

Congruent Numbers

Definition: Given a positive integer n (called the *modulus*), we say two integers a and b are *congruent modulo n* if $n|(a - b)$. If a and b are congruent modulo n we write $a \equiv b \pmod{n}$.

The odd numbers are exactly the numbers congruent to 1 modulo 2. The numbers congruent to 3 modulo 4 are

$$3, 7, 11, 15, 19, \dots \quad \text{and} \quad -1, -5, -9, -13, \dots$$

Notice by exercise #17 from section 1.1 that a and b are congruent modulo n if and only if they have the same remainder when divided by n via the division algorithm. This makes the following observations more transparent for any modulus n :

$$a \equiv a \pmod{n} \quad \text{for all integers } a,$$

$$\text{if } a \equiv b \pmod{n} \text{ then } b \equiv a \pmod{n}, \text{ and}$$

$$\text{if } a \equiv b \pmod{n} \text{ and } b \equiv c \pmod{n}, \text{ then } a \equiv c \pmod{n}.$$

In other words, congruence (with any modulus) behaves pretty much like equals, which helps explain the notation. It also means that we can attempt to do “algebra” with congruences.

The Euclidean Algorithm Yet Again

You've seen how the Euclidean Algorithm encapsulates how to solve $ax + by = d$, where d is the greatest common divisor of a and b . Rewrite this equation as $ax - d = -by$. In other words, b divides $ax - d$. So the Euclidean Algorithm can be used to solve *congruences* of the type

$$ax \equiv d \pmod{b},$$

where d is the greatest common divisor of a and b .

More generally, Theorem 1.1.6 says when one can solve $ax + by = c$: exactly when the greatest common divisor of a and b divides c . Thus, one can solve the congruence

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

if and only if the greatest common divisor of a and b divides c . Moreover, if it can be solved, the Euclidean algorithm can be used to find a solution.

Some simpler, but illuminating examples:

$$15x \equiv 2 \pmod{51}$$

$$15x \equiv 2 \pmod{50}$$

$$15x \equiv 3 \pmod{51}$$

Now suppose m and n are relatively prime. Then there are integers h and k with

$$hm + kn = 1.$$

Note how this one equation tells us the following two congruences:

$$hm \equiv 1 \pmod{n}$$

$$kn \equiv 1 \pmod{m}.$$

If we multiply both sides of the equation by an integer a , we see that

$$ahm \equiv a \pmod{n}.$$

We could also multiply by b and get

$$bkn \equiv b \pmod{m}.$$

Note how $bkn \equiv 0 \pmod{n}$ and $ahm \equiv 0 \pmod{m}$, though.

Putting these two (actually four) pieces of information together, we see that $ahm + bkn$ is a solution to the simultaneous congruences

$$x \equiv a \pmod{n} \quad x \equiv b \pmod{m}.$$