Number Theory

Modular Arithmetic, Units, and Order,
Recursion and Fibonacci Numbers,
Fermat's Little Theorem,
Chinese Remainder Theorem, Wilson's Theorem

Walter Johnson Mathematics Team

What is Number Theory?

Number Theory is the study of the **Integers**:

$$\boxed{\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}}$$

That's all in Number Theory! Just these numbers. No fractions or irrationals. Nevertheless, Number Theory has some truly beautiful nuance and applications in wild combinatorical scenarios.

Review

Every integer can be represented in its **Unique Prime Factorization**:

$$\boxed{N = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}}$$

Where $p_i, e_i \in \mathbb{Z}$. Some examples are below:

$$\begin{aligned} 27492 &= 2^2 \times 3^1 \times 29^1 \times 79^1 \\ 1738044 &= 2^2 \times 3^3 \times 7^1 \times 11^2 \times 19^1 \\ 314159 &= 314159^1 \end{aligned}$$

This can be very important, but easy to forget.

Review

The **Division Algorithm** for integers states that if integer p is divided by integer q, then we have the statement:

$$p = mq + r$$

for some integer m and some integer remainder r such that $0 \leq r < q$. q is said to be a factor of p if $r = 0$.

Although this is simple and easily forgettable, it can be incredibly powerful. Under certain circumstances and conditions, proving that r must be 0 proves that q is a factor of p.

Modulo

One of the fundamental lenses that we look at the integers through is what we call a **Modulus**. A modulus is a very simple idea.

Let's say we want to look at all the integers **modulus 5** or **mod 5** for short. This means we take all of the integers, and we **take their remainder** when **divided by 5**, our modulus.

Modulo

One of the fundamental lenses that we look at the integers through is what we call a **Modulus**. A modulus is a very simple idea.
Let's say we want to look at all the integers **modulus 5** or **mod 5** for short. This means we take all of the integers, and we **take their remainder** when **divided by 5**, our modulus.
Instead of using the equivalence operator (=), we use the **congruency operator** (≡) to show that two numbers are equal under a modulus:

$$\begin{aligned} 1 &\equiv 1 \pmod{5} \\ 4 &\equiv 4 \pmod{5} \\ 5 &\equiv 0 \pmod{5} \\ 23 &\equiv 3 \pmod{5} \\ -1 &\equiv 4 \pmod{5} \end{aligned}$$

Modulo

Now let's say we have all of the numbers that are congruent to some other number mod 5:

$$1 \equiv 1 \equiv 6 \equiv 11 \equiv 16 \equiv 21 \cdots \pmod 5$$

We call this a **Congruency Class**. The congruency class of 1 mod 5 is equal to the set containing all of those numbers.

Modulo

Now let's say we have all of the numbers that are congruent to some other number mod 5:

$$1 \equiv 1 \equiv 6 \equiv 11 \equiv 16 \equiv 21 \cdots \pmod{5}$$

We call this a **Congruency Class**. The congruency class of 1 mod 5 is equal to the set containing all of those numbers. For 5, there are 5 congruency classes:

$$\begin{aligned} 0 \equiv 5 \equiv 10 \equiv 15 \equiv 20 \equiv \cdots \pmod{5} \\ 1 \equiv 6 \equiv 11 \equiv 16 \equiv 21 \equiv \cdots \pmod{5} \\ 2 \equiv 7 \equiv 12 \equiv 17 \equiv 22 \equiv \cdots \pmod{5} \\ 3 \equiv 8 \equiv 13 \equiv 18 \equiv 23 \equiv \cdots \pmod{5} \\ 4 \equiv 9 \equiv 14 \equiv 19 \equiv 24 \equiv \cdots \pmod{5} \end{aligned}$$

Notice that **all of the integers** are contained in these 5 congruency classes!

$\mathbb{Z}/n\mathbb{Z}$

We take all of these congruency classes and put them into one finite 5 element set, and we just represent them with their trivial number:

$$\{0, 1, 2, 3, 4\}$$

$\mathbb{Z}/n\mathbb{Z}$

We take all of these congruency classes and put them into one finite 5 element set, and we just represent them with their trivial number:

$$\{0, 1, 2, 3, 4\}$$

We call this $\mathbb{Z}$ mod 5 $\mathbb{Z}$:

$$\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$$

$\mathbb{Z}/n\mathbb{Z}$

We take all of these congruency classes and put them into one finite 5 element set, and we just represent them with their trivial number: We call this $\mathbb{Z}$ mod 5 $\mathbb{Z}$:

$$\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$$

This is important because we can do this with **any number**! We do this with n:

$$\boxed{\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-2, n-1\}}$$

Notice that **all integers** exist in this set, they're in **one** of the congruency classes that the set has.

Modular Arithmetic

What's so special about $\mathbb{Z}/n\mathbb{Z}$?
What's special about $\mathbb{Z}/n\mathbb{Z}$ is that the rules of arithmetic stay true mod n. This means we can do arithmetic under a modulus!
We call this **Modular Arithmetic**:

$$1 + 6 \equiv 7 \pmod{9}$$
$$5 + 4 \equiv 0 \pmod{3}$$
$$4 \times 3 \equiv 1 \pmod{11}$$

Modular Arithmetic

What's so special about $\mathbb{Z}/n\mathbb{Z}$?
What's special about $\mathbb{Z}/n\mathbb{Z}$ is that the rules of arithmetic stay true mod n. This means we can do arithmetic under a modulus!
We call this **Modular Arithmetic**:

$$1 + 6 \equiv 7 \pmod{9}$$
$$5 + 4 \equiv 0 \pmod{3}$$
$$4 \times 3 \equiv 1 \pmod{11}$$

We can even look at variables:

$$n \equiv 0 \pmod{n}$$
$$(n+1)^2 \equiv n^2 + 2n + 1 \equiv 1 \pmod{n}$$
$$(n+1)(n+2) \equiv n^2 + 3n + 2 \equiv 2 \pmod{n}$$

Inverses

In the set of real numbers $\mathbb{R}$, we have two kinds of inverses. **Additive Inverses** and **Multiplicative Inverses**. You are very familiar with these:

$$\begin{aligned} 4 + (-4) &= 0 \\ 25 + (-25) &= 0 \end{aligned}$$

and

$$\begin{aligned} 3 \times \frac{1}{3} &= 1 \\ \sqrt{2} \times \frac{1}{\sqrt{2}} &= 1 \end{aligned}$$

For each number in $\mathbb{R}$, there is an additive and multplicative inverse. Just like this, for each number in $\mathbb{Z}/n\mathbb{Z}$, there is a multiplicative inverse and an additive inverse.

Inverses in $\mathbb{Z}/n\mathbb{Z}$

Let's look at $\mathbb{Z}/9\mathbb{Z}$ for a second. We see that 2 and 7, as well as 5 and 4 are additive inverses:

$$2 + 7 \equiv 7 + 2 \equiv 0 \pmod{9}$$

$$5 + 4 \equiv 4 + 5 \equiv 0 \pmod{9}$$

And we see that 6 and 3 are multiplicative inverses, as well as 3 and itself:

$$6 \times 3 \equiv 0 \pmod{9}$$

$$3 \times 3 \equiv 0 \pmod{9}$$

Inverses in $\mathbb{Z}/n\mathbb{Z}$

Multiplicative inverses are especially important because they allow us to solve congruencies like this:

$$5x \equiv 11 \pmod{12}$$

We notice that the modular inverse of 5 is 5 mod 12, since $5 \times 5 \equiv 25 \equiv 1 \bmod 12$, so when we multiply both sides by 5 we find:

$$\begin{aligned} 5x &\equiv 11 \pmod{12} \\ 5 \times 5x &\equiv 5 \times 11 \pmod{12} \\ 1 \times x &\equiv 55 \pmod{12} \\ x &\equiv 7 \pmod{12} \end{aligned}$$

Units

If a number is a **unit** mod n, it means that there is some power it can be raised to to be congruent to 1 mod n. For example, let's look at 3 mod 11:

$$\begin{aligned} 3^0 &\equiv 1 \pmod{11} \\ 3^1 &\equiv 3 \pmod{11} \\ 3^2 &\equiv 9 \pmod{11} \\ 3^3 &\equiv 5 \pmod{11} \\ 3^4 &\equiv 4 \pmod{11} \\ 3^5 &\equiv 1 \pmod{11} \end{aligned}$$

Why is this important?

Units

$$3^0 \equiv 1 \pmod{11}$$
$$3^1 \equiv 3 \pmod{11}$$
$$3^2 \equiv 9 \pmod{11}$$
$$3^3 \equiv 5 \pmod{11}$$
$$3^4 \equiv 4 \pmod{11}$$
$$3^5 \equiv 1 \pmod{11}$$

Why is this important?
What if we were asked to find

$$3^{2021} \pmod{11}?$$

Units

$$\begin{aligned}
3^0 &\equiv 1 \pmod{11} \\
3^1 &\equiv 3 \pmod{11} \\
3^2 &\equiv 9 \pmod{11} \\
3^3 &\equiv 5 \pmod{11} \\
3^4 &\equiv 4 \pmod{11} \\
3^5 &\equiv 1 \pmod{11}
\end{aligned}$$

What if we were asked to find $3^{2021} \pmod{11}$? We know that $3^5 \equiv 1$, so every multiple of 3^5 is going to be equivalent to 1. Thus, all we need to find is

$$2021 \equiv 1 \pmod{5}$$

And so

$$3^{2021} \equiv 3^1 \equiv 1 \pmod{11}$$

Order

In this scenario, we say that the number 3 has an **Order** of 5 under modulus 11. Order is defined as the least positive integer e such that

$$\boxed{a^e \equiv 1 \pmod{n}}$$

You would say that the order of $a \pmod{n}$ is e.
Order is important because it allows us to simplify very high powers of numbers. A number a only has an order mod n if a and n are relatively prime. If a number is not a unit $\pmod{n}$, then it is said to have an **infinite order**.

Order

Let's look at a classic example of this:

Let

$$k = 2008^2 + 2^{2008}$$

Find the units digit of k^2

Order

Let

$$k = 2008^2 + 2^{2008}$$

Find the units digit of k^2

This is a classic problem. The first thing to notice is, what is the units digit of an arbitrary integer n?

Order

Let

$$k = 2008^2 + 2^{2008}$$

Find the units digit of k^2

The thing to notice is whenever you are asked about the units digit of a number n, what you are really being asked is: What is $n \pmod{10}$? This makes the problem much easier.

Order

Let

$$k = 2008^2 + 2^{2008}$$

Find the units digit of k^2

The whole problem is essentially just finding

$$k^2 \pmod{10}$$

Order

Let

$$k = 2008^2 + 2^{2008}$$

Find the units digit of k^2

The whole problem is essentially just finding

$$k^2 \pmod{10}$$

We *could* try to evaluate k^2 and then find it's units digit, but this be incredibly tedius. Instead, we can just find

$$k \pmod{10}$$

and square it!

Order

Let

$$k = 2008^2 + 2^{2008}$$

Find the units digit of k^2

So now we're trying to find

$$k \pmod{10}$$

Which is

$$k \equiv 2008^2 + 2^{2008} \pmod{10}$$

Where do we go from here?

Order

Let

$$k = 2008^2 + 2^{2008}$$

Find the units digit of k^2

$$k \equiv 2008^2 + 2^{2008} \pmod{10}$$

Notice that $2008 \equiv 8 \pmod{10}$, so we can just plug that into there:

$$k \equiv 8^2 + 2^{2008} \pmod{10}$$

and we can further simplify by multiplying:

$$k \equiv 64 + 2^{2008} \equiv 4 + 2^{2008} \pmod{10}$$

Order

Let

$$k = 2008^2 + 2^{2008}$$

Find the units digit of k^2

$$k \equiv 64 + 2^{2008} \equiv 4 + 2^{2008} \pmod{10}$$

Hmm, we've done really well on the 2008^2 part, but how do we go about the 2^{2008} part?

Order

Let $k = 2008^2 + 2^{2008}$. Find the units digit of k^2

We can think about it like this:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{10} \\ 2^2 &\equiv 4 \pmod{10} \\ 2^3 &\equiv 8 \pmod{10} \\ 2^4 &\equiv 6 \pmod{10} \\ 2^5 &\equiv 2 \pmod{10} \end{aligned}$$

Ah-ha!

Order

Let $k = 2008^2 + 2^{2008}$. Find the units digit of k^2

$$\begin{aligned} 2^1 &\equiv 2 \pmod{10} \\ 2^2 &\equiv 4 \pmod{10} \\ 2^3 &\equiv 8 \pmod{10} \\ 2^4 &\equiv 6 \pmod{10} \\ 2^5 &\equiv 2 \pmod{10} \end{aligned}$$

We see the powers of $2 \pmod{10}$ are periodic with a period of 4!

Order

Let $k = 2008^2 + 2^{2008}$. Find the units digit of k^2

This means

$$2^1 \equiv 2^5 \equiv 2^9 \equiv 2^{13} \cdots \equiv 2 \pmod{10}$$

And any number that is 1 more than a multiple of 4 is congruent to 2 (mod 10). Looking back to our expression, we see that 2008 is pretty close to 2005, which is 1 more than a multiple of 4:

$$2^{2008} \equiv 2^{2005+3} \pmod{10}$$

Order

Let $k = 2008^2 + 2^{2008}$. Find the units digit of k^2

What we can do now is take this and break it up:

$$2^{2008} \equiv 2^{2005+3} \equiv 2^{2005} \times 2^3 \equiv 2 \times 8 \equiv 6 \pmod{10}$$

Order

Let $k = 2008^2 + 2^{2008}$. Find the units digit of k^2

What we can do now is take this and break it up:

$$2^{2008} \equiv 2^{2005+3} \equiv 2^{2005} \times 2^3 \equiv 2 \times 8 \equiv 6 \pmod{10}$$

And pluggint this back into the problem we have:

$$k \equiv 4 + 6 \equiv 0 \pmod{10}$$

So we know that

$$\boxed{k^2 \equiv 0 \pmod{10}}$$

Recursion

Fibonacci Numbers

Questions?

Fermat's Little Theorem

Fermat's Little Theorem is perhaps the most important theorem in Number Theory. We're going to prove it first. Let's consider the set

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-2, p-1\}$$

Which is the set $\mathbb{Z}$ mod p for p a prime number.

Fermat's Little Theorem

Fermat's Little Theorem is perhaps the most important theorem in Number Theory. We're going to prove it first. Let's consider the set

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-2, p-1\}$$

Now what we're going to do is multiply this set (every element in the set) by some number a:

$$a \times \{0, 1, 2, \dots, p-1, p-1\} = \{0a, 1a, 2a, \dots, (p-2)a, (p-1)a\}$$

Fermat's Little Theorem

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-2, p-1\}$$

Now what we're going to do is multiply this set (every element in the set) by some number a:

$$a \times \{0, 1, 2, \ldots, p-1, p-1\} = \{0a, 1a, 2a, \ldots, (p-2)a, (p-1)a\}$$

Because p is a prime number, this new set is simply a **reordering** of the original set mod p! All we did was rearrange the numbers in $\mathbb{Z}/p\mathbb{Z}$. Take a moment to convince yourself of that.

Fermat's Little Theorem

Because it was just a rearrangement, if we multiply all of the non-zero numbers from $\mathbb{Z}/p\mathbb{Z}$ and $a \times \mathbb{Z}/p\mathbb{Z}$, we will get the same value:

$$1 \times 2 \times \cdots \times (p-2) \times (p-1) \equiv 1a \times 2a \times \cdots \times (p-2)a, (p-1)a \pmod{p}$$

Fermat's Little Theorem

Because it was just a rearrangement, if we multiply all of the non-zero numbers from $\mathbb{Z}/p\mathbb{Z}$ and $a \times \mathbb{Z}/p\mathbb{Z}$, we will get the same value:

$$1\times 2\times\cdots\times(p-2)\times(p-1) \equiv 1a\times 2a\times\cdots\times(p-2)a, (p-1)a \pmod{p}$$

And with this, we see this is just:

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

Fermat's Little Theorem

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

With this, we can just factor out the $(p-1)!$:

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

Which is Fermat's Little Theorem!
This theorem is the crux of many competitive math problems we'll see. There are many ways to prove this, but you just need to understand that it is true for all numbers a and prime numbers p.

Fermat's Little Theorem

Let's look at a practice problem.

System Of Congruencies

Just like how there are systems of equations in algebra, there are **Systems of Congruencies** in Number Theory. An example is:

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 5 \pmod{11} \end{aligned}$$

System Of Congruencies

We can generalize this to some system with k moduli:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

This is a system of congruencies.

Chinese Remainder Theorem

The **Chinese Remainder Theorem** makes a claim about systems of congruencies:

Given a system of congruencies under coprime moduli $n_1, n_2, \ldots n_k$, there exists a unique solution to the system modulo N for

$$N = n_1 \times n_2 \times \cdots \times n_k$$

Notice, this theorem only states two things; the **existence** of a solution mod N, and the **uniqueness** of the solution mod N. It doesn't tell us how to get that solution! But don't worry, there is a simple algorithm to find it.

Questions?

Euler-Phi-Totient Function

Before we discuss more intricate theorems, we need to discuss **Euler's Totient Function**, or **Euler's Phi Function**, which counts the number of integers less than or equal to n which are relatively prime to n. This function is denoted

$$\phi(n)$$

Euler-Phi-Totient Function

The **Euler's Totient Function**, or the **Euler's Phi Function**, which counts the number of integers less than or equal to n which are relatively prime to n. This function is denoted

$$\phi(n)$$

A few examples are

$$\begin{aligned}
\phi(6) &= 2 \\
\phi(7) &= 6 \\
\phi(9) &= 6 \\
\phi(16) &= 8 \\
\phi(43) &= 42
\end{aligned}$$

Euler-Phi-Totient Function

The **Euler's Totient Function**, or the **Euler's Phi Function**, counts the number of integers less than or equal to n which are relatively prime to n. This function is denoted

$$\phi(n)$$

Notice, $\phi(p)$ for p a prime is always equal to $p-1$:

$$\begin{aligned}
\phi(6) &= 2 \\
\phi(7) &= 6 \leftarrow \\
\phi(9) &= 6 \\
\phi(16) &= 8 \\
\phi(43) &= 42 \leftarrow
\end{aligned}$$

Euler-Phi-Totient Function

The **Euler's Totient Function**, or the **Euler's Phi Function**, counts the number of integers less than or equal to n which are relatively prime to n.
We see a more rigorous definition:

$$\boxed{\phi(n) = \sum_{m:\gcd(m,n)=1} 1}$$

This function has a variety of cool properties, many of which we will not discuss.

Euler-Phi-Totient Function

Another interesting property of this function is that if $\gcd(m, n) = 1$, then the function is multiplicative:

$$\phi(mn) = \phi(m)\phi(n)$$

Fundamental Theorem of Orders

The **Fundamental Theorem of Orders** for **prime moduli** states that

If

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

Then the order of $a \pmod{p}$ divides N, or $a|N$.

This is quite intuitive when we think about it for a minute.

Fundamental Theorem of Orders

If $a^N \equiv 1 \pmod{p}$ then the order of $a \pmod{p}$ divides N, or $a|N$.

This makes sense, because let's say the order of $a \pmod{p}$ is e. Then the next smallest integer N which lets $a^N \equiv 1$ must be $N = 2e$, because $a^{2e} \equiv a^e \times a^e \equiv 1 \equiv 1$.
Conversely, if we assume $N = e + j < 2e$, then

$$1 \equiv a^N \equiv a^e \times a^j = 1 \times e^j \equiv e^j \equiv 1$$

for some $j < e$, which is a contradiction, because e is minimal.

Fundamental Theorem of Orders

> If $a^N \equiv 1 \pmod{p}$ then the order of $a \pmod{p}$ divides N, or $a|N$.

Another, more rigorous proof of this is as such:
If $a^N \equiv 1$ and e is the order of a, then by the division algorithm:

$$N = de + r$$

For some d and $r < e$. This also means we can write

$$a^N \equiv 1 \equiv a^{de+r} \equiv a^{de} \times a^r \pmod{p}$$

Then we can bring the de to the other side:

$$a^N \times a^{-de} \equiv a^r \pmod{p}$$

Fundamental Theorem of Orders

If $a^N \equiv 1 \pmod{p}$ then the order of a (mod p) divides N, or $a|N$.

$$a^N \equiv 1 \equiv a^{de+r} \equiv a^{de} \times a^r \pmod{p}$$

We could then bring the $-d$ out of the exponent:

$$a^N \times a^{-de} \equiv a^N \times (a^e)^{-d} \equiv a^r \pmod{p}$$

But since $a^N \equiv 1$ and $a^e \equiv 1$ we have

$$a^N \times (a^e)^{-d} \equiv 1 \times (1)^{-d} \equiv 1 \equiv a^r \equiv a^0 \pmod{p}$$

and thus $r = 0$, which means $e|N$.

Fundamental Theorem of Orders

If $a^N \equiv 1 \pmod p$ then the order of $a \pmod p$ divides N, or $a|N$.

When we combine this with Fermat's Little Theorem, we have:

The order of $a \pmod p$ divides $p-1$.

Fundamental Theorem of Orders

The order of $a \pmod p$ divides $p - 1$.

And with this, we can play with the theorem that

$$e|(p-1)$$

As this means

$$p - 1 \equiv 0 \pmod e$$

and

$$p \equiv 1 \pmod e$$

Which is a crazy result true for *all* numbers under a prime modulus!

Fundamental Theorem of Orders

We can extend this notion beyond prime numbers, under the condition that $\gcd(a, m) = 1$

If $\gcd(a, m) = 1$, then the order of $a \pmod{p}$:

$$a^e \equiv 1 \pmod{m}$$

Divides $\phi(m)$, or $e|\phi(m)$.

We will not prove this, but it is true!

Wilson's Theorem

Wilson's Theorem states that

An integer n is prime if and only if

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

We'll be proving this in the following slides.

Wilson's Theorem

An integer n is prime if and only if

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

Each a in $\mathbb{Z}/p\mathbb{Z}$ has an inverse $a^{-1} \in \mathbb{Z}/p\mathbb{Z}$, such that $a \times a^{-1} \equiv 1 \bmod p$.

Questions?