Math135 - November 4'th, 2015

Inverses and Fermat's Little Theorem

Recall all are equivalent:

- $a \equiv b \pmod{m}$
- $m|(a-b)$
- $\exists k \in \mathbb{Z}, a-b=km$
- a and b have the same remainder when divided by m.
- $[a]=[b]$ in $\mathbb{Z}_m$

Multiplicative Inverse

Example: Find $[5]^{-1}$ in $\mathbb{Z}_{17}$

$[5][x]=[1]$
By inspection, $[x]=[7]$.
Therefore $[5]^{-1}=[7]$.

If we couldn't find a solution by inspection, we could convert into Linear Diophantine and solve.
$5x+17y=1$
Solve by EEA.

Linear Congruence Theorem 2

Let $\gcd(a,m)=d\neq 0$
The equation $[a][x]=[c]$ in $\mathbb{Z}_m$ has a solution iff $d|c$ Also, if $[x]=[x_0]$ is one solution, the complete solution is $\{[x_0],[x_0+2\frac{m}{d}],\ldots,[x_0+(d-1)\frac{m}{d}]\}$

Prove:

i) $[a]^{-1}$ exists iff $\gcd(a,m)=1$

As this is an 'if and only if', we must prove the implication both ways.
$\Longrightarrow$:
Assume $[a]^{-1}$ exists.
$\iff [a][x]=[1]$
$\iff \gcd(a,m)|1$ (By LCD 2)
$\iff \gcd(a,m)=1$
Because every property we used was an iff (That is, they all apply both ways), we can say WLOG, the other direction must be true as well.
$\therefore [a]^{-1}$ exists iff $gcd(a,m)=1$

ii) The multiplicative inverse pf $[a]$ in $\mathbb{Z}_m$ is unique (if it exists)

if $[a]^{-1}$ exists in $\mathbb{Z}_m$, then
$[a][x]=[1]$ has a solution.
Thus, $\gcd(a,m)=1$
By LCT2, the complete solution of all inverses is:
$\{x_0, x_0+m, x_0+2m,\ldots\}$
$\equiv \{x_0\}$
$\therefore$ The inverse is unique.

Fermat's Little Theorem (FℓT)

If p is a prime number that does not divide an integer a, then
$a^{p-1} \equiv 1 \pmod{p}$

Examples:

i) $5^6 \equiv 1 \pmod{7}$

ii) $3^6 \equiv 1 \pmod{7}$

iii) $8^6 \equiv 1 \pmod{7}$

iv) $35^6 \not\equiv 1 \pmod{7}$ (Because $7|35$)

v) Find the remainder when 7^{32} is divided by 11.

By FℓT, $7^{10} \equiv 1 \pmod{11}$ (Since 11 is prime and $11 \nmid 7$)

$$\begin{aligned} 7^{32} &\equiv (7^{10})^9 7^2 \pmod{11} \\ &\equiv (1)^9 7^2 \pmod{11} \\ &\equiv 49 \pmod{11} \\ &\equiv 5 \pmod{11} \end{aligned}$$

$\therefore$ The remainder is 5

FℓT in Congruence Classes

$[a^{p-1}] = [1]$ in $\mathbb{Z}_p$
$[a]^{p-1} = [1]$ in $\mathbb{Z}_p$