数论初步

Author: 韩耀东

01 质数

02 约数

03 同余

质数的判定

试除法

若一个正整数N为合数，则存在一个能整除N的数T，其中 2<=T<=sqrt(N)

```
bool is_prime(int n){
    for(int i=2;i<=sqrt(n);i++)
        if(n % i == 0)return false;
    return true;
}
```

质数的筛选——Eratosthenes筛法

引子：给出正整数 n 和 m，区间$[n,m]$ 内的无平方因子的数有多少个？整数 p是无平方因子，当且仅当不存在 $k>1$，使得 p 是 k^2 的倍数。$(1\le n\le m\le 10^{12}, m-n\le 10^7)$

暴力是不可能暴力的

我们不是野蛮人

质数的筛选——Eratosthenes筛法

筛法思想：任意整数x 的倍数$2x, 3x, \cdots$ 都不是质数。

```
for(int i=2;i<=n;i++)
    for(int j=i*2;j<=n;j+=i) vis[j] = 1;
```

质数的筛选——Eratosthenes筛法

优化一：

不需要让每个数都被它的因数筛一次，如果这个数是合数，那么它的倍数其实已经被筛过了

```
for(int i=2;i<=n;i++)
    if(!vis[i])
    for(int j=i*2;j<=n;j+=i)vis[j] = 1;
```

质数的筛选——Eratosthenes筛法

优化二：

对于当前的一个数x，对于任意一个小于x^2的数，都已经被两个小于x的数 a,b筛选过了。所以我们从x^2开始筛选

```
for(int i=2;i<=n;i++)
    if(!vis[i])
    for(int j=i;j<=n/i;j++)vis[i*j] = 1;
```

质数的筛选——线性筛法

埃筛的复杂度为O(nlog(n)),已经是非常优秀的了。但是枚举几个例子就可以发现，它的筛选仍然有重复。例如12可以被2和3同时筛到。于是乎我们很有必要学一下线性筛法

线性筛法

提问一：如何做到线性？

提问二：每个合数可以被哪一种具有特殊意义的数来表示？

每个合数必有一个最大因子（不包括它本身），用这个因子把合数筛掉

换言之：每个合数必有一个最小质因子，用这个因数把合数筛掉

质数的筛选——线性筛法

```
int primes[N],v[N],m;
for(int i=2;i<=N;i++){
    if(!v[i])primes[++m] = i;
    for(int j=1;j<=m;j++){
        if(primes[j] > N/i)break;
        v[i*primes[j]] = 1;
        if(i%primes[j] == 0)break;
    }
}
```

质数的筛选——线性筛法

例题Prime Distance （POJ2689)

题意：给定两个整数L，R（$1 \le L \le R \le 2^{31}, R-L \le 10^6$），求闭区间$[L,R]$ 中相邻两个质数的差最大是多少，输出这两个质数

关键：R-L的范围很小，并且任何一个合数n必定包括一个不超过$\sqrt{n}$ 的质因子。

质数的筛选——线性筛法

例题 CF-1047C - Enlarge GCD

题意：给出n个正整数 $a_1, a_2, \cdots, a_n$ ，$(2 \le n \le 3 \cdot 10^5, q \le a_i \le 1.5 \cdot 10^7)$,求最少删除多少个数，可以使得gcd变大

关键：设原序列gcd为g，最大值为max 则遍历$g \sim max$ 中的每一个数，计算每一个数成为gcd所需要付出的代价，取一个最小值即可

有没有其他思路?

质因数分解

算术基本定理：

任何一个大于1的正整数都能唯一分解为有限个质数的乘积

$$N = p_1^{c_1} p_2^{c_2} \cdots p_m^{c_m}$$

试除法

扫描$2 \sim \lfloor \sqrt{N} \rfloor$ 的每个数d，若d能整除N，则从N中除掉所有的因子d，并且累计除去d的个数

质因数分解

```
//p[i]表示第i个质数
//c[i]表示第i个质数的指数
void divide(int n){
    m = 0;
    for(int i=2;i<=sqrt(n);i++){
        if(n % i == 0){
            p[++m] = i;c[m] =0;
            while(n % i == 0)n /= i, c[m]++;
        }
    }
    if(n > 1)p[++m] = n,c[m] = 1;
}
```

质因数分解

例题：阶乘分解（https://www.acwing.com/problem/content/description/199/ ）

分解$N!$ 的质因数 $(1 \le N \le 10^6)$

- 一个一个分解$O(N\sqrt{N})$
- 从每个质因数的角度考虑贡献有多少个
- 对于某一个质数 q 则$1 \sim N$ 中，p 的倍数， 则至少包含1个质因数 p 的显然有 $\lfloor N/q \rfloor$ 个。而p^2 的倍数，即至少包含2个质因数p的显然有$\lfloor N/p^2 \rfloor$个，不过其中一个已经在$\lfloor N/q \rfloor$ 里面统计过了，所以只需再加一次就好。
- 综上，N！ 中质因子p的个数为：
  - $\lfloor \frac{N}{p} \rfloor + \lfloor \frac{N}{p^2} \rfloor + \cdots + \lfloor \frac{N}{p^{log_p^N}} \rfloor = \Sigma_{p^k \le N} \lfloor \frac{N}{p^k} \rfloor$

01 质数

02 约数

03 同余

基本定理

唯一分解定理：$N = p_1^{c_1} p_2^{c_2} \cdots p_m^{c_m}$

约数个数

$$(c_1+1)*(c_2+1)*\cdots*(c_m+1) = \prod_{i=1}^{m}(c_i+1)$$

正约数和

$$(1+p_1+p_1^2+\cdots+p_1^{c_1})*\cdots*(1+p_m+p_m^2+p_m^{c_m}) = \prod_{i=1}^{m}(\Sigma_{j=0}^{c_i}(p_i)^j)$$

约数集合求法

- 试除法 $O(\sqrt{n})$

```
int factor[1600],m=0;
for(int i=1;i*i<=n;i++){
    if(n%i == 0){
        factor[++m] = i;
        if(i!=n/i)factor[++m] = n/i;
    }
}
```

推论：一个整数N的约数个数上限

约数集合求法

- 倍数法（基于埃筛思想）

```
vector<int> factor[500010];
for(int i=1;i<=n;i++)
    for(int j=1;j<=n/i;j++)
        factor[i*j].push_back(i);
```

可否想起西北校赛的某题呢?

约数集合例题

鸡尾酒被困入了一个迷宫！

这个迷宫总共有n个房间组成，鸡尾酒初始在1号房间，n号房间为迷宫的出口。每进入一次第i个房间都需要缴纳ai的过路费（包括初始的一号房间）。每个房间有一张纸条和一个箱子。纸条上写着的数字di代表鸡尾酒下一个可以到达的房间编号。

鸡尾酒也可以选择花费bi的金钱打开箱子，箱子中有一个密码ci，打开箱子之后鸡尾酒可以移动到i+k号房间，其中c可被k整除。但如果i+k>n，则不能移动。

求鸡尾酒从走出迷宫的最小花费。若鸡尾酒无法走出迷宫，输出-1。

把每个ci的约数集合求出来，然后跑最短路

最大公约数

$$gcd(a,b)=gcd(b,a-b)$$

$$gcd(a,b)=gcd(b,a\%b)$$

```
int gcd(int a,int b){
    return b?gcd(b,a%b):a;
}
```

最大公约数

例题：CF-1152C

题意：给定a, b,求一个 k 使得 $lcm(a+k, b+k)$ 最小。如果有多个答案，输出最小的一个 $1 \leq a, b \leq 10^9$

不妨假设 $a >= b$

$gcd(a, b) = gcd(b, a-b)$

又因为：$(a+k)-(b+k) = a-b$

故 $d = gcd(a+k, b+k) = gcd(b+k, a-b)$

其中 d 一定是 $a-b$ 的因数，枚举这个因数，然后求出一个最小的 k 使得 $b+k$ 是 d的倍数。然后计算当前的 lcm ，使得lcm最小的 k 即为答案

互质与欧拉函数

互质定义：$\forall a, b \in N$ 若 gcd(a,b) = 1,则称a,b互质。

欧拉函数：$1 \sim N$ 中与N互质的数的个数被称为欧拉函数，记为 $\psi(N)$

$$\psi(N) = N * \frac{p_1-1}{p_1} * \frac{p_2-1}{p_2} * \cdots * \frac{p_m-1}{p_m} = N * \prod_{\text{质数}p|N}(1 - \frac{1}{p})$$

互质与欧拉函数

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

互质与欧拉函数

1. 性质:

    - $\forall n > 1, 1 \sim n$ 中与n互质的数的和为$n * \psi(n)/2$
    - 若a，b互质，则$\psi(ab) = \psi(a)\psi(b)$
    - 若f 是积性函数，且在算术基本定理中 $n = \prod_{i=1}^{m} p_i^{c_i}$ ，则$f(n) = \prod_{i=1}^{m} f(p_i^{c_i})$
    - 若 $p|n$ 且 $p^2|n$ ，则 $\psi(n) = \psi(n/p) * p$
    - 若 $p|n$ 但 $n\%p^2! = 0$, 则 $\psi(n) = \psi(n/p) * (p-1)$
    - $\Sigma_{d|n}\psi(d) = n$

积性函数：如果当a，b互质时，有 $f(ab) = f(a) * f(b)$ 那么称函数 f 为积性函数

互质与欧拉函数

1. 性质:

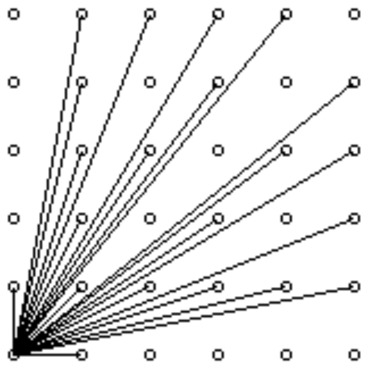
- $\forall n > 1, 1 \sim n$ 中与n互质的数的和为$n * \psi(n)/2$
- 若a，b互质，则$\psi(ab) = \psi(a)\psi(b)$
- 若f 是积性函数，且在算术基本定理中 $n = \prod_{i=1}^{m} p_i^{c_i}$ ，则$f(n) = \prod_{i=1}^{m} f(p_i^{c_i})$
- 若 $p|n$ 且 $p^2|n$ ，则 $\psi(n) = \psi(n/p) * p$
- 若 $p|n$ 但 $n\%p^2! = 0$, 则 $\psi(n) = \psi(n/p) * (p-1)$
- $\Sigma_{d|n}\psi(d) = n$

积性函数：如果当a，b互质时，有 $f(ab) = f(a) * f(b)$ 那么称函数 f 为积性函数

互质与欧拉函数

例题：Visible Lattice Point（POJ3090）

在一个平面直角坐标系的以（0，0）为左下角，（N，M）为右上角的矩形中，除了（0，0）之外，每个坐标上都插着一个钉子。一个钉子能被看到，当且仅当连接它和原点的线段上没有其他钉子。右图也画出了所有能看到的钉子以及视线。$1 \le N \le 1000$



- 除了$(1,0),(0,1),(1,1)$ 这三个钉子外，一个钉子(x,y)能被看到，当且仅当 $1 \le x,y \le N, x \ne y$ ，并且 $gcd(x,y) = 1$ 。
- $3 + 2 * \Sigma_{i=2}^{N} \psi(i)$

互质与欧拉函数

其实该题可以简化为求$1 \sim N$之间的欧拉函数，如果用Eratosthenes筛法，遇到一个质数时，将它的倍数进行计算（根据欧拉函数计算式）

```
for(int i=1;i<=1000;i++)phi[i] = i;
for(int i=2;i<=1000;i++){
    if(!v[i])
        for(int j=1;j*i<=1000;j++){
            v[i*j] = 1;
            phi[i*j] = phi[i*j] / i * (i-1);
        }
}
```

互质与欧拉函数

上述方法复杂度为$O(nlog(n))$, 有没有更快的呢? 类似于线性筛法的思想，借助欧拉函数的性质:

- 若 $p|n$ 且 $p^2|n$ ，则 $\psi(n) = \psi(n/p) * p$
- 若 $p|n$ 但 $n\%p^2! = 0$, 则 $\psi(n) = \psi(n/p) * (p-1)$

线性筛法中，每个合数n只会被它的最小质因子p筛一次。我们恰好可以在此时执行上述判断，由 $\psi(n/p)$ 递推到 $\psi(n)$

```
for(int i=2;i<=1000;i++){
    if(v[i] == 0){primes[++m] = i;phi[i] = i-1;}
    for(int j=1;j<=m;j++){
        if(primes[j] > 1000/i)break;
        v[primes[j] * i] = 1;
        phi[primes[j]*i] = phi[i] * (i % primes[j]?primes[j]-1 : primes[j]);
        if(i % primes[j] == 0)break;
    }
}
```

Here is the title

01 质数

02 约数

03 同余

同余

- 同余：若整数 a 和整数 b 除以正整数 m 的余数相等，则称 a,b 模 m 同余，记为 $a \equiv b(mod\ m)$
- 同余类：对于$\forall a \in [0, m-1]$，集合$a + km(k \in Z)$ 的所有数模 m 同余，余数都是 a。则称该集合为一个模 m 的同余类，简记为 $\bar{a}$
- 完全剩余系：模 m 的同余类一共有 m 个，分别为$\bar{0}, \bar{1}, \cdots, \overline{m-1}$ 。他们构成m的完全剩余系
- 简化剩余系：$1 \sim m$ 中与 m 互质的数代表的同余类共有 $\psi(m)$个，他们构成简化剩余系。
- 简化剩余系乘法封闭

同余

- 同余：若整数 a 和整数 b 除以正整数 m 的余数相等，则称 a,b 模 m 同余，记为 $a \equiv b(mod\ m)$
- 同余类：对于$\forall a \in [0, m-1]$，集合$a + km(k \in Z)$ 的所有数模 m 同余，余数都是 a。则称该集合为一个模 m 的同余类，简记为 $\bar{a}$
- 完全剩余系：模 m 的同余类一共有 m 个，分别为$\bar{0}, \bar{1}, \cdots, \overline{m-1}$。他们构成m的完全剩余系
- 简化剩余系：$1 \sim m$ 中与 m 互质的数代表的同余类共有 $\psi(m)$个，他们构成简化剩余系。
- 简化剩余系乘法封闭

欧拉定理

定理：若正整数 a，n互质，则 $a^{\psi(n)} \equiv 1 \pmod{n}$

当n为质数时，$\psi(n)$ 为 $n-1$，当a不为n的倍数时，a与n互质，故有欧拉定理成立：$a^{n-1} \equiv 1 \pmod{n}$ ，左右两边同乘a有$a^n \equiv a \pmod{n}$ 。当a为n的倍数时，该式依然成立

费马小定理：若 p 是质数，则对于任意整数a，有 $a^p \equiv a \pmod{p}$

例题 The Luckiest Number (POJ3696)

题意：给定一个正整数 L，$L \leq 2 * 10^9$ 。问至少多少个8练在一起组成的正整数是 L 的倍数?

欧拉定理

- x 个8连在一起的倍数为： $8*(10^x-1)/9$
- 求最小得x， 使得： $9L|8*(10^x-1)$
- 令 $d=gcd(8,L)$ 然后有：
  - $9L|8(10^x-1)$
    $\Leftrightarrow \frac{9L}{d}|10^x-1$
    $\Leftrightarrow 10^x\equiv 1 \pmod{\frac{9L}{d}}$

- 引理：若正整数a，n互质，则满足$a^x\equiv 1 \pmod n$ 的最小正整数 x_0 是 $\psi(n)$ 的约数。
  - 设$\psi(n)=qx_0+r(0<r<x_0)$
  - 因为 $a^x\equiv 1 \pmod n$，所以$a^{qx}\equiv 1 \pmod n$。根据欧拉定理，有 $a^{\psi(n)}\equiv 1 \pmod n$，所以$a^r\equiv 1 \pmod n$。这与$x_0$最小矛盾。故假设不成立，原命题成立

扩展欧几里得

已知a, b, c, 求x, y使得 $ax + by = c$

定理：对于任意整数a, b,存在一对整数x, y,满足 $ax + by = gcd(a, b)$

证明:

$ax + by = gcd(a, b)$

$gcd(b, a\%b) = gcd(a, b)$

$\Rightarrow bx + (a\%b)y = bx + (a - \lfloor a/b \rfloor * b)y = gcd(a, b) = ax + by$

可得：$ay + b(x - \lfloor a/b \rfloor * y) = bx + (a\%b)y$

带入原方程$ax_0 + by_0 = gcd(a, b)$ 可知$x_0 = y, y_0 = x - \lfloor a/b \rfloor * y$

扩展欧几里得

- 这个方程当且仅当$c\%gcd(a,b) == 0$时有解
- 求出$ax+by=gcd(a,b)$的一组解之后，当c为gcd的倍数时，$ax+by=c$的另一组解为：$(x_0*c/g,y_0*c/g)$，也就是都扩大c/g倍
- 通解：
  - $x=\frac{c}{d}x_0+k\frac{b}{d}$
  - $y=\frac{c}{d}y_0-k\frac{a}{d}$

```
int exgcd(int a,int b,int &x,int &y){
    if(b==0){x=1,y=0;return a;}
    int d = exgcd(b,a%b,x,y);
    int z=x;x=y;y=z-y*(a/b);
    return d;
}
```

乘法逆元

若整数 b,m 互质，并且 b|a, 则存在一个整数 x，使得 $a/b \equiv a * x \pmod{m}$ 。称 x 为 b 的 模 m 乘法逆元，记为 $b^{-1} \pmod{m}$。

- $b * b^{-1} \equiv 1 \pmod{m}$

解法一：

条件 : m为质数

由于 m 为质数，根据费马小定理：$b^{m-1} \equiv 1 \pmod{m}$

故：当模数 m 为质数时，b^{m-2} 即为 b 的乘法逆元

解法二：求解同余方程 $b * x \equiv 1 \pmod{m}$

该同余方程可以转换为：$b * x + m * y = 1$ 当且仅当$gcd(b, m) = 1$ 时有解

乘法逆元

例题：同余方程（NOIP2012）

题意：求关于x 的同余方程 $a * x \equiv 1 \pmod b$ 的最小正整数解。输入数据保证有解

例题：Sumdiv（POJ1845）

题意：求A^B 得所有约数之和 mod 9901 $(1 \leq A, B \leq 5 * 10^7)$

中国剩余定理

孙子定理

编辑 讨论

本词条由“科普中国”科学百科词条编写与应用工作项目 审核 。

孙子定理是中国古代求解一次同余式组（见同余）的方法。是数论中一个重要定理。又称中国余数定理。一元线性同余方程组问题最早可见于中国南北朝时期（公元5世纪）的数学著作《孙子算经》卷下第二十六题，叫做“物不知数”问题，原文如下：

有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何？即，一个整数除以三余二，除以五余三，除以七余二，求这个整数。《孙子算经》中首次提到了同余方程组问题，以及以上具体问题的解法，因此在中文数学文献中也会将中国剩余定理称为孙子定理。

例一：一个数，除以5余1，除以3余2。问这个数最小是多少？

一个一个试：1，6，11，16，21，26...

然后从小到大找除3余2的，发现最小的是11.

中国剩余定理

设 $m_1, m_2, \cdots, m_n$ 是两两互质得整数，$m = \prod_{i=1}^{n} m_i$ ，$M_i = m/m_i$,t_i 是线性同余方程 $M_i t_i \equiv 1 \pmod{m_i}$ 得一个解。对于任意的n 个整数 $a_1, a_2, \cdots, a_n$， 方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{1}$$

有整数解，解为 $x = \Sigma_{i=1}^{n} a_i M_i t_i$

证明：因为 $M_i = m/m_i$ 是除m_i 之外所有模数的倍数，所以
$\forall k \neq i, a_i M_i t_i \equiv 0 \pmod{m_k}$.又因为$a_i M_i t_i \equiv a_i \pmod{m_i}$，所以代入
$x = \Sigma_{i=1}^{n} a_i M_i t_i$，原方程组成立。

中国剩余定理

例题：Strange Way to Express Integers (POJ2891)

题意：给定2n个正整数：$a_1, a_2, \cdots a_n$ 和 $m_1, m_2, \cdots, m_n$ ，求一个最小的正整数x，满足 $\forall i \in [1, n],\ x \equiv a_i \pmod{m_i}$,或给出无解

因为m数组不一定满足两两互质，所以不能使用中国剩余定理。那么该怎么做呢?

- 对于 a_1, m_1 我们可以求出满足$x \equiv a_1 \pmod{m_1}$ 的通解 $a_1 + k * m_1$
- 对于$x \equiv a_2 \pmod{m_2}$ 我们可以求出一个 t 使得 $x = a_1 + t * m_1$ 满足前式，若没有，则无解。

以此类推，每一次都是求解一个同余方程，可用exgcd来求解

THANK YOU

Author: 韩耀东