Example 38. (HW) Determine all solutions of $4x+7y=67$ with x and y positive integers.

Solution. We see that $x=2$, $y=-1$ is a solution to $4x+7y=1$ (you can, of course, use the Euclidean algorithm if you wish).

Hence, a particular solution to $4x+7y=67$ is given by $x=134$, $y=-67$.

The general solution to $4x+7y=67$ is thus given by $x=134+7t$, $y=-67-4t$, where t can be any integer.

- $x>0$ if and only if $134+7t>0$ if and only if $t>-\frac{134}{7}\approx-19.14$. That is, $t=-19,-18,\ldots$
- $y>0$ if and only if $-67-4t>0$ if and only if $t<-\frac{67}{4}=-16.75$. That is, $t=-17,-18,\ldots$

Hence, we get a solution (x,y) with positive integers x,y for $t=-19,-18,-17$. The three corresponding solutions are: $(1,9)$, $(8,5)$, $(15,1)$.

4 Congruences

$$a\equiv b \pmod{n} \qquad \text{means} \qquad a=b+mn \quad (\text{for some } m\in\mathbb{Z})$$

In that case, we say that "a is congruent to b modulo n".

- In other words: $a\equiv b \pmod{n}$ if and only if $a-b$ is divisible by n.
- In yet other words: $a\equiv b \pmod{n}$ if and only if a and b leave the same remainder when dividing by n.

Example 39. $17\equiv 5 \pmod{12}$ as well as $17\equiv 29\equiv -7 \pmod{12}$

Example 40. We will discuss in more detail that, and how, we can calculate with congruences. Here is an appetizer: What is 2^{100} modulo 3? That is, what's the remainder upon division by 3?

Solution. $2\equiv-1 \pmod{3}$. Hence, $2^{100}\equiv(-1)^{100}=1 \pmod{3}$.

Example 41. Every integer x is congruent to one of $0,1,2,3,4$ modulo 5.

We therefore say that $0,1,2,3,4$ form a **complete set of residues** modulo 5.

Another natural complete set of residues modulo 5 is: $0,\pm1,\pm2$

A not so natural complete set of residues modulo 5 is: $-5,2,4,8,16$

A possibly natural complete set of residues modulo 5 is: $0,3,3^2=9,3^3=27,3^4=81$

[We will talk more about this last case. Because this worked as it did, we will say that "3 is a multiplicative generator modulo 5".]

Theorem 42. We can calculate with congruences.

- First of all, if $a\equiv b \pmod{n}$ and $b\equiv c \pmod{n}$, then $a\equiv c \pmod{n}$.

  In other words, being congruent is a **transitive property**.

  Why? $n|(b-a)$ and $n|(c-b)$, then $n|\underbrace{((b-a)+(c-b))}_{=c-a}$.

  Alternatively, we can note that each of a,b,c leaves the same remainder when dividing by n.

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

  (a) $a + c \equiv b + d \pmod{n}$

  Why? $(b + d) - (a + c) = (b - a) + (d - c)$ is indeed divisible by n (because $n|(b - a)$ and $n|(d - c)$).

  (b) $ac \equiv bd \pmod{n}$

  Why? $bd - ac = (bd - bc) + (bc - ac) = b(d - c) + c(b - a)$ is indeed divisible by n (because $n|(b - a)$ and $n|(d - c)$).

- In particular, if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Example 43. Show that $41|2^{20} - 1$.

Solution. In other words, we need to show that $2^{20} \equiv 1 \pmod{41}$.
$2^5 = 32 \equiv -9 \pmod{41}$. Hence, $2^{20} = (2^5)^4 \equiv (-9)^4 = 81^2 \equiv (-1)^2 = 1 \pmod{41}$.

Example 44. (but careful!) If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$ for any integer c.
However, the converse is not true! We can have $ac \equiv bc \pmod{n}$ without $a \equiv b \pmod{n}$ (even assuming that $c \not\equiv 0$).

For instance. $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$ but $4 \not\equiv 1 \pmod{6}$
However. $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$ means $2 \cdot 4 = 2 \cdot 1 + 6m$. Hence, $4 = 1 + 3m$, or, $4 \equiv 1 \pmod{3}$.

Similarly, $ab \equiv 0 \pmod{n}$ does not always imply that $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$.

For instance. $4 \cdot 15 \equiv 0 \pmod{6}$ but $4 \not\equiv 0 \pmod{6}$ and $15 \not\equiv 0 \pmod{6}$

These issues do not occur when n is a prime, as the next results shows.

Lemma 45. Let p be a prime.

(a) If $ab \equiv 0 \pmod{p}$, then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

(b) Suppose $c \not\equiv 0 \pmod{p}$. If $ac \equiv bc \pmod{p}$, then $a \equiv b \pmod{p}$.

Proof.

(a) This statement is equivalent to Lemma 31.

(b) $ac \equiv bc \pmod{p}$ means that p divides $ac - bc = (a - b)c$.
Since p is a prime, it follows that $p|(a - b)$ or $p|c$.
In the latter case, $c \equiv 0 \pmod{p}$, which we excluded. Hence, $p|(a - b)$. That is, $a \equiv b \pmod{p}$. □

Armin Straub
straub@southalabama.edu