3. Applications of Number Theory

3.1. Representation of Integers.

THEOREM 3.1.1. *Given an integer $b > 1$, every positive integer n can be expresses uniquely as*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where $k \geq 0$, $0 \leq a_0, a_1, a_2, \ldots, a_k < b$, and are all integers.

DEFINITION 3.1.1. **Base b expansion of** *n is $(a_k a_{k-1} \cdots a_1 a_0)_b$ if the a_i are as described in Theorem 3.1.1.*

EXAMPLE 3.1.1. *Here are examples of common expansions other than the more familiar decimal expansion.*

- **Binary expansion** *is the base 2 expansion.*
- **Octal expansion** *is the base 8 expansion.*
- **Hexadecimal expansion** *is base 16 expansion. The symbols A through F are used to represent 10 through 15 in the expansion.*

Discussion

Theorem 3.1.1 asserts that each positive integer n can be expressed uniquely as a linear combination of powers of a fixed integer $b > 1$. The coefficients in the linear combination must be less than b and must be greater than or equal to zero. These coefficients are, by definition, the digits of the **base b expansion of** n, $n = (a_k a_{k-1} \ldots a_1 a_0)_b$.

3.2. Constructing Base b Expansion of n.

Use the division algorithm to get the base b expansion of n:

1. $n = bq_1 + a_0$, $0 \leq a_0 < b$ and $q_1 < n$.
2. $q_1 = bq_2 + a_1$, $0 \leq a_1 < b$ and $q_2 < q_1$.
3. $q_2 = bq_3 + a_2$, $0 \leq a_2 < b$ and $q_3 < q_2$.
4. etc. until $q_i = 0$.

Then $n = (a_k a_{k-1} \ldots a_1 a_0)_b$.

EXAMPLE 3.2.1. *Find the binary expansion of 42.*

Solution: We can use the division algorithm to get the a_i's.

$$\begin{aligned}
42 &= 2(21) + 0\\
21 &= 2(10) + 1\\
10 &= 2(5) + 0\\
5 &= 2(2) + 1\\
2 &= 2(1) + 0\\
1 &= 2(0) + 1
\end{aligned}$$

This gives us $42 = (1)(2^5) + (0)(2^4) + (1)(2^3) + (0)(2^2) + (1)(2^1) + 0$. *Thus the binary expansion of 42 is* $(101010)_2$.

Example 3.2.2. *Find the hexadecimal expansion of 42.*

Solution: This time we use 16 for b.

$$\begin{aligned}
42 &= 16(2) + 10\\
2 &= 16(0) + 2
\end{aligned}$$

So the hexadecimal expansion of 42 is $(2A)_{16}$ *(recall we use* $A = 10$ *in hexadecimal notation).*

Example 3.2.3. *Find the decimal notation of the octal representation* $(1024)_8$.

$(1024)_8 = 1(8^3) + 0(8^2) + 2(8^1) + 4 = 532$

3.3. Cancellation in Congruences.

Theorem 3.3.1. *Suppose* $\text{GCD}(c, m) = 1$ *and* $ac \equiv bc(\textit{mod}\, m)$. *Then* $a \equiv b(\textit{mod}\, m)$.

Proof. Suppose $\text{GCD}(c, m) = 1$ and
$ac \equiv bc(\text{mod}\ m)$. (We may assume $m > 1$ so that $c \neq 0$.) Then

$$ac - bc = c(a - b) = km$$

for some integer k. This implies

$$c|km.$$

Since $\text{GCD}(c, m) = 1$, Lemma 2 from Module 5.2 asserts that if $c|km$, then

$$c|k.$$

Write $k = cd$ for some integer d, and substitute for k in the equation above:

$$c(a - b) = km = (cd)m = c(dm).$$

Since the cancellation law holds for integers and $c \neq 0$, we can cancel c to get

$$a - b = dm.$$

Thus, $a \equiv b(\text{mod } m)$. □

Discussion

Theorem 3.3.1 provides a criterion for being able to cancel when you have a congruence. Notice that in order to perform the cancellation, the modulus m and the factor to be cancelled must be relatively prime. Here is an example to illustrate why.

EXAMPLE 3.3.1. $3 \cdot 6 \equiv 1 \cdot 6(\textit{mod } 12)$*, but* $3 \not\equiv 1(\textit{mod } 12)$*. The reason cancellation fails is that 6 and 12 are not relatively prime.*

EXAMPLE 3.3.2. $3 \cdot 6 \equiv 8 \cdot 6(\textit{mod } 5)$*. Here 6 and 5 are relatively prime and we can easily check that* $3 \equiv 8(\textit{mod } 5)$*.*

3.4. Inverses mod m.

DEFINITION 3.4.1. *An integer a' is a* **(multiplicative) inverse to** a **modulo** m *if*

$$aa' \equiv 1(\textit{mod } m).$$

EXAMPLE 3.4.1. *The inverse of 14 modulo 9 is 2, since* $14 \cdot 2 \equiv 28 \equiv 1(\textit{mod } 9)$*. There is no inverse to 6 modulo 9, however.*

In general, an "inverse" refers to something that "undoes" another thing leaving something that is an "identity".

- With regular multiplication of real numbers, the inverse of x is $\frac{1}{x}$ since $x(\frac{1}{x}) = 1$. Inverses do not necessarily exist if we look only at integers.
- With regular addition of real numbers, the inverse of x is $-x$ since $x+(-x) = 0$,
- With matrices and matrix multiplication, the inverse of a matrix, A, is a matrix A^{-1}, such that $AA^{-1} = A^{-1}A = I$, where I is the identity matrix. Not all matrices have inverses.
- With functions and composition, the inverse of a function, f, is a function, f^{-1}, such that $(f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = x = \textit{identity}(x)$. Not all functions have inverses.
- Not all integers, even nonzero integers, have inverses modulo m. Moreover, if an inverse does exist it is not unique. This last part is different from all the other ones mentioned before! We shall see below, however, that if an integer a has an inverse modulo m, then it has a unique inverse lying between 0 and m.

3.5. Linear Congruence.

Definition 3.5.1. *A* **linear congruence** *is a congruence of the form $ax \equiv b(mod\, m)$, where a, b, and m are fixed integers and $m > 0$. One may solve for x by finding an inverse of a modulo m, if an inverse exists.*

Example 3.5.1. *Solve the linear congruence*
$2x \equiv 7(mod\ 15)$ for x.

Solution: An inverse of 2 modulo 15 is 8. Thus

$$\begin{aligned}(8 \cdot 2)x &\equiv 8(7)(mod\, 15)\\ x &\equiv 56(mod\, 15)\\ x &\equiv 11(mod\, 15)\end{aligned}$$

Discussion

Solving a linear congruence, $ax \equiv b\,(\text{ mod } m)$, is very similar to solving an ordinary linear equation $ax = b$. We can solve for x in the linear equation by multiplying through by the multiplicative inverse $1/a$ of a, provided $a \neq 0$. In a similar manner, we can solve a linear congruence, $ax \equiv b(\text{mod } m)$, provided a has a multiplicative inverse a' modulo m. Then $x \equiv a'ax \equiv a'b(\text{mod } m)$. To get a canonical choice for x, we would reduce $a'b$ modulo m.

Caution. DO NOT express the solution to a linear congruence $ax \equiv b(\text{mod } m)$ as $x = \frac{b}{a}$, as you would the solution to the linear equation $ax = b$. We have previously cautioned against using fractional notation when doing integer arithmetic, but, in the world of integers modulo m, they are expressly forbidden.

3.6. Criterion for Invertibility mod m.

Theorem 3.6.1. *Suppose a and m are integers and $m > 1$. Then a has an inverse modulo m if and only if* $\text{GCD}(a, m) = 1$. *Moreover, if* $\text{GCD}(a, m) = 1$, *then a has a unique inverse, a', with $0 \leq a' < m$.*

Proof. $\text{GCD}(a, m) = 1$ if and only if there are integers s and t such that $1 = as + mt$. This is true if and only if there is an integer s such that $1 \equiv as(\text{mod } m)$. By definition, this is true if and only if a has an inverse, namely s, modulo m. □

Discussion

Theorem 3.6.1 provides us with the conditions required for inverses modulo m to exist: For a to have an inverse modulo m, a and m must be relatively prime. The proof of the "moreover" part is complete once you solve the following exercise.

Exercise 3.6.1. *Prove that if* $ab \equiv 1(mod\, m)$ *and* $b \equiv c(mod\, m)$*, then* $ac \equiv 1(mod\, m)$*.*

3.7. Example 3.7.1.

We can use the Euclidean Algorithm and the division algorithm to find the "unique" inverse of a modulo m.

Example 3.7.1. *Find the inverse of 8 modulo 35.*

1. *Apply the Euclidean Algorithm.*

$$\begin{aligned} 35 &= 4(8) + 3 \\ 8 &= 2(3) + 2 \\ 3 &= 1(2) + 1 \\ 2 &= 2(1) + 0 \end{aligned}$$

2. *Find the linear combination of* 8 *and* 35 *that equals 1, the* GCD*.*

$$\begin{aligned} 1 &= 3 - 1(2) \\ &= [35 - 4(8)] - 1[8 - 2(3)] \\ &= [35 - 4(8)] - 1[8 - 2[35 - 4(8)]] \\ &= 3(35) - 13(8) \end{aligned}$$

3. *This gives*

$$-13(8) \equiv 1(mod\, 35),$$

so an inverse of 8 modulo 35 is -13*.*

4. *To find the inverse between 0 and 35 use the division algorithm*

$$-13 = -1(35) + 22.$$

The unique inverse of 8 modulo 35 between 0 and 35 is 22.

5. *Check:* $8 \cdot 22 = 176 = 5 \cdot 35 + 1 \equiv 1$ *(mod 35)*

3.8. Fermat's Little Theorem.

Theorem 3.8.1. *If* p *is a prime that does not divide the integer* a*, then*

$$a^{p-1} \equiv 1(mod\, p).$$

and

$$a^p \equiv a(mod\, p).$$

Example 3.8.1. *Find* 5^{158} **mod** 11.

Solution: Since $158 = 15(10) + 8$, *we have*

$$\begin{aligned} 5^{158} &= (5^{15})^{10}(5^8) \\ &\equiv 5^8 (mod\ 11), \end{aligned}$$

by Fermat's little theorem, applied to $a = 5^{15}$ *and* $p = 11$.

Now,

$$\begin{aligned} 5^8 &= (5^2)^4 \\ &= 25^4 \\ &\equiv 3^4 (mod\ 11)\ \cdot \\ &= 81 \\ &\equiv 4 (mod\ 11). \end{aligned}$$

Thus 5^{158} **mod** $11 = 4$.

Discussion

The problem of determining whether a given integer is a prime may be very difficult. This fact is both interesting mathematically and useful in coding theory. Fermat's little theorem provides some help in working with prime numbers and provides the basis for many *probabilistic primality tests*. We will not give a proof of Fermat's theorem, since it involves concepts from the theory of groups that would take us too far afield. An elementary proof can be found in *Introduction to Modern Algebra*, Fourth Edition, by McCoy and Janusz (Allyn and Bacon, 1987).

The converse of Fermat's little theorem is not true. In particular, there are composite numbers n such that

$$2^{n-1} \equiv 1 (\text{mod } n).$$

These are called *pseudoprimes.* They are very rare, but 341 is a pseudoprime.

Fermat's little theorem can be used to reduce the problem of finding the remainder of a large power modulo a prime. In Example 3.8.1, we use the fact that 5^{15} and 11 are relatively prime and Fermat's little theorem to get $(5^{15})^{10} \equiv 1(\text{mod } 11)$, thereby reducing 5^{158} to a smaller power of 5 modulo 11. One clearly has to be comfortable with the laws of exponents to carry out an exercise such as this.

3.9. RSA System. The RSA system is a public key cryptosystem based on modular exponentiation modulo the product of two large primes. This system, named after the researchers who introduced it: Rivest, Shamir, and Adleman, is a public key cryptosystem.

RSA Code

(1) Find p and q, large primes.
(2) Choose e so that $e < pq$ and $\text{GCD}(e, (p-1)(q-1)) = 1$. e must be odd, but not necessarily prime.
(3) Find d such that $de \equiv 1(\text{mod } (p-1)(q-1))$.
(4) Encryption function $f(t) = t^e(\text{mod } pq)$.
(5) Decryption function $f^{-1}(c) = c^d(\text{mod } pq)$.

The *public keys* are (p, q, e) and the *private key* is d.

EXAMPLE 3.9.1. *Here is the routine, using* $p = 61$, $q = 53$, $e = 17$, *and* $d = 2753$.

1. The first prime number (destroy after computing e and d): $p = 61$
2. The second prime number (destroy after computing e and d): $q = 53$
3. Modulus (give this to others): $pq = 3233$
4. Public exponent (give this to others): $e = 17$
5. Private exponent (keep this secret): $d = 2753$
6. Your public key is $(pq, e) = (3233, 17)$.
7. Your private key is $d = 2753$.
8. The encryption function is $f(t) = (t^{17})(mod\ 3233)$.
9. The decryption function is : $f^{-1}(c) = (c^{2753})(mod\ 3233)$.

To encrypt the plaintext value 123, do this:

$f(123) = (123^{17})(\text{mod } 3233) = 337587917446653715596592958817679803(\text{mod } 3233) = 855$

To decrypt the ciphertext value 855, do this:

$$\begin{aligned} f^{-1}(855) &= (855^{2753})(\text{mod } 3233) \\ &= \text{ (an incredibly huge number goes here) (mod 3233)} \\ &= 123 \end{aligned}$$

The large exponential expressions can be reduced modulo 3233 in a piecemeal fashion, however, so that you don't actually have to calculate these large numbers.