37181 DISCRETE MATHEMATICS

Lecture 16: Euler's theorem

PLAN

- Euler’s phi function
- Euler’s theorem
- Fermat’s little theorem

Let $d \in \mathbb{N}_+$.

Let $\mathbb{Z}_d^*$ denote the following *structure*:

- first of all, a set of numbers $\{x \in \mathbb{N}_+ \mid \gcd(x, d) = 1, x < d\}$
- second of all, the operation of *multiplication mod d*

Let $d \in \mathbb{N}_+$.

Let $\mathbb{Z}_d^*$ denote the following *structure*:

- first of all, a set of numbers $\{x \in \mathbb{N}_+ \mid \mathrm{gcd}(x, d) = 1, x < d\}$
- second of all, the operation of *multiplication mod d*

Eg: $\mathbb{Z}_{26}^*$ is the set:

plus multiplication mod 26.

Note that every element in this set has a multiplicative inverse mod 26.

EULER'S PHI FUNCTION

Let $n \in \mathbb{N}_+$. Define

$$\varphi(n) = |\{x \in \mathbb{N} \mid 1 \leqslant x < n, \gcd(x, n) = 1\}$$

to be the number of numbers between $0, n$ which are relatively prime to n.

EULER'S PHI FUNCTION

Let $n \in \mathbb{N}_+$. Define

$$\varphi(n) = |\{x \in \mathbb{N} \mid 1 \leqslant x < n, \gcd(x, n) = 1\}$$

to be the number of numbers between $0, n$ which are relatively prime to n. In other words, $\varphi(n) = |\mathbb{Z}_n^*|$.

Ex: $\varphi(7) =$

Ex: $\varphi(9) =$

Ex: $\varphi(16) =$

EULER'S PHI FUNCTION

Lemma

If p is prime, then $\varphi(p) = p - 1$.

EULER'S PHI FUNCTION

Lemma

If p is prime, then $\varphi(p) = p - 1$.

Lemma

If p is prime, then $\varphi(p^2) = ?$.

Lemma

If p is prime, then $\varphi(p) = p - 1$.

Lemma

If p is prime, then $\varphi(p^2) =?$.

$$\begin{array}{rrcr}
1 & 2 & \dots & p \\
p+1 & p+2 & \dots & 2p \\
2p+1 & 2p+2 & \dots & 3p \\
\vdots & & & (p-1).p \\
(p-1).p+1 & (p1).p+2 & \dots & (p-1).p+p
\end{array}$$

We can play around with φ and make some conjectures.

Lemma

If p is prime and $n \in \mathbb{N}_+$ then $\varphi(p^n) =$

We can play around with φ and make some conjectures.

Lemma

If p is prime and $n \in \mathbb{N}_+$ then $\varphi(p^n) =$

$$\begin{array}{llll}
1 & 2 & \dots & p \\
p+1 & p+2 & \dots & 2p \\
2p+1 & 2p+2 & \dots & 3p \\
 & & \vdots & \\
(p-1)p+1 & (p-1)p+2 & \dots & p^2 \\
 & & & \\
p^2+1 & p^2+2 & \dots & p^2+p \\
p^2+p+1 & p^2+p+2 & \dots & p^2+2p \\
 & & \vdots & \\
p^2+(p-1)p+1 & p^2+(p-1)p+2 & \dots & p^2+p^2 \\
 & & \vdots &
\end{array}$$

Lemma

If p is prime and $n \in \mathbb{N}_+$ then $\varphi(p^n) =$

PHI FUNCTION

Lemma

If p is prime and $n \in \mathbb{N}_+$ then $\varphi(p^n) = p^n - p^{n-1}$

Lemma

If a, b are relatively prime then $\varphi(ab) = \varphi(a)\varphi(b)$

Proof.

Lemma

If a, b are relatively prime then $\varphi(ab) = \varphi(a)\varphi(b)$

Proof.

Define a map $f : \mathbb{Z}_{ab}^* \to \mathbb{Z}_a^* \times \mathbb{Z}_b^*$ by $f([x]_{ab}) = ([x]_a, [x]_b)$.

Lemma

If a, b are relatively prime then $\varphi(ab) = \varphi(a)\varphi(b)$

Proof.

Define a map $f : \mathbb{Z}_{ab}^* \to \mathbb{Z}_a^* \times \mathbb{Z}_b^*$ by $f([x]_{ab}) = ([x]_a, [x]_b)$.

What is the size of each set?

Lemma

If a, b are relatively prime then $\varphi(ab) = \varphi(a)\varphi(b)$

Proof.

Define a map $f : \mathbb{Z}_{ab}^* \to \mathbb{Z}_a^* \times \mathbb{Z}_b^*$ by $f([x]_{ab}) = ([x]_a, [x]_b)$.

What is the size of each set?

One-to-one: if $f([x]_{ab}) = f([y]_{ab})$ then

Lemma

If a, b are relatively prime then $\varphi(ab) = \varphi(a)\varphi(b)$

Proof.

Define a map $f : \mathbb{Z}_{ab}^* \to \mathbb{Z}_a^* \times \mathbb{Z}_b^*$ by $f([x]_{ab}) = ([x]_a, [x]_b)$.

What is the size of each set?

One-to-one: if $f([x]_{ab}) = f([y]_{ab})$ then

Onto: $\square$

Theorem

Let $a, n \in \mathbb{N}_+$ be relatively prime. Then $a^{\varphi(n)} \equiv 1 \bmod n$.

Eg: (from lecture 15) Compute $121^{12} \mod 13$

Theorem

Let $a, n \in \mathbb{N}_+$ be relatively prime. Then $a^{\varphi(n)} \equiv 1 \mod n$.

Eg: (from lecture 15) Compute $121^{12} \mod 13$

Proof.

First, let $\mathbb{Z}_n^* = \{x \mid \gcd(x, n) = 1\}$. What is the size of this set?

Theorem

Let $a, n \in \mathbb{N}_+$ be relatively prime. Then $a^{\varphi(n)} \equiv 1 \bmod n$.

Eg: (from lecture 15) Compute $121^{12} \mod 13$

Proof.

First, let $\mathbb{Z}_n^* = \{x \mid \gcd(x, n) = 1\}$. What is the size of this set? $\varphi(n)$

Theorem

Let $a, n \in \mathbb{N}_+$ be relatively prime. Then $a^{\varphi(n)} \equiv 1 \bmod n$.

Eg: (from lecture 15) Compute $121^{12} \mod 13$

Proof.

First, let $\mathbb{Z}_n^* = \{x \mid \gcd(x, n) = 1\}$. What is the size of this set? $\varphi(n)$

Now consider $\mathbb{Z}_n^*$ as a structure with multiplication mod n.

EG

$\mathbb{Z}_{30}^{*} =$

EG

$\mathbb{Z}_{30}^{*} = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

$7.7 =$

$7.11 =$

$7.19 =$

EG

$\mathbb{Z}_{30}^* = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

$7.7 =$

$7.11 =$

$7.19 =$

Look what happens when you multiply everything by one number:

EG

$\mathbb{Z}_{30}^{*} = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

$7.7 =$

$7.11 =$

$7.19 =$

Look what happens when you multiply everything by one number:

$\{7.1,\ 7.7,\ 7.11,\ 7.13,\ 7.17,\ 7.19,\ 7.23,\ 7.29\} =$

List the elements of $\mathbb{Z}_n^*$: $\quad 0 < a_1 < a_2 < \cdots < a_{\varphi(n)} < n.$

EULER'S THEOREM: PROOF

List the elements of $\mathbb{Z}_n^*$: $\quad 0 < a_1 < a_2 < \cdots < a_{\varphi(n)} < n$.

Claim: multiplying (and reducing mod n) each element by some $a \in \mathbb{Z}_n^*$ simply *permutes* the elements around.

That is, $\{[aa_1]_n, [aa_2]_n, \ldots, [aa_{\varphi(n)}]_n\} \subseteq \mathbb{Z}_n^*$ is exactly the same set.

EULER'S THEOREM: PROOF

List the elements of $\mathbb{Z}_n^*$: $\quad 0 < a_1 < a_2 < \cdots < a_{\varphi(n)} < n.$

Claim: multiplying (and reducing mod n) each element by some $a \in \mathbb{Z}_n^*$ simply *permutes* the elements around.

That is, $\{[aa_1]_n, [aa_2]_n, \ldots, [aa_{\varphi(n)}]_n\} \subseteq \mathbb{Z}_n^*$ is exactly the same set.

Proof.

Suppose $aa_i \equiv aa_j$, then $a(a_i - a_j) \equiv 0$ which means $n \mid a(a_i - a_j)$.

List the elements of $\mathbb{Z}_n^*$: $0 < a_1 < a_2 < \cdots < a_{\varphi(n)} < n$.

Claim: multiplying (and reducing mod n) each element by some $a \in \mathbb{Z}_n^*$ simply *permutes* the elements around.

That is, $\{[aa_1]_n, [aa_2]_n, \ldots, [aa_{\varphi(n)}]_n\} \subseteq \mathbb{Z}_n^*$ is exactly the same set.

Proof.

Suppose $aa_i \equiv aa_j$, then $a(a_i - a_j) \equiv 0$ which means $n \mid a(a_i - a_j)$.

But since a is relatively prime to n, this means n divides $a_i - a_j$, but $-n < a_i - a_j < n$ so $a_i - a_j = 0$ so $a_i = a_j$.

List the elements of $\mathbb{Z}_n^*$: $0 < a_1 < a_2 < \cdots < a_{\varphi(n)} < n$.

Claim: multiplying (and reducing mod n) each element by some $a \in \mathbb{Z}_n^*$ simply *permutes* the elements around.

That is, $\{[aa_1]_n, [aa_2]_n, \ldots, [aa_{\varphi(n)}]_n\} \subseteq \mathbb{Z}_n^*$ is exactly the same set.

Proof.

Suppose $aa_i \equiv aa_j$, then $a(a_i - a_j) \equiv 0$ which means $n \mid a(a_i - a_j)$.

But since a is relatively prime to n, this means n divides $a_i - a_j$, but $-n < a_i - a_j < n$ so $a_i - a_j = 0$ so $a_i = a_j$.

So the map $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ defined by $f(a_i) = aa_i$ is one-to-one. It is onto because:

$\square$

EULER'S THEOREM: PROOF

Now

$$\begin{aligned} a^{\varphi(n)} \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)} &= (aa_1) \cdot (aa_2) \cdot \ldots \cdot (aa_{\varphi(n)}) \\ &\equiv a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)} \mod n \end{aligned}$$

EULER'S THEOREM: PROOF

Now

$$\begin{aligned} a^{\varphi(n)} \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)} &= (aa_1) \cdot (aa_2) \cdot \ldots \cdot (aa_{\varphi(n)}) \\ &\equiv a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)} \mod n \end{aligned}$$

So multiply both sides by the inverses of a_i in $\mathbb{Z}_n^*$ and you get

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

Now

$$\begin{aligned} a^{\varphi(n)} \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)} &= (aa_1) \cdot (aa_2) \cdot \ldots \cdot (aa_{\varphi(n)}) \\ &\equiv a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)} \mod n \end{aligned}$$

So multiply both sides by the inverses of a_i in $\mathbb{Z}_n^*$ and you get

$$a^{\varphi(n)} \equiv 1 \mod n \qquad \square$$

Using $a^{\varphi(n)} \equiv 1 \mod n$ we can find inverses quickly:

Quiz: find inverse of 11 mod 26

EULER'S THEOREM

Using $a^{\varphi(n)} \equiv 1 \mod n$ we can find inverses quickly:

Quiz: find inverse of 11 mod 26

$\varphi(26) = \varphi(2)\varphi(13) = 12$, so $11^{12} \equiv 1$ mod 26, so $11.(11^{11}) \equiv 1$ so 11^{11} is the inverse.

Using $a^{\varphi(n)} \equiv 1 \mod n$ we can find inverses quickly:

Quiz: find inverse of 11 mod 26

$\varphi(26) = \varphi(2)\varphi(13) = 12$, so $11^{12} \equiv 1$ mod 26, so $11.(11^{11}) \equiv 1$ so 11^{11} is the inverse.

Repeated squaring to finish. Hmm is that really quicker?

The old version of this course only looked at “Fermat’s little theorem” which is:

If p is prime and p does not divide $a \in \mathbb{N}_+$ then

$$a^{p-1} \equiv 1 \mod p$$

Prove it.

(Note: for RSA we need Euler’s theorem, not this one)

HOW HARD IS IT TO COMPUTE PHI?

Lemma

Let p, q be two (secret, large) distinct primes. Let $n = pq$. Suppose everybody knows n. Then:

You know $\varphi(n)$ if and only if you know p, q.

Proof.

HOW HARD IS IT TO COMPUTE PHI?

Lemma

Let p, q be two (secret, large) distinct primes. Let $n = pq$. Suppose everybody knows n. Then:

You know $\varphi(n)$ if and only if you know p, q.

Proof.

Consider the quadratic equation

$$X^2 + (\varphi(n) - n - 1)X + n = 0.$$

Find the roots.

$\square$

NEXT

Next lecture:

- RSA