

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Mathematics for Computer Science
MIT 6.042J/18.062J

Euler's Function



Albert R Meyer March 11, 2015

phi.1

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Euler ϕ function

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



Albert R Meyer March 11, 2015

phi.2

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Euler ϕ function

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



Albert R Meyer March 11, 2015

phi.3

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Euler ϕ function

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

so $\phi(n) = |\gcd1\{n\}|$
(some books write
 n^* for $\gcd1\{n\}$)



Albert R Meyer March 11, 2015

phi.4

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Euler ϕ function

$\text{gcd1}\{n\} ::=$

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

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

$\text{gcd1}\{12\} =$

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



Albert R Meyer March 11, 2015

phi.5

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Euler ϕ function

$\text{gcd1}\{n\} ::=$

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

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

$\text{gcd1}\{12\} =$

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



Albert R Meyer March 11, 2015

phi.6

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Euler ϕ function

$\text{gcd1}\{n\} ::=$

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

$\phi(7) = 6$

$\text{gcd1}\{12\} =$

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



Albert R Meyer March 11, 2015

phi.7

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Euler ϕ function

$\text{gcd1}\{n\} ::=$

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

$\phi(7) = 6$

$\phi(12) =$

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



Albert R Meyer March 11, 2015

phi.8

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Euler ϕ function

$\gcd1\{n\} ::=$

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

$$\phi(7) = 6$$

$$\phi(12) = 4$$



Albert R Meyer March 11, 2015

phi.9

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Calculating ϕ

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

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



Albert R Meyer March 11, 2015

phi.10

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

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

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



Albert R Meyer March 11, 2015

phi.11

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Calculating $\phi(p^k)$

0, 1, ..., p , ..., $2p$, ..., $p^k - p$, ..., $p^k - 1$

p divides every p th number

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



Albert R Meyer March 11, 2015

phi.12

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Calculating $\phi(p^k)$

So

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



Albert R Meyer March 11, 2015

phi.13

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Calculating $\phi(p^k)$

So

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



Albert R Meyer March 11, 2015

phi.14

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Calculating $\phi(a \cdot b)$

Lemma:

For a, b relatively prime,
 $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

pf: Given as problem.
 Also later by "counting."



Albert R Meyer March 11, 2015

phi.15

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Calculating $\phi(a \cdot b)$

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

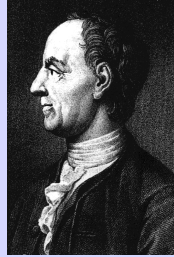


Albert R Meyer March 11, 2015

phi.16

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Euler's Theorem



For k relatively
prime to n ,

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



Albert R Meyer

March 11, 2015

phi.17