PROBLEM 1. When is $a \equiv b \pmod 2$? $a \equiv b \pmod 1$? $a \equiv b \pmod 0$?

SOLUTION: We have $a \equiv b \pmod 2$ exactly when a and b have the same parity: both are even or both are odd. We have $a \equiv b \pmod 1$ for all a and b: the only requirement is that they differ by a multiple of 1. We have $a \equiv b \pmod 0$ if a and b differ by a multiple of 0. That happens if and only if $a = b$.

PROBLEM 2. Suppose $a \equiv a' \pmod m$ and $b \equiv b' \pmod m$.

(a) Prove that $a + b \equiv a' + b' \pmod m$.

(b) Prove that $ab \equiv a'b' \pmod m$.

SOLUTION:

(a) See our text.

(b) We have that $a = km + a'$ and $b = \ell m + b'$ for some $k, \ell \in \mathbb{Z}$. Then

$$ab = (km + a')(\ell m + b') = (k\ell m + kb' + \ell a')m + a'b'.$$

It follows that $ab \equiv a'b' \pmod m$.

PROBLEM 3. Let $n \geq 1$.

(a) Show that if $a \equiv 1 \pmod m$, then $a^n \equiv 1 \pmod m$.

(b) Show that if $a \equiv m - 1 \pmod m$, then $a^n \equiv 1 \pmod m$ if n is even and $a^n \equiv m - 1 \pmod m$ if n is odd.

SOLUTION:

(a) By part (b) of the previous problem, we have $a^n \equiv 1^n \equiv 1 \pmod m$.

(b) Note that $a \equiv m - 1 \equiv -1 \pmod m$. Therefore, $a^n \equiv (-1)^n \pmod m$. This gives the result.

PROBLEM 4.

(a) Compute the remainder modulo 6 of

$$334 \cdot 545 + 191 \cdot 63.$$

(b) Today is Wednesday. What day will it be 3^{20} days from today?

SOLUTION:

(a)

$$334 \cdot 545 + 191 \cdot 63 \equiv 4 \cdot 5 + 5 \cdot 3 \equiv 20 + 15 \equiv 2 + 3 \equiv 5 \pmod 6.$$

Alternatively,

$$334 \cdot 545 + 191 \cdot 63 \equiv (-2) \cdot (-1) + (-1) \cdot 3 \equiv 2 - 3 \equiv -1 \equiv 5 \pmod 6.$$

(b) By Fermat's little theorem,

$$3^6 \equiv 1 \pmod 7.$$

Then,

$$3^{20} = 3^{18} \cdot 3^2 \equiv (3^6)^3 \cdot 3^2 \equiv 1^3 \cdot 2 \equiv 2 \pmod 7.$$

So if today is Wednesday, it will be Friday in 3^{20} days.

PROBLEM 5. Recall the equivalence relation from the mini-lecture: having fixed $m \in \mathbb{Z}$, for $a, b \in \mathbb{Z}$, we say $a \sim b$ if $a - b = km$ for some $k \in \mathbb{Z}$. In other words, $a \sim b$ if and only if $a = b \pmod m$. Take $m > 0$, for convenience.

(a) Show that $\sim$ is an equivalence relation directly from the definition.

(b) State the division algorithm for integers a and m, and use it to determine the number of equivalence classes for $\sim$.

SOLUTION:

(a) Let $a, b, c \in Z$. *Reflexivity:* $a \sim a$ since $a - a = 0 \cdot m$.

Symmetry: Suppose $a \sim b$. Then $a - b = km$ for some $k \in \mathbb{Z}$. It follows that $b - a = (-k)m$, and hence $b \sim a$.

Transitivity: Suppose $a \sim b$ and $b \sim c$. Then $a - b = km$ and $b - c - \ell m$ for some $k, \ell \in \mathbb{Z}$. It follows that

$$a - c = (a - b) + (b - c) = km + \ell m = (k + \ell)m,$$

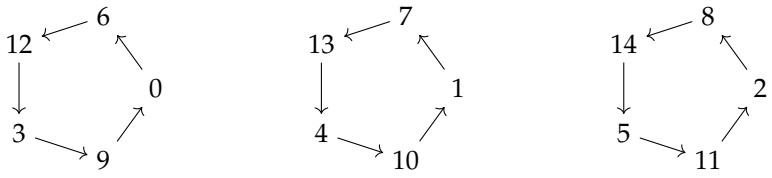
Therefore, $a \sim c$.

(b) We have that $a = qm + r$ for unique $q, r \in \mathbb{Z}$ with $0 \leq r < m$. It follows that $a = r \pmod m$ for a unique r such that $0 \leq r < n$. Further, suppose that $r, r' \in \{0, 1, \ldots, m-1\}$ and that $r - r' = km$ for some $k \in \mathbb{Z}$. Since $0 \leq |r - r'| < m$ and $|kn| = |k|m$, it follows that $k = 0$. Thus, $r = r'$. We have shown that there are m equivalence classes, represented by the integers $0, 1, \ldots, m-1$.

PROBLEM 6. (If you have extra time.) Let $V := \{0, 1, \cdots, m-1\}$ for some positive integer m, and fix $a \in V$. Let $G(a, n)$ be the directed graph with vertex set V and with an edge from b to c if $c \equiv b + a \pmod{m}$. Draw this graph for various a and n, and try to deduce its general structure.

SOLUTION: Starting at a vertex $b \in V$, we get the following string of edges: $b \to b + a \to b + 2a \to b + 3a \to \cdots \to b + \ell a$ where ℓ is the smallest positive integer such that $\ell a \equiv 0 \pmod{m}$, i.e., the smallest positive integer ℓ such that $m|(\ell a)$. This number is $\ell = \operatorname{lcm}(a, m)/a = m/\gcd(a, m)$. The full graph consists of $\gcd(a, m)$ cycles, each of length ℓ.

For example, in the case $m = 15$ and $a = 6$, we have $\ell = 15/\gcd(6, 15) = 5$.



If a and m are relatively prime, we get a connected graph with m vertices arranged in a single cycle.