Thursday, September 26

Homework #2 due Tuesday

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).

[same statement from end of Tuesday]

Proof: Start with general m.

$(3) \Rightarrow (1)$: Square both sides of $x \equiv \pm 1 \pmod m$.

$(2) \Rightarrow (1)$: Multiply both sides of $x^{-1} \equiv x \pmod m$ by x, to get $1 \equiv x^2 \pmod m$.

$(1) \Rightarrow (2)$: Since $(1, m) = 1$, we know $(x^2, m) = 1$, and so $(x, m) = 1$. Thus x^{-1} exists, and multiply both sides of the congruence by x^{-1}.

Finally, prove $(1) \Rightarrow (3)$ if m is prime: $x^2 \equiv 1 \pmod m$ implies $m \mid (x^2 - 1) = (x-1)(x+1)$. By Euclid's lemma, $m \mid (x-1)$ or $m \mid (x+1)$

$$m \mid (x-1) \Leftrightarrow x \equiv 1 \pmod m, \qquad m \mid (x+1) \Leftrightarrow x \equiv -1 \pmod m.$$

//

Wilson's Theorem: Let p be prime. Then $(p-1)! \equiv -1 \pmod p$.

Example: 101 divides $100! + 1$.

<u>Proof:</u> ($p=2,3$ by hand) Assume $p \geq 5$.

Pair up residue classes $\{2,3,\dots,p-2\}$ into $\frac{p-3}{2}$ pairs $\{a,a^{-1}\}$. Note that nothing here is its own inverse, by previous lemma, so this really is a pairing). Then

$$(p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-2) \times (p-1)$$
$$\equiv 1 \times \left\{ \frac{p-3}{2} \text{ pairs of the form } \{a,a^{-1}\} \right\} \times (p-1)$$
$$\equiv 1 \times 1^{(p-3)/2} \times (-1) \equiv -1 \pmod{p}.$$
//

Solutions of polynomial congruences

<u>Example:</u> How many solutions does
$$X^4 + 2X^3 + X + 1 \equiv 0 \pmod{5}$$
have?

The set of solutions is
$$\{\dots, -14, -13, -9, -8, -4, -3, 1, 2, 6, 7, 11, 12, \dots\},$$

but this is, more simply, all integers congruent to 1 or 2 (mod 5).

<u>Definition:</u> Given a polynomial $f(X)$ with integer coefficients ($f(X) \in \mathbb{Z}[X]$) and $m \in \mathbb{N}$, define $\sigma_f(m)$ to be number of residue classes (mod m) that satisfy the congruence $f(a) \equiv 0 \pmod{m}$; equivalently, $\sigma_f(m) = \#\{1 \leq a \leq m : f(a) \equiv 0 \pmod{m}\}$.

<u>Example:</u> Let $f(X) = X^2 - 1$.

By today's first lemma, $\sigma_f(p) = 2$ for any odd prime p (and $\sigma_f(2) = 1$).

On the other hand,
$$\sigma_f(24) = 8.$$

Linear congruences are quick:

Theorem: Let $f(x) = aX - b$.
Let $m \in \mathbb{N}$ and set $g = \gcd(a, m)$.
Then $\rho_f(m) = 0$ unless $g \mid b$, in which case $\rho_f(m) = g$.

Example: $f(X) = 5X - 70$, $m = 100$.
Solutions are $\{14, 34, 54, 74, 94\} \pmod{100}$,
so $\rho_f(100) = 5 = (5, 100)$.

Note $5 \mid 70$.

$g(x) = 5X - 71$: $(5, 100) \nmid 71$, and indeed no solutions.

Proof: $f(x) \equiv 0 \pmod m$ means $ax \equiv b \pmod m$.
This implies $ax \equiv b \pmod g$, which is
$0 \equiv 0x \equiv b \pmod g$. Thus if solutions
x exist then $g \mid b$.

Now assume $g \mid b$. Write
$a = \alpha g$, $b = \beta g$, $m = \mu g$.
Then $ax \equiv b \pmod m \iff$
$\alpha g x \equiv \beta g \pmod{\mu g} \iff$
$\alpha x \equiv \beta \pmod \mu$.

Note $(\alpha, \mu) = \left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$,
so $\alpha^{-1} \pmod \mu$ exists; thus the
solution is $x \equiv \alpha^{-1}\beta \pmod \mu$.
This single residue class $\pmod \mu$
is the union of g residue
classes $\pmod m$. //

General strategy for evaluating $\sigma_f(m)$

- Reduce to the case where m is a prime power:
  If $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ as a product of powers of distinct primes, then $(p_i^{r_i}, p_j^{r_j}) = 1$ for all $i \neq j$ (pairwise relatively prime), and so by the Chinese remainder theorem,
  $$f(x) \equiv 0 \pmod{m}$$
  is equivalent to
  $$\begin{cases} f(x) \equiv 0 \pmod{p_1^{r_1}} \\ f(x) \equiv 0 \pmod{p_2^{r_2}} \\ \quad\vdots \\ f(x) \equiv 0 \pmod{p_k^{r_k}}. \end{cases}$$

Hence $\sigma_f(m) = \sigma_f(p_1^{r_1})\sigma_f(p_2^{r_2}) \cdots \sigma_f(p_k^{r_k})$.

- Reduce further to the case of prime modulus.
  - Tool: "Hensel's Lemma"
- Theoretical stuff about $\sigma_f(p)$
- Special families of f:
  - $f(X) = X^k - a$
  - quadratic $f(X)$

Hensel's Lemma: (to be proved in Group Work #3) Let $f(X) \in \mathbb{Z}[X]$ and let p^j be a prime power ($j \geq 1$). Suppose that $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod p$. Then there exists a unique integer $0 \leq t \leq p-1$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

Note: f' means what you think:

$$\left(\sum a_k X^k\right)' = \sum k a_k X^{k-1}.$$

Example: $f(x) = x^2 - 2$, $a = 4$, $p^j = 7^1$. Confirm $f(a) = 4^2 - 2 = 14 \equiv 0 \pmod{7^1}$.

Hensel's lemma says that exactly one of $\{a + tp^j : 0 \leq t \leq p-1\} = \{4 + t \cdot 7^1 : 0 \leq t \leq 6\}$

$= \{4, 11, 18, 25, 32, 39, 46\}$

is a root of $X^2 - 2 \pmod{49}$.

Once we check $f'(a) = 2a = 8 \not\equiv 0 \pmod 7$).

It turns out to be $39 = 4 + 5 \cdot 7$:

$$39^2 - 2 = 1{,}519 = 49 \cdot 31.$$

Insight: the residue class $a \pmod{p^j}$ is the union of the p residue classes $a + tp^j \pmod{p^{j+1}}$ $(0 \leq t \leq p-1)$.

- Note $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$, then $f(a + tp^j) \equiv 0 \pmod{p^j}$

$$\Updownarrow$$

$$f(a) \equiv 0 \pmod{p^j}.$$

So if a is not a root of $f(X) \pmod{p^j}$, then none of $a + tp^j$ are roots of $f(x) \pmod{p^{j+1}}$.

- Given a root b of $f(x) \pmod{p^i}$ and $j > i$, a lift of b to a root of $f(x) \pmod{p^j}$ is some integer $c \equiv b\ (p^i)$ such that $f(c) \equiv 0 \pmod{p^j}$.
- Hensel's Lemma says, in the situation of nonsingular roots of $f(x) \pmod{p^i}$

— where "nonsingular" means $f'(a) \not\equiv 0 \pmod p$ —

every root $a \pmod{p^j}$ has a unique lift to a root $\pmod{p^{j+1}}$.

Corollary: Let $f(x) \in \mathbb{Z}[x]$, and let a be a root of $f(x) \pmod p$ with $f'(a) \not\equiv 0 \pmod p$. Then for every $j \geq 2$ there exists a unique lift a_j of a to a root of $f(x) \pmod{p^j}$: a unique residue class $a_j \pmod{p^j}$ with $a_j \equiv a \pmod p$ and $f(a_j) \equiv 0 \pmod{p^j}$.

In particular:

If all roots of $f(x) \pmod p$ are nonsingular, then $\sigma_f(p^j) = \sigma_f(p)$ for all $j \geq 2$.

There are versions of Hensel's lemma that deal with singular roots — see Niven/Zuckerman/Montgomery, Theorem 2.24.