Number Theory Section Summary: 7.1-7.3
Euler's Phi Function

1. Summary

   Now we put Euler's phi function to work, generalizing Fermat's Little Theorem.

2. **Theorems**

   Theorem 7.5 (Euler): If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1$(mod n).

   Proof (first form, requires the following lemma):

   Lemma: Let $n > 1$ and $\gcd(a, n) = 1$. If a_1, a_2,...,$a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then aa_1, aa_2,...,$aa_{\phi(n)}$ are congruent modulo n to a_1, a_2,...,$a_{\phi(n)}$ in some order.

   Corollary: Fermat's Little theorem!

   Proof (second form, which doesn't require the lemma, but which relies on Fermat's theorem):

   Lemma: If $p \nmid a$, p prime, then

   $(\gcd(a,p)=1)$ $$a^{\phi(p^k)} \equiv 1 \pmod{p^k}$$

   for $k \geq 1$.

   Proof (by induction, using the Binomial theorem and Fermat):
   on k

Base case: $k=1$

$a^{\varphi(p)} \equiv 1 \pmod{p}$ ✓ (Fermat's Little Theorem)

$\Rightarrow$: Assume true for k; demonstrate for $k+1$

Assume that $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$

Note: $\varphi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p\,\varphi(p^k)$

$$a^{\varphi(p^{k+1})} = a^{p\varphi(p^k)} = \left(a^{\varphi(p^k)}\right)^p = (1+mp^k)^p$$

$$= 1^p + \binom{p}{1}(mp^k)^1 + \dots + \binom{p}{p-1}(mp^k)^{p-1} + (mp^k)^p$$

$$= (1) + \underbrace{p(mp^k)}_{\equiv 0 \pmod{p^{k+1}}} + \dots + \underbrace{\binom{p}{p-1}(mp^k)^{p-1}}_{\equiv 0 \pmod{p^{k+1}}} + \underbrace{(mp^k)^p}_{\equiv 0 \pmod{p^{k+1}}}$$

$$\equiv 1 \pmod{p^{k+1}}$$

$\therefore$ the lemma is established by induction

Proof of the theorem:

Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be n's prime factorization.

Thus we can write $n = p_i^{k_i} \cdot m_i \quad \forall i \in \{1, \dots, r\}$, where $\gcd(p_i^{k_i}, m_i) = 1$

So $\varphi(n) = \varphi(p_i^{k_i})\varphi(m_i)$. From the lemma we know that

$$a^{\varphi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}$$

$$a^{\varphi(n)} = a^{\varphi(p_i^{k_i})\varphi(m_i)} = \left(a^{\varphi(p_i^{k_i})}\right)^{\varphi(m_i)},$$ so by the

lemma, $$\equiv 1^{\varphi(m_i)} \equiv 1 \pmod{p_i^{k_i}}$$

$$\therefore a^{\varphi(n)} \equiv 1 \pmod{p_i^{k_i}} \quad \forall i$$

$$\therefore a^{\varphi(n)} \equiv 1 \pmod{\underbrace{p_1^{k_1} \cdots p_r^{k_r}}_{\text{mutually relatively prime}}}$$

$$\therefore a^{\varphi(n)} \equiv 1 \pmod{n}$$

#1a $a^{37} \equiv a \pmod{1729}$

7.13.19

$$\varphi(1729) = \varphi(7)\,\varphi(13)\,\varphi(19)$$
$$= 6 \cdot 12 \cdot 18$$

Objective: $\qquad$ lcm $= 36$

$$a^{36} \equiv 1 \pmod{p_i}$$

By Euler,
$$a^{\varphi(7)} = a^{6} \equiv 1 \pmod 7$$
$$a^{\varphi(13)} = a^{12} \equiv 1 \pmod{13}$$
$$a^{\varphi(19)} = a^{18} \equiv 1 \pmod{19}$$

$$\therefore \quad a^{\operatorname{lcm}(6,12,18)} \equiv 1 \quad \text{mod}\,(\underbrace{7,\ 13,\ \&\ 19}_{\text{hence true for the product 1729}})$$

$$\therefore \quad a^{36} \equiv 1 \pmod{1729}$$
$$a^{37} \equiv a \pmod{1729}$$