Topic 8: Fast Fourier Transform

Polynomial Multiplication

$f(x) = 1+x$ $\quad g(x) = 1+x+x^2$ $\quad f \cdot g(x) = 1+2x+2x^2+x^3$

Naive $O(n^2)$

Observation: A poly of n coefficients is determined by n points

$f(1) = 2 \quad f(2) = 3 \quad f(3) = 4 \quad f(4) = 5$

$g(1) = 3 \quad g(2) = 7 \quad g(3) = 13 \quad g(4) = 21$

$f \cdot g(1) = 6 \quad f \cdot g(2) = 21 \quad f \cdot g(3) = 42 \quad f \cdot g(4) = 105$

$\Downarrow$

$f \cdot g(x) = 1 + 2x + 2x^2 + x^3$

Problem: compute $f(x)$ is $O(n) \Rightarrow O(n^2)$ for n points

assume $n = 2^k$

Intuition: We are going to find n points fast in $O(n \log n)$

$F = (f(p^0), f(p^1) \cdots f(p^{n-1}))$ for some p

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$

$= \underbrace{(a_0 + a_2 x^2 + \cdots + a_{n-2} x^{n-2})} + x \underbrace{(a_1 + a_3 x^2 + \cdots + a_{n-1} x^{n-2})}$

subproblems of size $\frac{n}{2}$

$= f_e(x^2) + x f_2(x^2)$

$F_e = (f_e(p^0), f_e(p^2), \cdots f_e(p^{n-2}))$

$F_2 = (f_2(p^0), f_2(p^2), \cdots f_2(p^{n-2}))$

$F_i = f(p^i) = f_e(p^{2i}) + p^i \cdot f_2(p^{2i}) = F_{e,i} + p_i \cdot F_{2,i}$
$(0 \le i < \frac{n}{2})$

What should we do when $i \ge \frac{n}{2}$?

"Magic Numbers"

Goal: Find magic numbers p s.t. $p^n = 1$.

Then $fe(p^{n+2i}) = fe(p^{2i})$ and problem solved

FFT: $e^{\pi i} = -1 \Rightarrow p = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + \sin(\frac{2\pi}{n})i$.

(Precision issues in CP...)

NTT:

(Fermat's little Thm) $p^{M-1} = 1 \bmod M$ for any p & prime M

(1) Make $M-1 = \alpha \cdot n$. then $(p^\alpha)^n = 1$

$998244353 = \underbrace{2^{23}}_{n} \cdot 7 \cdot 17 + 1$

(2) Make $p^0, p^1, p^2 \cdots p^{M-2}$ all different

Known as primal root / generator

3 sets of prime / generator in the reference

For 998244353, 3 is a generator

Reverse ?

(Almost) the same (see reference)

How to 774 in Practice

'Generating Function':

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$

x^i is not a value, but an abstract 'item' i

And a_i is the number of ways to obtain this 'item' i.

Lightsabers

Lightsabers

2 red sabers

1 blue saber

take 0 red sabers

take 2 red sabers

$(1 + x + x^2)$

$\cdot$

$(1 + x)$

$1 + 2x + 2x^2 + x^3$

2 ways to take 2 sabers

mod 1009?

observe that 1 poly mult will be at most

$n \cdot 1009 < 999 > 44353$

so use $999 > 44353$ gives accurate result

and we can clamp down by mod 1009.

Nikita and Order Statistics

Nikita and Order Statistics

s_i : number of elements in $a[0..i]$ that is $< x$

e.g. $a = (1, 2, 3, 4, 5)$ $x = 3$
$s = (0, 1, 2, 2, 2, 2)$

$[l..r]$ has k elements $< x$ $\iff$ $s_r - s_{l-1} = k$

Nikita and Order Statistics

s_i : number of elements in $a[0..i]$ that is $< x$

e.g. $a = (1, 2, 3, 4, 5)$ $x = 3$
$s = (0, 1, 2, 2, 2, 2)$

$[l..r]$ has k elements $< x$ $\iff$ $s_r - s_{l-1} = k$

$s = (0, 1, 2, 2, 2, 2) \Rightarrow f(x) = 1 + x + 4x^2$ ← pick r

$g(x) = 1 + x^{-1} + 4x^{-2}$ ← pick l

$f \cdot g(x) = \ldots + 18 + 5x + 4x^2$

$(x^2 \cdot g(x) = x^2 + x + 4)$

Largest $= n^2 > 999044333$?

Use two primes and Chinese Remainder Theorem
or 744 and pray for precision.