

FFT与NTT的原理简要解释 (by Singulet31258)

给定两个多项式 $F(x), G(x)$, 求 $F(x)G(x)$ 。

假定 $F(x), G(x)$ 均为 $n - 1$ 次多项式 (n 是 2 的幂), 它们的系数分别为 $\{a_0, a_1, \dots, a_{n-1}\}, \{b_0, b_1, \dots, b_{n-1}\}$ 。

现在, 我们需要将 $F(x)$ 用 n 个点表示出来 (因为 n 个点可以唯一确定一个 $n - 1$ 次多项式)。

设 $\omega_n = e^{\frac{2\pi}{n}i} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, 然后, 将 $F(x)$ 的系数进行分组:

$$F(x) = \sum_{i=0}^{\frac{n}{2}-1} a_{2i}x^{2i} + x \sum_{i=0}^{\frac{n}{2}-1} a_{2i+1}x^{2i}$$

可以讲它改写成:

$$\begin{aligned} P(x) &= \sum_{i=0}^{\frac{n}{2}-1} a_{2i}x^i \\ Q(x) &= x \sum_{i=0}^{\frac{n}{2}-1} a_{2i+1}x^i \\ F(x) &= P(x^2) + xQ(x^2) \end{aligned}$$

设 $0 \leq k < \frac{n}{2}$, 将 ω_n^k 与 $\omega_n^{k+\frac{n}{2}}$ 分别代入上式, 可得:

$$\begin{aligned} F(\omega_n^k) &= P(\omega_n^{\frac{k}{2}}) + \omega_n^k Q(\omega_n^{\frac{k}{2}}) \\ F(\omega_n^{k+\frac{n}{2}}) &= P(\omega_n^{\frac{k}{2}}) - \omega_n^k Q(\omega_n^{\frac{k}{2}}) \end{aligned}$$

因此, 我们只要知道了 $P(x)$ 与 $Q(x)$ 的点值表示, 就能知道 $F(x)$ 的点值表示。于是分治求解 $P(x)$ 与 $Q(x)$ 即可。

时间复杂度分析: 设 $T(n)$ 表示处理 $n - 1$ 次多项式所需时间。

$P(x)$ 与 $Q(x)$ 均为 $\frac{n}{2} - 1$ 次多项式, 因此分治求解的时间为 $2T(\frac{n}{2})$, 最后 $O(n)$ 枚举 k , 得到 $F(x)$ 。故 $T(n) = 2T(\frac{n}{2}) + O(n)$, 由主定理可知, $T(n) = O(n \log n)$

这就是著名的“快速傅里叶变换 (FFT)”算法!

在用 FFT 求出 $F(x), G(x)$ 的点值表示后, 将它们的点值直接乘起来即可, 最后再还原成系数表示。点值还原成系数同样可以用 FFT 完成, 只需要在上述算法流程结束以后, 把每个系数都除以 n , 最后

再把后 $n - 1$ 个系数 reverse 一遍即可。其正确性可用线性代数的矩阵知识证明，详见[快速傅里叶变换 - OI Wiki](#)

至此，我们成功在 $O(n \log n)$ 的时间内求出了 $F(x)G(x)$ 。

参考代码见 GitHub 的 [Luogu/P3803.cpp](#)

注：上述流程会进行 3 次 FFT ，实际上我们只需要 2 次 FFT 即可完成任务。

令多项式 $H(x) = F(x) + G(x)i$ ，对它做一次 FFT 。我们发现， $H^2(x) = F^2(x) - G^2(x) + 2F(x)G(x)i$ ，因此可以直接把点值表示的 $H(x)$ 平方之后再 FFT 得到系数表示，此时 $F(x)G(x)$ 就是 $H^2(x)$ 的虚部的 $\frac{1}{2}$ 。这样做可以使常数缩小 30%！

NTT 就是把 FFT 中的 ω_n 换成了 $g^{\frac{2^m q}{n}}$ 。在模 p 意义下，有 $g^{2^m q} \equiv 1$ ，其中 g 是模 p 意义下的原根（这意味着 p 必须是质数）， $2^m q = p - 1$ ，且 q 为奇数。 m 必须保证一定比 $\log_2 n$ 大，该算法的正确性才会有保证。

以下为 NTT 的一些可用的模数：

$$p = 1004535809 = 479 \times 2^{21} + 1, q = 479, m = 21, g = 3$$

$$p = 998244353 = 119 \times 2^{23} + 1, q = 119, m = 23, g = 3$$

注： $10^9 + 7$ ， $10^9 + 9$ 等数虽然是质数，但 m 太小，因此不能用作 NTT 的模数！

附赠一些趣味知识：早期 998244353 这个模数基本只会出现在 NTT 的题目当中，而常规的题目基本都用 $10^9 + 7$ 这种数当模数，这导致 998244353 当时能给很多高水平选手一个提示：“这道题的正解很可能是 NTT ！”后来为了消除 998244353 这个数的提示性，一些常规题目也开始用这个数当模数，如今 998244353 已经变得与 $10^9 + 7$ 等模数一样常见。