Tuesday, September 24

- Today: Group Work #2 (solutions posted after class)
- Homework #2 posted today, due next Tuesday

Definition: Given $m \in \mathbb{N}$ and $a \in \mathbb{Z}$, we call $x \in \mathbb{Z}$ a (multiplicative) inverse of a modulo m if $ax \equiv 1 \pmod{m}$.

Example: $6 \cdot 73 = 438 \equiv 1 \pmod{437}$, so 73 is an inverse of 6 (mod 437).

Theorem:
- If $(a,m) > 1$ then a has no inverse (mod m).
- If $(a,m) = 1$ then a has an inverse (mod m), which is unique as a residue class (mod m). We denote this inverse by $a^{-1} \pmod{m}$. $\Rightarrow$ Ex. $6^{-1} \equiv 73 \pmod{437}$.

Proof:
- Let $g = (a,m)$. If $ax \equiv 1 \pmod{m}$ then $ax \equiv 1 \pmod{g}$ since $g \mid m$; but since $g \mid a$, $0 = 0x \equiv ax \equiv 1 \pmod{g}$, forcing $g = 1$.
- Two quick proofs of existence when $(a,m) = 1$:
  - By Euler's theorem, $a \cdot a^{\phi(m)-1} = a^{\phi(m)} \equiv 1 \pmod{m}$, and so $a^{-1} \equiv a^{\phi(m)-1}$.
  - By Bézout's theorem, we can write $ax + my = 1$ for some x, y; then $ax = ax + 0y \equiv ax + my = 1 \pmod{m}$.
- Uniqueness: if $ax \equiv 1 \pmod{m}$ and $ay \equiv 1 \pmod{m}$, then $ax \equiv ay \pmod{m}$; since $(a,m) = 1$, we deduce $x \equiv y \pmod{m}$. //

Definition: If $k \in \mathbb{N}$, we define $a^{-k} \pmod m$ to be $(a^{-1})^k \pmod m$, when $(a,m)=1$. Exercise: check everything still works.

Exercise: Suppose $(a,m)=1$ and $(k, \phi(m))=1$. Let $l \equiv k^{-1} \pmod{\phi(m)}$.

Then $(a^k)^l \equiv a \pmod m$.

— Related to RSA cryptography.

Miscellaneous Lemma: If $ab \equiv c \pmod m$ and $(c,m)=1$, then $(a,m)=(b,m)=1$.

Proof: Write $c-ab=mn$. Then $c=ab+mn$ is a multiple of (a,m); so (a,m) divides both m and c, hence $(a,m) \mid (c,m)=1$. $\Rightarrow (a,m)=1$.

Same proof: $(b,m)=1$. //

Corollary: If $a^k \equiv c \pmod m$ and $(c,m)=1$, then $(a,m)=1$.

Lemma: Given $m \in \mathbb{N}$ and $x \in \mathbb{Z}$, consider these statements:

(1) $x^2 \equiv 1 \pmod m$;

(2) $x^{-1} \equiv x \pmod m$;

(3) $x \equiv \pm 1 \pmod m$.

- For any $m \in \mathbb{N}$, (1) $\Leftrightarrow$ (2) and (3) $\Rightarrow$ (1).

- If m is prime, then (1) $\Rightarrow$ (3) (so all three are equivalent).

Example: $9^2 = 81 \equiv 1 \pmod{20}$, so $9^{-1} \equiv 9 \pmod{20}$; but $9 \not\equiv \pm 1 \pmod{20}$.