University of Waterloo
Faculty of Mathematics

Centre for Education in
Mathematics and Computing

Intermediate Math Circles
November 25, 2009
Diophantine Equations II

Modular Math

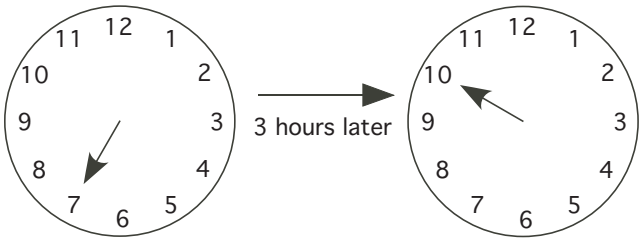
Number theory is about divisibility. So, which numbers are divisible by which?

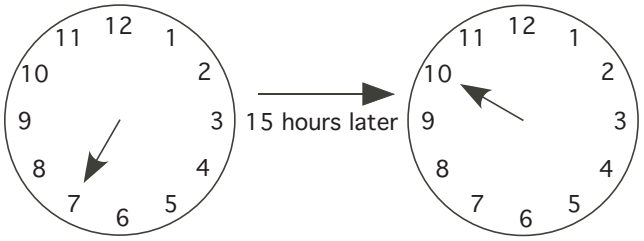
Every number is divisible by 1 and itself.

Prime numbers are those divisible only by one and themselves.

Sometimes it's useful to do math up to multiples of some number.

For example, a clock displays the hour up to a multiple of 12.





We say that the clock displays the hour "modulo 12".

"modulo" means "up to multiples of".

Two numbers a and b are the same "modulo 12" if $a = b +$ (some multiple of 12).

So $7 + 15 = 10 +$ (some multiple of 12).

We write $7 + 15 \equiv 10 \pmod{12}$

$$a \equiv b \pmod{m} \qquad \text{means} \qquad a = b + (\text{some multiple of } m).$$

$$3 + 6 \equiv 9 \pmod{12}$$
$$9 + 8 \equiv 17 \equiv 5 \pmod{12} \qquad \text{etc.}$$

We can even subtract:

$$3 - 10 \equiv -7 \equiv 5 \pmod{12} \qquad \text{since} \quad -7 = 5 + (-12)$$

Every number is congruent to either 0, 1, 2, 3, ..., or 11 (mod 12).

There's nothing special about 12. We can work modulo any number:

$$5 + 6 \equiv 11 \equiv 4 \pmod{7}$$
$$3 + 6 \equiv 9 \equiv 2 \pmod{7} \qquad \text{etc.}$$

If a and n are integers, and $a \equiv 0 \pmod{n}$, then that means

$$\begin{aligned} a &= 0 + (\text{a multiple of } n) \\ &= \text{a multiple of } n \end{aligned}$$

So, in fact, $a \equiv 0 \pmod{n}$ means the same thing as "n divides a".

We can even multiply modulo n:

$$3 \times 4 \equiv 12 \equiv 5 \pmod{7}$$
$$6 \times 9 \equiv 54 \equiv 14 \pmod{20} \qquad \text{etc.}$$
$$2 \times 3 \equiv 1 \pmod{5}.$$

Multiplication Table (mod 5)

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Exercise: Make a multiplication table (mod 11).

We may be asked to find a solution to $2x \equiv 1 \pmod 7$, $3x + 2 \equiv 6 \pmod 7$, etc.

One way to find a solution to something like $2x \equiv 1 \pmod 5$ is to look in the table: $x \equiv 3 \pmod 5$.

Is there another way? We're trying to write

$$\begin{aligned} & 2x = 1 + (\text{a multiple of } 5), \\ \text{so} \quad & 2x = 1 + 5y, \qquad \text{or} \\ & 2x - 5y = 1. \end{aligned}$$

We saw how to do this using the Euclidean algorithm.

The inverse of $a \pmod n$ is the number x that solves

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

We write $\overline{a} \pmod n$.

So $\overline{2} \pmod 5 \equiv 3$

$4 \cdot 2 \equiv 1 \pmod 7$, so $\overline{4} \equiv 2 \pmod 7$

If we can solve $ax + ny = 1$, then $\overline{a} \equiv x \pmod n$, since $ax \equiv 1 - ny \equiv 1 \pmod n$.

Of course, we can only solve $ax + ny = 1$ if a and n have no factors in common.

Exercise: Find the inverses:

$$\begin{aligned} & \overline{3} \pmod 5 \\ & \overline{5} \pmod 7 \\ & \overline{2} \pmod{13} \\ & \overline{22} \pmod{23} \\ & \overline{57} \pmod{101} \\ & \overline{235} \pmod{601} \end{aligned}$$

When is a number divisible by another number?

Divisible by 2: Easy → is the last digit divisible by 2?

Why does it work?

If $a = \boxed{\text{digits}}\, b$ (in other words, b is the last digit of the number)

then $a = b + 10 \times$ something.

10 is divisible by 2, so
$10 \times \text{something} \equiv 0 \pmod 2$

So $a \equiv b \pmod 2$, and so checking if $a \equiv 0 \pmod 2$ is the same as checking if $b \equiv 0 \pmod 2$.

Divisible by 3: Add up the digits, and see if <u>that</u> is divisible by 3. Why does this work?

Lets do an example: Consider 372.

We can write this number as

$$372 = 3 \times 100 + 7 \times 10 + 2$$

We want to know if $372 \equiv 0 \pmod 3$.

$$\begin{aligned} \text{So}\ldots \qquad 10 &\equiv 9 + 1 \equiv 1 \pmod 3 \\ 100 &\equiv 1 + 99 \equiv 1(mod 3) \end{aligned}$$

$$\begin{aligned} \text{So} \qquad 372 &\equiv 3 \times 100 + 7 \times 10 + 2 \\ &\equiv 3 + 7 + 2 \pmod 3 \\ &\equiv 12 \equiv 0 \pmod 3 \end{aligned}$$

So the point is, a number $\equiv$ (sum of the digits of the number) (mod 3).

Divisible by 9: This works for divisibility by 9 too...

$$\begin{aligned} 10 &\equiv 1 + 9 \equiv 1 (\text{mod } 9) \\ 100 &\equiv 1 + 99 \equiv 1 (\text{mod } 9) \\ 1000 &\equiv 1 + 999 \equiv 1 (\text{mod } 9) \end{aligned}$$

$$\begin{aligned} \text{so} \qquad 372 &\equiv 3 \times 100 + 7 \times 10 + 2 \\ &\equiv 3 + 7 + 2 \equiv 12 \\ &\equiv 3 \pmod 9 \end{aligned}$$

Divisible by 11: Here's the rule for 11:

Check if the "alternating sum" of the digits is divisible by 11:

(ones digit) − (tens digits) + (100's digits) − (1000's digit) + ...

Example: 1331
$\longrightarrow 1 - 3 + 3 - 1 = 0$, so this is divisible by 11.

Exercise: Explain why this works.
(hint: $10 \equiv -1 \pmod{11}$, $100 \equiv 1 \pmod{11}$, $1000 \equiv -1 \pmod{11}$)

Can you come up with a rule for divisibility by 7?

Perfect Squares: Are there any perfect squares that are one less than a multiple of 3?

1 no, 4 no, 9 no, 16 no, ...

Why not?

Any number is either 0, 1, or 2 (mod 3), so any perfect square is either 0^2, 1^2, or $2^2 \equiv 1 \pmod{3}$.

So perfect squares are either 0 or 1 (mod 3), not 2 (mod 3).

Problems

1. Do the addition/subtraction/multiplication
   (1) $2 + 7 \pmod 8$
   (2) $13 + 17 \pmod{21}$
   (3) $19 + 51 \pmod{60}$
   (4) $294 + 192 \pmod{307}$
   (5) $13 - 27 \pmod{30}$
   (6) $42 - 67 \pmod{75}$
   (7) $146 - 187 \pmod{201}$
   (8) $7 \times 8 \pmod{11}$
   (9) $14 \times 25 \pmod{29}$
   (10) $124 \times 425 \pmod{101}$
2. Here's a multiplication table modulo 5:

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

   (1) Find an x such that $2x \equiv 1 \pmod 5$.
   (2) Find an x such that $4x \equiv 1 \pmod 5$.
   (3) Find an x such that $3x \equiv 2 \pmod 5$.
   (4) Find an x such that $4x + 2 \equiv 3 \pmod 5$.
   (5) Find an x such that $2x + 1 \equiv 4x + 2 \pmod 5$.
3. Make a multiplication table modulo 11.
   (1) Find an x such that $5x \equiv 1 \pmod{11}$.
   (2) Find an x such that $7x \equiv 1 \pmod{11}$.
   (3) Find an x such that $3x \equiv 2 \pmod{11}$.
   (4) Find an x such that $4x + 5 \equiv 3 \pmod{11}$.
   (5) Find an x such that $2x + 6 \equiv 5x + 2 \pmod{11}$.

4. Find the inverses listed below. For small ones, guessing and checking will probably work. For the large ones, you need to use the Euclidean algorithm. Remember, the inverse of a is the number x such that $ax \equiv 1 \pmod{m}$.

   (1) $\overline{3} \pmod 7$

   (2) $\overline{6} \pmod{11}$

   (3) $\overline{8} \pmod{17}$

   (4) $\overline{15} \pmod{57}$

   (5) $\overline{36} \pmod{101}$

   (6) $\overline{128} \pmod{197}$

   (7) $\overline{1024} \pmod{2143}$

5. Find a rule for...

   (1) When a number is divisible by 4.

   (2) When a number is divisible by 5.

   (3) When a number is divisible by 6.

   (4) When a number is divisible by 10.

   (5) When a number is divisible by 12.

   The next two are harder, but if you can, find a rule for...

   (6) When a number is divisible by 8.

   (7) When a number is divisible by 7. (Hint: the rule has something to do with breaking the number down into the ones digit, and then the number made up of all the other digits: 1031 = 103 and 1: Now, can you figure out how to express whether or not the original number was divisible by 7 in terms of the two new numbers? It's not easy.)

6. The perfect squares (mod 5) are 1^2, $4^2 \equiv 1 \pmod 5$, and 2^2, $3^2 \equiv 4 \pmod 5$ (even though $0^2 \equiv 0 \pmod 5$, we always leave 0 out of the list of perfect squares, just like we leave it out of the multiplication tables).

   (1) List the perfects squares (mod 7).

   (2) List the perfects squares (mod 11).

   (3) List the perfects squares (mod 13).

7. (1) Look at the multiplication table (mod 5) on this sheet, and circle all of the perfect squares.

   (2) It's always true that a perfect square times a perfect square is a perfect square (since $a^2 \times b^2 = (a \times b)^2$). Can you find any other patterns like that? What about a perfect square times something that is NOT a perfect square? What about something that is NOT a perfect square times something that is NOT a perfect square?

   (3) Look at your multiplication table (mod 11), and circle all of the perfect squares. Do the same patterns hold as in the previous problem?