Bonus Lecture 2: Euler's Totient Theorem

Primes Are Overrated Anyways

Recall From the Future...

"Recall" Fermat's Little Theorem:
Theorem: Let p be prime and $a \not\equiv 0 \pmod{p}$.
Then $a^{p-1} \equiv 1 \pmod{p}$.

Recall From the Future...

"Recall" Fermat's Little Theorem:
Theorem: Let p be prime and $a \not\equiv 0 \pmod{p}$.
Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof:

- $f(x) = ax \pmod{p}$ is biject. on $\{1, 2, ..., p-1\}$
- So $\{1, ..., p-1\} = \{a, ..., (p-1)a\} \pmod{p}$

Recall From the Future...

"Recall" Fermat's Little Theorem:

Theorem: Let p be prime and $a \not\equiv 0 \pmod{p}$.
Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof:

- $f(x) = ax \pmod{p}$ is biject. on $\{1, 2, ..., p-1\}$
- So $\{1, ..., p-1\} = \{a, ..., (p-1)a\} \pmod{p}$
- Means $\prod_i i = \prod_i (ai \bmod p)$
- Factor out a: $\prod_i i \equiv a^{p-1} \prod_i i \pmod{p}$

Recall From the Future...

"Recall" Fermat's Little Theorem:

Theorem: Let p be prime and $a \not\equiv 0 \pmod{p}$.
Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof:

- $f(x) = ax \pmod{p}$ is biject. on $\{1, 2, ..., p-1\}$
- So $\{1, ..., p-1\} = \{a, ..., (p-1)a\} \pmod{p}$
- Means $\prod_i i = \prod_i (ai \bmod p)$
- Factor out a: $\prod_i i \equiv a^{p-1} \prod_i i \pmod{p}$
- i^{-1} exists for all $i \in \{1, 2, ..., p-1\}$
- Multiply by $(\prod_i i)^{-1} \equiv \prod_i (i^{-1}) \pmod{p}$

Recall From the Future...

"Recall" Fermat's Little Theorem:
Theorem: Let p be prime and $a \not\equiv 0 \pmod{p}$.
Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof:

- $f(x) = ax \pmod{p}$ is biject. on $\{1, 2, ..., p-1\}$
- So $\{1, ..., p-1\} = \{a, ..., (p-1)a\} \pmod{p}$
- Means $\prod_i i = \prod_i (ai \bmod p)$
- Factor out a: $\prod_i i \equiv a^{p-1} \prod_i i \pmod{p}$
- i^{-1} exists for all $i \in \{1, 2, ..., p-1\}$
- Multiply by $(\prod_i i)^{-1} \equiv \prod_i (i^{-1}) \pmod{p}$

What happens if p not prime?

Euler Attempt 1

Claim: If $a \not\equiv 0 \pmod{m}$, $a^{m-1} \equiv 1 \pmod{m}$.

Euler Attempt 1

Claim: If $a \not\equiv 0 \pmod{m}$, $a^{m-1} \equiv 1 \pmod{m}$.

"Proof":

- Is $ax \pmod{m}$ a biject. on $\{1, ..., m-1\}$?

Euler Attempt 1

Claim: If $a \not\equiv 0 \pmod{m}$, $a^{m-1} \equiv 1 \pmod{m}$.

"Proof":

- Is $ax \pmod{m}$ a biject. on $\{1, ..., m-1\}$?
- Not necessarily!
- $2x \pmod{4}$ maps $\{1, 2, 3\}$ to $\{2, 0, 2\}$!

Euler Attempt 1

Claim: If $a \not\equiv 0 \pmod{m}$, $a^{m-1} \equiv 1 \pmod{m}$.

"Proof":

- Is $ax \pmod{m}$ a biject. on $\{1, ..., m-1\}$?
- Not necessarily!
- $2x \pmod{4}$ maps $\{1, 2, 3\}$ to $\{2, 0, 2\}$!

Generally have issues if $\gcd(a, m) \neq 1$

Euler Attempt 1

Claim: If $a \not\equiv 0 \pmod{m}$, $a^{m-1} \equiv 1 \pmod{m}$.

"Proof":

- Is $ax \pmod{m}$ a biject. on $\{1, ..., m-1\}$?
- Not necessarily!
- $2x \pmod{4}$ maps $\{1, 2, 3\}$ to $\{2, 0, 2\}$!

Generally have issues if $\gcd(a, m) \neq 1$
Not recoverable: if $a^{m-1} \equiv 1 \pmod{m}$, a^{m-2} is a^{-1}!

Euler Attempt 2

Claim: If $\gcd(a, m) = 1$, $a^{m-1} \equiv 1 \pmod{m}$.

Euler Attempt 2

Claim: If $\gcd(a, m) = 1$, $a^{m-1} \equiv 1 \pmod{m}$.

Proof:

- $f(x) = ax \pmod{m}$ is biject. on $\{1, ..., m-1\}$
- So $\{1, ..., m-1\} = \{a, ..., (m-1)a\} \pmod{m}$

Euler Attempt 2

Claim: If $\gcd(a, m) = 1$, $a^{m-1} \equiv 1 \pmod{m}$.

Proof:

- $f(x) = ax \pmod{m}$ is biject. on $\{1, \ldots, m-1\}$
- So $\{1, \ldots, m-1\} = \{a, \ldots, (m-1)a\} \pmod{m}$
- Means $\prod_i i = \prod_i (ai \bmod m)$
- Factor out a: $\prod_i i \equiv a^{m-1} \prod_i i \pmod{m}$

Euler Attempt 2

Claim: If $\gcd(a, m) = 1$, $a^{m-1} \equiv 1 \pmod{m}$.

Proof:

- $f(x) = ax \pmod{m}$ is biject. on $\{1, ..., m-1\}$
- So $\{1, ..., m-1\} = \{a, ..., (m-1)a\} \pmod{m}$
- Means $\prod_i i = \prod_i (ai \bmod m)$
- Factor out a: $\prod_i i \equiv a^{m-1} \prod_i i \pmod{m}$
- Issue: not all is have inverses
- So $(\prod_i i)^{-1}$ DNE!

Euler Attempt 3

Theorem: Let $\phi(m)$ be $|\{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}|$.[1]
Then for a coprime to m, $a^{\phi(m)} \equiv 1 \pmod{m}$.

[1] $\phi(\cdot)$ is known as Euler's Totient Function.

Euler Attempt 3

Theorem: Let $\phi(m)$ be $|\{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}|$.[1]
Then for a coprime to m, $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof:

- Let $S = \{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}$
- $f(x) = ax \pmod{m}$ is bijection on S

[1] $\phi(\cdot)$ is known as Euler's Totient Function.

Euler Attempt 3

Theorem: Let $\phi(m)$ be $|\{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}|$.[1]
Then for a coprime to m, $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof:

- Let $S = \{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}$
- $f(x) = ax \pmod{m}$ is bijection on S
- So $S = \{ax \bmod m | x \in S\}$
- Hence $\prod_{i \in S} i = \prod_{i \in S} (ai \bmod m)$

[1] $\phi(\cdot)$ is known as Euler's Totient Function.

Euler Attempt 3

Theorem: Let $\phi(m)$ be $|\{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}|$.[1]
Then for a coprime to m, $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof:

- Let $S = \{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}$
- $f(x) = ax \pmod{m}$ is bijection on S
- So $S = \{ax \bmod m | x \in S\}$
- Hence $\prod_{i \in S} i = \prod_{i \in S} (ai \bmod m)$
- Factor out a: $\prod_{i \in S} i \equiv a^{|S|} \prod_{i \in S} i \pmod{m}$
- $\left(\prod_{i \in S} i\right)^{-1} \equiv \prod_{i \in S} (i^{-1}) \pmod{m}$, so exists!
- Multiply to get $a^{\phi(m)} \equiv 1 \pmod{m}$

[1] $\phi(\cdot)$ is known as Euler's Totient Function.

Understanding ϕ

Claim: Suppose m can be factored as $p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$.
Then $\phi(m) = (p_1 - 1)p_1^{n_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{n_k - 1}$.

Understanding ϕ

Claim: Suppose m can be factored as $p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$.
Then $\phi(m) = (p_1 - 1)p_1^{n_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{n_k - 1}$.

Examples:

- $m = 12 = 2^2 \cdot 3$
  - $\phi(12) = (2-1)2^1 \cdot (3-1)3^0 = 4$
  - 1, 5, 7, 11

Understanding ϕ

Claim: Suppose m can be factored as $p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$.
Then $\phi(m) = (p_1 - 1)p_1^{n_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{n_k - 1}$.

Examples:

- $m = 12 = 2^2 \cdot 3$
  - $\phi(12) = (2-1)2^1 \cdot (3-1)3^0 = 4$
  - 1, 5, 7, 11
- $m = 11$
  - $\phi(11) = (11-1)11^0 = 10$
  - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Understanding ϕ

Claim: Suppose m can be factored as $p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$.
Then $\phi(m) = (p_1 - 1)p_1^{n_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{n_k - 1}$.

Examples:

- $m = 12 = 2^2 \cdot 3$
  - $\phi(12) = (2-1)2^1 \cdot (3-1)3^0 = 4$
  - 1, 5, 7, 11
- $m = 11$
  - $\phi(11) = (11-1)11^0 = 10$
  - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
- $m = 90 = 2 \cdot 3^2 \cdot 5$
  - $\phi(90) = (2-1)2^0 \cdot (3-1)3^1 \cdot (5-1)5^0 = 24$
  - 1,7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77,79,83,89

ϕ Is Multiplicative

Lemma: If $\gcd(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$.

ϕ Is Multiplicative

Lemma: If $\gcd(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$.

Proof:

- Consider $b : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ such that $b(x) = (x \bmod m, x \bmod n)$

ϕ Is Multiplicative

Lemma: If $\gcd(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$.

Proof:

- Consider $b : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ such that $b(x) = (x \bmod m, x \bmod n)$
- CRT gives $b^{-1} : \mathbb{Z}_m \times \mathbb{Z}_n \rightarrow \mathbb{Z}_{mn}$

ϕ Is Multiplicative

Lemma: If $\gcd(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$.

Proof:

- Consider $b : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ such that $b(x) = (x \bmod m, x \bmod n)$
- CRT gives $b^{-1} : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$
- Claim: x invertible iff $b(x)$ is

ϕ Is Multiplicative

Lemma: If $\gcd(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$.

Proof:

- Consider $b : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ such that $b(x) = (x \bmod m, x \bmod n)$
- CRT gives $b^{-1} : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$
- Claim: x invertible iff $b(x)$ is
  - $xx^{-1} \equiv 1 \pmod{m}$, $xx^{-1} \equiv 1 \pmod{n}$
  - If $ax \equiv 1 \pmod{m}$ and $ax \equiv 1 \pmod{n}$, $ax \equiv 1 \pmod{mn}$

ϕ Is Multiplicative

Lemma: If $\gcd(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$.

Proof:

- Consider $b : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ such that $b(x) = (x \bmod m, x \bmod n)$
- CRT gives $b^{-1} : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$
- Claim: x invertible iff $b(x)$ is
  - $xx^{-1} \equiv 1 \pmod{m}$, $xx^{-1} \equiv 1 \pmod{n}$
  - If $ax \equiv 1 \pmod{m}$ and $ax \equiv 1 \pmod{n}$, $ax \equiv 1 \pmod{mn}$
- $\phi(m)$ inv. choices for $b(x)_1$, $\phi(n)$ for $b(x)_2$
- Thus, $\phi(m)\phi(n)$ inv. choices for $b(x)$

ϕ For Prime Powers

Lemma: For prime p, $\phi(p^k) = (p-1)p^{k-1}$.

ϕ For Prime Powers

Lemma: For prime p, $\phi(p^k) = (p-1)p^{k-1}$.

Proof:

- x not coprime to p^k iff $p|x$

ϕ For Prime Powers

Lemma: For prime p, $\phi(p^k) = (p-1)p^{k-1}$.

Proof:

- x not coprime to p^k iff $p|x$
- Not coprime: $p, 2p, 3p, ..., p^k = p^{k-1}p$

ϕ For Prime Powers

Lemma: For prime p, $\phi(p^k) = (p-1)p^{k-1}$.

Proof:

- x not coprime to p^k iff $p|x$
- Not coprime: $p, 2p, 3p, ..., p^k = p^{k-1}p$
- Total of p^{k-1} nums not coprime
- So num coprime $= p^k - p^{k-1} = (p-1)p^{k-1}$

Proving ϕ

Theorem: Suppose m factored as $p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$.
Then $\phi(m) = (p_1 - 1)p_1^{n_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{n_k - 1}$.

Proving ϕ

Theorem: Suppose m factored as $p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$.
Then $\phi(m) = (p_1 - 1)p_1^{n_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{n_k - 1}$.

Proof:

- Since ϕ is multiplicative:

$$\begin{aligned}
\phi(m) &= \phi(p_1^{n_1} \cdot \ldots \cdot p_{k-2}^{n_{k-2}} \cdot p_{k-1}^{n_{k-1}} \cdot p_k^{n_k}) \\
&= \phi(p_1^{n_1} \cdot \ldots \cdot p_{k-2}^{n_{k-2}} \cdot p_{k-1}^{n_{k-1}})\phi(p_k^{n_k}) \\
&= \phi(p_1^{n_1} \cdot \ldots \cdot p_{k-2}^{n_{k-2}})\phi(p_{k-1}^{n_{k-1}})\phi(p_k^{n_k}) \\
&\vdots \\
&= \phi(p_1^{n_1})\phi(p_2^{n_2})\ldots\phi(p_k^{n_k})
\end{aligned}$$

Proving ϕ

Theorem: Suppose m factored as $p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$.
Then $\phi(m) = (p_1 - 1)p_1^{n_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{n_k - 1}$.

Proof:

- Since ϕ is multiplicative:

$$\begin{aligned}
\phi(m) &= \phi(p_1^{n_1} \cdot \ldots \cdot p_{k-2}^{n_{k-2}} \cdot p_{k-1}^{n_{k-1}} \cdot p_k^{n_k}) \\
&= \phi(p_1^{n_1} \cdot \ldots \cdot p_{k-2}^{n_{k-2}} \cdot p_{k-1}^{n_{k-1}})\phi(p_k^{n_k}) \\
&= \phi(p_1^{n_1} \cdot \ldots \cdot p_{k-2}^{n_{k-2}})\phi(p_{k-1}^{n_{k-1}})\phi(p_k^{n_k}) \\
&\vdots \\
&= \phi(p_1^{n_1})\phi(p_2^{n_2})\ldots\phi(p_k^{n_k})
\end{aligned}$$

- Apply previous lemma to each prime power!

Fin

Have a great weekend!