Thursday, October 3

Example: Consider $f(X) = X^p - X$.

By Fermat's little theorem, every residue class (mod p) is a root of $f(x)$ (mod p). It follows that

$$f(X) \equiv X(X-1)(X-2)\cdots(X-(p-1))\,g(X) \pmod p$$

– but $g(X)$ must be the constant 1 by comparing degrees and leading coefficients.

So $X^p - X \equiv X(X-1)(X-2)\cdots(X-(p-1)) \pmod p$.

Extra gift: compare coefficients of X^1:

$$-1 \equiv (-1)^{p-1}(p-1)! \equiv (p-1)! \pmod p.$$

Wilson's theorem.

Same idea gives a stronger statement: if $f(a) \equiv g(a) \pmod p$ for every $a \in \mathbb{Z}$, then $f(X) - g(X) \equiv X(X-1)\cdots(X-(p-1))\,h(X)$

$$\equiv (X^p - X)\,h(X) \pmod p.$$

The "converse" is also true:

Theorem: Let $\mathbb{Z}_p$ denote the set of residue classes (mod p). Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be any function. Then there exists a unique polynomial $g(X)$ (mod p) of degree at most $p-1$ such that $f(a) \equiv g(a) \pmod p$ for every $a \in \mathbb{Z}_p$.

Proof of uniqueness: Let $g(X)$, $h(X)$ be two such polynomials. Then $g(a) \equiv f(a) \equiv h(a) \pmod p$ for all $a \in \mathbb{Z}$; so

$$g(X) - h(X) \equiv (X^p - X)\,k(X) \pmod p;$$

by comparing degrees, we must have $k(X)$ is the zero polynomial.

Proofs of existence:

(1) Note that for any $a \in \mathbb{Z}$,

$$1-(y-a)^{p-1} \equiv \begin{cases} 0, & \text{if } y \not\equiv a \pmod p, \\ 1, & \text{if } y \equiv a \pmod p. \end{cases}$$

by Fermat's little theorem. Then take

$$g(X) = \sum_{a=0}^{p-1} \left(1-(X-a)^{p-1}\right) f(a).$$

(2) There are p^p functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. There are p^p polynomials of the form $\sum_{k=0}^{p-1} c_k X^k$ where $c_j \in \{0,1,\dots,p-1\}$.
But each such polynomial represents a different function (by uniqueness); hence (by counting) every function is represented by some polynomial. //

Corollary (to Example): Suppose $d \mid (p-1)$. Then $X^d - 1$ has exactly d roots $\pmod p$.

Proof: We have the factorization

$$X^{p-1}-1 = \underbrace{(X^d-1)}_{(1)}\underbrace{\left(X^{p-1-d}+X^{p-1-2d}+\cdots+X^{2d}+X^d+1\right)}_{(2)}.$$

By last class, (1) has at most d roots and (2) has at most $(p-1-d)$ roots $\pmod p$. But $X^{p-1}-1$ has $p-1$ distinct roots $1,2,\dots,p-1 \pmod p$.
By counting, (1) and (2) must both have their maximum number of roots. //

Order and primitive roots

[Recall: if $a^n \equiv 1 \pmod m$, then $(a,m)=1$.]

Definition: Given $(a,m)=1$, the (multiplicative) order of $a \pmod m$ is the smallest $k \in \mathbb{N}$ such that $a^k \equiv 1 \pmod m$.

Example: $m=11$, $a=3$.

k	1	2	3	4	5	6
$3^k \equiv \_\_ \pmod{11}$	3	9	$\cancel{27}$ 5	$\cancel{15}$ 4	$\cancel{12}$ 1	3

and so the order of 3 (mod 11) is 5.

Lemma: Given $(a,m)=1$: $a^k \equiv 1 \pmod m$ if and only if the order of $a \pmod m$ divides k.

– In particular: the order of $a \pmod m$ always divides $\phi(m)$ (by Euler's theorem).

Proof: Let h be the order of $a \pmod m$. Write $k = hq + r$ where $0 \le r < h$.

Then $a^k = a^{hq+r} = (a^h)^q a^r$
$$\equiv 1^q a^r \equiv a^r \pmod m.$$

- If $r = 0$, then $h \mid k$ and $a^k \equiv 1 \pmod m$.
- If $r > 0$, then $h \nmid k$. Also $a^r \not\equiv 1 \pmod m$, because r is smaller than h, the order of a. //

Proposition: Let a have order $r \pmod m$ and b have order $s \pmod m$. If t is the order of $ab \pmod m$, then
$$t \,\Big|\, \frac{rs}{(r,s)} = \mathrm{lcm}[r,s], \text{ and}$$
$$\frac{rs}{(r,s)^2} \,\Big|\, t.$$

In particular, if $(r,s)=1$, then $t = rs$.

Proposition: Let a have order $r \pmod m$ and b have order $s \pmod m$. If t is the order of $ab \pmod m$, then

$$t \mid \frac{rs}{(r,s)} = \mathrm{lcm}[r,s], \text{ and}$$

$$\frac{rs}{(r,s)^2} \mid t.$$

Proof: Let's note that

$$(ab)^{\mathrm{lcm}[r,s]} = (a^r)^{s/(r,s)}(b^s)^{r/(r,s)}$$

$$= 1^{s/(r,s)}\, 1^{r/(r,s)} = 1 \pmod m;$$

by the previous lemma, $\mathrm{lcm}[r,s]$ is a multiple of t. ✓

Also,

$$a^{st} \equiv a^{st}(b^s)^t \equiv ((ab)^t)^s \equiv 1 \pmod m;$$

so r (the order of a) must divide st by the previous lemma. But:

$$r \mid st \iff$$

$$\frac{r}{(r,s)} \mid \frac{s}{(r,s)}\, t \iff$$

$$\frac{r}{(r,s)} \mid t. \quad \left(\text{since } \left(\frac{r}{(r,s)}, \frac{s}{(r,s)}\right) = 1\right).$$

The symmetric argument shows

$$\frac{s}{(r,s)} \mid t.$$

Since $\left(\frac{r}{(r,s)}, \frac{s}{(r,s)} = 1\right)$, we conclude that $\frac{r}{(r,s)} \frac{s}{(r,s)} \mid t$. //

Lemma: If a has order $h \pmod m$, then the order of $a^k \pmod m$ equals $\frac{h}{(h,k)}$.

Example: The order of $a^2 \pmod m$ equals $\begin{cases} h/2, & \text{if } h \text{ is even}, \\ h, & \text{if } h \text{ is odd}. \end{cases}$

Lemma: If a has order $h \pmod{m}$, then the order of $a^k \pmod{m}$ equals $\frac{h}{(h,k)}$.

Proof: The following statements about $j \in \mathbb{N}$ are equivalent:

(1) $(a^k)^j \equiv 1 \pmod{m}$

(2) $h \mid kj$

(3) $\frac{h}{(h,k)} \mid \frac{k}{(h,k)} j$

(4) $\frac{h}{(h,k)} \mid j$.

In particular, the smallest positive integer j satisfying (4) (and hence (1) as well) is $j = \frac{h}{(h,k)}$. //

Definition: a is a primitive root $\pmod{m}$ if the order of $a \pmod{m}$ equals $\phi(m)$ (which is as large as it could be).

Example: $m = 11$. $\phi(m) = 10$.

a	1	2	3	4	5	6	7	8	9	10
order of a (mod 11)	1	10	5	5	5	10	10	10	5	2

Thus 2, 6, 7, 8 are all primitive roots (mod 11).

Note: $\{2^1, 2^2, 2^3, \ldots, 2^{10}\}$

$$\equiv \underbrace{\{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}}_{\text{reduced residue system.}}$$

Lemma: If m has a primitive root, then it has exactly $\phi(\phi(m))$ primitive roots.

Proof: Let g be a primitive root (mod m). Then $\{g, g^2, \ldots, g^{\phi(m)}\}$ forms a reduced residue system (mod m). By the previous lemma, the order of g^k is $\dfrac{\phi(m)}{(k, \phi(m))}$; in particular, the order of g^k equals $\phi(m)$ precisely when $(k, \phi(m)) = 1$ — and there are $\phi(\phi(m))$ such integers $1 \leq k \leq \phi(m)$.

$\lightning$