Euler's Theorem

Ryan C. Daileda

Trinity University

Number Theory

Recall

Theorem 1

Let G be a finite abelian group. For any $a \in G$, $a^{|G|} = e$.

Taking $G = (\mathbb{Z}/p\mathbb{Z})^\times$ for a prime p, we deduced Fermat's Little Theorem as a corollary.

The analogue of Fermat's Little Theorem for an arbitrary modulus $n \in \mathbb{N}$ is known as *Euler's Theorem*.

To state it, we first need a definition.

Definition

For $n \in \mathbb{N}$, *Euler's totient function* is defined by

$$\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \left|\{a + n\mathbb{Z} \,|\, (a, n) = 1\}\right|$$
$$= \left|\{1 \le a < n \,|\, (a, n) = 1\}\right|.$$

Examples

- For any prime p, $\varphi(p) = p - 1$.
- Since every integer is coprime to 1, we have $\varphi(1) = 1$.
- Direct computation gives:

$$\varphi(4) = 2, \;\; \varphi(6) = 2, \;\; \varphi(8) = 4, \;\; \varphi(9) = 6,$$
$$\varphi(10) = 4, \;\; \varphi(12) = 4, \;\; \varphi(14) = 6, \;\; \varphi(15) = 8.$$

- Because $(a, 2^n) = 1$ if and only if a is odd,

$$\varphi(2^n) = 2^n/2 = 2^{n-1}.$$

Euler's Theorem

We can now state and prove our main result.

Theorem 2

For any $n \in \mathbb{N}$, if $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. If $(a, n) = 1$, then $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Since $(\mathbb{Z}/n\mathbb{Z})^\times$ has order $\varphi(n)$ (by definition),

$$1 + n\mathbb{Z} = (a + n\mathbb{Z})^{\varphi(n)} = a^{\varphi(n)} + n\mathbb{Z},$$

according to Theorem 1.

But this is equivalent to $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

It follows, for instance, that if a is odd and not divisible by 7, then

$$a^6 \equiv 1 \pmod{14}.$$

And if $(a, 15) = 1$, then

$$a^8 \equiv 1 \pmod{15}.$$

And if $n \in \mathbb{N}$ and a is odd, then

$$a^{2^{n-1}} \equiv 1 \pmod{2^n}.$$

Remark. One can use induction to establish the stronger conclusion that, in fact,

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

for all $n \geq 3$, which has interesting consequences...

Properties

The function $\varphi(n)$ has a number of important properties.

Theorem 3

Let $p \in \mathbb{N}$ be prime. For any $n \in \mathbb{N}$, $\varphi(p^n) = p^n - p^{n-1}$.

Proof. A natural number $a < p^n$ is coprime to p^n iff $p \nmid a$.

Equivalently, $a < p^n$ is *not* coprime to p^n iff $a = pk$ for some k.

Since $kp < p^n$ iff $k < p^{n-1}$, there are exactly $p^{n-1} - 1$ choices for k, and hence for a.

So the number of $1 \leq a < p^n$ coprime to p^n is given by

$$(p^n - 1) - (p^{n-1} - 1) = p^n - p^{n-1}.$$

□

Isomorphisms

The totient function enjoys a useful property known as *multiplicativity*.

To understand the multiplicative nature of φ we need to take a slight detour.

Definition

Let R_1 and R_2 be rings. A *(ring) isomorphism* between R_1 and R_2 is a bijective function $f : R_1 \to R_2$ which satisfies:

1. $f(a+b) = f(a) + f(b)$;
2. $f(ab) = f(a)f(b)$,

for all $a, b \in R_1$.

Remarks

One can show that if $f : R_1 \to R_2$ is an isomorphism of rings, then $f(0_{R_1}) = 0_{R_2}$ and $f(1_{R_1}) = 1_{R_2}$.

The inverse of a ring isomorphism $f : R_1 \to R_2$ is a also an isomorphism (in the reverse direction).

If there is an isomorphism $f : R_1 \to R_2$, we say that R_1 and R_2 are *isomorphic*.

Isomorphic rings are "the same." Any ring-theoretic property satisfied by R_1 is automatically satisfied by R_2.

Products of Rings

We require one more purely ring-theoretic construction.

Definition

Let R_1 and R_2 be rings. Their *direct product* is the set $R_1 \times R_2$ endowed with the coordinate-wise operations

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2),$$

for all $a_1, a_2 \in R_1$ and $b_1, b_2 \in R_2$.

Theorem 4

If R_1 and R_2 are rings, then the direct product $R_1 \times R_2$ is also a ring.

Proof. Exercise. □

We have already encountered ring isomorphisms and product rings.

Suppose $m, n \in \mathbb{N}$ are relatively prime. The CRT asserts that that map

$$\begin{aligned} R : \mathbb{Z}/mn\mathbb{Z} &\to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}), \\ a + mn\mathbb{Z} &\mapsto (a + m\mathbb{Z}, a + n\mathbb{Z}), \end{aligned}$$

is a well-defined bijection.

The map R is also a ring isomorphism. For instance, if $a, b \in \mathbb{Z}$, then

$$\begin{aligned} R((a+mn\mathbb{Z})+(b+mn\mathbb{Z})) &= R((a+b)+mn\mathbb{Z}) \\ &= ((a+b)+m\mathbb{Z},(a+b)+n\mathbb{Z}) \\ &= ((a+m\mathbb{Z})+(b+m\mathbb{Z}),(a+n\mathbb{Z})+(b+n\mathbb{Z})) \\ &= (a+m\mathbb{Z},a+n\mathbb{Z})+(b+m\mathbb{Z},b+n\mathbb{Z}) \\ &= R(a+mn\mathbb{Z})+R(b+mn\mathbb{Z}), \end{aligned}$$

proving that R preserves addition.

It follows that R provides a ring isomorphism

$$\boxed{\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \quad \text{for} \quad (m,n)=1}.$$

The connection to Euler's totient function is provided by the pair of results.

Lemma 1

If R_1 and R_2 are rings, then $(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$.

Proof (Sketch). Since the identity in $R_1 \times R_2$ is $(1_{R_1}, 1_{R_2})$, one can easily show that

$$(a, b)^{-1} = (a^{-1}, b^{-1}).$$

The result follows. □

Lemma 2

If $f : R_1 \to R_2$ is an isomorphism of rings, then $f| : (R_1)^\times \to (R_2)^\times$ is a multiplication preserving bijection (an isomorphism of groups*).*

Proof (Sketch). Every element of R_2 has the form $f(a)$ for some $a \in R_1$, and for every $a, b \in R_1$,

$$1_{R_2} = f(1_{R_1}) = f(ab) = f(a)f(b)$$

holds iff $a \in R_1^\times$ iff $f(a) \in R_2^\times$. □

A few remarks aside, we're ready to move on.

Remarks

One can form the direct product of any number (or indexed collection) of rings in an analogous manner, by simply performing addition and multiplication coordinate-wise.

Theorem 5 still holds in this more general setting: the unit group in the product is the product of the unit groups.

Applied in this setting, if $n_i \in \mathbb{N}$ are pairwise coprime, the CRT and Lemma 2 provide an isomorphism

$$(\mathbb{Z}/n_1 n_2 \cdots n_r\mathbb{Z})^\times \cong (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^\times.$$

Let $p_1, p_2, \ldots, p_r \in \mathbb{N}$ be distinct primes and $e_1, e_2, \ldots, e_r \in \mathbb{N}$.

For $i \neq j$, the FTA implies that $(p_i^{e_i}, p_j^{e_j}) = 1$.

It follows that there is an isomorphism

$$(\mathbb{Z}/p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times.$$

This immediately implies that

$$\varphi(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r}).$$

This is what we mean when we say that φ is *multiplicative*.

We arrive at the following formula for φ.

Theorem 5

Let $n \in \mathbb{N}$. Then

$$\varphi(n) = \prod_{p|n} (p^{e_p} - p^{e_p - 1}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where both products run over the prime divisors of n, and e_p denotes the exponent of p occurring in the canonical form of n.

Remarks.

- Remembering that the empty product equals 1 by caveat, both formulae are automatically valid for $n = 1$.
- It is often more convenient to use the equivalent form $p^{e_p} - p^{e_p - 1} = p^{e_p - 1}(p - 1)$.

Proof of Theorem 5

Since $n = \prod_{p|n} p^{e_p}$, the multiplicativity of φ and Theorem 3 immediately imply that

$$\varphi(n) = \varphi\left(\prod_{p|n} p^{e_p}\right) = \prod_{p|n} \varphi(p^{e_p})$$
$$= \prod_{p|n}(p^{e_p} - p^{e_p-1}) = \prod_{p|n} p^{e_p}\left(1 - \frac{1}{p}\right)$$
$$= n\prod_{p|n}\left(1 - \frac{1}{p}\right).$$

□

Examples

We have

$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8$$

and

$$\varphi(98) = \varphi(2 \cdot 7^2) = \varphi(2)\varphi(7^2) = (2-1) \cdot 7(7-1) = 42$$

and

$$\begin{aligned} \varphi(18000000) &= \varphi(2 \cdot 9 \cdot 10^6) = \varphi(2^7)\varphi(3^2)\varphi(5^6) \\ &= 2^{7-1}(2-1) \cdot 3^{2-1}(3-1) \cdot 5^{6-1}(5-1) \\ &= 2^6 \cdot 3 \cdot 2 \cdot 5^5 \cdot 2^2 \\ &= 48 \cdot 10^5 = 4800000. \end{aligned}$$