Euler's Theorem

UNIVERSITY OF TORONTO

March 2$^{\text{nd}}$, 2021

Euler's totient function – 1

Definition: Euler's totient function

We define *Euler's totient function* as $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ defined by

$$\varphi(n) := \#\left\{k \in \mathbb{N} \ : \ 1 \leq k \leq n \text{ and } \gcd(k,n) = 1\right\}$$

Euler's totient function – 2

Proposition

$\forall n_1, n_2 \in \mathbb{N} \setminus \{0\},\ \gcd(n_1, n_2) = 1 \implies \varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$

Euler's totient function – 2

Proposition

$\forall n_1, n_2 \in \mathbb{N} \setminus \{0\}, \gcd(n_1, n_2) = 1 \implies \varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$

Proof. If $n_1 = 1$ or $n_2 = 1$ then there is nothing to prove. So let's assume that $n_1, n_2 \geq 2$.
Set $S_i = \left\{r \in \mathbb{N} \;:\; 1 \leq r \leq n_i \text{ and } \gcd(r, n_i) = 1\right\}$ and $T = \left\{k \in \mathbb{N} \;:\; 1 \leq k \leq n_1 n_2 \text{ and } \gcd(k, n_1 n_2) = 1\right\}$.
For $k \in T$, write the Euclidean divisions $k = n_1 q_1 + r_1$ with $0 \leq r_1 < n_1$ and $k = n_2 q_2 + r_2$ where $0 \leq r_2 < n_2$.
Let's prove that $r_i \in S_i$:

- Assume that $r_i = 0$ then $n_i | k$ and $n_i | n_1 n_2$ so that $n_i | \gcd(k, n_1 n_2) = 1$: contradiction. So $1 \leq r_i < n_i$.
- $\gcd(r_i, n_i) = \gcd(k - n_i q_i, n_i) = \gcd(k, n_i) | \gcd(k, n_1 n_2) = 1$, hence $\gcd(r_i, n_i) = 1$.

Therefore we can define $f : T \to S_1 \times S_2$ by $f(k) = (r_1, r_2)$. Let's prove that f is a bijection.
Let $(r_1, r_2) \in S_1 \times S_2$.
By the Chinese remainder theorem, $\exists! k \in \{1, 2, \dots, n_1 n_2\}$ such that $k \equiv r_1 \pmod{n_1}$ and $k \equiv r_2 \pmod{n_2}$.
Note that $\gcd(k, n_1) = \gcd(r_1 + l n_1, n_1) = \gcd(r_1, n_1) = 1$ (for some $l \in \mathbb{Z}$).
Similarly $\gcd(k, n_2) = \gcd(r_2, n_2) = 1$.
Thus $\gcd(k, n_1 n_2) = 1$ (see Ex 3 of PS2), so that $k \in T$.
We proved that $\forall (r_1, r_2) \in S_1 \times S_2, \exists! k \in T, (r_1, r_2) = f(k)$, i.e. that f is bijective.
Therefore, $\#T = \#(S_1 \times S_2) = \#S_1 \#S_2$, i.e. $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$. ∎

Euler's totient function – 3

Proposition

Let $p_1, \dots, p_r$ be pairwise distinct prime numbers and $\alpha_1, \dots, \alpha_r \in \mathbb{N} \setminus \{0\}$, then

$$\varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

Euler's totient function – 3

Proposition

Let $p_1, \dots, p_r$ be pairwise distinct prime numbers and $\alpha_1, \dots, \alpha_r \in \mathbb{N} \setminus \{0\}$, then

$$\varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

Proof.

- *First case:* let p be a prime number and $\alpha \in \mathbb{N} \setminus \{0\}$.
  Then $\gcd(p^\alpha, m) > 1$ if and only if $p|m$.
  Hence $\varphi(p^\alpha) = \#\left(\{1, 2, \dots, p^\alpha\} \setminus \left\{1 \times p, 2 \times p, \dots, p^{\alpha-1} \times p\right\}\right) = p^\alpha - p^{\alpha-1}$.
- *General case:* using the previous proposition and the first case, we get that

$$\varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \varphi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

∎

Euler's totient function – 3

Proposition

Let $p_1, \dots, p_r$ be pairwise distinct prime numbers and $\alpha_1, \dots, \alpha_r \in \mathbb{N} \setminus \{0\}$, then

$$\varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

Proof.

- *First case:* let p be a prime number and $\alpha \in \mathbb{N} \setminus \{0\}$.
  Then $\gcd(p^\alpha, m) > 1$ if and only if $p|m$.
  Hence $\varphi(p^\alpha) = \#\left(\{1, 2, \dots, p^\alpha\} \setminus \left\{1 \times p, 2 \times p, \dots, p^{\alpha-1} \times p\right\}\right) = p^\alpha - p^{\alpha-1}$.
- *General case:* using the previous proposition and the first case, we get that

$$\varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \varphi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

∎

It $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ then $\varphi(n) = n \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$.

Euler's theorem

Euler's theorem

Let $n \in \mathbb{N} \setminus \{0\}$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then

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

Euler's theorem

Let $n \in \mathbb{N} \setminus \{0\}$ and $a \in \mathbb{Z}$ such that $\gcd(a,n) = 1$. Then

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

Proof. Write $S = \left\{k \in \mathbb{N} \ : \ 1 \leq k \leq n \text{ and } \gcd(k,n) = 1\right\} = \left\{k_1, k_2, \dots, k_{\varphi(n)}\right\}$.

(i) **Fact.** Given $k_i \in S$, there exists $k_j \in S$ such that $ak_i \equiv k_j \pmod{n}$.
Let $k_i \in S$ then $\gcd(ak_i, n) = 1$ by Exercise 3 of Problem Set 2. Thus $ak_i \equiv k_j \pmod{n}$ for some $k_j \in S$.

(ii) **Fact.** $\forall k_i, k_j \in S$, $ak_i \equiv ak_j \pmod{n} \implies k_i = k_j$.
Indeed, then $n | a(k_i - k_j)$ and hence $n | k_i - k_j$ by Gauss' lemma. Thus $k_i \equiv k_j \pmod{n}$.
Finally, $k_i = k_j$ since $1 \leq k_i, k_j \leq n$.

For $i \in \{1, 2, \dots, \varphi(n)\}$, there exists a unique $l_i \in \{0, 1, \dots, n-1\}$ such that $l_i \equiv ak_i \pmod{n}$. Then, $\{l_1, l_2, \dots, l_{\varphi(n)}\} = \{k_1, k_2, \dots, k_{\varphi(n)}\}$.
Indeed, by (i), $\{l_1, l_2, \dots, l_{\varphi(n)}\} \subset \{k_1, k_2, \dots, k_{\varphi(n)}\}$. And by (ii), $\#\{l_1, l_2, \dots, l_{\varphi(n)}\} = \#\{k_1, k_2, \dots, k_{\varphi(n)}\}$.

Hence $\displaystyle\prod_{i=1}^{\varphi(n)} k_i = \prod_{i=1}^{\varphi(n)} l_i \equiv \prod_{i=1}^{\varphi(n)} ak_i \pmod{n} \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} k_i \pmod{n}$. Therefore $\displaystyle n | (a^{\varphi(n)} - 1) \prod_{i=1}^{\varphi(n)} k_i$.

Since $\displaystyle\gcd\left(n, \prod_{i=1}^{\varphi(n)} k_i\right) = 1$ by Ex 3 of PS2, Gauss' lemma gives $n | a^{\varphi(n)} - 1$, i.e. $a^{\varphi(n)} \equiv 1 \pmod{n}$. ∎

Euler's theorem

Euler's theorem

Let $n \in \mathbb{N} \setminus \{0\}$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then

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

Proof. Write $S = \left\{k \in \mathbb{N} \ : \ 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\right\} = \left\{k_1, k_2, \dots, k_{\varphi(n)}\right\}$.

(i) **Fact.** Given $k_i \in S$, there exists $k_j \in S$ such that $ak_i \equiv k_j \pmod{n}$.
Let $k_i \in S$ then $\gcd(ak_i, n) = 1$ by Exercise 3 of Problem Set 2. Thus $ak_i \equiv k_j \pmod{n}$ for some $k_j \in S$.

(ii) **Fact.** $\forall k_i, k_j \in S$, $ak_i \equiv ak_j \pmod{n} \implies k_i = k_j$.
Indeed, then $n | a(k_i - k_j)$ and hence $n | k_i - k_j$ by Gauss' lemma. Thus $k_i \equiv k_j \pmod{n}$.
Finally, $k_i = k_j$ since $1 \leq k_i, k_j \leq n$.

For $i \in \{1, 2, \dots, \varphi(n)\}$, there exists a unique $l_i \in \{0, 1, \dots, n-1\}$ such that $l_i \equiv ak_i \pmod{n}$. Then, $\{l_1, l_2, \dots, l_{\varphi(n)}\} = \{k_1, k_2, \dots, k_{\varphi(n)}\}$.
Indeed, by (i), $\{l_1, l_2, \dots, l_{\varphi(n)}\} \subset \{k_1, k_2, \dots, k_{\varphi(n)}\}$. And by (ii), $\#\{l_1, l_2, \dots, l_{\varphi(n)}\} = \#\{k_1, k_2, \dots, k_{\varphi(n)}\}$.

Hence $\prod_{i=1}^{\varphi(n)} k_i = \prod_{i=1}^{\varphi(n)} l_i \equiv \prod_{i=1}^{\varphi(n)} ak_i \pmod{n} \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} k_i \pmod{n}$. Therefore $n | (a^{\varphi(n)} - 1) \prod_{i=1}^{\varphi(n)} k_i$.

Since $\gcd\left(n, \prod_{i=1}^{\varphi(n)} k_i\right) = 1$ by Ex 3 of PS2, Gauss' lemma gives $n | a^{\varphi(n)} - 1$, i.e. $a^{\varphi(n)} \equiv 1 \pmod{n}$. ∎

Remark

Fermat's little theorem is a special case of Euler's theorem: if p is prime then $\varphi(p) = p - 1$.