New Zealand Mathematical Olympiad Committee

Euler's ϕ-Function and Euler's Theorem

Arkadii Slinko

1 Introduction

These notes, the third in a series of short tutorials in number theory, cover some important machinery for dealing with congruences.

2 Euler's ϕ-function

Let n be a positive integer. The number of positive integers less than or equal to n that are relatively prime to n, is denoted by $\phi(n)$. This function is called *Euler's ϕ-function* or *Euler's totient function.*

Let us denote $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ and by $\mathbb{Z}_n^*$ the set of those nonzero numbers from $\mathbb{Z}_n$ that are relatively prime to n. Then $\phi(n)$ is the number of elements of $\mathbb{Z}_n^*$, i.e., $\phi(n) = |\mathbb{Z}_n^*|$.

Example 1. Let $n = 20$. Then $\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and $\phi(20) = 8$.

Lemma 1. *If $n = p^k$, where p is prime, then*

$$\phi(n) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right).$$

Proof. It is easy to list all integers that are less than or equal to p^k and not relatively prime to p^k. They are $p, 2p, 3p, \ldots, p^{k-1} \cdot p$. We have exactly p^{k-1} of them. Therefore $p^k - p^{k-1}$ nonzero integers from $\mathbb{Z}_n$ will be relatively prime to n. Hence $\phi(n) = p^k - p^{k-1}$. $\square$

An important consequence of the Chinese Remainder Theorem is that the function $\phi(n)$ is multiplicative in the following sense:

Theorem 2. *Let m and n be any two relatively prime positive integers. Then*

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. Let $\mathbb{Z}_m^* = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ and $\mathbb{Z}_n^* = \{s_1, s_2, \ldots, s_{\phi(n)}\}$. By the Chinese Remainder Theorem, for each pair (i, j), there exists a unique positive integer N_{ij} such that $0 \le N_{ij} < mn$ and

$$r_i = N_{ij} \pmod{m}, \qquad s_j = N_{ij} \pmod{n};$$

that is, N_{ij} has remainder r_i on dividing by m, and remainder s_j on dividing by n, or, in particular, for some integers a and b,

$$N_{ij} = am + r_i, \qquad N_{ij} = bn + s_j. \tag{1}$$

As in the Euclidean algorithm, we notice that $\gcd(N_{ij}, m) = \gcd(m, r_i) = 1$ and $\gcd(N_{ij}, n) = \gcd(n, s_j) = 1$, that is N_{ij} is relatively prime to m and also relatively prime to n. Since m and n are relatively prime, N_{ij} is relatively prime to mn, hence $N_{ij} \in \mathbb{Z}_{mn}^*$. Clearly, different pairs $(i, j) \ne (k, l)$ yield different numbers, that is $N_{ij} \ne N_{kl}$ for $(i, j) \ne (k, l)$. Suppose now that a number $N \ne N_{ij}$ for all i and j. Then

$$r = N \pmod{m}, \qquad s = N \pmod{n},$$

where either r does not belong to $\mathbb{Z}_m^*$ or s does not belong to $\mathbb{Z}_n^*$. Assuming the former, we get $\gcd(r,m) > 1$. But then $\gcd(N,m) = \gcd(m,r) > 1$ and N does not belong to $\mathbb{Z}_{mn}^*$. It shows that the numbers N_{ij} and only they form $\mathbb{Z}_{mn}^*$. But there are exactly $\phi(m)\phi(n)$ of the numbers N_{ij}, exactly as many as the pairs (r_i, s_j). Therefore $\phi(mn) = \phi(m)\phi(n)$. □

Theorem 3. *Let n be a positive integer with the prime factorisation*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

where the p_i are distinct primes and the α_i are positive integers. Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right).$$

Proof. We use Lemma 1 and Theorem 2 to compute $\phi(n)$:

$$\begin{aligned} \phi(n) &= \phi\left(p_1^{\alpha_1}\right)\phi\left(p_2^{\alpha_2}\right)\dots\phi\left(p_r^{\alpha_r}\right) \\ &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right)p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\dots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right). \end{aligned}$$

□

Example 2. $\phi(264) = \phi(2^3 \cdot 3 \cdot 11) = 264\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{10}{11}\right) = 80.$

3 Congruences. Euler's Theorem

If a and b are integers we write $a \equiv b \bmod m$, and say that a is congruent to b modulo m, if a and b have the same remainder on dividing by m. For example, $41 \equiv 80 \bmod 13$, $41 \equiv -37 \bmod 13$, $41 \not\equiv 7 \bmod 13$.

Lemma 4. *Let a and b be two integers and m is a positive integer. Then*

(a) *$a \equiv b \bmod m$ if and only if $a - b$ is divisible by m.*

(b) *If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $a + c \equiv b + d \bmod m$.*

(c) *If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $ac \equiv bd \bmod m$.*

(d) *If $a \equiv b \bmod m$ and n is a positive integer, then $a^n \equiv b^n \bmod m$.*

(e) *If $ac \equiv bc \bmod m$ and c is relatively prime to m, then $a \equiv b \bmod m$.*

Proof. (a) By the division algorithm

$$a = q_1 m + r_1, \quad 0 \le r_1 < m, \text{ and } \ b = q_2 m + r_2, \quad 0 \le r_2 < m.$$

Thus $a - b = (q_1 - q_2)m + (r_1 - r_2)$, where $-m < r_1 - r_2 < m$. We see that $a - b$ is divisible by m if and only if $r_1 - r_2$ is divisible by m but this can happen if and only if $r_1 - r_2 = 0$, i.e., $r_1 = r_2$.

(b) is an exercise.

(c) If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $m|(a - b)$ and $m|(c - d)$, i.e., $a - b = im$ and $c - d = jm$ for some integers i, j. Then

$$ac - bd = (ac - bc) + (bc - bd) = (a - b)c + b(c - d) = icm + jbm = (ic + jb)m,$$

whence $ac \equiv bd \bmod m$.

(d) Follows immediately from (c).

(e) Suppose that $ac \equiv bc \bmod m$ and $\gcd cm = 1$. Then there exist integers u, v such that $cu + mv = 1$ or $cu \equiv 1 \bmod m$. Then by (c)

$$a \equiv acu \equiv bcu \equiv b \bmod m$$

and $a \equiv b \bmod m$ as required.

□

The property in Lemma 2 (e) is called the *cancellation property.*

Theorem 5 (Fermat's Little Theorem)**.** *Let p be a prime. If an integer a is not divisible by p, then $a^{p-1} \equiv 1 \bmod p$. Also $a^p \equiv a \bmod p$ for all a.*

Proof. Let a, be relatively prime to p. Consider the numbers a, $2a$, ..., $(p-1)a$. All of them have different remainders on dividing by p. For suppose that for some $1 \le i < j \le p-1$ we have $ia \equiv ja \bmod p$. Then by the cancellation property a can be cancelled and $i \equiv j \bmod p$, which is impossible. Therefore these remainders are 1, 2, ..., $p-1$ and

$$a \cdot 2a \cdot \cdots \cdot (p-1)a \equiv (p-1)! \pmod{p},$$

which is

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}.$$

Since $(p-1)!$ is relatively prime to p, by the cancellation property $a^{p-1} \equiv 1 \bmod p$. When a is relatively prime to p, the last statement follows from the first one. If a is a multiple of p the last statement is also clear. □

Theorem 6 (Euler's Theorem)**.** *Let n be a positive integer. Then*

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

for all a relatively prime to n.

Proof. Let $\mathbb{Z}_n^* = \{z_1, z_2, \ldots, z_{\phi(n)}\}$. Consider the numbers z_1a, z_2a, ..., $z_{\phi(n)}a$. Both z_i and a are relatively prime to n, therefore z_ia is also relatively prime to n. Suppose that r_i is the remainder on dividing z_ia by n. Then $\gcd(r_i, n) = \gcd(z_ia, n) = 1$, so $r_i \in \mathbb{Z}_n^*$. These remainders are all different. For suppose to the contrary that $r_i = r_j$ for some $1 \le i < j \le n$. Then $z_ia \equiv z_ja \bmod n$; by the cancellation property, a can be cancelled and we get $z_i \equiv z_j \bmod n$, which is impossible. Therefore the remainders $r_1, r_2, ..., r_{\phi(n)}$ coincide with $z_1, z_2, \ldots, z_{\phi(n)}$, apart from the order in which they are listed. Thus

$$z_1a \cdot z_2a \cdot \ldots \cdot z_{\phi(n)}a \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv z_1 \cdot z_2 \cdot \ldots \cdot z_{\phi(n)} \pmod{n},$$

which is

$$Z \cdot a^{\phi(n)} \equiv Z \pmod{n},$$

where $Z = z_1 \cdot z_2 \cdot \ldots \cdot z_{\phi(n)}$. Since Z is relatively prime to n it can be cancelled, giving $a^{\phi(n)} \equiv 1 \bmod n$. □

January 24, 2009

http://www.mathsolympiad.org.nz