# 9 Modular Arithmetic

## 9.1 Modular Addition and Multiplication

In arithmetic **modulo** $n$, when we add, subtract, or multiply two numbers, we take the answer mod $n$. For example, if we want the product of two numbers modulo $n$, then we multiply them normally and the answer is the remainder when the normal product is divided by $n$. The value $n$ is sometimes called the **modulus**.

Specifically, let $\mathbb{Z}_n$ represent the set $\{0, 1, \ldots, n-1\}$ and define the two operations:

$$a +_n b = (a + b) \bmod n$$
$$a \cdot_n b = (a \times b) \bmod n$$

Modular arithmetic obeys the usual rules/laws for the operations addition and multiplication. For example, $a +_n b = b +_n a$ (commutative law) and $(a \cdot_n b) \cdot_n c = a \cdot_n (b \cdot_n c)$ (associative law).

Now, we can write down **tables** for modular arithmetic. For example, here are the tables for arithmetic modulo 4 and modulo 5.

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| $\cdot_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

| $+_5$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

| $\cdot_5$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

The table for addition is rather boring, and it changes in a rather obvious way if we change the modulus.

However, the table for multiplication is a bit more interesting. There is obviously a row with all zeroes. Consider the table for $\cdot_5$. Then in each of the other rows, every value is there and there is no repeated value. This does not always happen; for example, look at the table for modulus 4. Indeed, if both $x$ and the modulus are a multiple of $m$, then every value in the row for $x$ in the multiplication table will be a multiple of $m$. So the only way it can happen that all values appear in the multiplication table in every nonzero row is that the modulus is a prime. And in that case, yes this happens, as we now prove:

**Theorem 9.1** *If $p$ is a prime, and $1 \leq a \leq p-1$, then the values $0 \bmod p$, $a \bmod p$, $2a \bmod p$, $3a \bmod p$, ..., $(p-1)a \bmod p$ are all distinct.*

Proof. Proof by contradiction. Suppose $ia \bmod p = ja \bmod p$ with $0 \leq i < j \leq p-1$. Then $(ja - ia) \bmod p = ja \bmod p - ia \bmod p = 0$, and so $ja - ia = (j-i)a$ is a multiple of $p$. However, $a$ is not a multiple of $p$; so $j - i$ is a multiple of $p$. But that is impossible, because $j - i > 0$ and $j - i < p$. We have a contradiction. ♢

Since there are $p$ distinct values in the row, but only $p$ possible values, this means that every value must appear exactly once in the row.

We can also define **modular subtraction** in the same way, provided we say what the mod operation does when the first argument is negative: $c \bmod d$ is the smallest nonnegative number $r$ such that $c = qd + r$ for some integer $q$; for example, $-1 \bmod d = d - 1$.

## 9.2 Modular Inverses

An interesting question is whether one can define division. This is based on the concept of an inverse, which is actually the more important concept. We define:

> *the* **inverse** *of $b$, written $b^{-1}$, is a number $y$ in $\mathbb{Z}_n$ such that $b \cdot_n y = 1$.*

The question is: does such a $y$ exist? And if so, how to find it? Well, it certainly does exist in some cases.

---

Example 9.1.

For $n = 7$, it holds that $4^{-1} = 2$ and $3^{-1} = 5$.

---

But $0^{-1}$ never exists.

Nevertheless, it turns out that modulo a prime $p$, all the remaining numbers have inverses. Actually, we already proved this when we showed in Theorem 9.1 that all values appear in a row of the multiplication table. In particular, we know that somewhere in the row for $b$ there will be a 1; that is, there exists a $y$ such that $b \cdot_p y = 1$.

And what about the case where the modulus is not a prime? For example, $7^{-1} = 13$ when the modulus is 15.

**Theorem 9.2** *$b^{-1}$ exists in $\mathbb{Z}_n$ if and only if $b$ and $n$ are relatively prime.*

PROOF. There are two parts to prove. If $b$ and $n$ have a common factor say $a$, then any multiple of $b$ is divisible by $a$ and indeed $b \cdot_n y$ is a multiple of $a$ for all $y$, so the inverse does not exist.

If $b$ is relatively prime to $n$, then consider Euclid's extended algorithm. Given $n$ and $b$, the algorithm behind Theorem 8.2 will produce integers $x$ and $y$ such that:

$$n \times x + b \times y = 1.$$

And so $b \cdot_n y = 1$. $\Diamond$

And, by using the extension of Euclid's algorithm, one actually has a quick algorithm for finding $b^{-1}$. One of the exercises is to show that if an inverse exists, then it is unique.

> ▶ **For you to do!** ◀
> *1. List all the values in $\mathbb{Z}_{11}$ and their inverses.*

## 9.3 Modular Exponentiation

Modular arithmetic is used in cryptography. In particular, **modular exponentiation** is the cornerstone of what is called the RSA system.

We consider first an algorithm for calculating modular powers. The **modular exponentiation** problem is:

> compute $g^A \bmod n$, given $g$, $A$, and $n$.

The obvious algorithm to compute $g^A \bmod n$ multiplies $g$ together $A$ times. But there is a much faster algorithm to calculate $g^A \bmod n$, which uses at most $2 \log_2 A$ multiplications.

The algorithm uses the fact that one can reduce modulo $n$ at each and every point. For example, that $ab \bmod n = (a \bmod n) \times (b \bmod n) \bmod n$. But the key savings is the insight that $g^{2B}$ is the square of $g^B$.

```
DEXPO(g,A,n)
  if A = 0 then return 1
  else if A odd {
    z = dexpo(g, A − 1, n)
    return(zg mod n)        % uses g^A = g × g^(A−1)
    }
  else {
    z = dexpo (g, A/2, n)
    return(z^2 mod n)       % uses g^A = (g^(A/2))^2
    }
```

Note that the values of $g$ and $n$ are constant throughout the recursion. Further, at least every second turn the value of $A$ is even and therefore is halved. Therefore the depth of recursion is at most $2\log_2 A$.

We can do a modular exponentiation calculation by hand, by working out the sequence of values of $A$, and then calculating $g^A \bmod n$ for each of the $A$, starting with the smallest (which is $g^0 = 1$).

---

EXAMPLE 9.2. *Calculate* $3^{12} \bmod 5$.

| $A$ | $g^A \bmod n$ |
|---|---|
| 12 | $4^2 \bmod 5 = 1$ |
| 6 | $2^2 \bmod 5 = 1$ |
| 3 | $3 \times 4 \bmod 5 = 2$ |
| 2 | $3^2 \bmod 5 = 4$ |
| 1 | $3 \times 1 \bmod 5 = 3$ |
| 0 | 1 |

---

▶ **For you to do!** ◀

2. *Use the* DEXPO *algorithm to calculate* $4^{14} \bmod 11$.

## 9.4 Modular Equations

A related question is trying to solve modular equations. These arise in puzzles where it says that: there was a collection of coconuts and when we divided it into four piles there was one left over, and when we divided it into five piles, etc.

**Theorem 9.3** *Let $a \in \mathbb{N}$, and let $b$ and $c$ be positive integers that are relatively prime. Then the solution to the equation*

$$c \times x \bmod b = a$$

*is all integers of the form $ib + a \cdot_b c^{-1}$ where $i$ is an integer (which can be negative).*

PROOF. We claim that the solution is all integers $x$ such that $x \bmod b = a \cdot_b c^{-1}$, where $c^{-1}$ is calculated modulo $b$. The proof of this is just to multiply both sides of the equation by $c^{-1}$, which we know exists. From there the result follows. $\diamondsuit$

---

EXAMPLE 9.3. *Solve the equation* $3x \bmod 10 = 4$.

Then $3^{-1} = 7$ and $4 \cdot_{10} 7 = 8$. So $x \bmod 10 = 8$.

---

This is then generalized in the Chinese Remainder Theorem. Here is just a special case:

**Theorem 9.4** *If $p$ and $q$ are primes, then the solution to the pair of congruences*

$$x \equiv_p a \qquad \textit{and} \qquad x \equiv_q b$$

*is all integers $x$ such that*

$$x \equiv_{pq} qaq^{-1} + pbp^{-1}$$

*where $p^{-1}$ is the inverse of $p$ modulo $q$ and $q^{-1}$ is the inverse of $q$ modulo $p$.*

We omit the proof.

---

EXAMPLE 9.4. *Determine all integers that have remainder* 2 *when divided by* 5 *and remainder* 4 *when divided by* 7.

In the notation of the above theorem, $a = 2$, $p = 5$, $b = 4$, and $q = 7$. In $\mathbb{Z}_7$, $5^{-1} = 3$. In $\mathbb{Z}_5$, $7^{-1} = 2^{-1} = 3$. So the set of solutions has remainder $7 \cdot 2 \cdot 3 + 5 \cdot 4 \cdot 3 \equiv_{35} 32$. So the answer is $35x + 32$ for $x$ an integer.

---

## 9.5 Modular Exponentiation Theorems

We start with a famous theorem called **Fermat's Little Theorem**.

**Theorem 9.5** *Fermat's little theorem. If $p$ is a prime, then for $a$ with $1 \leq a \leq p-1$,*

$$a^{p-1} \bmod p = 1.$$

PROOF. Let $S$ be the set $\{ ia \bmod p : 1 \leq i \leq p-1 \}$. That is, multiply $a$ by all integers in the range 1 to $p-1$ and write down the remainders when each is divided by $p$. Actually, we already looked at this set: it is the row corresponding to $a$ from the multiplication table for $p$. And in Theorem 9.1 we showed that these values are all distinct. Therefore, $S$ is actually just the set of integers from 1 up to $p-1$.

Now, let $A$ be the product of the elements in $S$. To avoid ugly formulas, we use $x \equiv_p y$ to mean $x \bmod p = y \bmod p$. And we use $\Pi$-notation, which is the same as $\Sigma$-notation except that it is the product rather than the sum. By Theorem 9.1 and the above discussion,

$$\prod_{i=1}^{p-1} ((ia) \bmod p) = \prod_{i=1}^{p-1} i$$

But, we can also factor out the $a$'s:

$$\prod_{i=1}^{p-1} (ia) \bmod p \equiv_p a^{p-1} \prod_{i=1}^{p-1} i$$

It follows that

$$\prod_{i=1}^{p-1} i \equiv_p a^{p-1} \prod_{i=1}^{p-1} i$$

Divide both sides by $\prod_{i-1}^{p-1} i$ and we get that $a^{p-1} \equiv_p 1$; that is, $a^{p-1} \bmod p = 1$. $\diamondsuit$

The above result is generalized by **Euler's Theorem**. We will need the following special case in the next chapter:

**Theorem 9.6** *Special case of Euler's theorem. If $a$ and $n = pq$ are relatively prime, with $p$ and $q$ distinct primes, then $a^\phi \bmod n = 1$ where $\phi = (p-1)(q-1)$.*

We omit the proof.

## 9.6 Square-Roots

A **square-root** of $a$ in $\mathbb{Z}_n$ as any element $b$ such that $b^2 \bmod n$. For example, in $\mathbb{Z}_7$, 3 is a square-roots of 2, since $9 \bmod 7 = 2$.

Note that it is **not** guaranteed to exist. For example, 3 does not have a square-root in $\mathbb{Z}_7$. Further, if $b$ is a square-root of $a$, then so is $n-b$ (since $(n-b)^2 = n^2-2nb+b^2 \equiv_n b^2 \equiv_n a$). In the exercises you have to show that:

**Lemma 9.7** *If $n$ is any prime, then $a$ has at most two square-roots modulo $n$.*

***Exercises***

9.1. (a) Write out the addition and multiplication tables for $\mathbb{Z}_2$.

(b) If we define 1 as true and 0 as false, explain which boolean connectives correspond to $+_2$ and $\cdot_2$.

9.2. Give the multiplication tables for $\mathbb{Z}_6$ and $\mathbb{Z}_7$.

9.3. Calculate $5^{-1}$ and $10^{-1}$ in $\mathbb{Z}_{17}$.

9.4. Prove that if $b$ has an inverse in $\mathbb{Z}_n$, then it is unique.

9.5. How many elements of $\mathbb{Z}_{91}$ have multiplicative inverses in $\mathbb{Z}_{91}$?

9.6. How many rows of the table for $\cdot_{12}$ contain all values?

9.7. Consider $\mathbb{Z}_{10}$.

(a) List all elements of $\mathbb{Z}_{10}$.

(b) What is the inverse of 3?

(c) Give all square-roots of 6.

(d) How many rows of the multiplcation table contain every element?

9.8. (a) Consider the primes 5, 7, and 11 for $n$. For each integer from 1 through $n-1$, calculate its inverse.

(b) A number is **self-inverse** if it is its own inverse. For example, 1 is always self-inverse. Based on the data from (a), state a conjecture about the number of self-inverses when $n$ is a prime.

(c) Prove your conjecture.

9.9. Given $a, b \in \mathbb{Z}_n$, we say that $b$ is a **modular square-root** of $a$ if $b \cdot_n b = a$.

(a) List all the elements in $\mathbb{Z}_{11}$, and for each element, list all their modular square-roots, if they have any.

(b) Prove that if $n$ is prime then $a$ has at most two square-roots.

(c) Give an example that shows that it is possible for a number to have **more** than 2 square-roots.

9.10. (a) Consider the primes 5, 7, and 11 for $n$. For each $a$ from 1 through $n-1$, calculate $a^2 \bmod n$ (which is the same as $a \cdot_n a$).

(b) A number $y$ is a **quadratic residue** if there is some $a$ such that $y = a^2 \bmod n$. For example, 1 is always a quadratic residue (since it is $1^2 \bmod n$). Based on the data from (a), state a conjecture about the number of quadratic residues.

(c) Prove your conjecture.

9.11. (a) Compute $2^{38} \bmod 7$.

(b) Compute $3^{29} \bmod 20$.

(c) Compute $5^{33} \bmod 13$.

9.12. Describe all solutions to the modular equation $7x \bmod 8 = 3$.

9.13. Find the smallest positive solution to the set of modular equations:

$$x \bmod 3 = 2, \quad x \bmod 11 = 4, \quad x \bmod 8 = 7.$$

9.14. (a) Prove that $(a+b)^p \bmod p = (a^p + b^p) \bmod p$ if $p$ is a prime.

(b) Use part (a) to give a proof of Fermat's Little Theorem.

9.15. Using the Binomial Theorem (and without using Fermat's Little Theorem), prove that for any odd prime $p$, it holds that $2^p \bmod p = 2$.

---

***Solutions to Practice Exercises***

1.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 6 | 4 | 3 | 9 | 2 | 8 | 7 | 5 | 10 |

2.

| $A$ | $g^A \bmod n$ |
|---|---|
| 14 | 3 |
| 7 | 5 |
| 6 | 4 |
| 3 | 9 |
| 2 | 5 |
| 1 | 4 |
| 0 | 1 |