# Modular Arithmagic

Jacob Richey and Carl de Marcken

University of Washington 2nd year Math Circle

4/2/2020

# Modular arithmetic

Let's think about the world of numbers mod $n$, for some positive integer $n$. For integers $a, b$, we say "$a$ and $b$ are equivalent mod $n$" if

$$n \text{ divides } a - b$$

It's also the same as saying $a$ and $b$ leave the same remainder when divided by $n$. This is what we mean by

$$a \equiv b \mod n.$$

For example, $10 \equiv -3 \equiv 49 \equiv 13000010 \mod 13$.

# Modular arithmetic

There are $n$ different 'equivalence classes' mod $n$: for example, equivalence class of 0 mod 3 is

$$[0] = \{0, 3, -3, 6, -6, 9, -9, \ldots\}$$

The equivalence class of $-1$ is

$$[-1] = \{-1, -4, -7, 2, 5, 8, \ldots\}$$

The equivalence class of 2 is

$$[2] = \{2, 5, 8, -1, -4, -7, \ldots\}$$

Note that $[-1] = [2]$, since $-1$ and 2 differ by a multiple of 3.

We often drop the brackets and just write $0, 1, \ldots, n-1$ for the equivalence classes.

# Modular operations

We can do addition and multiplication with numbers mod $n$, and equivalence still works. For example, multiplying by 2 on both sides (leaving the mod unchanged):

$$10 \equiv -3 \mod 13, \implies 20 \equiv -6 \mod 13.$$

Powers work too:

$$10 \equiv -3 \mod 13 \implies 10^2 = 100 = 7 * 13 + 9 \equiv 9 = (-3)^2 \mod 13.$$

# Modular operations

Dividing and taking roots doesn't always do what you expect. For example, dividing by 2 would give

$$6 \equiv 2 \mod 4 \implies 3 \equiv 1 \mod 4,$$

which is false! With powers, weird things can happen:

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod 8.$$

So there are four 'square roots of 1' mod 8: 1, 3, 5, and 7.

# Multiplication

Mod 8 multiplication table

| × | 0 | 1 | 2 | 3 | 4 | −3 | −2 | −1 |
|---|---|---|---|---|---|---|---|---|
| 0 | | | | | | | | |
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 4 | | | | | | | | |
| −3 | | | | | | | | |
| −2 | | | | | | | | |
| −1 | | | | | | | | |

# Slight of hand

Q: What is $17^{2021} \mod 12$?

# Slight of hand

Q: What is $17^{2021} \mod 12$?

A: Use modular arithmagic! A clever observation:

$$17^2 \equiv$$

# Slight of hand

Q: What is $17^{2021} \mod 12$?

A: Use modular arithmagic! A clever observation:

$$17^2 \equiv (-5)^2 = 25 \equiv 1 \mod 12.$$

Thus,

$$17^{2021} = 17^{2020} \cdot 17 \equiv (17^2)^{1010} \cdot 17 \equiv 1^{1010} \cdot = 17 \equiv 5 \mod 12.$$

# Slight of hand

Now you try: find

$$3^{100} \mod 7.$$

# Slight of hand

Now you try: find

$$3^{100} \mod 7.$$

One way: note $3^3 = 27 \equiv -1 \mod 7$. So

$$3^{99} \equiv (-1)^{33} = -1 \mod 7.$$

Thus $3^{100} \equiv -1 \cdot 3 \equiv 4 \mod 7$.

# Divisibility testing

An easy way to find any number mod 3 is to add the digits: the sum is the same mod 3 as the original number.

$$1234 \to \text{ digit sum } = 10 \equiv 1 \pmod 3,$$

and $1234 = 3 \cdot 411 + 1 \equiv 1 \mod 3$.

# Divisibility testing

An easy way to find any number mod 3 is to add the digits: the sum is the same mod 3 as the original number.

$$1234 \to \text{ digit sum } = 10 \equiv 1 \pmod 3,$$

and $1234 = 3 \cdot 411 + 1 \equiv 1 \mod 3$.

Why does this work?

# Divisibility testing

An easy way to find any number mod 3 is to add the digits: the sum is the same mod 3 as the original number.

$$1234 \to \text{ digit sum } = 10 \equiv 1 \mod 3,$$

and $1234 = 3 \cdot 411 + 1 \equiv 1 \mod 3$.

Why does this work? Note $1 \equiv 10 \mod 3$, so

$$1 \equiv 10 \equiv 100 \equiv 1000 \equiv \cdots \mod 3$$

So for any number $x = 1000a + 100b + 10c + d$,

$$\begin{aligned} 1000a + 100b + 10c + d &\equiv 1a + 1b + 1c + 1d \mod 3 \\ &= a + b + c + d \mod 3. \end{aligned}$$

# Divisibility testing

Another number that has nice properties with respect to powers of 10 is 11: $10 \equiv -1 \mod 11$, so

$$10^n \equiv (-1)^n \mod 11.$$

# Divisibility testing

Another number that has nice properties with respect to powers of 10 is 11: $10 \equiv -1 \mod 11$, so

$$10^n \equiv (-1)^n \mod 11.$$

So, to find $x = 1000a + 100b + 10c + d \mod 11$, do the *alternating* digit sum:

$$x \equiv d - c + b - a \mod 11.$$

For example, $1852 \equiv 2 - 5 + 8 - 1 = 4 \mod 11$.

# Division

When is it OK to divide?

# Division

When is it OK to divide?

It's OK to divide mod $n$ by any number $x$ such that $\gcd(n, x) = 1$, i.e. if $x$ and $n$ are relatively prime.

# Division

When is it OK to divide?

It's OK to divide mod $n$ by any number $x$ such that $\gcd(n, x) = 1$, i.e. if $x$ and $n$ are relatively prime. For example, dividing by 3 mod 4:

$$6 \equiv 2 \mod 4 \implies 2 \equiv \frac{2}{3} \mod 4.$$

What does $2/3 \mod 4$ mean?

# Division

When is it OK to divide?

It's OK to divide mod $n$ by any number $x$ such that $\gcd(n, x) = 1$, i.e. if $x$ and $n$ are relatively prime. For example, dividing by 3 mod 4:

$$6 \equiv 2 \mod 4 \implies 2 \equiv \frac{2}{3} \mod 4.$$

What does $2/3 \mod 4$ mean? It means $2 \cdot 3^{-1}$, where $3^{-1}$ is the number such that $3 \cdot 3^{-1} \equiv 1 \mod 4$.

# Division

When is it OK to divide?

It's OK to divide mod $n$ by any number $x$ such that $\gcd(n, x) = 1$, i.e. if $x$ and $n$ are relatively prime. For example, dividing by 3 mod 4:

$$6 \equiv 2 \mod 4 \implies 2 \equiv \frac{2}{3} \mod 4.$$

What does $2/3 \mod 4$ mean? It means $2 \cdot 3^{-1}$, where $3^{-1}$ is the number such that $3 \cdot 3^{-1} \equiv 1 \mod 4$.

We have $3^{-1} \equiv 3 \mod 4$, since $3 \cdot 3 = 9 \equiv 1 \mod 4$. So

$$2/3 \equiv 2 \cdot 3 \equiv 6 \equiv 2.$$

# Inverses

How to find inverses?

# Inverses

How to find inverses? Use the Euclidean algorithm!

# Inverses

How to find inverses? Use the Euclidean algorithm!

The Euclidean algorithm outputs the gcd of two integers $a$ and $b$.
Example with $a = 43$ and $b = 17$:

# Inverses

How to find inverses? Use the Euclidean algorithm!

The Euclidean algorithm outputs the gcd of two integers $a$ and $b$. Example with $a = 43$ and $b = 17$:

$$\begin{aligned} 43 &= 2 \cdot 17 + 9 \\ 17 &= 1 \cdot 9 + 8 \\ 9 &= 1 \cdot 8 + 1 \\ 8 &= 8 \cdot 1 \end{aligned}$$

The final number (when there was no remainder) was 1, so $\gcd(43, 17) = 1$.

# Inverses

The Euclidean algorithm gets us half way there. The other half is:

**Theorem (Bezout)**

*For any integers $a$ and $b$, there exist $x$ and $y$ such that*

$$ax + by = \gcd(a, b).$$

*For example, if $a = 43$ and $b = 17$,*

# Inverses

The Euclidean algorithm gets us half way there. The other half is:

**Theorem (Bezout)**

*For any integers a and b, there exist x and y such that*

$$ax + by = \gcd(a, b).$$

*For example, if $a = 43$ and $b = 17$,*

Why is this helpful? If we could find the $x$ and $y$, and $\gcd(a, b) = 1$, we would get

$$ax = -by + 1, \text{ or } ax \equiv 1 \mod b.$$

# Inverses

The Euclidean algorithm gets us half way there. The other half is:

**Theorem (Bezout)**

*For any integers a and b, there exist x and y such that*

$$ax + by = \gcd(a, b).$$

*For example, if* $a = 43$ *and* $b = 17$*,*

Why is this helpful? If we could find the $x$ and $y$, and $\gcd(a, b) = 1$, we would get

$$ax = -by + 1, \text{ or } ax \equiv 1 \mod b.$$

So $a \equiv x^{-1} \mod b$!

# Inverses

How to find the $x$ and $y$? Reverse the Euclidean algorithm steps.

$$43 = 2 \cdot 17 + 9$$
$$17 = 1 \cdot 9 + 8$$
$$9 = 1 \cdot 8 + 1 \qquad 1 = 9 - 1 \cdot 8$$
$$8 = 8 \cdot 1$$

# Inverses

How to find the $x$ and $y$? Reverse the Euclidean algorithm steps.

$$
\begin{aligned}
43 &= 2 \cdot 17 + 9 \\
17 &= 1 \cdot 9 + 8 \qquad 1 = 9 - 1 \cdot (17 - 1 \cdot 9) = -1 \cdot 17 + 2 \cdot 9 \\
9 &= 1 \cdot 8 + 1 \qquad 1 = 9 - 1 \cdot 8 \\
8 &= 8 \cdot 1
\end{aligned}
$$

# Inverses

How to find the $x$ and $y$? Reverse the Euclidean algorithm steps.

$$43 = 2 \cdot 17 + 9 \qquad 1 = -1 \cdot 17 + 2 \cdot (43 - 2 \cdot 17) = -3 \cdot 17 + 2 \cdot 43$$
$$17 = 1 \cdot 9 + 8 \qquad 1 = 9 - 1 \cdot (17 - 1 \cdot 9) = -1 \cdot 17 + 2 \cdot 9$$
$$9 = 1 \cdot 8 + 1 \qquad 1 = 9 - 1 \cdot 8$$
$$8 = 8 \cdot 1$$

# Inverses

How to find the $x$ and $y$? Reverse the Euclidean algorithm steps.

$$
\begin{aligned}
43 &= 2 \cdot 17 + 9 & 1 &= -1 \cdot 17 + 2 \cdot (43 - 2 \cdot 17) = -3 \cdot 17 + 2 \cdot 43 \\
17 &= 1 \cdot 9 + 8 & 1 &= 9 - 1 \cdot (17 - 1 \cdot 9) = -1 \cdot 17 + 2 \cdot 9 \\
9 &= 1 \cdot 8 + 1 & 1 &= 9 - 1 \cdot 8 \\
8 &= 8 \cdot 1 & &
\end{aligned}
$$

So $1 = -3 \cdot 17 + 2 \cdot 43$, i.e. $x = -3$ and $y = 2$, and

$$17^{-1} \equiv -3 \equiv 40 \mod 43$$

(Also, $43^{-1} \equiv 2 \mod 17$.)

# Discussion questions

Some questions we might think about in the future:

- Why does $x$ have an inverse mod $n$ if and only if $\gcd(x, n) = 1$? (Why does the Reverse Euclidean Algorithm fail if the gcd isn't 1?)

# Discussion questions

Some questions we might think about in the future:

- Why does $x$ have an inverse mod $n$ if and only if $\gcd(x, n) = 1$? (Why does the Reverse Euclidean Algorithm fail if the gcd isn't 1?)
- If $x$ has an inverse mod $n$, then we can talk about $y/x = yx^{-1}$ mod $n$ for any integer $y$. What about irrational numbers, like $\sqrt{2}$ mod 3? Do those 'make sense'?

# Discussion questions

Some questions we might think about in the future:

- Why does $x$ have an inverse mod $n$ if and only if $\gcd(x, n) = 1$? (Why does the Reverse Euclidean Algorithm fail if the gcd isn't 1?)
- If $x$ has an inverse mod $n$, then we can talk about $y/x = yx^{-1} \mod n$ for any integer $y$. What about irrational numbers, like $\sqrt{2} \mod 3$? Do those 'make sense'?
- In the real numbers, there is no number $x$ such that $x^2 = -1$. So, we made one up: $i^2 = -1$. Also, there is no integer $x$ such that $x^2 \equiv 3 \mod 5$. What if we made one up, say $\alpha^2 \equiv 3 \mod 5$? What properties would $\alpha$ have?

# Discussion questions

Some questions we might think about in the future:

- Why does $x$ have an inverse mod $n$ if and only if $\gcd(x, n) = 1$? (Why does the Reverse Euclidean Algorithm fail if the gcd isn't 1?)
- If $x$ has an inverse mod $n$, then we can talk about $y/x = yx^{-1} \mod n$ for any integer $y$. What about irrational numbers, like $\sqrt{2} \mod 3$? Do those 'make sense'?
- In the real numbers, there is no number $x$ such that $x^2 = -1$. So, we made one up: $i^2 = -1$. Also, there is no integer $x$ such that $x^2 \equiv 3 \mod 5$. What if we made one up, say $\alpha^2 \equiv 3 \mod 5$? What properties would $\alpha$ have?
- We found an algorithm to compute the inverse of a number mod $n$ if the inverse exists. Can you come up with an algorithm to compute the square root of a number mod $n$ if it exists?