TW 314 Lecture 30 (Fr. 28 April 2017)

Proposition 8 p prime $\Rightarrow \phi(p^e) = p^e - p^{e-1}$

Proof: If p is prime, then an integer x in the range $1 \le x \le p^e$ is not relatively prime to p^e if and only if x is a multiple of p. The multiples of p in this range is $p, 2p, 3p, \ldots, p^{e-1}p$. There are p^{e-1} such multiples, and therefore $\phi(p^e) = p^e - p^{e-1}$.

Theorem 9 If m has the prime factorization $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then $\phi(m) = m \prod_{i=1}^{r} (1 - \frac{1}{p_i})$.

Proof:
$$\begin{aligned}
\phi(m) &= \phi(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) \\
&= \phi(p_1^{e_1})\,\phi(p_2^{e_2}) \cdots \phi(p_r^{e_r}) \quad \text{— by Prop. 7} \\
&= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_r^{e_r} - p_r^{e_r-1}) \quad \text{— by Prop 8} \\
&= m\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right) \cdots \left(1 - \tfrac{1}{p_r}\right).
\end{aligned}$$

Example: Since $12 = 2^2 \cdot 3$, $\phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$
$= 12 \times \frac{1}{2} \times \frac{2}{3} = 4$ →

Theorem 10 (Euler's Theorem)

If b and n are relatively prime, $0 < b < n$,

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

Proof: Let $\mathbb{Z}_n^* = \{a_1, a_2, \ldots, a_{\phi(n)}\}$

and $b\mathbb{Z}_n^* = \{ba_1, ba_2, \ldots, ba_{\phi(n)}\}$.

Since $\gcd(n, b) = 1$, $b \in \mathbb{Z}_n^*$ and therefore $b\mathbb{Z}_n^* \subseteq \mathbb{Z}_n^*$.

Furthermore, all elements of $b\mathbb{Z}_n^*$ are distinct

since $ba_i = ba_j$ in $\mathbb{Z}_n^*$ implies $a_i = a_j$ in $\mathbb{Z}_n^*$.

Therefore $b\mathbb{Z}_n^* = \mathbb{Z}_n^*$ and therefore

$$(ba_1)(ba_2)\cdots(ba_{\phi(n)}) = a_1 a_2 \cdots a_{\phi(n)},$$

so $$b^{\phi(n)} a_1 a_2 \cdots a_{\phi(n)} = a_1 a_2 \cdots a_{\phi(n)}$$

and so $b^{\phi(n)} = 1$ in $\mathbb{Z}_n^*$, that is,

$b^{\phi(n)} \equiv 1 \pmod{n}$. ∎

Example: $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ and $\phi(12) = 4$.

Now $1^4 \equiv 1 \pmod{12}$

$5^4 \equiv 25^2 \equiv 1^2 \equiv 1 \pmod{12}$

$7^4 \equiv 49^2 \equiv 1^2 \equiv 1 \pmod{12}$

$11^4 \equiv (-1)^4 \equiv 1 \pmod{12}$.

Corollary 11 (Fermat's Little Theorem)

If n is prime and b is not divisible by n, then $b^{n-1} \equiv 1 \pmod{n}$.

Example: Modular 7 arithmetic...

11 is not divisible by 7, and

$11^6 \equiv 4^6 \equiv (4^2)^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod{7}$.

The square-and-multiply algorithm for finding $c \equiv a^b \pmod{n}$:

Let b have binary representation

$$b = b_0 + 2b_1 + 2^2 b_2 + \cdots + 2^{l-1} b_{l-1}$$