

数学模板使用建议

杨思逸

May 6, 2015

杂学

线性筛法

```
for (int i = 2; i < MAXN; ++i) {  
    if (is_prime[i]) {  
        prime.push_back(i);  
    }  
    for (int j = 0; j < (int)prime.size(); ++j) {  
        int p = prime[j];  
        if (p * i >= MAXN) {  
            break;  
        }  
        is_prime[p * i] = false;  
        if (i % p == 0) {  
            break;  
        }  
    }  
}
```

杂学

多项式插值

对于给定的 $n(n \leq 2 \times 10^9)$, 计算如下表达式对 10007 取模:

$$T = \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n \sum_{l=1}^n \sum_{m=1}^n |i-j| \times |j-k| \times |k-l| \times |l-m| \times |m-i|$$

来源: 2008 年 Dhaka 赛区 J 题

杂学

多项式插值

给定函数 $f(x)$ 在 $\{x_0, x_1, \dots, x_n\}$ 上的取值 $\{y_0, y_1, \dots, y_n\}$, 构造辅助函数

$$\eta_i = \frac{(x - x_0) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_n)}{(x_i - x_0) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_n)}$$

则多项式插值函数 $f^*(x) = \sum_{i=0}^n y_i \eta_i$ 是 $f(x)$ 在这 $n+1$ 个点上的拟合。

杂学

牛顿迭代

求函数 $f(x)$ 的根，对于初始解 x_0 不断进行 $x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$ 的迭代。

```
int square_root(int x) {  
    if (x == 0) {  
        return 0;  
    }  
    int root = 1, last = -1;  
    while (true) {  
        int next = (root + x / root) / 2;  
        if (next == last) {  
            return min(last, root);  
        }  
        last = root; root = next;  
    }  
}
```

杂学

扩展欧几里得

求 $an + bm = \gcd(n, m)$ 的所有整数解

```
int ex_gcd(int &a, int n, int &b, int m) {  
    if (m == 0) {  
        a = 1; b = 0;  
        return n;  
    }  
    int d = ex_gcd(b, m, a, n % m);  
    b -= n / m * a;  
    return d;  
}
```

有限域

求逆

求有限域 \mathbb{F}_p 上 x 的逆元（复杂度不清楚!!!）

```
int mul_mod(int a, int b, int m) {  
    return (long long) a * b % m;  
}
```

```
int inverse(int x, int m) {  
    assert(0 < x && x < m);  
    if (x == 1) {  
        return 1;  
    }  
    return mul_mod(m - m / x, inverse(m % x, m), m);  
}
```

有限域

Lucas 及 Wilson 定理

Theorem (Wilson)

$$\prod_{i=1}^{p-1} i = -1 \pmod{p}$$

Theorem (Lucas)

$$\binom{n}{m} = \binom{n_0}{m_0} \binom{n_1}{m_1} \cdots \binom{n_k}{m_k} \pmod{p}$$

其中 $\overline{n_0 n_1 \cdots n_k}, \overline{m_0 m_1 \cdots m_k}$ 分别为 n, m 的 p 进制表示。

有限域

离散对数及开根

对于方程 $a^x = b \pmod{p}$

1. 给定 a, b, p 求 x
2. 给定 x, b, p 求 a

有限域

离散对数及开根

对于方程 $a^x = b \pmod{p}$

1. 给定 a, b, p 求 x
2. 给定 x, b, p 求 a

折半搜索

有限域

二次剩余

在有限域 \mathbb{F}_p 上求 \sqrt{x}

矩阵

高斯消元

给一个整数集合 $\{a_0, a_1, \dots, a_n\}$, 求其中异或和小于 m 的子集个数

来源: 2014 年校选某题

矩阵

高斯消元改

给一个无向图，求生成树个数对 m 取模

矩阵

高斯消元改

给一个无向图，求生成树个数对 m 取模
辗转相除

矩阵

最小二乘法

求方程组 $Ax = b$ 在 2 范数下的最优近似解

矩阵

最小二乘法

求方程组 $Ax = b$ 在 2 范数下的最优近似解

$$A^t Ax = A^t b$$

矩阵

最小二乘法

求 $\arg \min \|Ax - b\|_2$, 若有多组 x 满足, 取其中 $\|x\|_2$ 最小的
来源: Ural 1668

FFT

基本原理

多项式 $f(x), g(x)$ 相乘

1. 基底变换
2. 复数域上的原根
3. 变换矩阵求逆
4. 精度问题

FFT

离散版本

1. 原根 g 的次幂互不相同
2. 原根 g 的 n 次幂为单位元
3. 精度问题
4. 原根参考 $(31, 15 \times 2^{27} + 1), (10, 3 \times 2^{18} + 1)$

FFT

花式应用

给定母串 S 和模式串 T ，只包含 $0, 1$ 和通配符 $?$ ，求所有匹配位置

来源：某老毛子题

FFT

花式应用

给 2^n 个变量 x_i ，求问自运算一次以后的结果，运算定义为

$$x_i * x_j \rightarrow_+ x_{i|j}$$

来源：某新毛子题

作业

1. degree of an algebraic number
2. fibonacci gcd again