Fast Integer Multiplication Cont'd.

From Last time

Thm 1 Let $m = 2^k$. (FFT)

If R is a ring with $\omega \in R$ being a principal m^{th} root of 1, then

there is an $O(m \log m)$-operation (over R)

to take a polynomial $A(X) \in R[X]$ of deg $< m$, and evaluate it at

$$1, \omega, \omega^2, \ldots, \omega^{m-1}.$$

Thm 2 Let $m = 2^k$.

Let R be such that it has a principal m^{th} root of 1 in it.

Then there is an $O(m \log m)$-operation algorithm that takes in

the coefficients of

$A(X), B(X) \in R[X]$ with

$\deg(A), \deg(B) < \frac{m}{2}$

and outputs the coefficients of

$(A \cdot B)(X)$.

Now: how to do polynomial multiplication over any finite field F.

Strategy:

Introduce roots of unity into F,

while also recursing to smaller problems.

Let $m/2 = n$.

Take $A(X) \in F[X]$

$B(X) \in F[X]$

$A(X) = \sum_{i}^{n-1} a_i X^i$

$$B(X) = \sum_{i=0}^{m-1} b_i X^i$$

Define

$$A^*(X,Y) = \sum_{i=0}^{\sqrt{n}-1} a_i(X)\, Y^i$$

where $\deg(a_i) < \sqrt{n}$

so that

$$A^*(X, X^{\sqrt{n}}) = A(X).$$

Similarly $B^*(X,Y) = \sum_{i=0}^{\sqrt{n}-1} b_i(X)\, Y^i$

where $\deg(b_i) < \sqrt{n}$.

$$B^*(X, X^{\sqrt{n}}) = B(X).$$

Consider $C^*(X,Y) = A^*(X,Y) \cdot B^*(X,Y)$

From $C^*(X,Y)$, we can find $A(X) \cdot B(X)$.

by $A(X) \cdot B(X) = A^*(X, X^{\sqrt{n}}) \cdot B^*(X, X^{\sqrt{n}})$

$$= C^*(X, X^{\sqrt{n}}).$$

View $A^*(X,Y)$, $B^*(X,Y)$ as elements $\tilde{A}(Y), \tilde{B}(Y)$ of $\left(F[X]/\langle X^{2\sqrt{n}}+1\rangle\right)[Y]$

$$= R[Y].$$

Claim: If we know the coefficients of $\tilde{A}(Y)\cdot\tilde{B}(Y)$, then we know the coefficients of Y^i in $A^*(X,Y)\cdot B^*(X,Y)$.

Coefficient of Y^i in $\tilde{A}(Y)\cdot\tilde{B}(Y)$

$$= \left(\sum_{i,i' \text{ s.t. } } \alpha_i(X)\,\beta_{i'}(X)\right) \pmod{X^{2\sqrt{n}}+1}$$

$i+i' = j$

$\deg < 2\sqrt{n}$

so modding doesn't affect the coefficients.

Let a be a power of 2.

Claim $\langle X \rangle \in \underbrace{F[X]/\langle X^a + 1 \rangle}_{=R}$ is a principal $2a^{th}$ root of 1.

Proof Want to say: $X^j - 1$ is invertible in R for all j in $\{1, 2, \ldots, 2a-1\}$.

$$(X^{2a} - 1) = (X^a - 1) \cdot (X^a + 1)$$

Write $j = 2^u \cdot v$ where v is odd.

$$(X^j - 1) = (X^{2^u \cdot v} - 1)$$

$$= (X^{2^{u-1} \cdot v} - 1)(X^{2^{u-1} \cdot v} + 1)$$

$$= (X^{2^{u-2} \cdot v} - 1)(X^{2^{u-2} \cdot v} + 1) \cdot (X^{2^{u-1} \cdot v} + 1)$$

$$\vdots$$

$$= (X^v - 1)(X^v + 1)(X^{2v} + 1)(X^{4v} + 1)$$

$$\cdots \quad (X^{2^{u-1} \cdot v} + 1)$$

$(X-1)$ invertible?

$$(X-1)(Q(X)) = 1 + (X^q + 1)\,a(X)$$

$\|$

$$(X-1)\underbrace{(1+X+\cdots X^{q-1})}_{-2} = \underbrace{X^q-1}_{-2} \equiv 1$$

$$\mod (X^q+1)$$

$$(X^2-1) = (X-1)(X+1)$$

$$(1+X^2+X^4+\cdots+X^{q-2})$$

$$\equiv (X^q-1) \equiv -2 \pmod{X^q+1}$$

$(X^{2^i}-1)$ is similarly invertible.

$$(X^3-1) = (X-1)(X^2+X+1)$$

$$\left(X^{3\cdot a} - 1\right) \equiv \left(X^{a} - 1\right) \pmod{X+1}$$

$$\| \qquad \text{(since } X^{2a} \equiv 1\text{)}$$

$$\left(X^{3\frac{a}{2}} - 1\right)\left(X^{3a/2} + 1\right)$$

$$\|$$

$$\left(X^{\frac{3a}{4}} - 1\right)\left(X^{\frac{3a}{4}} + 1\right)\left(X^{\frac{3a}{2}} + 1\right)$$

$$\|$$

$$\vdots$$

$$\left(X^{3} - 1\right)\cdot\left(X^{3} + 1\right)\left(X^{6} + 1\right)\cdots\left(X^{\frac{3a}{2}} + 1\right)$$

By FFT thms, Can Multiply polys $\tilde{A}(Y), \tilde{B}(Y)$ using $O(\sqrt{n}\log\sqrt{n})$ operations in R.

$R = F[X] / \langle X^{2\sqrt{n}} + 1 \rangle$.

Elts of R are $2\sqrt{n}$-tuples of elements of F.

Addition is $O(\sqrt{n})$ per operation.

Multiplication takes time $O(\sqrt{n})$ + time to multiply polys of degree $2\sqrt{n}$.

Total time for multiplying degree n polys, $T(n)$ satisfies.

$$T(n) \leq O(\sqrt{n} \log(\sqrt{n})) \cdot T(2\sqrt{n}) + O(\sqrt{n} \log n)$$

So

$$T(n) \leq O(n \operatorname{polylog} n).$$

For int multiplication.

To multiply

$$\sum_{i=0}^{n} a_i 2^i \quad \text{and} \quad \sum_{i=0}^{n} b_i 2^i$$

Consider

$A(x) = \sum a_i x^i$ and $B(x) = \sum b_i x^i \in F[x]$

(for some finite field F $|F| > n$.)

and multiply them

to get $C(x) \sum_{i=0}^{2n} c_i x^i$.

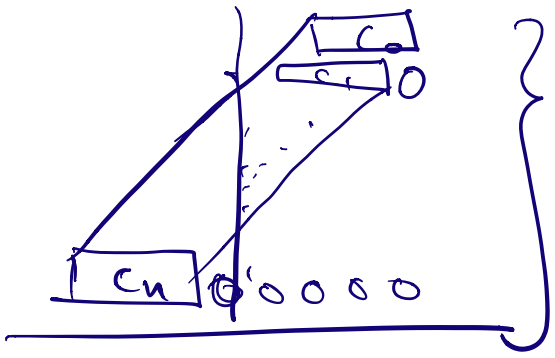
Then $C(2) = A(2) \cdot B(2)$.

and $c_i \in [0, n]$

Problem Given integers

$$c_0, c_1, \ldots, c_n$$

where each c_i is a $\log n$ bit integer, find the the base 2 rep'n of $c_0 + 2 \cdot c_1 + 4 \cdot c_2 + \cdots + 2^i \cdot c_i + \cdots + 2^n \cdot c_n$



Can be done in $n \log n$ time.

Overall n polylog n time for integer multiplication.