24.13 Example Find all solutions of the congruence $12x \equiv 27 \pmod{18}$.

Solution The gcd of 12 and 18 is 6, and 6 is not a divisor of 27. Thus by the preceding corollary, there are no solutions. ▲

24.14 Example Find all solutions of the congruence $15x \equiv 27 \pmod{18}$.

Solution The gcd of 15 and 18 is 3, and 3 does divide 27. Proceeding as explained before Example 24.13, we divide everything by 3 and consider the congruence $5x \equiv 9 \pmod{6}$, which amounts to solving the equation $5x = 3$ in $\mathbb{Z}_6$. Now the units in $\mathbb{Z}_6$ are 1 and 5, and 5 is clearly its own inverse in this group of units. Thus the solution in $\mathbb{Z}_6$ is $x = (5^{-1})(3) = (5)(3) = 3$. Consequently, the solutions of $15x \equiv 27 \pmod{18}$ are the integers in the three residue classes

$$3 + 18\mathbb{Z} = \{\cdots, -33, -15, 3, 21, 39, \cdots\},$$
$$9 + 18\mathbb{Z} = \{\cdots, -27, -9, 9, 27, 45, \cdots\}.$$
$$15 + 18\mathbb{Z} = \{\cdots, -21, -3, 15, 33, 51, \cdots\},$$

illustrating Corollary 24.12. Note the $d = 3$ solutions 3, 9, and 15 in $\mathbb{Z}_{18}$. All the solutions in the three displayed residue classes modulo 18 can be collected in the one residue class $3 + 6\mathbb{Z}$ modulo 6, for they came from the solution $x = 3$ of $5x = 3$ in $\mathbb{Z}_6$. ▲

EXERCISES 24

Computations

We will see later that the multiplicative group of nonzero elements of a finite field is cyclic. Illustrate this by finding a generator for this group for the given finite field.

1. $\mathbb{Z}_7$ **2.** $\mathbb{Z}_{11}$ **3.** $\mathbb{Z}_{17}$

4. Using Fermat's theorem, find the remainder of 3^{47} when it is divided by 23.

5. Use Fermat's theorem to find the remainder of 37^{49} when it is divided by 7.

6. Compute the remainder of $2^{(2^{17})} + 1$ when divided by 19. [*Hint:* You will need to compute the remainder of 2^{17} modulo 18.]

7. Make a table of values of $\varphi(n)$ for $n \leq 30$.

8. Compute $\varphi(p^2)$ where p is a prime.

9. Compute $\varphi(pq)$ where both p and q are primes.

10. Use Euler's generalization of Fermat's theorem to find the remainder of 7^{1000} when divided by 24.

In Exercises 11 through 18, describe all solutions of the given congruence, as we did in Examples 24.13 and 24.14.

11. $2x \equiv 6 \pmod{4}$ **12.** $22x \equiv 5 \pmod{15}$

13. $36x \equiv 15 \pmod{24}$ **14.** $45x \equiv 15 \pmod{24}$

15. $39x \equiv 125 \pmod{9}$ **16.** $41x \equiv 125 \pmod{9}$

17. $155x \equiv 75 \pmod{65}$ **18.** $39x \equiv 52 \pmod{130}$

19. Let p be a prime ≥ 3. Use Exercise 28 below to find the remainder of $(p-2)!$ modulo p.

20. Using Exercise 28 below, find the remainder of 34! modulo 37.

21. Using Exercise 28 below, find the remainder of 49! modulo 53.

22. Using Exercise 28 below, find the remainder of 24! modulo 29.

Concepts

23. Determine whether each of the following is true or false.

a. $a^{p-1} \equiv 1 \pmod{p}$ for all integers a and primes p.

b. $a^{p-1} \equiv 1 \pmod{p}$ for all integers a such that $a \not\equiv 0 \pmod{p}$ for a prime p.

c. $\varphi(n) \leq n$ for all $n \in \mathbb{Z}^+$.

d. $\varphi(n) \leq n - 1$ for all $n \in \mathbb{Z}^+$.

e. The units in $\mathbb{Z}_n$ are the positive integers less than n and relatively prime to n.

f. The product of two units in $\mathbb{Z}_n$ is always a unit.

g. The product of two nonunits in $\mathbb{Z}_n$ may be a unit.

h. The product of a unit and a nonunit in $\mathbb{Z}_n$ is never a unit.

i. Every congruence $ax \equiv b \pmod{p}$, where p is a prime, has a solution.

j. Let d be the gcd of positive integers a and m. If d divides b, then the congruence $ax \equiv b \pmod{m}$ has exactly d incongruent solutions.

24. Give the group multiplication table for the multiplicative group of units in $\mathbb{Z}_{12}$. To which group of order 4 is it isomorphic?

Proof Synopsis

25. Give a one-sentence synopsis of the proof of Theorem 24.1.

26. Give a one-sentence synopsis of the proof of Theorem 24.7.

Theory

27. Show that 1 and $p - 1$ are the only elements of the field $\mathbb{Z}_p$ that are their own multiplicative inverse. [*Hint:* Consider the equation $x^2 - 1 = 0$.]

28. Using Exercise 27, deduce the half of *Wilson's theorem* that states that if p is a prime, then $(p - 1)! \equiv -1 \pmod{p}$. [The other half states that if n is an integer >1 such that $(n - 1)! \equiv -1 \pmod{n}$, then n is a prime. Just think what the remainder of $(n - 1)!$ would be modulo n if n is not a prime.]

29. Use Fermat's theorem to show that for any positive integer n, the integer $n^{37} - n$ is divisible by 383838. [*Hint:* $383838 = (37)(19)(13)(7)(3)(2)$.]

30. Referring to Exercise 29, find a number larger than 383838 that divides $n^{37} - n$ for all positive integers n.

SECTION 25 ENCRYPTION

An encryption scheme is a method to disguise a message so that it is extremely difficult for anyone other than the intended receiver to read. The sender **encrypts** the message and the receiver **decrypts** the message. One method, called cypher encryption, requires the sender to use a permutation of the letters in the alphabet to replace each letter with a different letter. The receiver then uses the inverse of the permutation to recover the original message. This method has two major weaknesses. First, both the sender and the receiver need to know the permutation, but no one else should know the permutation or else the message is not secure. It would be difficult to implement a cypher for a transaction when a company wishes to receive many orders each day, each using a different permutation that only the customer and the company know. Furthermore, cyphers are generally not difficult to crack. In fact, some newspapers carry a daily puzzle, which is essentially decrypting an encrypted message.

Researchers in the second half of the twentieth century sought a method that allows the receiver to publish public information that any sender could use to encrypt a message, yet only the receiver could decrypt it. This means that knowing how a message was encrypted is little help in decryption. This method relies on a function that is easy for computers to compute, but whose inverse is virtually impossible to compute without

more information. Functions of this type are called **trap door functions**. Most commercial online transactions are communicated with trap door functions. This allows anyone to make a secure credit card purchase with little risk of a third party gaining private information.

RSA Public and Private Keys

Euler's generalization of Fermat's Theorem is the basis of a very common trap door encryption scheme referred to as **RSA encryption**. RSA comes from the names of the three inventors of the system, Ron Rivest, Adi Shamir, and Leonard Adleman. The trap door function relies on the fact that it is easy to multiply two large prime numbers, but if you are only given their product, it is very difficult to factor the number to recover the two prime numbers. The following theorem is the key to this encryption scheme.

25.1 Theorem Let $n = pq$ where p and q are distinct prime numbers. If $a \in \mathbb{Z}$ with $\gcd(a, pq) = 1$ and $w \equiv 1 \pmod{(p-1)(q-1)}$, then $a^w \equiv a \pmod{n}$.

Proof Since $w \equiv 1 \pmod{(p-1)(q-1)}$, we can write

$$w = k\,(p-1)(q-1) + 1$$

for some integer k. Recall that the Euler phi-function $\phi(n)$ counts the number of positive integers less than or equal to n that are relatively prime to n. Since $n = pq$, we can compute $\phi(pq)$ by subtracting the number of integers less than n that are divisible by either p or q from $n - 1$. There are $p - 1$ multiples of q and $q - 1$ multiples of p that are less than pq. Furthermore, the least common multiple of p and q is pq since p and q are distinct primes. Thus

$$\begin{aligned}\phi(pq) &= (pq-1) - (p-1) - (q-1)\\ &= pq - p - q + 1\\ &= (p-1)(q-1).\end{aligned}$$

By Euler's Theorem (Theorem 24.7),

$$\begin{aligned}a^w &= a^{k(p-1)(q-1)+1}\\ &= a\left(a^{(p-1)(q-1)}\right)^k\\ &= a\left(a^{\phi(n)}\right)^k\\ &\equiv a(1^k)\\ &\equiv a \pmod{n}.\end{aligned}$$

◆

The RSA encryption scheme requires two sets of positive integers called the **private key** and the **public key**. The private key is known only by the person who will receive the message, and the public key is available to anyone who wishes to send a message to the receiver.

The private key consists of

- Two prime numbers p and q with $p \neq q$.
- The product $n = pq$.
- An integer $1 < r < (p-1)(q-1) - 1$ that is relatively prime to $(p-1)(q-1)$.

We know that r has an inverse in $\mathbb{Z}_{(p-1)(q-1)}$ since r is relatively prime to $(p-1)(q-1)$.

The public key consists of

- The integer s where $1 < s < (p-1)(q-1)$ and s is the inverse of r in $\mathbb{Z}_{(p-1)(q-1)}$.
- The product $n = pq$.

The public key does not include p, q, r, or $(p-1)(q-1)$. Knowing any of these numbers and the numbers in the public key would make it relatively easy to decrypt any encrypted message.

We can now give the encryption and decryption algorithms. The sender wishes to send a message to the receiver. We will assume the message is simply a number between 2 and $n-1$. To send a text message, the sender would use a standard way of representing the text as a number, such as the ASCII code. A long text would be broken up into smaller texts so that each would be coded as a number in the allowable range 2 to $n-1$ and each would be sent separately. Let $2 \leq m \leq n-1$ be the message to be sent.

Encryption Using the public key, the sender encrypts the message as a number $0 \leq y \leq n-1$ to be sent to the receiver where

$$y \equiv m^s \pmod{n}.$$

That is, the sender computes y to be the remainder when m^s is divided by n and sends y to the receiver.

Decryption Using the private key, the receiver decrypts y, the message received from the sender, by computing

$$y^r \pmod{n},$$

the remainder when y^r is divided by n. Since $rs \equiv 1 \pmod{(p-1)(q-1)}$, Theorem 25.1 says,

$$y^r = (m^s)^r = m^{rs} \equiv m \pmod{n}.$$

Thus the receiver reconstructs the original message m.

Of course, in practice the prime numbers p and q are very large. As of the writing of this book it is thought that prime numbers requiring 4096 bits or approximately 1200 digits are sufficient to make the RSA scheme secure. To illustrate how the process works, we will use small primes.

25.2 Example Let $p = 17$ and $q = 11$. The private key consists of

- $p = 17$, $q = 11$,
- $n = pq = 187$ and
- a number r relatively prime to $(p-1)(q-1) = 160$. For this example we take $r = 23$.

The public key consists of

- $n = 187$ and
- $s = 7$. A little calculation shows that $23 \cdot 7 = 161 = 160 + 1 \equiv 1 \pmod{160}$, which implies that $s = 7$. Since the public key consists of only n and s, $(p-1)(q-1)$ is unknown to all but the receiver. Without knowing $(p-1)(q-1)$, the value of r cannot be determined from the value of s.

Suppose the sender wishes to send the message $m = 2$ to the the receiver. The message is encrypted by computing

$$y = 2^7 \equiv 128 \pmod{187}.$$