Math135 - November 5'th, 2015

Existence of Inverses, Chinese Remainder Theorem

Corollary to FℓT

For any integer a and prime p,
$a^p = a \pmod{p}$

Existence of Inverses in $\mathbb{Z}_p$

Let p be a prime number. If $[a]$ is any non-zero element in $\mathbb{Z}_p$, then there exists an element $[b] \in \mathbb{Z}_p$ such that $[a][b] = [1]$

Proof:

Assume $[a]$ is a non-zero element in $\mathbb{Z}_p$.
$a \not\equiv 0 \pmod{p}$
So, $p \nmid a$
By FℓT, $a^{p1} \equiv 1 \pmod{p}$
Consider $[b] = [a^{p-2}]$ (Allowed since $p \geq 2$)
$[a][b] = [a][p-2]$
$[a][b] = [a^{p-1}] = [1]$

This proof gives us another method to find the inverse of an element in $\mathbb{Z}_p$ if p is prime.

$[a^{-1}] = [a]^{p-2}$

Example: What is the inverse of 7 in $\mathbb{Z}_{11}$?

$$
\begin{aligned}
[7]^{-1} &= [7]^{11-2} \\
&= [7]^9 \\
&= [5^4 \cdot 7] \text{ (Because } 7^2 \equiv 5 \pmod{11}) \\
&= [3^2 \cdot 7] \text{ (Because } 5^2 \equiv 3 \pmod{11}) \\
&= [63] \\
&= [8]
\end{aligned}
$$

Examples of FℓT Proofs

Let p be prime, $r, k, s \in \mathbb{Z}$:

i) If $p \nmid a$ and $r \equiv s \pmod{p-1}$, then $a^r \equiv a^s \pmod{p}$.
Assume $p \nmid a$ and $r \equiv s \pmod{p}$
$r - s = (p-1)k,\ k \in \mathbb{Z}$
$r = (p-1)k + s$

$$
\begin{aligned}
a^r &\equiv a^{(p-1)k+s} \pmod{p} \\
&\equiv a^{(p-1)k} a^s \pmod{p} \\
&\equiv 1^k a^s \pmod{p} \\
&\equiv a^s \pmod{p} \\
&\equiv a^s \pmod{p}
\end{aligned}
$$

ii) If $r = pk + s$, then $a^4 \equiv a^{s+k} \pmod{p}$.

$$
\begin{aligned}
a^r &\equiv a^{pk+s} \pmod{p} \\
&\equiv (a^p)^k a^s \pmod{p} \\
&\equiv a^k a^s \pmod{p} \\
&\equiv a^{k+s} \pmod{p}
\end{aligned}
$$

Chinese Remainder Theorem

Let $a_1, a_2 \in \mathbb{Z}$. If $\gcd(m_1, m_2) = 1$, then the simultaneous linear congruences:

$n \equiv a_1 \pmod{m_1}$
$n \equiv a_2 \pmod{m_2}$

have a unique solution modulo $(m_1)(m_2)$. Thus, if $n = n_0$ is one integer solution, then the complete solution is:

$n \equiv n_0 \pmod{m_1 m_2}$