Exercise. Write a Mathematica program to find a primitive root mod n if it exists.

Note. Although we can prove that primitive roots exist for any prime modulus, we won't be able to provide an easy way to find them. Trial and error is the standard method. That would be rather time consuming for large moduli.

Before proving our theorem, we need the following lemma.

Lemma. Let k be a field and suppose that $f(x) \in k[x]$, that is, that $f(x)$ is a polynomial with coefficients in the field k. Let n be the degree of f. Then f has at most as many roots as the degree of f.

Proof. Use the division algorithm for polynomials, which works in any field. This says that if we are given $f(x)$ and $g(x) \in k[x]$, we can find $q(x)$ and $r(x) \in k[x]$ so that $f(x) = g(x)q(x) + r(x)$, where degree $r <$ degree g or r is the 0-polynomial. The point is that if a is a root of $f(x)$, then $x - a$ divides $f(x)$ (with remainder 0). And you get factors for each distinct root of $f(x)$. Moreover, the degree of a product of polynomials is the sum of the degrees of the factors. Thus you can have no more than n distinct linear factors. ■

Theorem 4. $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic for any prime p. This means that there is a primitive root modulo any prime p.

Proof. We seek to show that $(\mathbb{Z}/p\mathbb{Z})^*$ has an element of order $p - 1$. If d is a divisor of $(p - 1)$, let $\psi(d)$ denote the number of elements x of $(\mathbb{Z}/p\mathbb{Z})^*$ of order d (meaning that $x^r \equiv 1 \pmod{p}$ holds for $r = d$ and no smaller positive power r). Then, if $\psi(d) \neq 0$, there is an $x \pmod{p}$ such that the set

$$\langle x \rangle = \{1, x, x^2, x^3, \ldots, x^{d-1} \pmod{p}\}$$

is a cyclic subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ with *exactly d* elements. Why are there exactly d elements?

By the lemma, the equation

$$T^d \equiv 1 \pmod{p}$$

can have at most d solutions in the field $\mathbb{Z}/p\mathbb{Z}$. Therefore the set $\langle x\rangle$ includes all the solutions to $T^d \equiv 1 \pmod{p}$ in $\mathbb{Z}/p\mathbb{Z}$. Hence the set $\langle x\rangle$ contains all elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order d.

But the cyclic group $\langle x\rangle$ is isomorphic to the additive group $\mathbb{Z}/d\mathbb{Z}$, by an exercise above. The latter has $\phi(d)$ elements of order d (exercise). Here $\phi(d)$ is Euler's phi function. Thus $\psi(d) \neq 0$ implies $\psi(d) = \phi(d)$.

It follows that since every element of $(\mathbb{Z}/p\mathbb{Z})^*$ has an order dividing $p-1$, we have

$$p-1 = \sum_{\substack{0<d \\ d\,|\,(p-1)}} \psi(d) \leq \sum_{\substack{0<d \\ d\,|\,(p-1)}} \phi(d) = p-1.$$

The last equality comes from an earlier exercise. It follows that the inequality must, in fact, be an equality. Thus $\psi(d) = \phi(d)$ for every divisor d of $p-1$, including $d = p-1$. This proves the theorem. ■

Exercise.

a) Find all the primitive roots modulo all primes ≤ 20.

b) How many primitive roots are there mod p, for a given prime p?

Remarks. It is also possible to show that the multiplicative group of any finite field is cyclic. See Herstein [1964, p. 317]. The proof is also in Dornhoff and Hohn [1978]. In fact, a little use of field theory shortens the proof considerably.

Theorem 4 was first proved by Gauss. Gauss conjectured that 10 is a primitive root for infinitely many primes p, after "laborious calculations." In 1927, Emil Artin conjectured that if $a \neq -1$ and $a \neq$ square, then there are infinitely many primes p such that a is a primitive root mod p. The conjecture is still unproved. See L. J. Goldstein [1971] for details on the state of the conjecture twenty years ago. Other references are Shanks [1985] and Silverman [1997].

Artin actually had a more specific conjecture to the effect that if $a \neq -1$ and $a \neq$ square, then approximately $3/8$ of all primes will have a for a primitive root. The heuristic probabilistic argument that led to this conjecture will be discussed soon. The conjecture needs modification for certain values of a.

Robert Baillie of the Computer Center of the University of Illinois at Urbana computed lengthy tables verifying the Artin conjecture (see Table I.6). Baillie's tables say, for example, that if $A \cong .37395\ 58136\ 19$ is Artin's constant defined

Table I.6. *A computer verification of Artin's conjecture by Baillie*

a	# Primes $\leq 33 \times 10^6$ with a as primitive root	Artin factor, A in (6)
2	759,733	759,754
3	759,658	759,754
5	800,218	$799{,}741 = \frac{20}{19}759{,}754$
6	760,037	759,754
7	760,133	759,754
8	455,894	$455{,}854 = \frac{3}{5}759{,}754$
10	760,192	759,754
11	760,352	759,754
12	759,988	759,754
13	764,719	$764{,}655 = \frac{156}{155}759{,}754$

by (6) below, then, since the number of primes $\leq 33 \times 10^6$ is 2,031,667, we have

$$A \cdot 2{,}031{,}667 \cong 759{,}754.$$

Perhaps we should explain Artin's mysterious constant. A heuristic probabilistic argument shows it to be given by the infinite product

$$A = \prod_{p \text{ prime}} \left[1 - \frac{1}{p(p-1)}\right]. \tag{6}$$

The argument goes as follows:

Consider $a = 2$. Look at the primes less than or equal to N. For every prime p, choose a primitive root g (mod$p$) and write $g^m \equiv 2 \pmod{p}$ and g.c.d. $(m, p-1) = G$. What is the probability that 2 divides G? Except for $p = 2$, $p - 1$ is always even, and m is even in half the cases – that is, when 2 is a square mod p. Since G must be 1 if 2 is to be a primitive root mod p, we must delete such cases. This leaves on the average

$$\left(1 - \frac{1}{2}\right)\pi(N) \text{ primes},$$

where $\pi(N)$ is the *number of primes* $\leq N$.

What is the probability that 3 divides G? Except for $p = 3$, all primes are congruent to 1 or 2 mod 3. Thus 3 divides $p - 1$ in half the cases, while 3 divides m in one third of the cases. Elimination of the primes in which 3 divides G leaves

$$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3 \cdot 2}\right)\pi(N).$$

Continuing with the same argument for G divisible by 5, 7, etc., we obtain the formula above for Artin's constant. One can actually compute the infinite product with various tricks. Wrench obtains 40 significant digits, for example.

Question. Why isn't this a proof of Artin's conjecture?
Answer. We are assuming things are independent events that cannot be proved independent. See Schroeder [1986, pp. 40–42] for a similar probabilistic argument for the *prime number theorem* (proved, for example, in Davenport, [1980]), which says

$$\pi(N) \sim N/\log N, \quad \text{as } N \to \infty. \tag{7}$$

Also see Pólya [1984, Vol. III, pp. 436–45].

There is one more interesting facet of Artin's conjecture. Hooley [1667] modified the conjecture and showed that it is implied by the Riemann hypothesis for zeta functions of certain algebraic number fields. These zeta functions are analogous to the Riemann zeta function. We will discuss another sort of zeta function in Chapter 2.

H. Bilharz [1937] proved the Artin conjecture for the ring $k[x]$ of polynomials over a finite field. His proof required the Riemann hypothesis for the zeta functions associated to such rings. That was proved by A. Weil several years later. See Ireland and Rosen [1993].

The group $(\mathbb{Z}/n\mathbb{Z})^*$ is a finite abelian group. By the fundamental theorem of abelian groups,† any such group is a direct product of finite cyclic groups. Here, by the direct product of two groups, we mean the analogue of direct sum of rings defined before the Chinese remainder theorem, except that now there is only one operation (multiplication, in our case). You might want to write $(\mathbb{Z}/n\mathbb{Z})^*$ explicitly as a direct product of cyclic groups. First note that if

$$n = p_1^{e_1} \cdots p_r^{e_r}, \quad \text{with distinct primes } p_i,$$

† See Chapter 10 and Herstein [1964].

the Chinese remainder theorem tells us that

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^*.$$

Here we use the symbol $\times$ to denote the direct product of multiplicative groups.

It follows from the above argument that it suffices to consider $(\mathbb{Z}/p^e\mathbb{Z})^*$ for prime p. One can prove the following proposition.

Proposition 1. If p is an odd prime and e is a positive integer, then $(\mathbb{Z}/p^e\mathbb{Z})^*$ is cyclic.

Proof Sketch. We know that there exists a primitive root $g \pmod{p}$. Look at $g + p$. It is also a primitive root mod p. And $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$ if $g^{p-1} \equiv 1 \pmod{p^2}$. Why? Thus we can assume that $g^{p-1} \not\equiv 1 \pmod{p^2}$.

We claim that such a g is a primitive root mod p^e. To show this, it suffices to prove that if $g^n \equiv 1 \pmod{p^e}$, then $\phi(p^e)$ divides n.

Now $g^{p-1} = 1 + ap$, with p not dividing a. And one can show (as an exercise) that if p is an odd prime and p does not divide a, then p^{e-1} is the order of $(1 + ap) \pmod{p^e}$.

It follows that $n = p^{e-1}n'$. By Fermat's little theorem, $g^{n'} \equiv \pmod{p}$. Thus $p - 1$ divides n' and so $\phi(p^e)$ divides n. ■

For the powers of 2, the result is as follows.

Proposition 2. $(\mathbb{Z}/2\mathbb{Z})^*$ and $(\mathbb{Z}/4\mathbb{Z})^*$ are cyclic. For $e \geq 3$, $(\mathbb{Z}/2^e\mathbb{Z})^*$ is the direct product of two cyclic groups, one of order 2 and one of order 2^{e-2}. Thus $(\mathbb{Z}/2^e\mathbb{Z})^*$ is not cyclic if $e \geq 3$.

Proof Sketch. One can show (as an exercise) that for $e \geq 3$

$$\{(-1)^a 5^b \pmod{2^e} \mid a = 0, 1; b = 0, 1, \ldots, 2^{e-2} - 1\} = (\mathbb{Z}/2^e\mathbb{Z})^*.$$

■

Theorem 5. There are primitive roots mod n if and only if n is of the form $2, 4, p^e, 2p^e$, where p is an odd prime.

Proof Sketch. Suppose that $n = ab$, with g.c.d. $(a, b) = 1$ and $a, b > 2$. Then $\phi(a)$ and $\phi(b)$ are both even. So both $(\mathbb{Z}/a\mathbb{Z})^*$ and $(\mathbb{Z}/b\mathbb{Z})^*$ have elements of order 2. But then the direct product of these two groups cannot be cyclic, because a cyclic group can only have one element of order 2.

We know that 2, 4, and p^e yield cyclic groups. The same holds for $2p^e$ since

$$(\mathbb{Z}/2p^e\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^e\mathbb{Z})^*.$$

■

Exercise. Complete the proof of the last theorem by explaining why $(\mathbb{Z}/2^e\mathbb{Z})^*$ is not cyclic for $e \geq 3$.

The next exercise introduces another important multiplicative function.

Exercise. Show that the sum of all the primitive roots mod p is congruent to $\mu(p-1)$ mod p. Here $\mu(n)$ is the *Möbius function* defined by

$$\mu(n) = \begin{cases} 1, & n = 1, \\ 0, & n \text{ not square-free, } n > 1, \\ (-1)^r, & \text{if } n = p_1 \cdots p_r, \\ & \text{where the } p_i \text{ are distinct primes.} \end{cases} \tag{8}$$

Exercise. Show that if $n > 1$ and μ denotes the Möbius function of the preceding exercise, we have

$$\sum_{\substack{d|n \\ d>0}} \mu(d) = 0.$$

Exercise. ***The Möbius Inversion Formula.*** Suppose that $f : \mathbb{Z}^+ \to \mathbb{C}$ and let μ denote the Möbius function defined in the exercise above. Let

$$F(n) = \sum_{\substack{d|n \\ d>0}} f(d).$$

Show that

$$f(n) = \sum_{\substack{d|n \\ d>0}} \mu(d) F\left(\frac{n}{d}\right).$$

A Few Remarks on Multiplicative Functions

We have given three examples of multiplicative functions $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ in this section: $\phi(n)$, $\sigma_k(n)$, and $\mu(n)$. It is useful to make the following definition.

Definition. Suppose that f and g are any multiplicative functions $f, g : \mathbb{Z}^+ \to \mathbb{C}$, that is, $f(mn) = f(m)f(n)$, if g.c.d.$(m, n) = 1$. Define *convolution* $f * g$ by

$$f * g(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right). \tag{9}$$

Exercise. Show the following properties of convolution of functions $f, g, h : \mathbb{Z}^+ \to \mathbb{C}$:

a) $f * g = g * f$,

b) $f * (g * h) = (f * g) * h$.

Exercise.

a) Define

$$\delta_a(n) = \begin{cases} 1, & n = a, \\ 0, & \text{otherwise.} \end{cases} \tag{10}$$

Show that $\delta_1 = \mu * 1$, where μ is the Möbius function and 1 denotes the constant function that has value 1 for all $n \in \mathbb{Z}^+$.

b) Prove that $\delta_a * \delta_b = \delta_{ab}$ and $\delta_1 * f = f$.

c) Use the properties of $*$ to show the Möbius inversion formula in an earlier exercise, which says that $f = \mu * (f * 1)$.

Here we are considering convolution of functions with domain the infinite discrete set $\mathbb{Z}^+$ of positive integers, which is *not* a group under multiplication. Instead it is what is called a monoid. See Dornhoff and Hohn [1978, p. 165]. Since this is really a book about *finite groups*, we will say no more about this example. In the next Chapter we will consider convolution with $\mathbb{Z}^+$ replaced by the finite additive group $\mathbb{Z}/n\mathbb{Z}$. Later we will replace $\mathbb{Z}^+$ with any finite group G. It is possible to do convolution for continuous infinite groups such as the additive groups $\mathbb{R}$ or $\mathbb{R}/\mathbb{Z}$, but one has to use series or integrals rather than sums. See Dym and McKean [1972] or Terras [1985].

A Look Forward

We have already considered systems of linear congruences. The logical next question is: How do you solve quadratic congruences? That is, we will ask the question:

> For a fixed prime $p \geq 3$ and given $a \in \mathbb{Z}$, can we find $x \in \mathbb{Z}$ so that $x^2 \equiv a \pmod{p}$?

That is, we will be looking for square roots in $\mathbb{Z}/p\mathbb{Z}$. Since we know that $\mathbb{Z}/p\mathbb{Z}$ is a field which we hope is a finite model for the field of real numbers, we might expect the answer to be similar to that for the field of real numbers. Half the nonzero real numbers (the positive reals) are squares of other real numbers and half aren't. Indeed, that is the case in $\mathbb{Z}/p\mathbb{Z}$ as well.

There is a surprising theorem in this area – the quadratic reciprocity law. One of our first applications of the discrete Fourier transform will be to prove it. See Chapter 8.

An Application – Public–Key Cryptography

There are many situations in which one wants to send a message which can only be deciphered by the recipient. Public-key cryptography allows one to do this fairly easily and feel fairly secure, assuming that no one has figured out something about number theory that we don't know.

Think of your message as a number m mod pq, where p and q are very large primes. The encryption of m is just m^t (mod pq), for some power t. To decrypt one must find a power s so that

$$m^{ts} \equiv m \pmod{pq}.$$

From what we now know about $(\mathbb{Z}/pq\mathbb{Z})^*$, assuming that p and q don't divide m, we know that we need to solve

$$ts \equiv 1 \pmod{\phi(pq)}.$$

The easiest way to solve this linear congruence for s may be to take

$$ts \equiv t^{\phi(\phi(pq))} \pmod{\phi(pq)}$$

and thus

$$s \equiv t^{\phi(\phi(pq))-1} \pmod{\phi(pq)}.$$

Why? This requires one to know $\phi(pq) = (p-1)(q-1)$, for prime p, q.

What happens is that everyone who wants to receive a secret message chooses a triple p, q, t and publishes t and the product pq. Then anyone who wants to send a secret message m will compute m^t (mod pq) and send this number.

Why can't anyone figure out m from this? Well, the catch is that if p and q are large enough then no one can compute $\phi(pq)$, because, to do that, one would have to factor a very large number pq. It is much easier to find two primes with 50 digits than to factor a 100-digit number. The size of the primes p and q is dependent on the state of the art of factoring and primality testing.

References for public–key cryptography are Rosen [1993] and Schroeder [1986].

Exercise. Investigate public-key cryptography and write a Mathematica program to encode and decode messages.

Exercise. Show that for any prime p if $a \in (\mathbb{Z}/p\mathbb{Z})^n, a \neq 0, b \in \mathbb{Z}/p\mathbb{Z}$, then the number of solutions $x \in (\mathbb{Z}/p\mathbb{Z})^n$ of the equation $\sum_{j=1}^n a_j x_j = b$ is p^{n-1}. Another way to say this is:

$$|\{x \in (\mathbb{Z}/p\mathbb{Z})^n \mid {}^t ax = b\}| = p^{n-1}.$$

Hint. The set whose order we seek is a hyperplane in n-space over a finite field, as the elements of the set are vectors satisfying one linear equation in n unknowns. Use the standard methods of linear algebra, which work as well over a finite field $\mathbb{Z}/p\mathbb{Z}$ as over the real numbers $\mathbb{R}$.

Question. Can you generalize the last exercise replacing the linear equation with a quadratic equation

$$\sum_{j=1}^{n} a_j x_j^2 = b?$$

This will be of interest in Chapter 5.