37181 DISCRETE MATHEMATICS

Lecture 16: Euler's theorem

PLAN

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

relatively prime to d.

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

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

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

SOME NOTATION

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

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

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

Eg: $\mathbb{Z}_{26}^*$ is the set: $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$.

plus multiplication mod 26. Eg $7 \cdot 7 = 49 \equiv 23$

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

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.

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: $\varphi(7) =$ $7-1 = 6$

prime

Ex: $\varphi(9) =$ 6 $\qquad \mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

Ex: $\varphi(\underset{2^4}{16}) =$ $8.$ $\qquad 1, 3, 5, \ldots 15$

$\{1, 2, \ldots p-1\}$.

Lemma

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

EULER'S PHI FUNCTION

$\varphi(9) = 9 - 3 = 6$

$p^2 \longrightarrow p$

Lemma

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

$\gcd > 1$

Lemma

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

$\gcd = 1$

$1 \quad 2 \quad 3 \quad \ldots$

$p+1 \quad p+2 \quad p+3 \quad \ldots$

$2p+1 \quad 2p+2 \quad 2p+3 \quad \ldots$

$(p-1)p+1 \quad (p-1)p+2 \quad \ldots$

$1 \cdot p$

$p + p = 2p$

$3p$

$4p$

$\vdots$

$p^2 = (p-1)p + p$

Guess
$\varphi(p^n) = p^n - p^{n-1}$

Lemma

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

Lemma

If p is prime, then $\varphi(p^2) = \cancel{?}\ p^2 - p$

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

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 $\varphi(p^n) =$

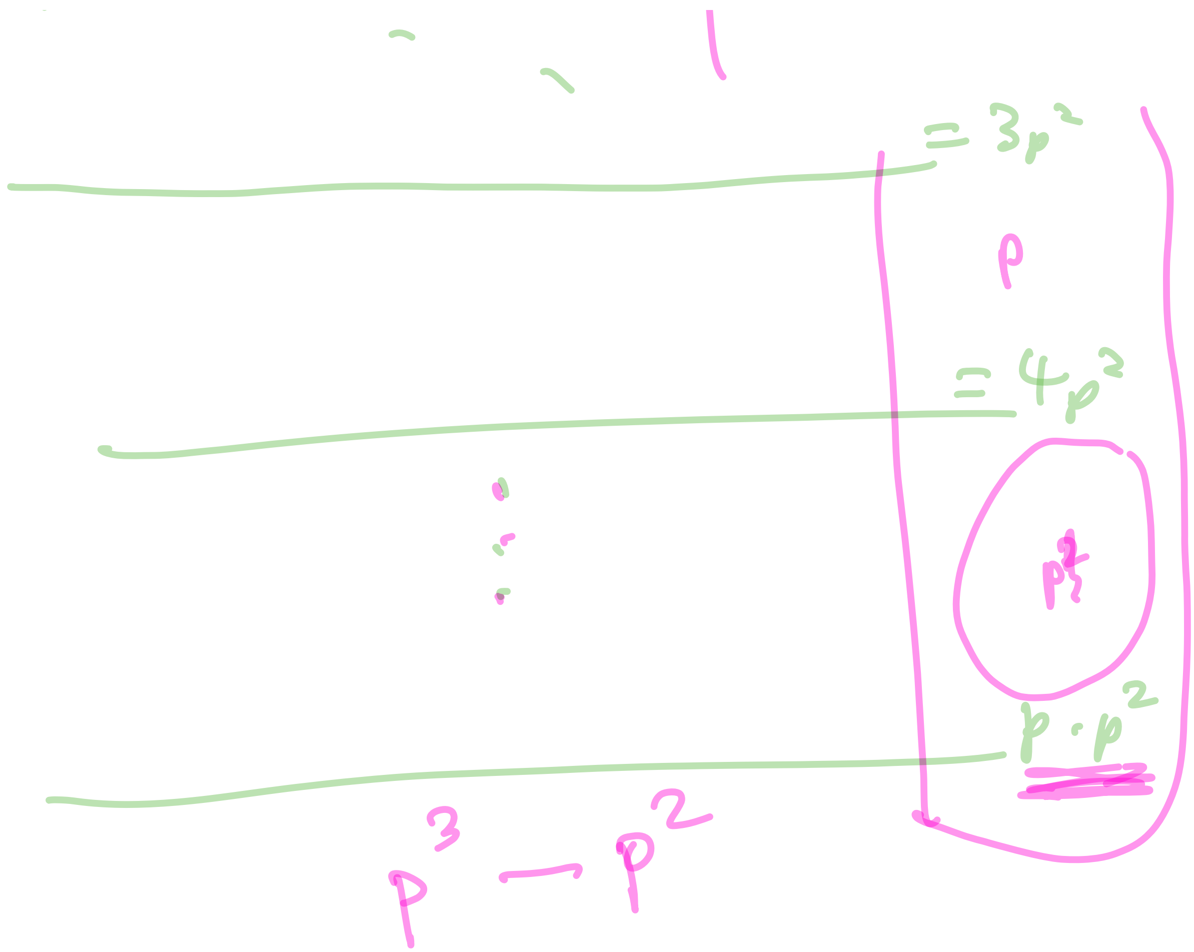
gcd $(p^n, -) > 1$

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

$= 1p^2$

$= 2p^2$

$2p^2+1$



Claim for $n \in \mathbb{N}$: $\varphi(p^n) = p^n - p^{n-1}$

Lemma

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

Lemma

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

$\varphi(9) = 6$

$\neq \varphi(3)\varphi(3)$

$= 2 \cdot 2$

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 $f([x]_{ab}) = ([x]_a, [x]_b)$.

size?

$\varphi(ab)$

E.g: $f : \mathbb{Z}_{30}^* \to \mathbb{Z}_5^* \times \mathbb{Z}_6^*$

$f(11) \to (1, 5)$

$f(29) \to (4, 5)$

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 $f([x]_{ab}) = ([x]_a, [x]_b)$.

(,)

$\mathbb{Z}_a^*$ $\mathbb{Z}_b^*$

$\varphi(a)$ $\varphi(b)$

What is the size of each set?

$\varphi(ab)$ $\varphi(a) \cdot \varphi(b)$

One-to-one: Exercise

Onto: Exercise

Note: $\mathbb{Z}_{20}^* \to \mathbb{Z}_5^* \times \mathbb{Z}_6^*$

if I tell you (3, !)

13

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? $\varphi(ab)$ $\neq$ $\varphi(a) \cdot \varphi(b)$.

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

$[x]_b = [y]_b$

Onto: $\therefore$ bijection

$\square$

Theorem

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

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

$\gcd(121, 13) = 1$

$\varphi(13) = 12$

$\therefore$ By Euler's theorem

$121^{12} \equiv 1 \mod 13.$

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? $\varphi(n)$

$1 \leq x < n$

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? $\varphi(n)$

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

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

$\varphi(30) = 8$

$\varphi(5)\varphi(6)$

$\varphi(5)\varphi(3)\varphi(2)$

$4 \cdot 2 \cdot 1$

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

$7.7 = 49 \equiv 19$

$7.11 = 77 \equiv 17$

$7.19 = 13$

$7 \cdot 13 \equiv 1$

$$\begin{array}{r} 13 \\ 7 \\ \hline 91 \end{array}$$

19

133

mult every number in $\mathbb{Z}_{30}^{*}$ by 7

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:

$\{7.1,\ 7.7,\ 7.11,\ \underline{7.13},\ 7.17,\ 7.19,\ 7.23,\ 7.29\} = \{7, 19, 17, 1, \ldots\}$

Claim ↗ same set (re-ordered)

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

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.

= ?

subset.

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 ~~$a \in \mathbb{Z}_n^*$~~ simply *permutes* the elements around.

$\gcd(a, n) = 1$

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

Proof. (contrad) a, a_i a_j rel. prime to n.

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

Homework exercise: a rel prime to n, and $n \mid ab \Rightarrow n \mid b$

$\therefore n \mid (a_i - a_j)$

But $-n < a_i - a_j < n$

$-n \quad 0 \quad n$

$a_i - a_j = 0$

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 $n \mid a(a_i - a_j)$.

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 $a_i = a_j$.

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 $n \mid a(a_i - a_j)$.

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:

$\square$

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

distinct $\varphi(n)$ numbers.

Now

$$\underbrace{a^{\varphi(n)}}_{a\,a\,a \cdots a} \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)} = (aa_1) \cdot (aa_2) \cdot \ldots \cdot (aa_{\varphi(n)})$$
$$\equiv a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)} \quad \text{mod } n$$

$$a\,a\,a \cdots a = \underbrace{a\,a\,a \cdots a}_{\varphi(n)}$$

$$a^{\varphi(n)}\, a_1 \cdots a_{\varphi(n)} - 1 \cdot a_1\, a_2 \cdots a_{\varphi(n)} \equiv 0 \mod n$$

$$\left(a^{\varphi(n)} - 1\right) a_1 \cdots a_{\varphi(n)}$$

So $n \mid a_1\, a_2 \cdots a_{\varphi(n)} \left(a^{\varphi(n)} - 1\right)$

rel prime to n.

So by Homework exercise

$$n \mid a^{\varphi(n)} - 1 \quad \therefore a^{\varphi(n)} - 1 \equiv 0 \mod n$$

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

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

$\varphi(26) = \varphi(2)\varphi(13)$

$= 1 \cdot 12$

$11^{12} \equiv 1 \mod 26.$

$= 11 \cdot 11^{11}$

$[11^{11}]_{26}$ is 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 $11^{12} \equiv 1 \bmod 26$, 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

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

$\varphi(p) = p-1$

Prove it. Just use Euler's theorem.

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

HOW HARD IS IT TO COMPUTE PHI?

~~1002111547~~

Lemma

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

$\varphi(n) = (p-1)(q-1)$

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

Proof.

Lemma

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

easy

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.

$$X = \frac{-(\varphi(n) - n - 1) \pm \sqrt{(\varphi(n) - n - 1)^2 - 4n}}{2}$$

$\square$

$$= -\frac{\left((p-1)(q-1) - pq - 1\right) \pm 1}{2} \quad \cdot \; -p \cdot q -$$

$pq - p - q + 1$

$p + q$

Claim $= \begin{cases} p \\ q \end{cases}$

Next lecture:

- RSA cryptosystem.