Math 465 - Spring 2021 February 11th, 2021
Group Discussion 3

The kind of knowledge which is supported only by observations and is not yet proved must be carefully distinguished from the truth

— Leonhard Euler

---

(1) Suppose $a, b, m, h \in \mathbb{Z}$ with $m, h > 0$, and let $g := \gcd(a, m)$. Prove:
  (a) If $g \nmid b$ then $ax \equiv b \bmod m$ has no solution $x \in \mathbb{Z}$.
  (b) If $g = 1$ then $ax \equiv b \bmod m$ has a unique solution modulo m. (Hint: show that if x' is another solution, then $m \mid (x - x')$.)
  (c) If $g = 1$ and x is the unique solution to $ax \equiv b \pmod{m}$ then the every solution to $ahy \equiv bh \pmod{hm}$ is of the form
$$y = x + mk$$
  for some $k \in \mathbb{Z}$ and that there are h distinct residues modulo hm of this form.
  (d) Use this to show that if $g \mid b$ then $ax \equiv b \bmod m$ has g distinct solutions x modulo m.

(2) Suppose $a, m \in \mathbb{Z}$ with $m > 0$ and $\gcd(a, m) = 1$, and let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced residue system modulo m.
  (a) Show that $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ is also a reduced residue system modulo m.
  (b) Conclude that $r_1 r_2 \cdots r_{\phi(m)} \equiv (ar_1)(ar_2) \cdots (ar_{\phi(m)}) \bmod m$ and, consequently, that
$$a^{\phi(m)} \equiv 1 \pmod{m}.$$
  (This is *Euler's theorem.*)
  (c) Explain how this implies that, if p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \bmod p$. (This is *Fermat's little theorem.*)
  (d) Use Fermat's Little theorem to prove that, if p is prime and $a, b \in \mathbb{Z}$, then $(a+b)^p \equiv a^p + b^p \bmod p$. (This is called the *freshman's dream.*)

(3) Suppose p is prime. Prove that $x^2 \equiv 1 \bmod p$ has precisely the two solutions $x \equiv \pm 1 \bmod p$.

(4) Suppose $m \in \mathbb{Z}_{>0}$.
  (a) Suppose m is prime. Use (1b) and (3) to show that if $a \not\equiv 0, \pm 1 \bmod m$ then there exists $b \not\equiv 0, \pm 1, a \bmod m$ such that $ab \equiv 1 \bmod m$.
  (b) Conclude that $(m-1)! \equiv -1 \bmod m$ if m is prime. (This is one direction of *Wilson's Theorem*, which states that $(m-1)! \equiv -1 \bmod m$ if and only if m is prime.)