Mathematics for Computer Science
MIT 6.042J/18.062J

Euler's Function

Euler ϕ function

$\phi(n) ::= \#\ k \in [0,n)$
s.t. k rel. prime to n

Euler ϕ function

$\phi(n) ::= \#\ k \in [0,n)$
s.t. $\gcd(k,n) = 1$

Euler ϕ function

$gcd1\{n\} ::=$
$\{k \in [0,n) \mid \gcd(k,n)=1\}$

so $\phi(n) = |gcd1\{n\}|$

(some books write
n^* for $gcd1\{n\}$)

Euler ϕ function

$gcd1\{n\} ::=$

$\{k \in [0,n) \mid gcd(k,n)=1\}$

$gcd1\{7\} = \{1,2,3,4,5,6\}$

$gcd1\{12\} =$

$\{0,1,2,3,4,5,6,7,8,9,10,11\}$

Euler ϕ function

$gcd1\{n\} ::=$

$\{k \in [0,n) \mid gcd(k,n)=1\}$

$\phi(7) = |\{1,2,3,4,5,6\}|$

$gcd1\{12\} =$

$\{0,1,2,3,4,5,6,7,8,9,10,11\}$

Euler ϕ function

$gcd1\{n\} ::=$

$\{k \in [0,n) \mid gcd(k,n)=1\}$

$\phi(7) = 6$

$gcd1\{12\} =$

$\{0,1,2,3,4,5,6,7,8,9,10,11\}$

Euler ϕ function

$gcd1\{n\} ::=$

$\{k \in [0,n) \mid gcd(k,n)=1\}$

$\phi(7) = 6$

$\phi(12) =$

$|\{1, 5, 7, 11\}|$

Euler ϕ function

$gcd1\{n\} ::=$

$\{k \in [0,n) \mid gcd(k,n)=1\}$

$\phi(7) = 6$

$\phi(12) = 4$

Calculating ϕ

If p prime, everything in [1,p) is rel. prime to p, so

$$\phi(p) = p - 1$$

Calculating ϕ

$\phi(9)$? 0,1,2,3,4,5,6,7,8

k rel. prime to 9 iff
k rel. prime to 3
3 divides every 3rd number

so, $\phi(9) = 9-(9/3) = 6$

Calculating $\phi(p^k)$

0,1,…,p,…,2p,…..,p^k-p,…,p^k-1

p divides every pth number

p^k/p of these numbers are not rel. prime to p^k

Calculating $\phi(p^k)$

so

$$\phi(p^k) = p^k - p^k/p$$

Calculating $\phi(p^k)$

so

$$\phi(p^k) = p^k - p^{k-1}$$

Calculating $\phi(a \cdot b)$

Lemma:

For a, b relatively prime,

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

pf: Pset 5. Another way later by "counting."

Calculating $\phi(a \cdot b)$

$$\begin{aligned}\phi(12) &= \phi(3 \cdot 4)\\ &= \phi(3) \cdot \phi(4)\\ &= (3 - 1) \cdot (2^2 - 2^{2-1})\\ &= 2 \cdot (4 - 2) = 4\end{aligned}$$

Euler's Theorem

For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

6.042J / 18.062J Mathematics for Computer Science
Spring 2015