山东大学附属中学信息学奥赛资料

数论-2(2023-12-5)

1.欧拉函数的定义

欧拉函数 $\varphi(n)$ 是指不超过 n 且与 n 互质的正整数的个数， n 是正整数。

$\varphi(n)=\sum_{i=1}^{n}[gcd(i,n)=1]$

$[gcd(i,n)=1]$ 的值：当 $gcd(i,n)=1$ 时（即 i,n 互质）值为 1，否则为 0。

如 $n=10$,与 10 互质的正整数有 $1,3,7,9$ ，则 $\varphi(10)=4$。

其中 $\varphi(1)=1$。

2.欧拉函数的性质

性质1：

如果 p是质数，则 $\varphi(p)=p-1$。

显然， $1,2,..,p-1$ 都与质数 p 互质。

性质2：

如果 p 是质数，则 $\varphi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)=p^{k-1}\varphi(p)$。

证明：

1 到 p^k 之间所有的数中，其中 p 的倍数有：$1p,2p,3p,..,p^{k-1}\times p$ ，共有 p^{k-1} 个。

（原理：$1..n$ 中，p 的倍数有 $\lfloor\frac{n}{p}\rfloor$ 个，显然 $1..p^k$ 中 p 的倍数有 $\frac{p^k}{p}=p^{k-1}$ 个）

因为 p 是质数，除上述外没有其他因子了。

如：$\varphi(3)=2,\varphi(81)=\varphi(3^4)=3^{4-1}\varphi(3)=54=3^4-3^3$

$1*3,2*3,3*3,4*3,5*3,..,27*3$ 这 27 个数与 81 至少有一个因子 3

性质3：

（1）如果 $gcd(p,q)=1$ ，即 p 与 q 互质，则 $\varphi(pq)=\varphi(p)\varphi(q)$

特别的：

如果 p 与 q 都是质数，则 $\varphi(pq)=(p-1)(q-1)$

（2）如果 $gcd(p,q)=d$ ，则 $\varphi(pq)=\varphi(p)\times\varphi(q)\times d/\varphi(d)$

如果 $q=d$，则 $\varphi(pq)=\varphi(p)\times q$

利用 $p=2*3^2,q=3^4*5$ 可以验证一下。

性质4：

设正整数 n 的素数幂分解：$n = p_1^{a_1}.p_2^{a_2}..p_k^{a_k}$，那么

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

根据性质2和性质3：

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

本质是容斥原理：去掉 p_1 的倍数，去掉 p_2 的倍数，...，但有去重复的。

$n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} + \frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \frac{n}{p_2p_3} - \frac{n}{p_1p_2p_3} = n \cdot (1-\frac{1}{p_1}) \cdot (1-\frac{1}{p_2}) \cdot (1-\frac{1}{p_3})$

性质4的特殊情况：

（1）如果 n 是质数，即 $n = p_1$，$\varphi(n) = n(1-\frac{1}{p_1}) = n-1$。得到性质1。

（2）如果 $n = p^k$，得到性质2。

求 $\varphi(n)$ 的方法：

一开始ans=n,找到第一个质数 p_1, $ans = ans(1-\frac{1}{p_1}) = ans/p_1 * (p_1 - 1);$

再找到一个素数 p_2， $ans = ans/p_2 * (p_2 - 1);$

依次类推，直到找到最后的质因数 p_k。

具体看后面的求法。

根据上述性质：

$\varphi(2) = 1, \varphi(3) = 2, \varphi(5) = 4, \varphi(7) = 6$

$\varphi(360) = \varphi(2^3.3^2.5) = \varphi(2^3).\varphi(3^2).\varphi(5) = 2^{3-1}\varphi(2).3^{2-1}\varphi(3).\varphi(5) = 96$

$\varphi(360*2) = \varphi(360)*2 = 192$, 在$\varphi(360)$ 的基础上2 的指数加1，即乘以 2即可。

$\varphi(360*3) = \varphi(360)*3 = 96*3$

$\varphi(360*5) = \varphi(360)*5 = 96*5$

$\varphi(360*7) = \varphi(360)*\varphi(7) = 96*6$

得出结论：

已知求得了$\varphi(i)$ 和 $\varphi(p)$ 的值，其中 p 是质数，我们可以求 $\varphi(i*p)$ 的值：

如果 $i\%p = 0$, 则 $\varphi(i*p) = \varphi(i)*p$

否则 $\varphi(i*p) = \varphi(i)*\varphi(p)$

后面欧拉筛线性求$1..n$ 欧拉函数用到的实现方法。

另外：

如果 p 与 q 互质，则 $\varphi(pq)=\varphi(p)\varphi(q)$

特别的：如果 p 与 q 都是质数，则 $\varphi(pq)=(p-1)(q-1)$

利用性质3证明。

设 p 的质因子个数为k1, q的质因子个数为k2.

$\varphi(p)\varphi(q)=p\cdot(1-\frac{1}{p_1})\cdot(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k1}).q\cdot(1-\frac{1}{p_1})\cdot(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k2})$

$\varphi(p)\varphi(q)=p.q\cdot(1-\frac{1}{p_1})\cdot(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k1})\cdot(1-\frac{1}{p_1})\cdot(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k2})$

因为 pq 互质，所以质因子互不相同。

性质5

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

n 的正因子（包括 1 和自身）的欧拉函数之和等于 n 。

如：$20=\varphi(1)+\varphi(2)+\varphi(4)+\varphi(5)+\varphi(10)+\varphi(20)=1+1+2+4+4+8$

证明：分数 $\frac{1}{n},\frac{2}{n},..,\frac{n}{n}$，共有 n个，且互不相等。化简这些分数，得到新的 n个分数，它们的分母和分子互质，形如 $\frac{a}{d}$， d | n且 a 与 d互质。在所有 n个分数中，分母为 d的分数，数量是 $\varphi(d)$。所有不同分母的分数，其总数是 $\sum_{d|n}\varphi(d)$，所以$n=\sum_{d|n}\varphi(d)$。

$\frac{1}{20},\frac{1}{10},\frac{3}{20},\frac{1}{5},\frac{1}{4},\frac{3}{10},\frac{7}{20},\frac{2}{5},\frac{9}{20},\frac{1}{2},\frac{11}{20},\frac{3}{5},\frac{13}{20},\frac{7}{10},\frac{3}{4},\frac{4}{5},\frac{17}{20},\frac{9}{10},\frac{19}{20},\frac{1}{1}$

2.欧拉函数的计算方法

根据$\varphi(n)=n\cdot(1-\frac{1}{p_1})\cdot(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k})$，求 n的质因子即可。

一开始 $ans=n$,找到第一个质因数 p_1 ,然后执行：

$ans=ans.(1-\frac{1}{p_1})=ans/p_1*(p_1-1)$

后面依次类推即可。

方法1：直接实现，时间 $O(n)$。

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

方法2：方法1的优化：

质因数的枚举到从 2到 $\sqrt{n}$即可，时间 $O(\sqrt{n})$ 。注意最后剩下的一定也是质数，不要忘了。

如n=34,最后剩下的是17。

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

进一步优化的话，可以先求出素数表。枚举 $\sqrt{n}$以内的素数（个数 x），$O(x)$。

方法3：递推法

求1到n的所有数的欧拉函数 $phi[i]$。类似筛法。时间 $O(nlgn)$

一开始令 $phi[i]=i$，如果在遍历过程中发现还是$phi[i]=i$，说明 i是一个素数，那么 i 的倍数 $i*j$ 的欧拉函数都要因为素数 i 而修改：

$phi[i \times j]=phi[i \times j](1-\frac{1}{i})$

```
    for(int i=1;i<=n;i++)phi[i]=i;
    for(int i=2;i<=n;i++){
        if(phi[i]==i){
            for(int j=1;j*i<=n;j++)
                phi[i*j]=phi[i*j]/i*(i-1);
        }
    }
```

方法4：线性筛（欧拉筛）求 $1..n$ 的欧拉函数

在欧拉筛求素数的基础上稍微修改即可：

```
#include<cstdio>
#include<iostream>
using namespace std;
const int N=1e7+10;
bool vis[N];
int prime[N],phi[N];
int n,cnt=0;
int main(){
    scanf("%d",&n);
    vis[1]=1;
    phi[1]=1;
    for(int i=2;i<=n;i++){
        if(!vis[i])prime[++cnt]=i,phi[i]=i-1;
        for(int j=1;j<=cnt&&i*prime[j]<=n;j++){
            vis[i*prime[j]]=1;
            if(i%prime[j]==0){phi[i*prime[j]]=phi[i]*prime[j];break;}
            else phi[i*prime[j]]=phi[i]*phi[prime[j]];
        }
    }
    for(int i=1;i<=n;i++)printf("%d : %d\n",i,phi[i]);
```

```
    return 0;
}
```

3.欧拉定理

对应任意互质的正整数 $a, m(m \geq 2)$ 有 $a^{\varphi(m)} \equiv 1 \pmod m$。

4.费马小定理

当 m为质数时，$\varphi(m) = m - 1$，所以有：$a^{m-1} \equiv 1 \pmod m$。

提示：$a^{m-2}. a \equiv 1 \pmod m$,可以求出 a 的逆元。

5.扩展欧拉定理（欧拉降幂）

扩展欧拉定理适用于模数较小，指数较大（如 $b = 10^{200000}$）的情况下，进行降幂操作。

$$a^b \bmod m = \begin{cases} a^{b \bmod \varphi(m) + \varphi(m)} \bmod m & b \geq \varphi(m) \\ a^{b \bmod \varphi(m)} \bmod m & gcd(a, m) = 1 \\ a^b \bmod m & b < \varphi(m) \end{cases}$$

第一种情况是一般情况。

第二种情况根据欧拉定理可以得到。 $a^{b \bmod \varphi(m) + \varphi(m)} \bmod m = a^{b \bmod \varphi(m)} \bmod \times a^{\varphi(m)} \bmod m$

后面是欧拉定理等于1。

第三种情况显然成立。

题目：

1.【P5091 【模板】扩展欧拉定理

题目描述

给你三个正整数，a, m, b，你需要求：$a^b \bmod m$

输入格式

一行三个整数，a, m, b

输出格式

一个整数表示答案

样例 #1

样例输入 #1

```
2 7 4
```

样例输出 #1

```
2
```

样例 #2

样例输入 #2

```
998244353 12345 98765472103312450233333333333
```

样例输出 #2

```
5333
```

提示

注意输入格式，a,m,b 依次代表的是底数、模数和次数

【样例 1 解释】
$2^4 \bmod 7 = 2$

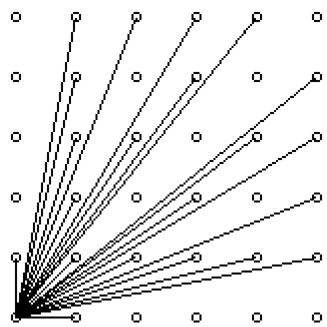
【数据范围】
对于 100% 的数据，$1\le a\le 10^9$，$1\le b\le 10^{20000000}$，$1\le m\le 10^8$。

参考代码

2.P2158[SDOI2008] 仪仗队

题目描述

作为体育委员，C 君负责这次运动会仪仗队的训练。仪仗队是由学生组成的 $N \times N$ 的方阵，为了保证队伍在行进中整齐划一，C 君会跟在仪仗队的左后方，根据其视线所及的学生人数来判断队伍是否整齐（如下图）。



现在，C 君希望你告诉他队伍整齐时能看到的学生人数。

输入格式

一行，一个正整数 N。

输出格式

输出一行一个数，即 C 君应看到的学生人数。

样例 #1

样例输入 #1

```
4
```

样例输出 #1

```
9
```

提示

对于 100% 的数据，$1 \le N \le 100000$。

分析

把左下角看做坐标原点，能看到的点：
$(1,0),(0,1),(1,1),(2,1),(1,2),(3,1),(1,3),(3,2),(2,3)$，$(x,y)$..

除了前3个点，其他点x和y是互质的，对称出现，所以答案是 $3+2(phi(2)+..+phi(n-1))$。

3.CF615D Multipliers

题面翻译

给你一个数，输出其所有因数的乘积。

这个数以质因子乘积的形式给出。

例如第一个样例 $2\times3=6$，6 的因子有$1,2,3,6$，故答案为 $1\times2\times3\times6=36$。

第二个样例 $2\times3\times2=12$，12 的因子有 $1,2,3,4,6,12$，故答案为
$1\times2\times3\times4\times6\times12=1728$。

由于答案可能过大，对 10^9+7 取模。

输入：

第一行一个正整数 n，代表质因子的个数

第二行 n 个正整数，为质因子。

注意同一个质因子可能出现多次。

输出：

其所有因子的乘积并取模。

题目描述

Ayrat has number n , represented as it's prime factorization p_i of size m , i.e. $n=p_{1}\cdot p_{2}\cdot...\cdot p_{m}$. Ayrat got secret information that that the product of all divisors of n taken modulo $10^{9}+7$ is the password to the secret data base. Now he wants to calculate this value.

输入格式

The first line of the input contains a single integer m ($1 <= m <= 200000$) — the number of primes in factorization of n .

The second line contains m primes numbers p_i ($2 <= p_i <= 200000$).

输出格式

Print one integer — the product of all divisors of n modulo $10^9 + 7$.

样例 #1

样例输入 #1

```
2
2 3
```

样例输出 #1

```
36
```

样例 #2

样例输入 #2

```
3
2 3 2
```

样例输出 #2

```
1728
```

提示

In the first sample $n = 2 \cdot 3 = 6$. The divisors of 6 are 1 , 2 , 3 and 6 , their product is equal to $1 \cdot 2 \cdot 3 \cdot 6 = 36$.

In the second sample $2 \cdot 3 \cdot 2 = 12$. The divisors of 12 are 1 , 2 , 3 , 4 , 6 and 12 . $1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 12 = 1728$.

题意

求n的所有因子的乘积。

分析：

求每个质因子的乘积的贡献。

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

通过一个具体实例：$n = 2^4 * 3^2 * 5^3$,观察总结。

对于每个质因子 p_i ,可能出现的指数次数：$1, 2, . . , a_i$ ，总的和为 $x = \frac{a_i(a_i+1)}{2}$。

p_i 以外其他质因子的贡献情况是：$y = \frac{(a_1+1)(a_2+1)..(a_k+1)}{a_i+1}$

所以 p_i对乘积的贡献是：

$p_i^{x.y}$

其中 y 的计算可以利用一个前缀积和后缀积。

然后利用欧拉降幂即可。这题的模MOD是质数，欧拉函数MOD-1。否则需要求。

注意数据类型。