Housekeeping

Daniel's contact hours: 1:15–2:15 Wednesday, 1:15–2:15 Thursday.

Tutorial sheet 1 & assignment 1 are now available on moodle.

Remember that support classes start next week.

MAT1830

Lecture 3: Congruences

We're used to classifying the integers as either even or odd. The even integers are those that can be written as $2k$ for some integer k. The odd integers are those that can be written as $2k + 1$ for some integer k.

even	$\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots$
odd	$\ldots, -5, -3, -1, 1, 3, 5, \ldots$

This classification is useful because even and odd integers have particular properties. For example, the sum of any two odd integers is even.

Similarly we can split the integers into three classes: those that are $3k$ for some integer k, those that are $3k+1$ for some integer k, and those that are $3k+2$ for some integer k.

$3k$	$\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots$
$3k+1$	$\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots$
$3k+2$	$\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots$

These classes also have particular properties. For example, the sum of an integer in the second class and an integer in the third class will always be in the first class.

We don't have to stop with 3. We could divide integers into 4 different classes according to their remainders when divided by 4, and so on.

3.1 Congruences

Let $n \geq 2$ be an integer. We say integers a and b are *congruent modulo* n and write

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

when n divides $a - b$.

Example.

$$\begin{aligned} 19 &\equiv 13 \pmod{6} &&\text{because 6 divides } 19 - 13 \\ 12 &\equiv 20 \pmod{4} &&\text{because 4 divides } 12 - 20 \\ 22 &\equiv 13 \pmod{3} &&\text{because 3 divides } 22 - 13 \end{aligned}$$

Let n be a positive integer and let a and b be integers.

Basically $a \equiv b \pmod{n}$ means that a and b have the same remainder when you divide them by n.

Definition We say $a \equiv b \pmod{n}$ if n divides $a - b$.

Equivalent definition We say $a \equiv b \pmod{n}$ if $a = kn + b$ for some integer k.

Note we're talking about "congruence modulo n" as a relation here, which is not quite the same as using a mod operation.

Really "$a \underset{n}{\equiv} b$" would be better notation than "$a \equiv b \pmod{n}$".

If we represent the mod operation without brackets then "$a \equiv b \pmod{n}$" means the same thing as "$a \bmod n = b \bmod n$".

Questions

Is $25 \equiv 9 \pmod 4$? Yes.

Is $9 \equiv 16 \pmod 3$? No.

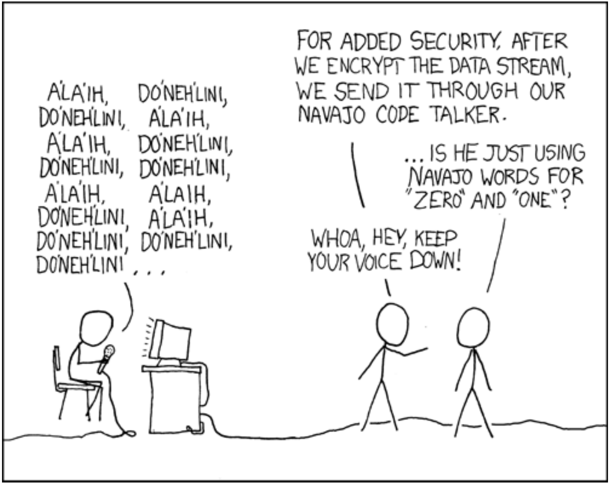
What integers are congruent to 3 modulo 4?
$\ldots, -9, -5, -1, 3, 7, 11, \ldots$

Question 3.1

Is $6 \equiv 3 \pmod 3$? Yes.

Is $9 \equiv 18 \pmod 8$? No.

Is $5x + 6 \equiv 2x \pmod 3$? Yes.


A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LA'IH, DO'NEH'LINI, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI . . .
FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
... IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!

3.2 Working with congruences

When working with congruences modulo some fixed integer n, we can "substitute in" just like we can with equalities.

> If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then
>
> $$a \equiv c \pmod{n}.$$

Example. Suppose $x \equiv 13 \pmod{7}$. Then $x \equiv 6 \pmod{7}$ because $13 \equiv 6 \pmod{7}$.

$\Uparrow$

note typo correction

We can add, subtract and multiply congruences just like we can with equations.

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
- $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$
- $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Example. If $x \equiv 3 \pmod{8}$ and $y \equiv 2 \pmod{8}$, then

- $x + y \equiv 5 \pmod{8}$
- $x - y \equiv 1 \pmod{8}$
- $xy \equiv 6 \pmod{8}$.

We can also deduce that $x + 4 \equiv 7 \pmod{8}$, that $4x \equiv 12 \pmod{8}$ and so on, because obviously $4 \equiv 4 \pmod{8}$. Note as well that $4x \equiv 12 \pmod{8}$ can be simplified to $4x \equiv 4 \pmod{8}$.

Examples

We know that $6 \equiv 10 \pmod{4}$ and $81 \equiv 21 \pmod{4}$.

Adding these, we see $87 \equiv 31 \pmod{4}$.

We know that $5 \equiv 1 \pmod{2}$ and $20 \equiv 0 \pmod{2}$.

Adding these, we see $25 \equiv 1 \pmod{2}$.

Question

You probably knew that you could add congruences modulo 2 for a long time before you learned what congruences were. How?

You knew even+even=even, odd+odd=even, even+odd=odd, and odd+even=odd.

Examples

We know that $22 \equiv 27 \pmod 5$ and $9 \equiv 19 \pmod 5$.

Subtracting the second from the first, we see $13 \equiv 8 \pmod 5$.

We know that $6 \equiv 10 \pmod 4$ and $5 \equiv 21 \pmod 4$.

Multiplying these, we see $30 \equiv 210 \pmod 4$.

Questions

What does the fact we can multiply congruences modulo 2 tell us about multiplying evens and odds?

That even$\times$anything$=$even, anything$\times$even$=$even, and odd$\times$odd$=$odd.

If $a \in \mathbb{Z}$ such that $a \equiv 0 \pmod 6$, then $ab \equiv 0 \pmod 6$ for any $b \in \mathbb{Z}$. What's another way of saying this?

If you take a multiple of 6 and multiply it by any number, then the result is also a multiple of 6.

Question 3.2 (one part)

Fact. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$.

Proof.
Because $a_1 \equiv b_1 \pmod{n}$, n divides $a_1 - b_1$
This means that $a_1 - b_1 = k_1 n$ for some integer k_1.
Because $a_2 \equiv b_2 \pmod{n}$, n divides $a_2 - b_2$
This means that $a_2 - b_2 = k_2 n$ for some integer k_2.

$$\begin{array}{lrcl} \text{So,} & (a_1 - b_1) + (a_2 - b_2) & = & k_1 n + k_2 n. \\ \text{So,} & (a_1 + a_2) - (b_1 + b_2) & = & (k_1 + k_2) n. \end{array}$$

Because $k_1 + k_2$ is an integer, this means n divides $(a_1 + a_2) - (b_1 + b_2)$.
So $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$. $\square$

Substituting in

In the two most common situations, “subbing in” using congruences is legal:

Fact If $a \equiv b + c \pmod{n}$ and $c \equiv d \pmod{n}$, then $a \equiv b + d \pmod{n}$.

Proof Because $c \equiv d \pmod{n}$ and $b \equiv b \pmod{n}$, we have
$b + c \equiv b + d \pmod{n}$.
So because $a \equiv b + c \pmod{n}$, we have $a \equiv b + d \pmod{n}$.

Fact If $a \equiv bc \pmod{n}$ and $c \equiv d \pmod{n}$, then $a \equiv bd \pmod{n}$.

Proof Because $c \equiv d \pmod{n}$ and $b \equiv b \pmod{n}$, we have
$bc \equiv bd \pmod{n}$.
So because $a \equiv bc \pmod{n}$, we have $a \equiv bd \pmod{n}$.

But in more complicated situations, “subbing in” is not always legal:

Example We know $6 \equiv 1 \pmod{5}$, but $2^6 \not\equiv 2^1 \pmod{5}$.

In some situations we can also “divide through” a congruence by an integer.

If $a \equiv b \pmod{n}$ and d divides a, b and n, then

$$\tfrac{a}{d} \equiv \tfrac{b}{d} \pmod{\tfrac{n}{d}}.$$

Examples

We know that $18 \equiv 42 \pmod{12}$.

Dividing through by 6, we see $3 \equiv 7 \pmod{2}$.

Suppose that $7x \equiv 21 \pmod{28}$ for an integer x.

Dividing through by 7, we see $x \equiv 3 \pmod{4}$.

Be careful!

Remember to divide the modulus as well.

If we have $2x \equiv 0 \pmod{10}$ for an integer x, we <u>cannot</u> conclude that $x \equiv 0 \pmod{10}$.

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

3.3 Solving linear congruences

Think of a congruence like $7x \equiv 5 \pmod 9$. This will hold if 9 divides $7x - 5$ or in other words if there is an integer y such that $7x - 5 = 9y$. So to solve our original congruence we can find an integer solution to $7x - 9y = 5$.

Some congruences don't have solutions. For example, there is no solution to $10x \equiv 6 \pmod{20}$ because there are no integers x and y such that $10x - 20y = 6$.

We can find an expression for all the integers x that satisfy a congruence like $ax \equiv b \pmod{n}$ in the following way:

1. Find $d = \gcd(a, n)$.
2. If d doesn't divide b, then there are no solutions.
3. If d divides b, then divide through the congruence by d to get an equivalent congruence $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.
4. Find integers x' and y' such that $\frac{a}{d}x' - \frac{n}{d}y' = \frac{b}{d}$. The integers x that satisfy the original congruence are exactly those for which $x \equiv x' \pmod{\frac{n}{d}}$.

Question 3.3 Find an expression for all the integers x that satisfy $9x \equiv 36 \pmod{60}$.

First calculate $\gcd(9, 60) = 3$.
3 does divide 36 so there are solutions.
Divide through by 3 to get $3x \equiv 12 \pmod{20}$.
We now want to find x' and y' such that $3x' - 20y' = 12$.
$x' = 4$ and $y' = 0$ work.
So the integers x that satisfy $9x \equiv 36 \pmod{60}$ are exactly those for which $x \equiv 4 \pmod{20}$.

Example. Find all integers x such that $36x \equiv 10 \pmod{114}$.

Using the Euclidean algorithm we find $\gcd(36, 114) = 6$. So 6 divides $36x - 114y$ for any integers x and y, and consequently $36x - 114y \neq 10$. This means that there are no integers x such that $36x \equiv 10 \pmod{114}$.

Example. Find all integers x such that $24x \equiv 8 \pmod{44}$.

Using the Euclidean algorithm we find $\gcd(24, 44) = 4$. So we divide through by 4 to get the equivalent congruence $6x \equiv 2 \pmod{11}$. Using the extended euclidean algorithm we see that $2\times 6 - 1\times 11 = 1$, and hence $4\times 6 - 2\times 11 = 2$. Thus the integers x such that $24x \equiv 8 \pmod{44}$ are exactly the integers $x \equiv 4 \pmod{11}$.

3.4 Modular inverses

A modular multiplicative inverse of an integer a modulo n is an integer x such that

$$ax \equiv 1 \pmod{n}.$$

From the last section we know that such an inverse will exist if and only if $\gcd(a, n) = 1$. If inverses do exist then we can find them using the extended Euclidean algorithm (there will be lots of inverses, but they will all be in one congruence class modulo n). These inverses have important applications to cryptography and random number generation.