数论基础

by zj (zj@webturing.com)

知识点概述

数论基础

- 数和进制
  - Definition k进制($k\geq 2$)数: $b_n,b_{n-1}....b_2b_1b_0$ （$b_n\neq 0$）每一位满足$0\leq b_i\leq k-1$ 是k的n次多项式 $b_nk^n+b_{n-1}k^{n-1}+....+b_1k+b_0$
  - Algorithm计算n长度 $\lceil \log_k^n \rceil$
  - Algorithm计算最后一位n%k /奇偶性 n%2
  - Algorithm计算第一位（方法 字符串/循环/数学方法）?
  - Algorithm计算各位数之和（逆转）
- 整除：合数和素数
  - Definition整除 如果整数 c,d,k 满足 $d=ck$ 称 c是d的因子，称c可以整除 d 记：$c\mid d$ 否则记做$c\nmid d$
  - Lemma :如果 $c\mid a,c\mid b$ 则有 $c\mid a\pm b$,$c\mid (a \mod b)$, $c\mid ab$, 特别的 $c^2\mid ab$
  - Lemma2: 如果 $c|d$ 则有 $\frac{d}{c}\mid d$
  - Lemma3: 自然数n的所有正因子数不超过 $\sqrt{n}$ 对
  - Lemma4: 平方数有奇数个因子（反之亦然）
  - Definition素数: 整数n 只有平凡因子1, n则称n为素数primer（质数）通常记p
  - Definition合数: 整数n至少还有一个非平凡因子则称n是合数
- 整数唯一分解定理
  - Definition 质数无限序列 $p_1=2,p_2=3,p_3=5,7,11,13,17,19,...,61,67,71,73,79,83,89,97.....$
  - Theorem唯一分解定理: 任何自然数n都可以对应唯一的非负序列 $k_1,k_2,....k_m$ 满足 $n=p_1{}^{k_1}p_2{}^{k_2}...p_m{}^{k_m}$
- 所有因子计算：
  - Algorithm暴力枚举1 $O(n)$
  - Algorithm优化枚举2 $O(\sqrt{n})$
  - Algorithm 利用整数的分解定理 $d(n)=(k_1+1)(k_2+1)....(k_n+1)$

公约数和公倍数

- Definition 最大公约数
  - 如果$c\mid a,c\mid b$ 称c是a,b的公因子（约数）(Common Divisor)
  - a,b最大的公因子(约数)(Greatest Common Divisor) 记做$gcd(a,b)$
  - Algorithm 欧几里得算法：$gcd(a,b)$

```
T gcd(T a,T b){
  if(b==0) return a;
  return gcd(b,a%b);
}
```

    - Algorithm ??计算N个数的最大公约数
- Definition 最小公倍数
    - 如果$c \mid a, d \mid a$ 称a是c, d的公倍数(Common Multiplier)
    - a,b所有公约数中最小的称为最小公倍数(Least Common Multiplier) 记做$lcm(a,b)$
    - Algorithm 计算两个数的最小公倍数
    - Algorithm 计算多个数的最小公倍数?
- Lemma:$gcd(a,b)*lcm(a,b)=ab$

素数

- 函数判断方法//$O(\sqrt{n})$

```
bool prime(int n){
    if(n==2)return true;
    if(n<2||n%2==0)return false;
    for(int n=3;n/i>=i;i+=2)
        if(n%i==0)return false;
    return true;
}
```

- 基本筛法//初始化$O(n\log\log n)$ 判定$O(1)$

```
const int N=1000+10;
bool prime[N];
void fill(){
    fill(prime+2,prime+N,true);
    for(int i=2;N/i>=i;i++)
        if(prime[i])for(int j=i*i;j<N;j+=i)prime[j]=false;
}
```

- 线性筛法

模算术（快速幂）

- Definition 模运算（同余）
    - $(a\pm b)\%M=(a\%M\pm b\%M)\%M$
    - $(ab)\%M=(a\%M)(b\%M)\%M$
- Definition 幂 $a^n=a^{n-1}a$
- Algorithm 快速幂（二分算法） $O(\log_2^n)$

```
const int M=1e9+7;
int mpower(int a,int b){
      a%=M;
      if(b==0||a==1)return 1;
      if(a==0||b==1)return a;
      if(b%2==0) return mpower(a*a%M,b/2);
      return (mpower(a*a%M,b/2)*a)%M;
}
```

矩阵及快速幂：

- $f_n = f_{n-1} + f_{n-2}$
- $n < 20$
-

典型习题

- 1150 进制转换
- 1065 欧几里得算法
- 1170 质因数分解
- 1024 因子个数

扩展

- 扩展欧几里得算法
- 中国剩余定理：韩信点兵
- 欧拉函数$\phi(x)$
- 分数/方程/同余方程/RSA