Sec 5 | Recurrences

$$f = f_0 + f_1 x + \cdots + f_d x^d \in \mathbb{F}_p[x]$$

$$d = 2g+2.$$

$h = f^m$ $\quad m = \frac{p-1}{2}.$ $\quad$ **Assume $f_0 \neq 0$.**

Goal: Compute A_f, i.e. Cartier coeffs of h.

Calculus: $(f^m)' = m \cdot f' \cdot f^{m-1}.$

Better: $\partial = x \frac{d}{dx}$ ⟵ preserves degrees.

$$\partial(f^m) = m \cdot \partial f \cdot f^{m-1}.$$

$$\boxed{f \cdot \partial h = m \cdot \partial f \cdot h}$$ diff. eq. satisfied by h

Equate coeffs of x^k: (do algebra)

$$\Rightarrow h_k = \frac{1}{k f_0} \sum_{j=1}^{d} \left(\tfrac{1}{2} j - k\right) f_j h_{k-j}.$$

(in $\mathbb{F}_p$)

provided $k \neq 0 \pmod p$

$\frac{p+1}{2}$

Start with $h_0 = f_0^m$.

Then $\Rightarrow h_1 \Rightarrow h_2 \Rightarrow \cdots \Rightarrow h_{p-1}$ 

yields first row of A_f.

(h_{p-j} $j=1..g$)

 $k=p$ bad.. cannot divide by k.

cannot get h_p.

SOLUTION: LIFT! to $\mathbb{Z}/p^\mu\mathbb{Z}$ some $\mu \geq 2$.

Choose lift

$$F = F_0 + F_1 x + \cdots + F_d x^d \in (\mathbb{Z}/p^\mu\mathbb{Z})[x].$$

i.e. $F_j \equiv f_j \pmod{p}$.

Put $H = F^m \in (\mathbb{Z}/p^\mu\mathbb{Z})[x]$.

Enough to compute H_j's mod p.

H satisfies same d.e.:

$$F \cdot \partial H = m \cdot H \cdot \partial F.$$

$$\Rightarrow k H_k = \frac{1}{F_0} \sum_{j=1}^{d} ((m+1)j - k) F_j H_{k-j}$$

(in $\mathbb{Z}/p^r\mathbb{Z}$)

Division by k might cause "precision loss".

Algo: start with $\widetilde{H}_0 = F_0^m$ $(= H_0)$

Compute $\widetilde{H}_1, \widetilde{H}_2, \ldots$ by solving

$$k \widetilde{H}_k = \frac{1}{F_0} \sum_{j=1}^{d} ((m+1)j - k) F_j \widetilde{H}_{k-j}.$$

<u>Example:</u> $g=3$ $(d=8)$ $\mu=3$.

$\tilde{H}_0 \quad \tilde{H}_1 \quad \tilde{H}_2 \quad \cdots \quad \underbrace{\quad \tilde{H}_{p-1}}_{\text{first row of } A_f} \quad \tilde{H}_p$

$\tilde{H}_1$: correct mod p^3

$\tilde{H}_p$: only correct mod p^3.

$\tilde{H}_{p+1} \quad \tilde{H}_{p+2} \quad \cdots \quad \underbrace{\quad \tilde{H}_{2p-1}}_{\text{2nd row.}} \quad \tilde{H}_{2p}$

correct mod p^2

$\tilde{H}_{2p}$: correct mod p. actually correct mod p^2.

$\tilde{H}_{2p+1} \quad \tilde{H}_{2p+2} \quad \cdots \quad \underbrace{\quad \tilde{H}_{3p-1}}_{\text{3rd row.}}$

correct mod p

In general suffices to take

$$\mu = v_p((gp-1)!) + 1.$$

SHOCKING FACT: enough to take

$$\mu = \lfloor \log_p (gp-1) \rfloor + 1.$$

In example $\mu=2$ is enough (assuming $g \le p$).

Proof: see notes

Complexity of "recurrence strategy" for computing Af.

$O(g^2 p (\log p)^{1+\varepsilon})$ $(p \geq g)$

basically cost of evaluating recurrence p times.

expansion strategy: $O(g p (\log p)^2)$

uses almost no memory!

Sec 6 — Square root alg.

Warmup: Wilson primes

$$(p-1)! \equiv -1 \pmod{p^2}.$$

5 13 563 no other $< 2\times 10^{13}$.

Goal: given p, compute $(p-1)! \bmod p^2$.

Strassen's idea: Let $s = p-1$.

$(p-1)! = 1\times 2\times 3\times \cdots \times s$.

Let $t = \lfloor \sqrt{s} \rfloor$

Then $s = t^2 + t'$ $t' = O(\sqrt{s})$

$(1\times 2\times \cdots \times t)((t+1)(t+2)\cdots(2t))$

$\cdots$ t blocks $\cdots$ $((t-1)t+1)\cdots(t^2)\times$

[t blocks of length t] (t' leftover terms)

Define $Q(k) = (k+1)(k+2)\cdots(k+t)$

$\in (\mathbb{Z}/p^2\mathbb{Z})[k]$ deg t.

So:

$(p-1)! = Q(0)\,Q(t)\,Q(2t)\cdots Q((t-1)t)$

$\cdot$ leftovers.

Algo: ① Compute $Q(k)$. (i.e. its coeffs)

using a product tree

(assume t = power of 2).

$k+1 \quad k+2 \quad k+3 \quad k+4 \quad \cdots \quad k+t$

$k^2+3k+2 \qquad k^2+7k+12 \qquad \cdots$

$k^4 + \cdots + 24$

$\vdots$

$Q(k)$

total cost:

$O(p^{1/2}\log^3 p)$.

(2) evaluate $Q(h)$ at
$h = 0, t, 2t, \ldots (t-1)t$.
$= \alpha_1, \alpha_2, \ldots \alpha_t \in \mathbb{Z}/p^2\mathbb{Z}$

Multipoint eval. problem.
Std. algo uses $O(p^{1/2} \log^3 p)$ time.

(3) Combine leftover terms:
$O(p^{1/2})$ mults in $\mathbb{Z}/p^2\mathbb{Z}$.

Conclusion! can compute $(p-1)! \bmod p^2$
in time $O(p^{1/2} \log^3 p)$.

$O(p^{1/2} \log^2 p)$ BGS 2007?

$O\left(\frac{p^{1/2} \log^2 p}{(\log\log p)^?}\right)$??? 202?.

B-a

0!+

??

$\cancel{0!+}\,1! + 2! + 3! + \cdots + (p-1)! \not\equiv 0 \pmod{p}$

Kurepa ~~p odd~~