3 Integer Properties II

3.1 Modular Arithmetic

Reference Buchmann 2.1

Definition 3.1. Let $m \geq 1$ be an integer. If a, b are integers, we say that

$$a \text{ is } \textit{congruent} \text{ to } b \bmod m$$

if $m \mid (a - b)$. We write this as $a \equiv b \bmod m$.

Example 3.1.

Exercise 3.2. Show that $a \equiv b \bmod m$ if and only if there is an integer k such that $a = b + km$.

Theorem 3.2. Let $m \geq 1$. Then each integer is congruent mod m to *exactly one* of $0, 1, \ldots, m - 1$.

Proof.

Lemma 3.3. Let $m \geq 1$. Let $a, b, c \in \mathbb{Z}$. Then the following hold:

(i) $a \equiv a \bmod m$.

(ii) If $a \equiv b \bmod m$, then $b \equiv a \bmod m$.

(iii) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $a \equiv c \bmod m$.

(iv) If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then

$$a \pm c \equiv b \pm d \bmod m$$

and

$$ac \equiv bd \bmod m.$$

Proof. Exercise.

It follows from Lemma 3.3(iv) that the ordinary rules of addition, subtraction, and multiplication all hold in modular arithmetic.

But beware,

$$ac \equiv bc \bmod m$$

does not imply

$$a \equiv b \bmod m,$$

that is, we cannot *divide* in general.

Example 3.3.

However, we do have the following.

Theorem 3.4. Let $m \geq 1$. Let $a, b, c \in \mathbb{Z}$. If $ac \equiv bc \bmod m$ and $\gcd(m, c) = 1$, then

$$a \equiv b \bmod m.$$

Proof. Now $m \mid (ac - bc)$, that is, $m \mid c(a - b)$. Since $\gcd(m, c) = 1$, it follows by Example 2.11 that $m \mid (a - b)$. So $a \equiv b \bmod m$.

Example 3.4. "Casting out nines".

This method for checking multiplications was widely popular in pre-calculator days. It was even taught in primary schools!

Exercise 3.5. Show that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

3.2 Arithmetic in $\mathbb{Z}_m$

Reference Buchmann 2.1

Recall that $\mathbb{Z}$ denotes the set of all integers. Let m be a positive integer. (In practice, $m \geq 2$.)

Definition 3.5. Set

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}.$$

Furthermore, define addition and multiplication on $\mathbb{Z}_m$ by $a + b = r$, where r is the remainder when $a + b$ is divided by m, and $a \times b = s$, where s is the remainder when $a \times b$ is divided by m.

Note on notation. Buchmann uses the notation $\mathbb{Z}/m\mathbb{Z}$ for $\mathbb{Z}_m$.

Example 3.6.

Definition 3.6. Let $m \geq 1$. An element $a \in \mathbb{Z}_m$ is *invertible* if there exists an element $b \in \mathbb{Z}_m$ such that $ab = 1$ in $\mathbb{Z}_m$, that is $ab \equiv 1 \bmod m$.

- b is called the *inverse* of a and we sometimes write $b = a^{-1}$.

Note. If an element is invertible, then it is non-zero. But non-zero elements need not be invertible.

Example 3.7.

The next result tells us when an element of $\mathbb{Z}_m$ has an inverse.

Theorem 3.7. Let $m \geq 1$. An element $a \in \mathbb{Z}_m$ is invertible if and only if $\gcd(a, m) = 1$.

Proof.

Corollary 3.8. If p is *prime*, then all non-zero elements in $\mathbb{Z}_p$ are invertible.

Definition 3.9. Define $\mathbb{Z}_m^*$ to be the set of all *invertible* elements in $\mathbb{Z}_m$. By Theorem 3.7,

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m : \gcd(a, m) = 1\}.$$

Example 3.8.

In general, *if p is prime*, then $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$.

Exercise 3.9. Find the inverse of each element in the previous example.

An important result!

Theorem 3.10. Let $m \geq 1$. If $a, b \in \mathbb{Z}_m^*$, then $ab \in \mathbb{Z}_m^*$.

(We say that $\mathbb{Z}_m^*$ is *closed* under multiplication. Note too that $\mathbb{Z}_m^*$ is closed under taking inverses, that is, if $a \in \mathbb{Z}_m^*$, then $a^{-1} \in \mathbb{Z}_m^*$.)

Proof. Exercise.

3.3 Finding Inverses in $\mathbb{Z}_m^*$

Recall. If we are working mod m, then we can only divide by an integer k if k has a multiplicative inverse in $\mathbb{Z}_m$. This condition on k is the same as requiring that $\gcd(k, m) = 1$, that is, $k \in \mathbb{Z}_m^*$.

For smallish values of m, we can draw up a multiplication table for $\mathbb{Z}_m^*$ and read off inverses from that table. But for larger values of m, it is much more efficient to use Euclid's Algorithm to find inverses.

Example 3.10.

But for large values of m, use Euclid's Algorithm as is shown in the next example.

Example 3.11. Find $117^{-1} \bmod 173$.

3.4 Solving Equations in $\mathbb{Z}_m$

Case 1. Solving a linear equation of the type $ax = b$ in $\mathbb{Z}_m$, that is, $ax \equiv b \bmod m$.

The technique requires finding a^{-1} in $\mathbb{Z}_m^*$ to get

$$\begin{aligned} a^{-1}(ax) &\equiv a^{-1}b \bmod m \\ x &\equiv a^{-1}b \bmod m \end{aligned}$$

Example 3.12. Solve the equation $3x \equiv 11 \bmod 17$.

Case 2. Solving two or more linear equations of the type $ax \equiv b \bmod m$.

We take each equation in turn, solve it, and substitute in the next one.

Example 3.13. Solve the system of equations

$$2x \equiv 1 \bmod 3$$
$$5x \equiv 2 \bmod 7$$

3.5 The Order of Invertible Elements

Definition 3.11. Let $m \geq 1$ and $a \in \mathbb{Z}_m^*$. The *order* of a is the smallest positive integer n such that $a^n \equiv 1 \bmod m$ or, equivalently, $a^n = 1$ in $\mathbb{Z}_m^*$.

Example 3.14.

Note that if $a \in \mathbb{Z}_m^*$ has order n, then $a^{2n} = a^n \times a^n = 1 \times 1 = 1$ and, more generally,

$$a^{kn} = a^n \times a^n \times \cdots \times a^n = 1 \times 1 \times \cdots \times 1 = 1$$

for any integer k.

The converse is also true and is an important result.

Theorem 3.12. (Buchmann, Theorem 2.9.2) If $a \in \mathbb{Z}_m^*$ has order n and, for some integer k, we have $a^k = 1$, then $n \mid k$, that is, k is a *multiple* of n.

Proof.

There is another useful result which links the order of an element in $\mathbb{Z}_m^*$ to the *number of elements* in $\mathbb{Z}_m^*$.

Theorem 3.13. Let $m \geq 1$ and let $a \in \mathbb{Z}_m^*$. Suppose that $\mathbb{Z}_m^*$ has N elements. Then the order of a divides N.

Example 3.15.

Proof.

Exercise 3.16. If $m \geq 3$, then $|\mathbb{Z}_m^*|$ is even.

This theorem has a corollary which is important in number theory and cryptography. This is *Fermat's Little Theorem*–not to be confused with his somewhat larger *Last Theorem* which took 300 years and Andrew Wiles to prove.

Theorem 3.14. (Fermat's Little Theorem) If p is prime and $a \in \mathbb{Z}$ such that $p \nmid a$ (that is, a is not a multiple of p), then $a^{p-1} \equiv 1 \bmod p$.

Proof.

Example 3.17. Check Fermat's Little Theorem for $p = 5$.

Fermat's Little Theorem also gives us a method for simplifying exponents (modulo a prime). The following example shows how it works.

Example 3.18. Find $1945^{12} \bmod 11$.

3.6 Euler's Totient or Phi-Function

The number of elements in $\mathbb{Z}_p^*$ is $p-1$ when p is a *prime*. What is the number of elements in $\mathbb{Z}_m^*$ when m is composite? The answer to this question is given by Euler's phi-function.

Consider again $\mathbb{Z}_m^* = \{k : 1 \leq k \leq n \text{ with } \gcd(k,m) = 1\}$. The *number of elements* in $\mathbb{Z}_m^*$ is written as $\phi(m)$.

Example 3.19.

We know that if $m = p$ is *prime*, then $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ so that $\phi(p) = p-1$. A formula for $\phi(m)$ for general m is more difficult to find and we will only prove the two special cases important in cryptography.

Case 1. If m is a power of a prime, that is $m = p^\alpha$, then $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Proof. If $k \in \mathbb{Z}_{p^\alpha}^*$, then $1 \leq k \leq p^\alpha$ and $\gcd(k, p^\alpha) = 1$ which means that p does

not divide k, that is, k is not a multiple of p. So from $\{1, 2, 3, \ldots, p^\alpha\}$ (which has p^α numbers), we must remove $p, 2p, 3p, \ldots, p^{\alpha-1}p$. In other words, we must remove $p^{\alpha-1}$ numbers from a set of p^α numbers. This leaves $p^\alpha - p^{\alpha-1}$ numbers in $\mathbb{Z}^*_{p^\alpha}$.

Case 2. If p, q are primes, then $\phi(pq) = (p-1)(q-1)$. *This is a central idea behind the RSA cipher which we will shortly study.*

Proof.

Case 3. The general formula for $\phi(m)$ is in terms of the prime decomposition of m. If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\phi(m) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}).$$

A proof can be found in any good text in number theory.

The next theorem is a generalisation of Fermat's Little Theorem, and it also follows from Theorem 3.13. Why?

Theorem 3.15. (Euler's Theorem) If $a \in \mathbb{Z}$ and $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \bmod m$.

Written in terms of $\mathbb{Z}_m$, Euler's Theorem says that if $a \in \mathbb{Z}^*_m$, then $a^{\phi(m)} = 1$ in $\mathbb{Z}_m$.

Note. Buchmann mistakenly calls Euler's Theorem, Fermat's Little Theorem (see Theorem 2.11.1) but don't lose any sleep over this. Mathematics is full of results

named after the wrong person. For example, the equation $x^2 - dy^2 = 1$ is called Pell's equation though Pell had nothing to do with it. It's really due to the Indian mathematician Brahmagupta who lived about 900 years before Pell. But Euler called it Pell's equation and no-one has ever dared to contradict Euler.

3.7 Generators (Primitive Roots) in $\mathbb{Z}_m^*$

Reference Buchmann 2.10

By way of introduction, consider the set $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$. Consider the element 2 of this set. Its powers are

$$2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1.$$

(Note higher powers don't give us anything new in $\mathbb{Z}_5^*$.) So, *every* element of $\mathbb{Z}_5^*$ can be written as a power of 2. We say that 2 is a *generator* or *primitive element* of $\mathbb{Z}_5^*$.

Exercise 3.20. Show that 3 is also a generator of $\mathbb{Z}_5^*$ but that 4 is not.

Example 3.21. Find the generators in $\mathbb{Z}_7^*$. (There are two of them.)

Exercise 3.22. Show that $\mathbb{Z}_8^*$ *has no generators*. Consider in turn all the elements of $\mathbb{Z}_8^*$ (they are $1, 3, 5, 7$) and show, with each of these, their powers cannot generate all

the elements of $\mathbb{Z}_8^*$.

So $\mathbb{Z}_m^*$ does not always have a generator. The obvious question is—*For which m, does $\mathbb{Z}_m^*$ have a generator?* The answer is not easy (See Buchmann 2.10), but a partial and (very useful) answer is the following, stated without proof.

Theorem 3.16. If p is *prime*, then $\mathbb{Z}_p^*$ always has a generator.

We won't prove this result since the proof is more than a little difficult (see Buchmann 2.22). However, you should check a few cases such as $p = 11$ and $p = 13$. In each case, find all the generators. (There are 4 generators in each case.)

In general, if p is prime, $\mathbb{Z}_p^*$ has $\phi(p-1)$ generators, where ϕ is Euler's phi-function (this is also too difficult to prove here). But it follows easily from all this, that if p is a prime of the form $p = 2q + 1$, where q is also prime (for example, $p = 5, 7, 11, 23$ but not $p = 13, 17$), then $\mathbb{Z}_p^*$ has

$$\frac{p-1}{2}$$

generators. If p is large, this means that an element taken at random from $\mathbb{Z}_p^*$ has about a 50% chance of being a generator. This is a useful result in the Diffie-Hellman Key Exchange procedure described later.

Exercise 3.23. Let p and q be primes with $p = 2q + 1$. Show that $\mathbb{Z}_p^*$ has $\frac{p-1}{2}$ generators.

3.8 The Discrete Logarithm Problem in $\mathbb{Z}_p^*$

Reference Buchmann 8.5

Let p be a prime and let g be a generator for $\mathbb{Z}_p^*$. Suppose that we are given an element $a \in \mathbb{Z}_p^*$. Since g is a generator of $\mathbb{Z}_p^*$, the element a is a power of g. In other words, we know that

$$a = g^k \qquad \text{for some integer } k$$

The *discrete logarithm problem* is to find k.

Notation. If $a = g^k$, we call k the *discrete logarithm* of a (to the base g). Some authors write $k = \operatorname{dlog}_g a$.

Example 3.24. With $p = 13$ and $g = 2$, find the discrete logarithm of each element in $\mathbb{Z}_{13}^*$ to the base 2.

Finding discrete logarithms is a difficult problem and in many cases there is no known *efficient* algorithm for solving this problem. We shall see that a very secure encryption scheme can be devised around this fact. It also allows us to find a procedure to transmit secret information over an insecure channel.

3.9 Fast Exponentiation

Reference Buchmann 2.12

In many cryptographic schemes, we have to calculate large powers of an integer, modulo some other integer, that is, to calculate $a^n \bmod m$, when n and m are large. (It is not uncommon in practice to calculate this when $n, m \approx 10^{200}$). If we try to calculate a^n as $a \cdot a \cdots a$ (n times), this requires about $n \approx 10^{200}$ multiplications and a calculating time

scale many times greater than the life span of the universe. This is not satisfactory!

A much better algorithm uses *fast exponentiation*. We illustrate the method with an example. But we first need to learn the binary representation of an integer.

Integers are usually written to *base* 10. There is nothing special about 10, we can choose any integer $b > 1$ for a base.

Example 3.25.

Apart from base 10, other useful bases are 2, 8, and 16—giving respectively the *binary*, *octal*, and *hexadecimal* representations for integers.

- When we use base 16, we write A for 10, B for 11, and so on, up to F for 15.

To emphasize the base, we sometimes write n_b meaning that n has been written to the base b.

Example 3.26. Show that $29_{10} = 11101_2$.

Exercise 3.27. Show that

$$123_{(10)} = 7B_{(16)} = 173_{(8)} = 1111011_{(2)}$$

□

The binary (base 2) representation of an integer is particularly useful. It is the way computers store and calculate. Because binary operations are so fast, it is also the basis for many cryptographic systems. We will see more on this later.

Example 3.28. Calculate $9^{83} \bmod 326$.