# **从多项式乘法到快速傅里叶变换**

[April 25, 2015](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform)  [miskcoo](http://blog.miskcoo.com/author/miskcoo)  [Algorithm](http://blog.miskcoo.com/category/algorithm), [Math](http://blog.miskcoo.com/category/math)

**Contents**[[hide](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform)]

* [1 概述](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i)
* [2 准备知识](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-2)
  + [2.1 多项式](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-3)
    - [2.1.1 多项式的系数表示法](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-4)
    - [2.1.2 多项式的点值表示法](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-5)
  + [2.2 复数](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-6)
    - [2.2.1 单位根](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-7)
* [3 多项式的乘法](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-8)
* [4 快速傅里叶变换](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-9)
  + [4.1 Cooley-Tukey算法](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "Cooley-Tukey)
  + [4.2 傅里叶逆变换（IDFT）](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "IDFT)
  + [4.3 算法实现](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-10)
    - [4.3.1 递归实现](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-11)
    - [4.3.2 迭代实现](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-12)
* [5 快速数论变换](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-13)
  + [5.1 原根](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-14)
  + [5.2 模数任意的解决方案](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-15)
  + [5.3 代码实现](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-16)
* [6 应用](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-17)
  + [6.1 快速卷积](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-18)
    - [6.1.1 例1：[ZJOI2014]力](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "1ZJOI2014)
  + [6.2 生成函数运算](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-19)
    - [6.2.1 例2：[BZOJ3771]Triple](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "2BZOJ3771Triple)
  + [6.3 多项式求逆、除法、取模](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-20)
  + [6.4 多项式多点求值和快速插值](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "i-21)

## **概述**

计算多项式的乘法，或者计算两个大整数的乘法是在计算机中很常见的运算，如果用普通的方法进行，复杂度将会是 O(n2)O(n2) 的，还有一种分治乘法，可以做到 O(nlog23)O(nlog2⁡3) 时间计算（可以看[这里](http://blog.miskcoo.com/2014/10/karatsuba-multiplication)）。下面从计算多项式的乘法出发，介绍****快速傅里叶变换****（Fast Fourier Transform, FFT）如何在 O(nlogn)O(nlog⁡n) 的时间内计算出两个多项式的乘积

## **准备知识**

这里介绍一些后面可能会用到的知识（主要是关于多项式、卷积以及复数的），如果你已经知道觉得它太水了或者想用到的时候再看就跳过吧

### **多项式**

简单来说，形如 a0+a1X+a2X2+⋯+anXna0+a1X+a2X2+⋯+anXn 的代数表达式叫做****多项式****，可以记作P(X)=a0+a1X+a2X2+⋯+anXnP(X)=a0+a1X+a2X2+⋯+anXn，a0,a1,⋯,ana0,a1,⋯,an 叫做多项式的****系数****，XX 是一个不定元，不表示任何值，不定元在多项式中最大项的次数称作多项式的****次数****

#### **多项式的系数表示法**

像刚刚我们提到的那些多项式，都是以系数形式表示的，也就是将 nn 次多项式 A(x)A(x) 的系数 a0,a1,⋯,ana0,a1,⋯,an 看作 n+1n+1 维向量 a⃗ =(a0,a1,⋯,an)a→=(a0,a1,⋯,an)，其****系数表示****（coefficient representation）就是向量 a⃗ a→

#### **多项式的点值表示法**

如果选取 n+1n+1 个****不同****的数 x0,x1,⋯,xnx0,x1,⋯,xn 对多项式进行求值，得到 A(x0),A(x1),⋯,A(xn)A(x0),A(x1),⋯,A(xn)，那么就称 {(xi,A(xi)):0≤i≤n,i∈Z}{(xi,A(xi)):0≤i≤n,i∈Z} 为多项式 A(x)A(x) 的****点值表示****（point-value representation）

多项式 A(x)A(x) 的点值表示不止一种，你只要选取不同的数就可以得到不同的点值表示，但是任何一种点值表示都能唯一确定一个多项式，为了从点值表示转换成系数表示，可以直接通过****插值****的方法

### **复数**

后面提到的 ii，除非作为 ∑∑ 求和的变量，其余的都表示虚数单位 −1−−−√−1

#### **单位根**

nn 次单位根是指能够满足方程 zn=1zn=1 的复数，这些复数一共有 nn 个它们都分布在复平面的单位圆上，并且构成一个正 nn 边形，它们把单位圆等分成 nn 个部分

根据复数乘法相当于模长相乘，幅角相加就可以知道，nn 次单位根的模长一定是 11，幅角的 nn倍是 00

这样，nn 次单位根也就是

e2πkin,k=0,1,2,⋯,n−1e2πkin,k=0,1,2,⋯,n−1

再根据欧拉公式

eθi=cosθ+isinθeθi=cos⁡θ+isin⁡θ

就可以知道 nn 次单位根的算术表示

如果记 ωn=e2πinωn=e2πin，那么 nn 次单位根就是 ω0n,ω1n,⋯,ωn−1nωn0,ωn1,⋯,ωnn−1

## **多项式的乘法**

给定两个多项式 A(x),B(x)A(x),B(x)

A(x)=∑i=0naixi=anxn+an−1xn−1+⋯+a1x+a0B(x)=∑i=0nbixi=bnxn+bn−1xn−1+⋯+b1x+b0A(x)=∑i=0naixi=anxn+an−1xn−1+⋯+a1x+a0B(x)=∑i=0nbixi=bnxn+bn−1xn−1+⋯+b1x+b0

将这两个多项式相乘得到 C(x)=∑2ni=0cixiC(x)=∑i=02ncixi，在这里

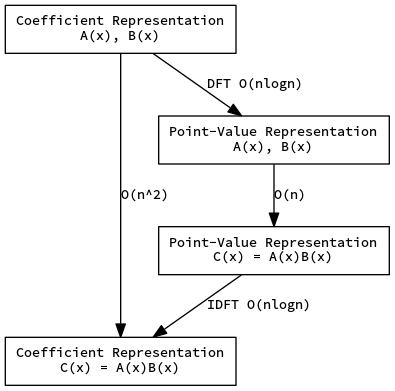
ci=∑j+k=i,0≤j,k≤najbkxici=∑j+k=i,0≤j,k≤najbkxi

如果一个个去算 cici 的话，要花费 O(n2)O(n2) 的时间才可以完成，但是，这是在系数表示下计算的，如果转换成点值表示，知道了 A(x),B(x)A(x),B(x) 的点值表示后，由于只有 n+1n+1 个点，就可以直接将其相乘，在 O(n)O(n) 的时间内得到 C(x)C(x) 的点值表示

如果能够找到一种有效的方法帮助我们在多项式的点值表示和系数表示之间转换，我们就可以快速地计算多项式的乘法了，快速傅里叶变换就可以做到这一点

## **快速傅里叶变换**

快速傅里叶变换你可以认为有两个部分，DFT 和 IDFT，分别可以在 O(nlogn)O(nlog⁡n) 的时间内将多项式的系数表示转化成点值表示，并且转回来，就像下面这张图所示



### **Cooley-Tukey算法**

FFT 最常见的算法是 Cooley-Tukey 算法，它的基本思路在 1965 年由 J. W. Cooley 和 J. W. Tukey 提出的，它是一个基于分治策略的算法

假设现在有一个 n−1n−1 次多项式 A(x)=∑n−1i=0aixiA(x)=∑i=0n−1aixi（为了方便，假设 n=2m,m∈Zn=2m,m∈Z，如果不足可以在高次项系数补成 00）

将 nn 个 nn 次单位根 ω0n,ω1n,⋯,ωn−1nωn0,ωn1,⋯,ωnn−1 带入 A(x)A(x) 将其转换成点值表达

A(ωkn)=∑i=0n−1aiωki,k=0,1,⋯,n−1A(ωnk)=∑i=0n−1aiωki,k=0,1,⋯,n−1

点值向量 y⃗ =(A(ω0n),A(ω1n),⋯,A(ωn−1n))y→=(A(ωn0),A(ωn1),⋯,A(ωnn−1)) 称作系数向量 a⃗ =(a0,a1,⋯,an−1)a→=(a0,a1,⋯,an−1) 的****离散傅里叶变换****（Discrete Fourier Transform, DFT），也记作 y⃗ =DFTn(a⃗ )y→=DFTn(a→)

到此为止，直接计算 DFTn(a⃗ )DFTn(a→) 还是需要 O(n2)O(n2) 的时间，Cooley-Tukey 算法接下来做的事情是将每一项按照指数奇偶分类

A(ωkn)==∑i=0n−1aiωkin∑i=0n2−1a2iω2kin+ωkn∑i=0n2−1a2i+1ω2kinA(ωnk)=∑i=0n−1aiωnki=∑i=0n2−1a2iωn2ki+ωnk∑i=0n2−1a2i+1ωn2ki

但是，如果直接这样递归下去，你需要带入的值还是有 nn 个，也就是说，现在只是将系数减半，而没有将需要带入的值减半，上面的 kk 还是 0,1,⋯,n−10,1,⋯,n−1，这样的话复杂度还是 O(n2)O(n2)

但是你会注意到，根据准备知识中 ω2n=(e2πin)2=e2πin/2=ωn2ωn2=(e2πin)2=e2πin/2=ωn2，并且 n2n2 次单位根只有 n2n2个，也就是说，我们要带入的值再平方以后似乎变少了一半？仔细想想就会发现，既然单位根把单位圆等分，那么肯定会对称，也就是有一个正的，就会有一个负的，平方后这两个当然就相同了。严格一点的证明就是

ωn2+kn=ωn2n⋅ωkn=−ωknωnn2+k=ωnn2⋅ωnk=−ωnk

这也就是说，对于 k<n2k<n2 的时候

A(ωkn)=∑i=0n2−1a2iωkin2+ωkn∑i=0n2−1a2i+1ωkin2A(ωnk)=∑i=0n2−1a2iωn2ki+ωnk∑i=0n2−1a2i+1ωn2ki

并且

A(ωk+n2n)==∑i=0n2−1a2iωkin2+ωk+n2n∑i=0n2−1a2i+1ωkin2∑i=0n2−1a2iωkin2−ωkn∑i=0n2−1a2i+1ωkin2A(ωnk+n2)=∑i=0n2−1a2iωn2ki+ωnk+n2∑i=0n2−1a2i+1ωn2ki=∑i=0n2−1a2iωn2ki−ωnk∑i=0n2−1a2i+1ωn2ki

这样我们就将需要带入的值也减少成了 1,ωn2,ω2n2,⋯,ωn2−1n21,ωn2,ωn22,⋯,ωn2n2−1，问题变成了两个规模减半的子问题，只要递归下去计算就可以了，至于复杂度

T(n)=2T(n2)+O(n)=O(nlogn)T(n)=2T(n2)+O(n)=O(nlog⁡n)

### **傅里叶逆变换（IDFT）**

刚刚计算的是 y⃗ =DFTn(a⃗ )y→=DFTn(a→)，可以将多项式转化成点值表示，现在为了将点值表示转化成系数表示，需要计算 IDFT（Inverse Discrete Fourier Transform），它是 DFT 的逆

这个问题实际上相当于是一个解线性方程组的问题，也就是给出了 nn 个线性方程

⎧⎩⎨⎪⎪⎪⎪⎪⎪⎪⎪⎪⎪a0(ω0n)0a0(ω1n)0⋮a0(ωn−1n)0+++⋯⋯⋮⋯+++an−2(ω0n)n−2an−2(ω1n)n−2⋮an−2(ωn−1n)n−2++++an−1(ω0n)n−1+an−1(ω1n)n−1⋮+an−1(ωn−1n)n−1===A(ω0n)A(ω1n)⋮A(ωn−1n){a0(ωn0)0+⋯+an−2(ωn0)n−2++an−1(ωn0)n−1=A(ωn0)a0(ωn1)0+⋯+an−2(ωn1)n−2++an−1(ωn1)n−1=A(ωn1)⋮⋮⋮⋮⋮a0(ωnn−1)0+⋯+an−2(ωnn−1)n−2++an−1(ωnn−1)n−1=A(ωnn−1)

写成矩阵方程的形式就是

⎡⎣⎢⎢⎢⎢⎢(ω0n)0(ω1n)0⋮(ωn−1n)0(ω0n)1(ω1n)1⋮(ωn−1n)1⋯⋯⋱⋯(ω0n)n−1(ω1n)n−1⋮(ωn−1n)n−1⎤⎦⎥⎥⎥⎥⎥⎡⎣⎢⎢⎢⎢a0a1⋮an−1⎤⎦⎥⎥⎥⎥=⎡⎣⎢⎢⎢⎢⎢A(ω0n)A(ω1n)⋮A(ωn−1n)⎤⎦⎥⎥⎥⎥⎥(1)(1)[(ωn0)0(ωn0)1⋯(ωn0)n−1(ωn1)0(ωn1)1⋯(ωn1)n−1⋮⋮⋱⋮(ωnn−1)0(ωnn−1)1⋯(ωnn−1)n−1][a0a1⋮an−1]=[A(ωn0)A(ωn1)⋮A(ωnn−1)]

记上面的系数矩阵为 VV 现在考虑下面这个矩阵 dij=ω−ijndij=ωn−ij

D=⎡⎣⎢⎢⎢⎢⎢⎢(ω−0n)0(ω−1n)0⋮(ω−(n−1)n)0(ω−0n)1(ω−1n)1⋮(ω−(n−1)n)1⋯⋯⋱⋯(ω−0n)n−1(ω−1n)n−1⋮(ω−(n−1)n)n−1⎤⎦⎥⎥⎥⎥⎥⎥D=[(ωn−0)0(ωn−0)1⋯(ωn−0)n−1(ωn−1)0(ωn−1)1⋯(ωn−1)n−1⋮⋮⋱⋮(ωn−(n−1))0(ωn−(n−1))1⋯(ωn−(n−1))n−1]

设它们相乘后的结果是 E=D⋅VE=D⋅V

eij===∑k=0n−1dikvkj∑k=0n−1ω−iknωkjn∑k=0n−1ωk(j−i)neij=∑k=0n−1dikvkj=∑k=0n−1ωn−ikωnkj=∑k=0n−1ωnk(j−i)

当 i=ji=j 时，eij=neij=n

当 i≠ji≠j 时，

eij===∑k=0n−1(ωj−in)k1−(ωj−in)n1−ωj−in0eij=∑k=0n−1(ωnj−i)k=1−(ωnj−i)n1−ωnj−i=0

因此可以知道 In=1nEIn=1nE，所以 1nD=V−11nD=V−1

将 1nD1nD 在 [1](http://blog.miskcoo.com/2015/04/polynomial-multiplication-and-fast-fourier-transform" \l "mjx-eqn-IDFT-equation)1 左乘就会得到

⎡⎣⎢⎢⎢⎢a0a1⋮an−1⎤⎦⎥⎥⎥⎥=1n⎡⎣⎢⎢⎢⎢⎢⎢(ω−0n)0(ω−1n)0⋮(ω−(n−1)n)0(ω−0n)1(ω−1n)1⋮(ω−(n−1)n)1⋯⋯⋱⋯(ω−0n)n−1(ω−1n)n−1⋮(ω−(n−1)n)n−1⎤⎦⎥⎥⎥⎥⎥⎥⎡⎣⎢⎢⎢⎢⎢A(ω0n)A(ω1n)⋮A(ωn−1n)⎤⎦⎥⎥⎥⎥⎥[a0a1⋮an−1]=1n[(ωn−0)0(ωn−0)1⋯(ωn−0)n−1(ωn−1)0(ωn−1)1⋯(ωn−1)n−1⋮⋮⋱⋮(ωn−(n−1))0(ωn−(n−1))1⋯(ωn−(n−1))n−1][A(ωn0)A(ωn1)⋮A(ωnn−1)]

### **算法实现**

#### **递归实现**

根据前面的说明，递归实现的 FFT 应该不是什么大问题，下面就直接给出 C++ 代码了（主意 nn 要补齐到 2m2m）

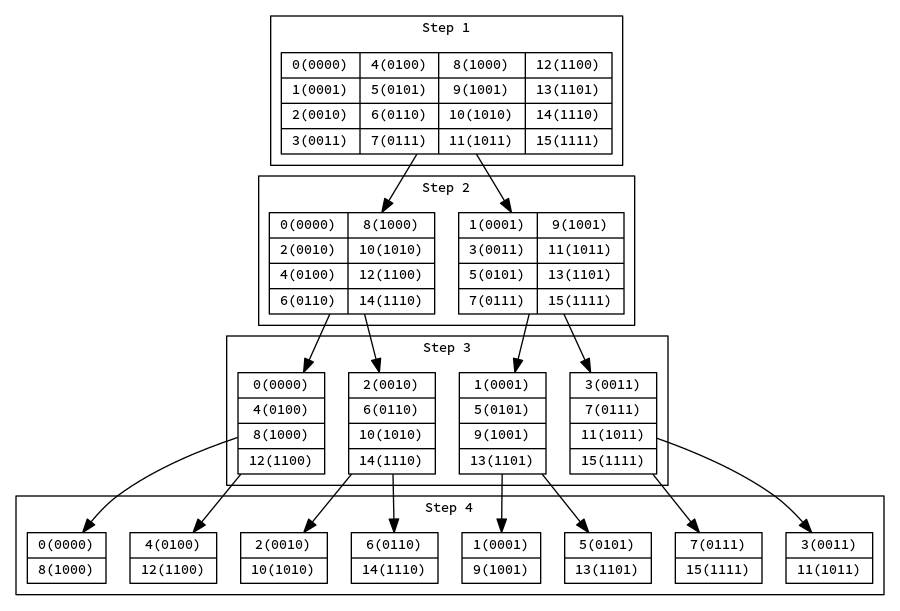
|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16 | **void** fft(**int** n, complex<**double**>\* buffer, **int** offset, **int** step, complex<**double**>\* epsilon)  {  **if**(n == 1) **return**;  **int** m = n >> 1;  fft(m, buffer, offset, step << 1, epsilon);  fft(m, buffer, offset + step, step << 1, epsilon);  **for**(**int** k = 0; k != m; ++k)  {  **int** pos = 2 \* step \* k;  temp[k] = buffer[pos + offset] + epsilon[k \* step] \* buffer[pos + offset + step];  temp[k + m] = buffer[pos + offset] - epsilon[k \* step] \* buffer[pos + offset + step];  }    **for**(**int** i = 0; i != n; ++i)  buffer[i \* step + offset] = temp[i];  } |

这里的 epsilon 是事先打好了的 ωnωn 的表

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | **void** init\_epsilon(**int** n)  {  **double** pi = acos(-1);  **for**(**int** i = 0; i != n; ++i)  {  epsilon[i] = complex<**double**>(cos(2.0 \* pi \* i / n), sin(2.0 \* pi \* i / n));  arti\_epsilon[i] = conj(epsilon[i]);  }  } |

#### **迭代实现**

假设现在有 1616 个数要进行 DFTDFT 来看看递归的过程

[](http://blog.miskcoo.com/wp-content/uploads/2015/04/bit-reverse.png)

在 Step1 -> Step2 的过程中，按照奇偶分类，二进制位中最后一位相同的被分到同一组

在 Step2 -> Step3 的过程中，仍然按照奇偶，只不过不是按照数字的奇偶性，而是下标的奇偶性，二进制位中最后两位相同的才被分到同一组

在 Step3 -> Step4 的过程中，二进制位中最后三位相同的数字被分在同一组

现在将整个二进制位反转，例如 0010 就变成 0100，这时候每次在同一组的数字，反转后的二进制位前几位都是相同的，这似乎十分类似加法，相邻两组二进制位反转之后数字会是连续的一段区间。例如在 Step3 中，1、5、9、13 这一组，反转二进制后是 1(1000)、5(1010)、9(1001)、13(1011)，分组后是 1(1000)、9(1001) 和 5(1010)、13(1011)

假设 reverse(i) 是将二进制位反转的操作，DFT 最后一步的数组是 B，原来的数组是 A，那么 A 和 B 之间有这样的关系 B[reverse(i)]=A[i]，也就是说，B[i+1]=A[reverse(reverse(i)+1)]，B 中第 i 项的下一项就是将 i 反转后加 1 再反转回来 A 中的那一项，所以现在要模拟的就是从高位开始的二进制加法

考虑正向二进制加法的过程，相当于从最低位开始，找到第一个 0，然后把这个 0 改成 1，之前的 1 全部变成 0。那么反向二进制加法就是从最高位开始，找到第一个 0，然后把这个 0 改成 1，前面的 1 全部改成 0，所以就是这样

|  |  |
| --- | --- |
| 1  2  3  4  5 | **int** reverse\_add(**int** x)  {  **for**(**int** l = 1 << bit\_length; (x ^= l) < l; l >>= 1);  **return** x;  } |

为了从原来的 A 数组，得到最后一步所需要的 B 数组，只要维护两个变量，一个是当前下标 i，一个是反向加的下标 j，表示 B[i] 应该放 A[j] 放的东西，如果 i > j，只要将 i 和 j 存的东西交换，这样最后就可以得到所需要的 B 数组

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | */\* 这时候 n 已经补齐到 2 的幂次 \*/*  **void** bit\_reverse(**int** n, complex\_t \*x)  {  **for**(**int** i = 0, j = 0; i != n; ++i)  {  **if**(i > j) swap(x[i], x[j]);  **for**(**int** l = n >> 1; (j ^= l) < l; l >>= 1);  }  } |

现在已经把要变换的元素排在相邻位置了，所以从下往上 22 开始到 2m2m 来进行计算，每次枚举一块往上迭代即可！

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17 | **void** transform(**int** n, complex\_t \*x, complex\_t \*w)  {  bit\_reverse(n, x);  **for**(**int** i = 2; i <= n; i <<= 1)  {  **int** m = i >> 1;  **for**(**int** j = 0; j < n; j += i)  {  **for**(**int** k = 0; k != m; ++k)  {  complex\_t z = x[j + m + k] \* w[n / i \* k];  x[j + m + k] = x[j + k] - z;  x[j + k] += z;  }  }  }  } |

## **快速数论变换**

由于 FFT 涉及到复数运算，难免有精度问题，在计算一些只要求整数的卷积或高精度乘法的时候就有可能由于精度出现错误，这便让我们考虑是否有在模意义下的方法，这就是****快速数论变换****（Fast Number-Theoretic Transform，FNT）

首先来看 FFT 中能在 O(nlogn)O(nlog⁡n) 时间内变换用到了单位根 ωω 的什么性质

1. ωnn=1ωnn=1
2. ω0n,ω1n,⋯,ωn−1nωn0,ωn1,⋯,ωnn−1 是互不相同的，这样带入计算出来的点值才可以用来还原出系数
3. ω2n=ωn2,ωn2+kn=−ωknωn2=ωn2,ωnn2+k=−ωnk，这使得在按照指数奇偶分类之后能够把带入的值也减半使得问题规模能够减半

∑k=0n−1(ωj−in)k={0,   n,   i≠ji=j∑k=0n−1(ωnj−i)k={0,   i≠jn,   i=j

1. 这点保证了能够使用相同的方法进行逆变换得到系数表示

### **原根**

现在我们要在数论中寻找满足这三个性质的数，首先来介绍原根的概念，根据费马定理我们知道，对于一个素数 pp，有下面这样的关系

ap−1≡1(modp)ap−1≡1(modp)

这一点和单位根 ωω 十分相似，pp 的****原根**** gg 定义为使得 g0,g1,⋯,gp−2(modp)g0,g1,⋯,gp−2(modp) 互不相同的数

如果我们取素数 p=k⋅2n+1p=k⋅2n+1，并且找到它的原根 gg，然后我们令 gn≡gk(modp)gn≡gk(modp)，这样就可以使得 g0n,g1n,⋯,gn−1n(modp)gn0,gn1,⋯,gnn−1(modp) 互不相同，并且 gnn≡1(modp)gnn≡1(modp)，这便满足了性质一和性质二

由于 pp 是素数，并且 gnn≡1modpgnn≡1modp，这样 gn2nmodpgnn2modp 必然是 −1−1 或 11，再根据 gkgk 互不相同这个特点，所以 gn2n≡−1(modp)gnn2≡−1(modp)，满足性质三

对于性质四，和前面一样也可以验证是满足的，因此再 FNT 中，我们可以用原根替代单位根，[这里](http://blog.miskcoo.com/2014/07/fft-prime-table" \t "http://blog.miskcoo.com/2015/04/_blank)已经有了一些数 pp 及其原根，可以满足大部分需求

### **模数任意的解决方案**

前面说了，要进行快速数论变换需要模数是 a⋅2k+1a⋅2k+1 形式的素数，但是在实际应用中，要求的模数可能不是这样的形式，甚至是一个合数！

假设现在需要模 mm，并且进行变换的长度是 nn

那么这样任何多项式系数的范围是 [0,m)[0,m)，两个相乘，不会超过 (m−1)2(m−1)2，一共 nn 项相加，不会超过 n(m−1)2n(m−1)2

这样的话，选取 kk 个有上面形式的素数 p1,p2,⋯,pkp1,p2,⋯,pk，要求满足

∏i=1kpk>n(m−1)2∏i=1kpk>n(m−1)2

然后分别在 modkmodk 的剩余系下做变换，最后使用[中国剩余定理](http://blog.miskcoo.com/2014/09/chinese-remainder-theorem" \t "http://blog.miskcoo.com/2015/04/_blank)合并（当然这时候或许是需要高精度或者 \_\_int128 的）

### **代码实现**

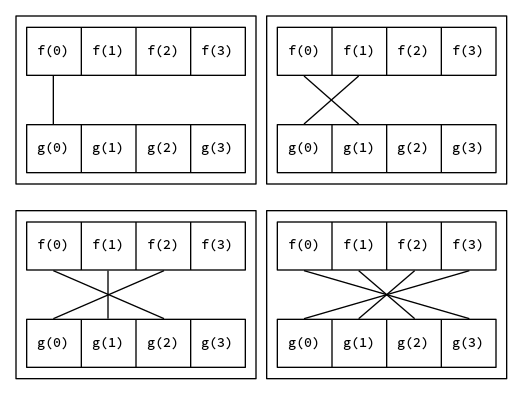
FNT 的代码实现和 FFT 是一样的，只要把复数运算换成在 modpmodp 剩余系下的运算即可

## **应用**

### **快速卷积**

现有两个定义在 NN 上的函数 f(n),g(n)f(n),g(n)，定义 ff 和 gg 的****卷积****（convolution）为 f⊗gf⊗g

(f⊗g)(n)=∑i=0nf(i)g(n−i)(f⊗g)(n)=∑i=0nf(i)g(n−i)

[](http://blog.miskcoo.com/wp-content/uploads/2015/04/convolution.png)

就像上面的图一样，注意到卷积的形式和多项式乘法的形式是相同的，也就是两个多项式 A(x),B(x)A(x),B(x)，令 C(x)=A(x)B(x)C(x)=A(x)B(x)，那么会有 ci=(a⊗b)(i)ci=(a⊗b)(i)，因此可以用 FFT 来计算卷积

对于要计算某些形如 h(k)=∑ni=0f(i)g(i+k)h(k)=∑i=0nf(i)g(i+k) 的问题，可以令 f′(x)=f(n−x)f′(x)=f(n−x)，这样问题就变成计算 ∑ni=0f′(n−i)g(i+k)∑i=0nf′(n−i)g(i+k)，也就是一个卷积的形式

#### **例1：[[ZJOI2014]力](http://www.lydsy.com/JudgeOnline/problem.php?id=3527" \t "http://blog.miskcoo.com/2015/04/_blank)**

题目给出 nn 个数 q1,q2,⋯,qnq1,q2,⋯,qn，要求计算

Fi=∑j=1i−1qiqj(j−i)i−∑j=i+1nqiqj(j−i)iFi=∑j=1i−1qiqj(j−i)i−∑j=i+1nqiqj(j−i)i

观察一下，假设有四个数 q1,q2,q3,q4q1,q2,q3,q4，那么

F1q1F2q2F3q3F4q4====−q212−q322−q432+q112−q312−q422+q122+q212−q412+q132+q222+q312F1q1=−q212−q322−q432F2q2=+q112−q312−q422F3q3=+q122+q212−q412F4q4=+q132+q222+q312

初看之下似乎没什么规律，但是这之中出现的几个数列出来

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| q1q1 | q2q2 | q3q3 | q4q4 | 00 | 00 | 00 |
| −132−132 | −122−122 | −112−112 | 00 | 112112 | 122122 | 132132 |

列出来之后你看看每个 FiqiFiqi 的计算，就会发现刚好是像上面那张图一样的顺序相乘再相加，是个卷积的形式！因此最后只需要用 FFT 优化计算卷积，就可以解决此问题，不过要注意精度问题

ZJOI2014. 力

### **生成函数运算**

对于一些需要用到生成函数的计数问题，在列出生成函数之后有可能需要将其平方、求对数、求逆元或者开方，这时便可以用 FFT 来加速计算

#### **例2：[[BZOJ3771]Triple](http://blog.miskcoo.com/2015/04/bzoj-3771" \t "http://blog.miskcoo.com/2015/04/_blank)**

这个问题就是用 FFT 加速多项式乘法的过程，具体可以看上面这篇题解

### **多项式求逆、除法、取模**

关于多项式的求逆元，可以看[这里](http://blog.miskcoo.com/2015/05/polynomial-inverse" \t "http://blog.miskcoo.com/2015/04/_blank)

关于多项式的除法和求模，可以看[这里](http://blog.miskcoo.com/2015/05/polynomial-division" \t "http://blog.miskcoo.com/2015/04/_blank)

### **多项式多点求值和快速插值**

关于多项式的多点求值和快速插值，可以看[这里](http://blog.miskcoo.com/2015/05/polynomial-multipoint-eval-and-interpolation)

### **Related Posts:**

1. **[多项式的多点求值与快速插值](http://blog.miskcoo.com/2015/05/polynomial-multipoint-eval-and-interpolation" \o "多项式的多点求值与快速插值)**
2. **[多项式求逆元](http://blog.miskcoo.com/2015/05/polynomial-inverse" \o "多项式求逆元)**
3. **[BZOJ-3557. [Ctsc2014]随机数](http://blog.miskcoo.com/2015/05/bzoj-3557" \o "BZOJ-3557. [Ctsc2014]随机数)**
4. **[多项式除法及求模](http://blog.miskcoo.com/2015/05/polynomial-division" \o "多项式除法及求模)**
5. **[BZOJ-3771. Triple](http://blog.miskcoo.com/2015/04/bzoj-3771" \o "BZOJ-3771. Triple)**