Theorems of Fermat and Euler

**Theorem (Fermat).** Let $p$ be a prime number. Then:

(a). $a^{p-1} \equiv 1 \pmod{p}$ for all $a \in \mathbb{Z}$ such that $p \nmid a$

(b). $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$

**Proof.** Part (a) was done last time. It used Exercise 10.40: If $G$ is an abelian group of finite order $n$ then $a^n = 1$ for all $a \in G$.

(b). Let $a \in \mathbb{Z}$. If $p \mid a$ then $a^p \equiv 0 \equiv a \pmod{p}$.

If $p \nmid a$ then $a^p = a \cdot a^{p-1} \equiv a \cdot 1 = a \pmod{p}$. □

**Example (Modulo 7)**

$$
egin{align*}
1^6 & = 1 \\
2^6 & = (2^3)^2 = 8^2 \equiv 1^2 = 1 \pmod{7} \\
3^6 & = (3^2)^3 = 9^3 \equiv 2^3 = 8 \equiv 1 \pmod{7} \\
4^6 & \equiv (-3)^6 = 3^6 \equiv 1 \pmod{7} \\
5^6 & \equiv (-2)^6 = 2^6 \equiv 1 \pmod{7} \\
6^6 & \equiv (-1)^6 = 1 \pmod{7}
\end{align*}
$$

**Euler’s $\phi$ Function**

**Definition.** Let $n \in \mathbb{Z}^+$. Then

$$
\phi(n) = |\{a \in \mathbb{Z}^+: a \leq n \text{ and } \gcd(a,n) = 1\}| = |\{a \in \mathbb{N}: a < n \text{ and } \gcd(a,n) = 1\}| = |\mathbb{Z}_n^*| .
$$

**Examples.** $\phi(1) = 1$ and $\phi(p) = p - 1$ for all primes $p$.

**Euler’s Theorem**

**Theorem (Euler).** Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. If $\gcd(a,n) = 1$ then

$$
a^{\phi(n)} \equiv 1 \pmod{n} .
$$

**Proof.** Let $\gamma: \mathbb{Z} \to \mathbb{Z}_n$ be the group homomorphism from earlier in the semester. Then $\gamma(a) \in \mathbb{Z}_n^*$.

(This is true because $a \equiv \gamma(a) \pmod{n}$, and if $a \equiv b \pmod{n}$ then $\gcd(a,n) = \gcd(b,n)$. The latter can be seen from the definition of $\gcd$.)

We then have $\gamma(a)^{\phi(n)} = 1$ in $\mathbb{Z}_n$ (by Exercise 10.40); therefore $\gamma(a^{\phi(n)}) = 1$ in $\mathbb{Z}_n$; therefore $a^{\phi(n)} \equiv 1 \pmod{n}$. □
Solving $ax \equiv b \pmod{m}$

**Theorem.** Let $m \in \mathbb{Z}^+$, let $a, b \in \mathbb{Z}_m$, and let $d = \gcd(a, m)$. Then the equation

$$ax = b$$

has no solutions in $\mathbb{Z}_m$ if $d \nmid b$, and exactly $d$ solutions in $\mathbb{Z}_m$ if $d \mid b$.

**Theorem.** Let $m \in \mathbb{Z}^+$, let $a, b \in \mathbb{Z}$, and let $d = \gcd(a, m)$. Then the equation

$$ax \equiv b \pmod{m}$$

has no solutions if $d \nmid b$, and its solutions set is the union of exactly $d$ congruence classes modulo $m$ if $d \mid b$.

**Examples**

$$36x \equiv 15 \pmod{24}$$

$$155x \equiv 75 \pmod{65}$$

(on blackboard)