

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 Theorem: Proof



Albert R Meyer October 13, 2015

Euler1

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

\mathbb{Z}_n^* ::= elements of \mathbb{Z}_n
relatively prime to n

$$\phi(n) ::= |\mathbb{Z}_n^*|$$



Albert R Meyer October 13, 2015

Euler2

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

Euler's Theorem

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

for $k \in \mathbb{Z}_n^*$



Albert R Meyer October 13, 2015

Euler3

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

\mathbb{Z}_n^* closed under \cdot

For $i, j \in \mathbb{Z}_n$

$i, j \in \mathbb{Z}_n^*$ IFF $i \cdot j \in \mathbb{Z}_n^*$
(both sides cancel)



Albert R Meyer October 13, 2015

Euler4

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

\mathbb{Z}_n^* closed under \cdot

For $i, j \in \mathbb{Z}_n$

$i, j \in \mathbb{Z}_n^*$ IFF $i \cdot j \in \mathbb{Z}_n^*$
 (...both have inverses)



Albert R Meyer October 13, 2015

Euler5

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

\mathbb{Z}_n^* closed under \cdot

For $i, j \in \mathbb{Z}_n$

$i, j \in \mathbb{Z}_n^*$ IFF $i \cdot j \in \mathbb{Z}_n^*$
 (...same prime factors)



Albert R Meyer October 13, 2015

Euler6

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

proof of Euler

if $\mathbb{Z}_n^* = \{k_1, k_2, \dots, k_{\phi(n)}\}$

then

$\mathbb{Z}_n^* = \{kk_1, kk_2, \dots, kk_{\phi(n)}\}$

for $k \in \mathbb{Z}_n^*$



Albert R Meyer October 13, 2015

Euler7

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

proof of Euler

if $\mathbb{Z}_n^* = \{k_1, k_2, \dots, k_{\phi(n)}\}$
 $= \{ \underbrace{kk_1, kk_2, \dots, kk_{\phi(n)}} \}$

different because
 k cancels



Albert R Meyer October 13, 2015

Euler10

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

proof of Euler

$$\text{if } \mathbb{Z}_n^* = \{k_1, k_2, \dots, k_{\phi(n)}\}$$

$$= \{kk_1, kk_2, \dots, kk_{\phi(n)}\}$$

and $(k k_i)$ in \mathbb{Z}_n^*



Albert R Meyer October 13, 2015

Euler11

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

permuting \mathbb{Z}_9

$$\phi(9) = 3^2 - 3 = 6$$

$$\mathbb{Z}_9^* = \boxed{1} \boxed{2} \boxed{4} \boxed{5} \boxed{7} \boxed{8}$$



Albert R Meyer October 13, 2015

Euler14

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

permuting \mathbb{Z}_9

$$\mathbb{Z}_9^* = \boxed{1} \boxed{2} \boxed{4} \boxed{5} \boxed{7} \boxed{8}$$

$$2 \cdot \boxed{2} \boxed{4} \boxed{8} \boxed{1} \boxed{5} \boxed{7}$$



Albert R Meyer October 13, 2015

Euler15

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

permuting \mathbb{Z}_9

$$\mathbb{Z}_9^* = \boxed{1} \boxed{2} \boxed{4} \boxed{5} \boxed{7} \boxed{8}$$

$$2 \cdot \boxed{2} \boxed{4} \boxed{8} \boxed{1} \boxed{5} \boxed{7}$$

$$7 \cdot \boxed{7} \boxed{5} \boxed{1} \boxed{8} \boxed{4} \boxed{2}$$



Albert R Meyer October 13, 2015

Euler16

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

proof of Euler

$$\begin{aligned}
 & \cancel{k_1 k_2 \cdots k_{\phi(n)}} \\
 &= (k_1 k_2) \cdots (k_{\phi(n)}) \\
 &= k_1^{\phi(n)} \cdot \cancel{(k_1 k_2 \cdots k_{\phi(n)})}
 \end{aligned}$$



Albert R Meyer October 13, 2015

Euler17

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

proof of Euler

$$\begin{aligned}
 & 1 \\
 &= k^{\phi(n)}
 \end{aligned}$$

QED



Albert R Meyer October 13, 2015

Euler19