Example 60. 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: $-5,2,4,8,16$

Theorem 61. 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 $n|(d-c)$).

  (c) In particular, $a^k\equiv b^k \pmod{n}$ for any positive integer k.

Example 62. 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 63. (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. $2\cdot4\equiv 2\cdot1 \pmod{6}$ but $4\not\equiv 1 \pmod{6}$
However. $2\cdot4\equiv 2\cdot1 \pmod{6}$ means $2\cdot4=2\cdot1+6m$. 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. $4\cdot15\equiv 0 \pmod{6}$ 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 64. 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 49.

(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

Example 65. Let $n \geqslant 0$ be an integer. Prove the following divisibility statements:

(a) $8|5^{2n}+7$ (b) $15|2^{4n}-1$

Solution. Previously, we used induction (see Homework #2). Now, we can prove these directly:

(a) $5^{2n}=25^n \equiv 1^n = 1 \pmod{8}$. Hence, $5^{2n}+7 \equiv 1+7 \equiv 0 \pmod{8}$. That is, $8|5^{2n}+7$.

(b) $2^{4n}-1=16^n-1 \equiv 1^n-1=0 \pmod{15}$. That is, $15|2^{4n}-1$.

Example 66. Which are the possible remainders that the square of an integer leaves upon division by 5?

Solution. We consider the following 5 cases:

- If $x \equiv 0 \pmod{5}$, then $x^2 \equiv 0 \pmod{5}$.
- If $x \equiv 1 \pmod{5}$, then $x^2 \equiv 1 \pmod{5}$.
- If $x \equiv 2 \pmod{5}$, then $x^2 \equiv 4 \pmod{5}$.
- If $x \equiv 3 \pmod{5}$, then $x^2 \equiv 9 \equiv 4 \pmod{5}$.
- If $x \equiv 4 \pmod{5}$, then $x^2 \equiv 16 \equiv 1 \pmod{5}$.

Hence, the possible remainders are $0, 1, 4$.

Comment. We can see why we are getting (apart from 0) only exactly half of the possible residues, if, instead of $0, 1, 2, 3, 4$, we choose $0, \pm 1, \pm 2$ as our complete set of residues: if $x \equiv \pm 1 \ (\mathrm{mod}\, 5)$, then $x^2 \equiv 1 \ (\mathrm{mod}\, 5)$, and if $x \equiv \pm 2 \ (\mathrm{mod}\, 5)$, then $x^2 \equiv 4 \ (\mathrm{mod}\, 5)$.

Example 67. Which are the possible remainders that the fourth power of an integer leaves upon division by 5? In other words, what are the possible values of x^4 modulo 5?

Solution. We can through the same five cases as in the last example to find that the possible remainders are only $0, 1$. Alternatively, we can make our life easier by noting that x^4 is the square of x^2. Since x^2 takes the values $0, 1, 4$ modulo 5, its square x^4 takes the values $0^2, 1^2, 4^2 \equiv 1$ modulo 5.

Comment. If $x \not\equiv 0 \ (\mathrm{mod}\ 5)$, then we just saw that $x^4 \equiv 1 \ (\mathrm{mod}\ 5)$. The next, possibly surprising, result states that this happens for every prime!

Theorem 68. (Fermat's little theorem) Let p be a prime, and suppose that $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. The first $p-1$ multiples of a,

$$a, 2a, 3a, \ldots, (p-1)a$$

are all different modulo p. (Otherwise, $r a \equiv s a \ (\mathrm{mod}\, p)$ for some $r, s \in \{1, 2, \ldots, p-1\}$. Since p is prime, this implies $r \equiv s \ (\mathrm{mod}\, p)$.) Clearly, none of them is divisible by p.

Consequently, these values must be congruent (in some order) to the values $1, 2, \ldots, p-1$ modulo p. Thus,

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Cancelling the common factors (allowed because p is prime!), we get $a^{p-1} \equiv 1 \ (\mathrm{mod}\, p)$. □

Remark. The "little" in this theorem's name is to distinguish this result from Fermat's last theorem that $x^n + y^n = z^n$ has no integer solutions if $n > 2$ (only recently proved by Wiles).

Comment. An alternative proof based on induction is given in the book (bottom of page 88).