

MAXimal

[home](#)
[algo](#)
[bookz](#)
[forum](#)
[about](#)

 added: 10 Jun 2008 10:57
 edited by: on Oct 18, 2011 8:20 pm

Euler function

Definition

The Euler function $\phi(n)$ (sometimes denoted by $\varphi(n)$ or $\text{phi}(n)$) is the number of numbers from 1 to n , relatively prime to n . In other words, this is the number of such numbers in a segment $[1; n]$ whose **greatest common divisor** with n is one.

The first few values of this function ([A000010 in the OEIS encyclopedia](#)):

$$\begin{aligned}\phi(1) &= 1, \\ \phi(2) &= 1, \\ \phi(3) &= 2, \\ \phi(4) &= 2, \\ \phi(5) &= 4.\end{aligned}$$

Properties

The following three simple properties of the Euler function are sufficient to learn how to calculate it for any numbers:

- If p is a prime number, then $\phi(p) = p - 1$.

(This is obvious, because any number, except for itself p , is mutually simple with it.)

- If p is prime, a is a natural number, then $\phi(p^a) = p^a - p^{a-1}$.

(Since the numbers are p^a not mutually simple only the numbers of the species pk ($k \in \mathcal{N}$), which $p^a/p = p^{a-1}$ pieces.)

- If a and b are relatively prime, then $\phi(ab) = \phi(a)\phi(b)$ (the "multiplicativity" of the Euler function).

(This fact follows from the [Chinese remainder theorem](#), consider an arbitrary number, $z \leq ab$ and denote by x the remainder of the division z by a and, y respectively. Then it is z relatively prime to ab if and only if z is relatively prime to a and b , or, equivalently, x is mutually simple with a and y is relatively prime to b . Applying the Chinese remainder theorem, we find that every pair of numbers x and y ($x \leq a$, $y \leq b$) one-to-one correspond to a number z ($z \leq ab$), which completes the proof.)

From here one can obtain the Euler function for any n in terms of its **factorization** (decomposition n into simple factors):

if

Contents [hide]

- Euler function
 - Definition
 - Properties
 - Implementation
 - Applications of the Euler function
 - Tasks for online judges

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

(where all p_i are simple), then

$$\begin{aligned} \phi(n) &= \phi(p_1^{a_1}) \cdot \phi(p_2^{a_2}) \cdot \dots \cdot \phi(p_k^{a_k}) = \\ &= (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \cdot \dots \cdot (p_k^{a_k} - p_k^{a_k-1}) = \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

Implementation

The simplest code that computes the Euler function, factoring the number by an elementary method for $O(\sqrt{n})$:

```
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 to calculate the Euler function is to find the **factorization of a number** n . It can be performed in a time much less $O(\sqrt{n})$: see [Effective algorithms for factorization](#).

Applications of the Euler function

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

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

where a and m are relatively simple.

In the special case, when m simple, Euler's theorem turns into the so-called **Fermat's small theorem** :

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

Euler's theorem is often encountered in practical applications, for example, see the [Inverse element in the field modulo](#).

Tasks for online judges

List of tasks in which you want to calculate the Euler function, either use Euler's theorem or use the value of the Euler function to restore the original number:

- [UVA # 10179 "Irreducible Basic Fractions"](#) [difficulty: low]
- [UVA # 10299 "Relatives"](#) [difficulty: low]
- [UVA # 11327 "Enumerating Rational Numbers"](#) [complexity: medium]
- [TIMUS # 1673 "Admission to the exam"](#) [complexity: high]

18 Комментариев

e-maxx

1 Войти ▾

♥ Рекомендовать 27

🔗 Поделиться

Лучшее в начале ▾



ВОЙТИ С ПОМОЩЬЮ

ИЛИ ЧЕРЕЗ DISQUS ?

**Сула** • 5 лет назад

```
if (n % i == 0) {
while (n % i == 0)
n /= i;
result -= result / i;
```

Зачем там while, ведь мы проверили что $n \% i == 0$? Объясните пожалуйста: например ввел 18, а он мне возвращает 4, а по идее должен 6?

6 ^ | ▾ • Ответить • Поделиться ›

**траль** ➔ Сула • 4 года назад

ты лалка потому что делитель млжет повторяться несколько раз

9 ^ | ▾ • Ответить • Поделиться ›

**Артём Чистяков** ➔ Сула • год назад

18 :
1 5 7 11 13 17

^ | ▾ • Ответить • Поделиться ›

**rishabh roy** • 5 лет назад

unable to solve UVA # 10179 "Irreducible Basic Fractions" [Difficulty: Easy]
please help the function is giving the correct results for given text cases but the uva judge is not Accepting my solutions

2 ^ | v • Ответить • Поделиться ›



Eunix Trix → rishabh roy • 2 месяца назад

Take care of the inputs as it is going to end with 0;

^ | v • Ответить • Поделиться ›



tm-green • 4 года назад

В определении функции:

"это количество чисел от 1 до n" - до (n-1) полагаю логически будет более понятным и правильным. Исправьте пожалуйста.

1 ^ | v • Ответить • Поделиться ›



Ульянич Михаил → tm-green • 4 года назад

Нет, это не правильней. При таком определении изменяется значение функции при n=1.

1 ^ | v • Ответить • Поделиться ›



Guest • 5 лет назад

Hello, world!

1 ^ | v • Ответить • Поделиться ›



Татьяна • 5 лет назад

Чем первая задача из списка отличается от второй??Вторая у меня почему то не сдается..

1 ^ | v • Ответить • Поделиться ›



Владислав → Татьяна • 5 лет назад

во второй задаче $\phi(1)=0$

1 ^ | v • Ответить • Поделиться ›



Vlad • 5 лет назад

Я не совсем понял, зачем в конце проверять $n > 1$, ведь мы уже разложили вроде n

1 ^ | v • Ответить • Поделиться ›



e_maxx Модератор → Vlad • 5 лет назад

Нет, т.к. мы перебрали только делители до квадратного корня из n, однако, если n было простым числом (или стало таковым в процессе факторизации), мы не найдём этот последний делитель, равный самому числу. Простой пример: если $n=11$, то цикл совершит две итерации ($i=2$ и $i=3$), не найдёт ни одного делителя, и завершится с $n=11$.

1 ^ | v • Ответить • Поделиться ›



незнакомец • 6 лет назад

Кроме этого $\phi(x)$, есть $L(m)$ - обобщенная функция эйлера, используется она в олимпиадах?

<http://www.pifagor.kz/categ...>

1 ^ | v • Ответить • Поделиться ›

1 ^ | v • Ответить • Поделиться ›



e_maxx Модератор ➔ незнакомец • 5 лет назад

Никогда про такую не слышал. По вашей ссылке ничего не понял, мне кажется, там закрался ряд ошибок.

2 ^ | v • Ответить • Поделиться ›



Guest • 5 лет назад

[code]

Hello, world!

[/code]

1 ^ | v • Ответить • Поделиться ›



Сенья • год назад

result -= result / i; почему?

и

if (n > 1)

result -= result / n;

и не легче сделать result -= 1;?

^ | v • Ответить • Поделиться ›



Denis sas • 2 года назад

```
int phi (int n) {
```

```
int res=1;
```

```
if(n%2) return res = n-1;
```

```
for(int i = 1; i!=n; i++){
```

```
if((n % i)==0){res++;}}
```

```
return res;
```

```
}
```

Лично я так понимаю.

^ | v • Ответить • Поделиться ›



Guest • 3 года назад

ктонибудь знает как решить последнюю задачу???

^ | v • Ответить • Поделиться ›