

多项式 2

FFT

算法简介

$O(n \log n)$ 时间实现多项式点值表示法与系数表示法之间的转化，主要用于加速多项式乘法。

算法实现

假设 $f(x)$ 为 $n-1$ 次多项式，且 n 是 2 的幂次。(如果不满足条件可以将高次系数视为 0)

快速傅里叶变换

考虑如何实现 $O(n \log n)$ 时间根据多项式系数表示法得到多项式点值表示法。

设 $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$

构造辅助函数 $g(x) = a_0 + a_2x + \dots + a_{n-2}x^{\frac{n-2}{2}}$, $h(x) = a_1 + a_3x + \dots + a_{n-1}x^{\frac{n-1}{2}}$

于是有 $f(x) = g(x^2) + xh(x^2)$

记 $\omega_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ 将 $x = \omega_n^k, x = \omega_n^{k+\frac{n}{2}}$ ($k=0, 1, \dots, \frac{n-1}{2}$) 代入，有

$$f(\omega_n^k) = g(\omega_n^{2k}) + \omega_n^{kh}(\omega_n^{2k}) = g(\omega_{\frac{n}{2}}^k) + \omega_n^{kh}(\omega_{\frac{n}{2}}^k)$$

$$f(\omega_n^{k+\frac{n}{2}}) = g(\omega_n^{2k+n}) + \omega_n^{k+\frac{n}{2}}h(\omega_n^{2k+n}) = g(\omega_{\frac{n}{2}}^k) - \omega_n^{kh}(\omega_{\frac{n}{2}}^k)$$

于是根据 $g(x)$ 的点值表示法 $\{g(\omega_{\frac{n}{2}}^k) | k=0, 1, \dots, \frac{n-1}{2}\}$ 和 $h(x)$ 的点值表示法 $\{h(\omega_{\frac{n}{2}}^k) | k=0, 1, \dots, \frac{n-1}{2}\}$

可以 $O(n)$ 时间计算出 $f(x)$ 的点值表示法 $\{f(\omega_n^k) | k=0, 1, \dots, n-1\}$ 考虑分治算法，即可 $O(n \log n)$ 解决上述问题。

递归边界为当分治到多项式只剩下一个常数项时，多项式点值表示法即为系数表示法，于是直接返回。

快速傅里叶逆变换

考虑如何实现 $O(n \log n)$ 时间根据多项式系数点值法得到多项式系数表示法。

记 $y_i = f(\omega_n^i)$ 假设 $f(x)$ 系数表示法为 $\{a_0, a_1, \dots, a_{n-1}\}$ 点值表示法为

$$\mathcal{F}\{(\omega_n^0, y_0), (\omega_n^1, y_1) \cdots (\omega_n^{n-1}, y_{n-1})\}$$

构造多项式 $A(x) = \sum_{i=0}^{n-1} y_i x^i$ 将 $x = \omega_n^{-k} (k=0, 1, \dots, n-1)$ 代入，有

$$A(\omega_n^{-k}) = \sum_{i=0}^{n-1} \omega_n^{-ki} \sum_{j=0}^{n-1} a_j \omega_n^{ij} = \sum_{j=0}^{n-1} a_j \sum_{i=0}^{n-1} \omega_n^{i(j-k)}$$

如果 $j=k$ 则 $\sum_{i=0}^{n-1} \omega_n^{i(j-k)} = \sum_{i=0}^{n-1} 1 = n$

如果 $j \neq k$ 则 $\sum_{i=0}^{n-1} \omega_n^{i(j-k)} = \frac{\omega_n^{n(j-k)} - 1}{\omega_n^{j-k} - 1} = \frac{1 - 1}{\omega_n^{j-k} - 1} = 0$

于是有 $A(\omega_n^{-k}) = na_k$ 考虑快速傅里叶变换计算 $A(x)$ 的点值表示法即可快速解决上述问题。

递归版 FFT 板子

```
complex temp[MAXN<<2];
void FFT(complex *f, int n, int type) { // type=1 为正变换, type=-1 为逆变换, 逆变换最终结果需要除以n
    if (n==1) return;
    int m=n>>1;
    memcpy(temp, f, sizeof(complex)*n);
    for (int i=0; i<n; i+=2)
        f[i>>1] = temp[i], f[(i>>1)+m] = temp[i+1];
    complex *f1=f, *f2=f+m;
    FFT(f1, m, type); FFT(f2, m, type);
    complex cur(1.0, 0.0), w(cos(2.0*pi/n), type*sin(2.0*pi/n));
    for (int i=0; i<m; i++) {
        temp[i] = f1[i] + cur*f2[i];
        temp[i+m] = f1[i] - cur*f2[i];
        cur = cur*w;
    }
    memcpy(f, temp, sizeof(complex)*n);
}
```

算法优化

蝴蝶变换

考虑倍增模拟分治过程，于是需要调整运算顺序。观察下面分治过程

$$\{x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$$

$$\{x_0, x_2, x_4, x_6\}, \{x_1, x_3, x_5, x_7\}$$

$$\{x_0, x_4\}, \{x_2, x_6\}, \{x_1, x_5\}, \{x_3, x_7\}$$

$\{x_0\}, \{x_4\}, \{x_2\}, \{x_6\}, \{x_1\}, \{x_5\}, \{x_3\}, \{x_7\}$

发现将 x_i 的下标用二进制表示，然后将其翻转就可以得到 x_i 的最终位置。例如 $3=011, 6=110$ ，于是 x_3 与 x_6 位置互换。

非递归版 FFT 板子

```
int rev[MAXN<<2];
int build(int k){
    int n, pos=0;
    while((1<<pos)<=k) pos++;
    n=1<<pos;
    _for(i, 0, n) rev[i]=(rev[i>>1]>>1)|((i&1)<<(pos-1));
    return n;
}
void FFT(complex *f, int n, int type){
    _for(i, 0, n) if(i<rev[i])
        swap(f[i], f[rev[i]]);
    complex t1, t2;
    for(int i=1; i<n; i<=1){
        complex w(cos(pi/i), type*sin(pi/i));
        for(int j=0; j<n; j+=(i<<1)){
            complex cur(1.0, 0.0);
            _for(k, j, j+i){
                t1=f[k], t2=cur*f[k+i];
                f[k]=t1+t2, f[k+i]=t1-t2;
                cur=cur*w;
            }
        }
    }
    if(type== -1) _for(i, 0, n)
        f[i].x/=n;
}
```

算法练习

[洛谷p3803](#)

题意

给定两个多项式的系数表示法，求两个多项式乘积的系数表示法。

题解

记这两个多项式为 $g(x)=b_0+b_1x+\dots+b_nx^n, h(x)=c_0+c_1x+\dots+c_mx^m$ 所求多项式为 $f(x)=a_0+a_1x+\dots+a_{n+m}x^{n+m}$

设 s^s 是 2^s 的幂次且 $\frac{s^2}{n+m} \leq s$

对 $g(x) = b_0 + b_1x + \dots + b_nx^n + 0x^{n+1} + \dots + 0x^{s-1}$ 套用快速傅里叶变换求出点值表示法 $\{(w_s^0, g_0), \dots, (w_s^{s-1}, g_{s-1})\}$

同样对 $h(x)$ 进行上述操作，于是得到 $f(x)$ 的点值表示法 $\{(w_s^0, g_0h_0), \dots, (w_s^{s-1}, g_{s-1}h_{s-1})\}$

再根据快速傅里叶逆变换，即可得到 $f(x)$ 的系数表示法，时间复杂度 $O(s \log s)$

```
const int MAXN=1e6+5;
const double pi=acos(-1.0);
struct complex{
    double x,y;
    complex(double x=0.0,double y=0.0):x(x),y(y){}
    complex operator + (const complex &b){
        return complex(x+b.x,y+b.y);
    }
    complex operator - (const complex &b){
        return complex(x-b.x,y-b.y);
    }
    complex operator * (const complex &b){
        return complex(x*b.x-y*b.y,x*b.y+y*b.x);
    }
}a[MAXN<<2],b[MAXN<<2];
int rev[MAXN<<2];
int build(int k){
    int n,pos=0;
    while((1<<pos)<=k)pos++;
    n=1<<pos;
    _for(i,0,n)rev[i]=(rev[i>>1]>>1)|((i&1)<<(pos-1));
    return n;
}
void FFT(complex *f,int n,int type){
    _for(i,0,n)if(i<rev[i])
        swap(f[i],f[rev[i]]);
    complex t1,t2;
    for(int i=1;i<n;i<=1){
        complex w(cos(pi/i),type*sin(pi/i));
        for(int j=0;j<n;j+=(i<<1)){
            complex cur(1.0,0.0);
            _for(k,j,j+i){
                t1=f[k],t2=cur*f[k+i];
                f[k]=t1+t2,f[k+i]=t1-t2;
                cur=cur*w;
            }
        }
    }
    if(type==-1)_for(i,0,n)
        f[i].x/=n;
```

```

}
int main()
{
    int n1=read_int(),n2=read_int(),n=build(n1+n2);
    _rep(i,0,n1)
    a[i].x=read_int();
    _rep(i,0,n2)
    b[i].x=read_int();
    FFT(a,n,1);FFT(b,n,1);
    _for(i,0,n)
    a[i]=a[i]*b[i];
    FFT(a,n,-1);
    _rep(i,0,n1+n2)
    space((int)(a[i].x+0.5));
    return 0;
}

```

优化

考虑式子 $\left|g(x)+h(x)\right|^2=g^2(x)+h^2(x)+2g(x)h(x)$

于是将 $g(x)$ 作为实部， $h(x)$ 作为虚部，两次 FFT 计算出 $\left|g(x)+h(x)\right|^2$ 表达式系数，即可得到 $f(x)$ 系数。

```

const int MAXN=1e6+5;
const double pi=acos(-1.0);
struct complex{
    double x,y;
    complex(double x=0.0,double y=0.0):x(x),y(y){}
    complex operator + (const complex &b){
        return complex(x+b.x,y+b.y);
    }
    complex operator - (const complex &b){
        return complex(x-b.x,y-b.y);
    }
    complex operator * (const complex &b){
        return complex(x*b.x-y*b.y,x*b.y+y*b.x);
    }
}a[MAXN<<2];
int rev[MAXN<<2];
int build(int k){
    int n,pos=0;
    while((1<<pos)<=k)pos++;
    n=1<<pos;
    _for(i,0,n)rev[i]=(rev[i>>1]>>1)|((i&1)<<(pos-1));
    return n;
}
void FFT(complex *f,int n,int type){
    _for(i,0,n)if(i<rev[i])

```

```
swap(f[i],f[rev[i]]);
complex t1,t2;
for(int i=1;i<n;i<=1){
    complex w(cos(pi/i),type*sin(pi/i));
    for(int j=0;j<n;j+=(i<=1)){
        complex cur(1.0,0.0);
        _for(k,j,j+i){
            t1=f[k],t2=cur*f[k+i];
            f[k]=t1+t2,f[k+i]=t1-t2;
            cur=cur*w;
        }
    }
}
if(type==-1)_for(i,0,n)
f[i].y/=n;
}
int main()
{
    int n1=read_int(),n2=read_int(),n=build(n1+n2);
    _rep(i,0,n1)
a[i].x=read_int();
    _rep(i,0,n2)
a[i].y=read_int();
    FFT(a,n,1);
    _for(i,0,n)
a[i]=a[i]*a[i];
    FFT(a,n,-1);
    _rep(i,0,n1+n2)
space((int)(a[i].y/2+0.5));
    return 0;
}
```

应用

洛谷p1919

进行高精度乘法时，将 10 进制数视为 $x=10$ 多项式，进行多项式乘法后考虑进位情况即可。

```
const int MAXN=1e6+5;
const double pi=acos(-1.0);
struct complex{
    double x,y;
    complex(double x=0.0,double y=0.0):x(x),y(y){}
    complex operator + (const complex &b){
        return complex(x+b.x,y+b.y);
    }
    complex operator - (const complex &b){
        return complex(x-b.x,y-b.y);
    }
}
```

```

    }
    complex operator * (const complex &b){
        return complex(x*b.x-y*b.y,x*b.y+y*b.x);
    }
}a[MAXN<<2],b[MAXN<<2];
int rev[MAXN<<2];
int build(int k){
    int n,pos=0;
    while((1<<pos)<=k)pos++;
    n=1<<pos;
    _for(i,0,n)rev[i]=(rev[i>>1]>>1)|((i&1)<<(pos-1));
    return n;
}
void FFT(complex *f,int n,int type){
    _for(i,0,n)if(i<rev[i])
        swap(f[i],f[rev[i]]);
    complex t1,t2;
    for(int i=1;i<n;i<<=1){
        complex w(cos(pi/i),type*sin(pi/i));
        for(int j=0;j<n;j+=(i<<1)){
            complex cur(1.0,0.0);
            _for(k,j,j+i){
                t1=f[k],t2=cur*f[k+i];
                f[k]=t1+t2,f[k+i]=t1-t2;
                cur=cur*w;
            }
        }
    }
    if(type==-1)_for(i,0,n)
        f[i].x/=n;
}
char s1[MAXN<<2],s2[MAXN<<2];
int ans[MAXN<<2];
int main()
{
    scanf("%s%s",s1,s2);
    int n1=strlen(s1)-1,n2=strlen(s2)-1,n=build(n1+n2);
    _rep(i,0,n1)
        a[i].x=s1[n1-i]-'0';
    _rep(i,0,n2)
        b[i].x=s2[n2-i]-'0';
    FFT(a,n,1);FFT(b,n,1);
    _for(i,0,n)
        a[i]=a[i]*b[i];
    FFT(a,n,-1);
    _for(i,0,n){
        ans[i]+=(int)(a[i].x+0.5);
        ans[i+1]+=ans[i]/10;
        ans[i]%=10;
    }
    while(n>=0&&!ans[n])n--;
}

```

```
if(n==-1) putchar('0');  
else  
while(n>=0) putchar(ans[n--]+'0');  
return 0;  
}
```

NTT

算法简介

$O(n \log n)$ 时间实现多项式特定模数意义下的点值表示法与系数表示法之间的转化，无精度误差。

理论基础

阶

定义

设 $n > 1, \gcd(a, n) = 1$ 称 $a^x \equiv 1 \pmod n$ 的最小正整数解为 a 对 n 的阶，记为 $\delta_n(a)$

性质

设 $a^x \equiv 1 \pmod n$ 则 $\delta_n(a) \mid x$ 特别的 $\delta_n(a) \mid \varphi(n)$

原根

定义

如果 (n, a) 满足 $a > 1, \delta_n(a) = \varphi(n)$ 则称 a 为 n 的原根。

性质

1. 一个正整数 n 具有原根的充要条件为 $n = 2, 4, p^\alpha, 2p^\alpha$ 其中 p 为素数
2. 如果 n 具有原根，则 n 具有 $\varphi(\varphi(n))$ 个原根
3. 如果 g 为 n 的原根，则 $1, g^1, g^2 \cdots g^{\varphi(n)}$ 构成 n 的最简剩余系
4. 设 $\varphi(n) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 且 $n \nmid a^{\frac{\varphi(n)}{p_i}} - 1 (i = 1, 2, \cdots, k)$ 则 a 为 n 的原根

算法实现

当模数是素数 p 时，记 $\omega_n \equiv g^{\frac{p-1}{n}} \pmod p$ 发现 ω_n 满足以下性质

1. $\omega_n^{2k} = \omega_{\frac{n}{2}}^k$
2. $\omega_n^{k+\frac{n}{2}} \equiv -\omega_n^k \pmod p$
3. $\sum_{i=0}^{p-1} \omega_n^i \equiv 0 \pmod p$

于是考虑用 $g^{\frac{p-1}{n}}$ 替代 FFT 中的 ω_n 其余过程与 FFT 类同。

注意算法过程中需要保证 $\frac{p-1}{n}$ 为整数，故需要选择含 2 的幂次较多的模数 p

一般常见模数为 $998244353, 1004535809, 469762049$ ，这三个数的原根均包含 3 。

```

const int MAXN=1e6+5,Mod=998244353,G=3,Inv_G=332748118;
int rev[MAXN<<2];
int build(int k){
    int n,pos=0;
    while((1<<pos)<=k)pos++;
    n=1<<pos;
    _for(i,0,n)rev[i]=(rev[i>>1]>>1)|((i&1)<<(pos-1));
    return n;
}
void NTT(int *f,int n,int type){
    _for(i,0,n)if(i<rev[i])
        swap(f[i],f[rev[i]]);
    int t1,t2;
    for(int i=1;i<n;i<<=1){
        int w=quick_pow(type==1?G:Inv_G,(Mod-1)/(i<<1));
        for(int j=0;j<n;j+=(i<<1)){
            int cur=1;
            _for(k,j,j+i){
                t1=f[k],t2=1LL*cur*f[k+i]%Mod;
                f[k]=(t1+t2)%Mod,f[k+i]=(t1-t2)%Mod;
                cur=1LL*cur*w%Mod;
            }
        }
    }
    if(type==-1){
        int div=quick_pow(n,Mod-2);
        _for(i,0,n)
            f[i]=(1LL*f[i]*div%Mod+Mod)%Mod;
    }
}

```

MTT

[洛谷p4245](#)

算法简介

$O(n \log n)$ 时间实现多项式任意模数意义下乘法。

算法实现

三模数NTT

设所求多项式系数表示法为 $\{a_0, a_1 \dots a_{n-1}\}$ 考虑取用三个不同的大模数 $469762049, 998244353, 1004535809$ 。

跑三轮 NTT 可以得到三组同余方程，利用中国剩余定理将同余方程合并，可以得到 $a_i \equiv b_i \pmod{471064322751194440790966273}$

如果 $0 \leq a_i \leq 10^{26} \ll 471064322751194440790966273$ 显然有 $a_i = b_i$

设两条多项式的最高次幂为 n 系数最大值为 v 则两多项式相乘得到的多项式的最大系数不超过 $(n+1)v^2$

故绝大多数题目的数据范围都满足上述约束条件。

关于同余方程的合并，为防止整型溢出，考虑先合并其中两条，设结果为 $a_i \equiv A \pmod{M}$ 令 $a_i = A + MK$ 代入第三条同余方程。

于是有 $A + MK \equiv t \pmod{m}$ 移项，得 $K \equiv (t - A)M^{-1} \pmod{m}$

由此解得 A 与 K 后即可在乘法不溢出得情况下计算 a_i 在给定模数意义下的结果。

```
const int m[3]={469762049,998244353,1004535809},G=3;
int rev[MAXN<<2];
LL mul(LL a,int b,LL mod){
    LL ans=0;
    while(b){
        if(b&1)
            ans=(ans+a)%mod;
        b>>=1;
        a=(a<<1)%mod;
    }
    return ans;
}
void NTT(int *f,int n,int type,int mod){
    _for(i,0,n)if(i<rev[i])
        swap(f[i],f[rev[i]]);
    int t1,t2,Inv_G=quick_pow(G,mod-2,mod);
    for(int i=1;i<n;i<=<1){
        int w=quick_pow(type==1?G:Inv_G,(mod-1)/(i<<1),mod);
        for(int j=0;j<n;j+=(i<<1)){
            int cur=1;
            _for(k,j,j+i){
```

```

        t1=f[k],t2=1LL*cur*f[k+i]%mod;
        f[k]=(t1+t2)%mod,f[k+i]=(t1-t2)%mod;
        cur=1LL*cur*w%mod;
    }
}
}
if(type==-1){
    int div=quick_pow(n,mod-2,mod);
    _for(i,0,n)
        f[i]=(1LL*f[i]*div%mod+mod)%mod;
}
}
int f2[MAXN<<2],g2[MAXN<<2],temp[3][MAXN<<2];
void MTT(int *f,int n1,int *g,int n2,int *ans,int mod){
    int n=build(n1+n2);
    _for(i,0,3){
        memcpy(f2,f,sizeof(f2));memcpy(g2,g,sizeof(g2));
        NTT(f2,n,1,m[i]);NTT(g2,n,1,m[i]);
        _for(j,0,n)temp[i][j]=1LL*f2[j]*g2[j]%m[i];
        NTT(temp[i],n,-1,m[i]);
    }
    LL A,K,M=1LL*m[0]*m[1];
    int
    inv1=quick_pow(m[1],m[0]-2,m[0]),inv2=quick_pow(m[0],m[1]-2,m[1]),inv3=quick
    _pow(M%m[2],m[2]-2,m[2]);
    _rep(i,0,n1+n2){
A=(mul(1LL*temp[0][i]*m[1]%M,inv1,M)+mul(1LL*temp[1][i]*m[0]%M,inv2,M))%M;
        K=((temp[2][i]-A)%m[2]+m[2])%m[2]*inv3%m[2];
        ans[i]=(((K%mod)*(M%mod)+A%mod)%mod+mod)%mod;
    }
}
}

```

拆系数FFT

From:

<https://wiki.cvbbacm.com/> - CVBB ACM Team

Permanent link:

https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:legal_string;jxm2001:%E5%A4%9A%E9%A1%B9%E5%BC%8F_2&rev=1596614518

Last update: 2020/08/05 16:01