Euler function

Definition

Euler function $\phi(n)$ (sometimes denoted $\varphi(n)$or $phi(n)$) - the number of properties $1$to $n$prime to n. In other words, is the amount of numbers in the interval $[1; n]$, the greatest common divisor which with $n$unity.

The first few values of this function (A000010 in OEIS encyclopedia):

$\phi(1) = 1,$

$\phi(2) = 1,$

$\phi(3) = 2,$

$\phi(4) = 2,$

$\phi(5) = 4.$

Properties

The following three simple properties of the Euler - enough to learn how to calculate it for any number:

- If p- prime, then $\phi(p) = p - 1$.
- (This is obvious, since any number, except for the $p$relatively easy with him.)
- If p- simple a- natural number, then $\phi(p^a) = p^a - p^{a-1}$.
- (Because the number of p^anot only relatively prime numbers of the form , which pieces.)$pk \; (k \in \mathcal{N}) p^a / p = p^{a-1}$
- If $a$and $b$are relatively prime, then $\phi(ab) = \phi(a)\phi(b)$("multiplicative" Euler function).
- (This follows from the Chinese Remainder Theorem . Consider an arbitrary number $z \le ab$. denote $x$and $y$remainders $z$on $a$and $b$respectively. then z coprime abif and only if $z$coprime $a$and $b$individually, or what is the same, x mutually simply $a$and $y$coprime b. Applying the Chinese remainder theorem, we see that any pair of numbers $x$and the number of one-to-one correspondence , which completes the proof.)$y \; (x \le a, \; y \le b) z \; (z \le ab)$

We can obtain the Euler function for any $n$through its **factorization** (decomposition n into prime factors):

if

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

(Where all p_i- simple), then

$$\phi(n) = \phi(p_1^{a_1}) \cdot \phi(p_2^{a_2}) \cdot \ldots \cdot \phi(p_k^{a_k}) =$$

$$= (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \cdot \ldots \cdot (p_k^{a_k} - p_k^{a_k-1}) =$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Implementation

The simplest code calculating the Euler function, factoring in the number of elementary method $O(\sqrt{n})$:

```
int phi (int n) {
	int result = n;
	for (int i=2; i*i<=n; ++i)
		if (n % i == 0) {
			while (n % i == 0)
				n /= i;
			result -= result / i;
		}
	if (n > 1)
		result -= result / n;
	return result;
}
```

The key place for the calculation of the Euler function - is to find the **factorization of** the number n. It can be carried out for a time considerably shorter $O(\sqrt{n})$: see Efficient algorithms for factorization .

Applications of the Euler function

The most famous and important property of Euler's function is expressed in **Euler's theorem** :

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

where a and m are relatively prime.

In the particular case when m a simple Euler's theorem turns into the so-called **Fermat's little theorem** :

$$a^{m-1} \equiv 1 \pmod m$$

Euler's theorem often occurs in practical applications, for example, see Reverse item in the mod .

Problem in online judges

Task List, which requires a function to calculate the Euler or use Euler's theorem, either by value of the Euler function to restore the original number:

- UVA # 10179 **"Irreducible Basic Fractions"** [Difficulty: Easy]
- UVA # 10299 **"Relatives"** [Difficulty: Easy]
- UVA # 11327 **"Enumerating Rational Numbers"** [Difficulty: Medium]
- TIMUS # 1673 **"Admission to the exam"** [difficulty: high]