Mathematics for Computer Science
MIT 6.042J/18.062J

Euler's Theorem: Proof

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

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

Euler's Theorem

$$k^{\phi(n)} = 1 \ (\mathbb{Z}_n)$$

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

$\mathbb{Z}_n^*$ closed under $\bullet$

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

$i, j \in \mathbb{Z}_n^*$ IFF $i \bullet j \in \mathbb{Z}_n^*$

(both sides cancel)

$\mathbb{Z}_n^*$ closed under $\bullet$

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

$i, j \in \mathbb{Z}_n^*$ IFF $i \bullet j \in \mathbb{Z}_n^*$

(…both have inverses)

$\mathbb{Z}_n^*$ closed under $\bullet$

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

$i, j \in \mathbb{Z}_n^*$ IFF $i \bullet j \in \mathbb{Z}_n^*$

(…same prime factors)

proof of Euler

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

then

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

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

proof of Euler

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

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

different because

k cancels

proof of Euler

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

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

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

permuting $\mathbb{Z}_9$

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

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

permuting $\mathbb{Z}_9$

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

permuting $\mathbb{Z}_9$

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

proof of Euler

$$k_1 k_2 \cdots k_{\phi(n)}$$
$$= (kk_1)(kk_2)\cdots(kk_{\phi(n)})$$
$$= k^{\phi(n)} \cdot (k_1 k_2 \cdots k_{\phi(n)})$$

proof of Euler

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

QED