Properties of Euler's Totient Function

Ryan C. Daileda

Trinity University

Number Theory

Recall

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

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

Last time we proved that φ is *multiplicative*: given distinct primes p_i and $e_i \in \mathbb{N}$,

$$\varphi(p_1^{e_1} \cdots p_r^{e_r}) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r});$$

and we used this to deduce the formulae

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

If we partition $\{1 \le a \le n\}$ according to (a, n), we can use φ to count the partitions and arrive at another useful identity.

Lemma 1

Let $n \in \mathbb{N}$ and suppose $d|n$. There is a bijection

$$\{1 \le a \le n \,|\, (a, n) = d\} \longleftrightarrow \left\{1 \le b \le \frac{n}{d} \,\middle|\, \left(b, \frac{n}{d}\right) = 1\right\}.$$

Proof. If $1 \le a \le n$ and $(a, n) = d$, let $f(a) = \frac{a}{d}$.

We have

$$d = (a, n) = \left(d\frac{a}{d}, d\frac{n}{d}\right) = d\left(f(a), \frac{n}{d}\right) \;\Rightarrow\; \left(f(a), \frac{n}{d}\right) = 1.$$

Thus $f : \{1 \le a \le n \,|\, (a, n) = d\} \to \left\{1 \le b \le \frac{n}{d} \,|\, \left(b, \frac{n}{d}\right) = 1\right\}$.

On the other hand, if $1 \leq b \leq \frac{n}{d}$ and $(b, \frac{n}{d}) = 1$, define $g(b) = bd$.

Then

$$d = d\left(b, \frac{n}{d}\right) = (bd, n) = (g(b), n)$$

so that $g : \left\{1 \leq b \leq \frac{n}{d} \,\middle|\, \left(b, \frac{n}{d}\right) = 1\right\} \to \{1 \leq a \leq n \,|\, (a, n) = d\}$.

Since $f(g(b)) = f(bd) = \frac{bd}{d} = b$ and $g(f(a)) = g(\frac{a}{d}) = d\frac{a}{d} = a$, f and g are inverses.

The result follows. □

Lemma 1 has the following immediate corollary.

Corollary 1

Let $n \in \mathbb{N}$ and suppose $d|n$. Then

$$\left|\{1 \leq a \leq n \,|\, (a,n) = d\}\right| = \varphi\left(\frac{n}{d}\right).$$

For $d|n$, the sets $\{1 \leq a \leq n \,|\, (a,n) = d\}$ partition $\{1 \leq a \leq n\}$.

Thus

$$n = \sum_{d|n} \left|\{1 \leq a \leq n \,|\, (a,n) = d\}\right| = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

But as d runs through the positive divisors of n, so does n/d. This proves:

Theorem 1

For $n \in \mathbb{N}$,

$$n = \sum_{d|n} \varphi(d).$$

This identity will prove useful when we discuss *primitive roots*.

Before turning in that direction we prove one more identity involving φ.

Theorem 2

Let $n \in \mathbb{N}$. If $n > 1$, then

$$\sum_{\substack{1 \le a < n \\ (a,n)=1}} a = \frac{1}{2} n\varphi(n).$$

Proof. If $1 \le a \le n$ and $(a, n) = 1$, then

$$1 \le n - a < n \quad \text{and} \quad (n - a, n) = (-a, n) = (a, n) = 1.$$

Thus

$$\sum_{\substack{1 \le a < n \\ (a,n)=1}} a = \sum_{\substack{1 \le a < n \\ (a,n)=1}} (n - a) = n \sum_{\substack{1 \le a < n \\ (a,n)=1}} 1 - \sum_{\substack{1 \le a < n \\ (a,n)=1}} a = n\varphi(n) - \sum_{\substack{1 \le a < n \\ (a,n)=1}} a.$$

The result follows. □

The Order of an Element

Definition

Let G be a group and $a \in G$. The *order (or period)* of a, denoted $|a|$, is the least $n \in \mathbb{N}$ so that $a^n = e$. If no such n exists, we say that $|a|$ is infinite.

Examples.

- If G is a group and $a \in G$, then $|a| = 1$ iff $a = e$.
- Every nonzero element of $\mathbb{Z}$ has infinite order, since if $a \in \mathbb{Z}$ and $a \neq 0$, then $an \neq 0$ for all $n \in \mathbb{N}$.
- $2 + 6\mathbb{Z}$ has (additive) order 3 since $2(2 + 6\mathbb{Z}) = 4 + 6\mathbb{Z}$ and $3(2 + 6\mathbb{Z}) = 6 + 6\mathbb{Z} = 0 + 6\mathbb{Z}$.
- $2 + 5\mathbb{Z}$ has (multiplicative) order 4 since

$$(2 + 5\mathbb{Z})^2 = 4 + 5\mathbb{Z}, (2 + 5\mathbb{Z})^3 = 3 + 5\mathbb{Z}, (2 + 5\mathbb{Z})^4 = 1 + 5\mathbb{Z}.$$

Properties of the Order

Theorem 3

Let G be a group and $a \in G$. If a has finite order $n \in \mathbb{N}$, then $a^m = e$ if and only if $n|m$.

Proof. Suppose $a^m = e$. Use the Division Algorithm to write $m = qn + r$ with $0 \leq r < n$.
Then

$$e = a^m = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r.$$

If $r > 0$, this contradicts the fact that $n = |a|$. So we must have $r = 0$ and hence $n|m$.
The converse is immediate. If $m = nq$, then

$$a^m = a^{nq} = (a^n)^q = e^q = e.$$

□

Corollary 2

Let G be a group and $a \in G$. If a has finite order $n \in \mathbb{N}$, then $a^i = a^j$ iff $i \equiv j \pmod{n}$.

Proof. We have

$$a^i = a^j \iff a^i(a^j)^{-1} = e \iff a^{i-j} = e.$$

The result now follows from Theorem 1. □

This immediately implies:

Corollary 3

Let G be a group and $a \in G$. If a has finite order $n \in \mathbb{N}$, then the distinct powers of a are $e, a, a^2, a^3, \ldots, a^{n-1}$.

It remains to address the powers of an element with infinite order.

Theorem 4

Let G be a group and $a \in G$. If $|a|$ is infinite, then $a^i = a^j$ iff $i = j$. That is, the powers of a are all distinct.

Proof. Suppose $a^i = a^j$ and $i \neq j$. Without loss of generality, suppose $i > j$.

Then, as above, we have $a^{i-j} = e$. Since $i - j > 0$, this implies $|a|$ is finite, which is a contradiction.

Thus we must have $i = j$. □

Corollary 4

Let G be a group. If G contains an element of infinite order, then G is infinite. Conversely, if G is finite, every element of G has finite order.

Proof. If $a \in G$ has infinite order, then the subset $\{a^i \mid i \in \mathbb{Z}\}$ is infinite, by Theorem 2.

Hence G is infinite as well. □

Corollary 5

Let G be a finite group and $a \in G$. Then $|a| \leq |G|$.

Proof. Let $n = |a|$. Then G contains the elements $e, a, a^2, \ldots, a^{n-1}$, which are distinct by Corollary 2. Thus $|G| \geq n$. □

When G is a finite abelian group, we can give a more precise relationship between $|a|$ and $|G|$.

Theorem 5

Let G be a finite abelian group. For any $a \in G$, $|a|$ divides $|G|$.

Proof. For $a \in G$, we know that $a^{|G|} = e$.

The result now follows from Theorem 3. □

Remark. The conclusion of Theorem 5 holds for arbitrary finite groups, but the proof would take us too far afield.

Orders of Powers of Elements

Let G be a group, let $a \in G$, and suppose that $|a| = n \in \mathbb{N}$.

Let $m \in \mathbb{Z}$ and set $b = a^m$. Since

$$b^n = (a^m)^n = a^{mn} = (a^n)^m = e^m = e,$$

b necessarily has finite order.

Let's compute $|b|$. We have

$$b^k = e \;\Leftrightarrow\; (a^m)^k = e \;\Leftrightarrow\; a^{mk} = e \;\Leftrightarrow\; n|mk,$$

by Theorem 3.

Write $m = (m,n)m'$ and $n = (m,n)n'$, so that $(m',n') = 1$. Then

$$n|mk \;\Leftrightarrow\; (m,n)n'|(m,n)m'k \;\Leftrightarrow\; n'|m'k \;\Leftrightarrow\; n'|k,$$

by Euclid's lemma.

The smallest positive k so that $n'|k$ is n'. Thus:

Theorem 6

Let G be a group and let $a \in G$ have finite order n. Then for any $m \in \mathbb{Z}$,

$$|a^m| = \frac{n}{(m,n)}.$$

Corollary 6

Let G be a group and let $a \in G$ have finite order n. If $(m,n) = 1$ and $b = a^m$, then

$$\{e, a, a^2, \ldots, a^{n-1}\} = \{e, b, b^2, \ldots, b^{n-1}\}.$$

Proof. If $(m,n) = 1$, then $|b| = |a^m| = \frac{n}{(m,n)} = n$. Thus b has exactly n distinct powers.

But so does a, and every power of b is a power of a.

The result follows. □

Additive Orders Modulo n

We will primarily be interested in the orders of elements in the groups $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

We can very easily determine the orders of elements in $\mathbb{Z}/n\mathbb{Z}$.

We first notice that $|1 + n\mathbb{Z}| = n$, since

$$k(1 + n\mathbb{Z}) = k + n\mathbb{Z} = 0 + n\mathbb{Z} \iff n|k.$$

Let $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$. Then $a + n\mathbb{Z} = a(1 + n\mathbb{Z})$. By Theorem 6 we have:

Theorem 7

The additive order of $a + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ is $\dfrac{n}{(a, n)}$.

Example. Consider $a = 4$ modulo 10. Since $\frac{10}{(10,4)} = \frac{10}{2} = 5$, 4 should have additive order 5 modulo 10. Indeed:

$$2 \cdot 4 = 8, \;\; 3 \cdot 4 \equiv 2 \pmod{10}, \;\; 4 \cdot 4 \equiv 6 \pmod{10}, \;\; 5 \cdot 4 \equiv 0 \pmod{10}.$$

Similar computations produce the following table.

Order	Elements
1	$0 + 10\mathbb{Z}$
2	$5 + 10\mathbb{Z}$
5	$2 + 10\mathbb{Z}$, $4 + 10\mathbb{Z}$, $6 + 10\mathbb{Z}$, $8 + 10\mathbb{Z}$
10	$1 + 10\mathbb{Z}$, $3 + 10\mathbb{Z}$, $7 + 10\mathbb{Z}$, $9 + 10\mathbb{Z}$

By Corollary 6, it follows, for instance, that every element of $\mathbb{Z}/10\mathbb{Z}$ is a multiple of $7 + 10\mathbb{Z}$.

This is equivalent to the statement that for any $a \in \mathbb{Z}$, the linear congruence $7x \equiv a \pmod{10}$ has a solution.

We can explain the preceding table by counting how many elements of $\mathbb{Z}/n\mathbb{Z}$ have a given order.

Let d divide $\left|\mathbb{Z}/n\mathbb{Z}\right| = n$. Then $a + n\mathbb{Z}$ has order d iff $d = \frac{n}{(a,n)}$ iff $(a, n) = \frac{n}{d}$.

Thus, the number of elements in $\mathbb{Z}/n\mathbb{Z}$ with order d is equal to

$$\left|\{1 \leq a \leq n \,|\, (a, n) = n/d\}\right| = \varphi\left(\frac{n}{n/d}\right) = \varphi(d),$$

by Corollary 1. These computations prove the next result.

Theorem 8

Let $n \in \mathbb{N}$ and suppose $d|n$. There are exactly $\varphi(d)$ elements in $\mathbb{Z}/n\mathbb{Z}$ of order d.