# Molular Arithmetic & Inverses

Alston Yam

## 1 Preview/Review of our class!

### 1.1 Modular Arithmetic

**Definition 1.1** We write

$$a \equiv b \pmod{n}$$

if and only if $n \mid a - b$.

Notice that, with this handy notation, we have

$$a = qn + r \iff a \equiv r \pmod{n}$$

This means that this modular arithmetic notation is closely related to the division algorithm and remainders.

**Exercise 1.1** Evaluate $86 \equiv\ ?\ \pmod{17}$

**Exercise 1.2** Evaluate $91 \equiv\ ?\ \pmod{13}$

The power of modular arithmetic actually extends beyond just remainders! As we will soon see, our addition, subtraction, multiplication, and division operations still (mostly) hold true in modular arithmetic.

#### 1.1.1 Addition, Subtraction, and Multiplication

The operations of addition, subtraction, and multiplication are compatible with modular arithmetic. Specifically, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

$$\begin{aligned} a + c &\equiv b + d \pmod{n} \\ a - c &\equiv b - d \pmod{n} \\ ac &\equiv bd \pmod{n} \end{aligned}$$

**Exercise 1.3** By writing $a = An + r_1, b = Bn + r_1, c = Cn + r_2, d = Dn + r_2$, prove each of the above statements.

#### 1.1.2 Division

Unlike the three other operations we have seen, division is not always compatible with modular arithmetic. See below:

**Example 1.1**

$$6 \equiv 0 \pmod 3$$

but

$$\frac{6}{3} = 2 \not\equiv 0 = \frac{0}{3} \pmod 3$$

So, to handle division, we must introduce the concept of **inverses**.

## 1.2 Inverses

**Definition 1.2 – Inverses** Let $a$ be an integer and $n$ a positive integer. We say that $x$ is the **inverse** of $a$ modulo $n$ if

$$a \cdot x \equiv 1 \pmod n$$

Here, we may write $x \equiv a^{-1} \pmod n$.

Inverses **do not** always exist.

**Example 1.2** if $n = 6$, then 2 does not have an inverse modulo 6 because

$$2 \cdot x \equiv 1 \pmod 6$$

has no solution.

So instead of jumping to the general $n$, lets first investigate the special case where $n = p$ is a prime. Consider the set of integers $\{1, 2, \ldots, p-1\}$, and multiply each element by an integer $a$ coprime to $p$ (This will become important later). So we arrive at the set $\{a, 2a, \ldots, (p-1)a\}$. I claim that:

**Lemma:** The second set is actually a permutation of the first under mod $p$.

*Proof.* We will go by arguing that every element in the second set is distinct under mod $p$. This is sufficient, as we can see that if no two elements are the same under mod $p$, then the $p-1$ elements in the second set must each match up to one of the $p-1$ elements in the first set.
So suppose $\exists\ i, j$ such that $ia \equiv ja \pmod p$ for some $1 \leq i < j \leq p-1$. Then we have

$$ia - ja \equiv 0 \pmod p \iff (i-j)a \equiv 0 \pmod p \iff p \mid a(i-j)$$

Since $a$ is coprime to $p$, we must have that $p \mid i - j$, which implies that $i = j$, a contradiction to $i < j$. Thus, every element in the second set is distinct under mod $p$, and we're done. □

What does this mean? Well, for any $a$ coprime to $p$, we can actually find an $x \in \{1, 2, \ldots, p-1\}$ such that

$$ax \equiv 1 \pmod p$$

This means that every integer $a$ coprime to $p$ has an inverse modulo $p$, which is a really cool result!

Now lets think about how we can generalise this to any positive integer $n$.

**Exercise 1.4** Prove that for an integer $n$, every integer $a$ coprime to $n$ has an inverse modulo $n$.

Hint: think about where did we use the fact that $a$ was coprime to $p$ in our previous proof? Does our proof still hold true even if $n$ is now no longer a prime?

Let's turn our attention back to our goal: dividing in modular arithmetic.

**Example 1.3** Solve for $x$ in

$$ax \equiv b \pmod{p}$$

**Solution:**

$$x \equiv ax \cdot a^{-1} \equiv b \cdot a^{-1} \pmod{p}$$

As we can see, we have essentially "divided" both sides by $a$. In fact, if we write $a^{-1} \equiv \frac{1}{a} \pmod{p}$, we have the property that inverses will behave just like fractions.

**Example 1.4** Show that

$$\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd} \pmod{p}$$

**Solution:**

$$ab^{-1} + cd^{-1} \equiv (ad+bc)(bd)^{-1} \equiv \frac{ad+bc}{bd} \pmod{p}$$

**Exercise 1.5** In a similar fasion, show that

$$\frac{a}{b} \cdot \frac{c}{d} \equiv \frac{ac}{bd} \pmod{p}$$

## 1.3 A Couple of Useful Results

**Theorem 1.1 – Fermat's Little Theorem** Let $a$ be any integer relatively prime to a prime $p$. Then

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

**Theorem 1.2 – Euler's Totient Theorem** If $gcd(a, m) = 1$, then we have

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Where $\phi(m)$ represents the number of positive integers $k \leq m$ with $gcd(k, m) = 1$.

Keen eyed readers might notice that Euler's Totient Theorem is in fact a generalisation of Fermat's Little Theorem!

**Theorem 1.3 – Wilson's Theorem** Let $p$ be a prime. Then

$$(p-1)! \equiv -1 \pmod{p}$$

## 2 Problems

**Problem 2.1** Prove that $15m - 3 \equiv 0 \pmod 7$ if and only if $41m - 10 \equiv 0 \pmod 7$

**Problem 2.2** Is $3^{16} - 2^{16}$ divisible by 17?

**Problem 2.3** Let $p$ be a prime. Prove that if $a$ is an integer such that $gcd(a, p) = 1$, then $a^{p-2} \equiv a^{-1} \pmod p$.

**Problem 2.4** Let $p$ be a prime, show that if $p$ divides $a^p - 1$ then $p^2$ divides $a^p - 1$.

**Problem 2.5** Prove each of the three theorems in section 1.3.

**Problem 2.6 – St. Petersburg 2008** Given three distinct natural numbers $a, b, c$, show that

$$gcd(ab + 1, bc + 1, ca + 1) \leq \frac{a + b + c}{3}$$

**Problem 2.7 – IMO 2005 Q4** Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n = 2^n + 3^n + 6^n - 1, n \geq 1$$