Setup from Sec 5:

$$y^2 = f(x) \qquad f \in \mathbb{F}_p[x]$$

lift: $F \in (\mathbb{Z}/p^2\mathbb{Z})[x]$ $\quad (p^2 > g,\ \mu = 2)$

$$= F_0 + F_1 x + \cdots + F_d x^d \qquad d = 2g+1$$

$$H = F^m \qquad m = \frac{p-1}{2}.$$

Recurrence in <u>matrix form</u>.

$$U_k = (H_{k-d+1}, \ldots H_{k-1}, H_k) \in (\mathbb{Z}/p^2\mathbb{Z})^d$$

$$U_0 = (0, 0 \ldots, H_0)$$

$$T_k = \begin{bmatrix} 0 & & & (d(m+1)-k)F_d \\ kF_0 & 0 & & \vdots \\ & kF_0 & & \vdots \\ & & \ddots & \\ 0 & & & (2(m+1)-k)F_2 \\ & & kF_0 & ((m+1)-k)F_1 \end{bmatrix}$$

$$\in \mathrm{Mat}_d(\mathbb{Z}/p^2\mathbb{Z})$$

$$k \cdot U_k = \frac{1}{F_0} U_{k-1} T_k$$

First row of A_f:

need $U_{p-1} = [\cdots, H_{p-2}, H_{p-1}]$

$\to$ g entries

ie $$U_{p-1} = \frac{1}{1 \cdot 2 \cdots (p-1) F_0^{p-1}} U_0 T_1 T_2 \cdots T_{p-1}$$

Compute this using Strassen.

$t := \lfloor \sqrt{5} \rfloor = \lfloor \sqrt{p-1} \rfloor$.

Put $Q(k) = T_{k+1} \cdots T_{k+t}$

a matrix of polys of degree t in k (over $\mathbb{Z}/p^2$).

$\Rightarrow$ Can compute $T_1 \cdots T_{p-1}$ in time

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

So far only have 1st row of A_f.

Other runs? \tilde

$\tilde{H}_0, \tilde{H}_1, \tilde{H}_2, \ldots \in \mathbb{Z}/p^2\mathbb{Z}$

$\tilde{U}_k := (\tilde{H}_{k-d+1}, \ldots, \tilde{H}_{k-1}, \tilde{H}_k)$.

Algo: start with $\tilde{U}_0$.

Compute $T_1 \cdots T_{p-1} \Rightarrow \tilde{U}_{p-1}$.

Single step (ind div by p) $\Rightarrow \tilde{U}_p$.

Compute $T_{p+1} \cdots T_{2p-1} \Rightarrow \tilde{U}_{2p-1}$

etc

$\cdots \Rightarrow \tilde{U}_{gp-1}$.

$\therefore$ all runs of A_f.

Complexity to get A_f is

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

"Interpolation trick".

Sec 7 – avg. poly time

Input: $y^2 = F(x) \leftarrow$ hyperelliptic curve / $\mathbb{Q}$ genus g

$F \in \mathbb{Z}[x]$ squarefree

deg $= 2g+1$ or $2g+2$

For any p, f_p = reduction mod p

$\in \mathbb{F}_p[x]$.

Except for "bad primes", $y^2 = f_p(x)$ is hyp. curve / $\mathbb{F}_p$.

$C/\mathbb{F}_p$ $\quad L_p(T) \in \mathbb{Z}[T]$.

Q: How fast can we compute $L_p(T)$ (mod p) for $p \leq N$? (good)

So far: can do that in time

$$O(g^\omega N^{3/2+\varepsilon})$$

Thm 7.4.1 Can compute $L_p(T) \bmod p$ (good) $\forall p \le N$ in time

$$O(g^\omega N \log^3 N).$$

Avg. time per prime is:

$$O(g^\omega (\log N)^4) \qquad \text{"}O(g^\omega (\log p)^4)\text{"}$$

↑ polynomial in $g \log p$ = input size.

Warmup: Wilson primes

Thm (Gerbicz, 2011) Can compute $(p-1)! \pmod{p^2}$ $\forall p \le N$ in time

$$O(N \log^3 N).$$

want: $1 \cdot 2 \bmod 3^2$

$1 \cdot 2 \cdot 3 \cdot 4 \bmod 5^2$

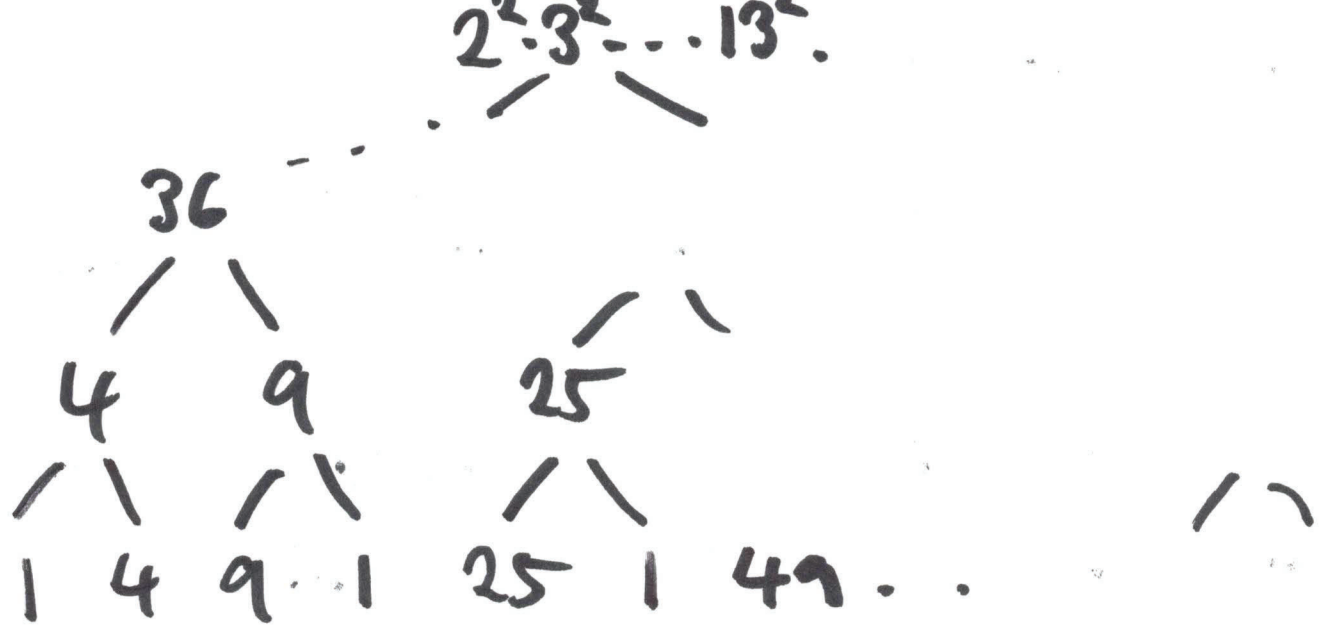
$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \bmod 7^2$

$\vdots$

N.

Modulus tree:

product tree on p^2's up to N.
(sec 7.4 Fig 3).

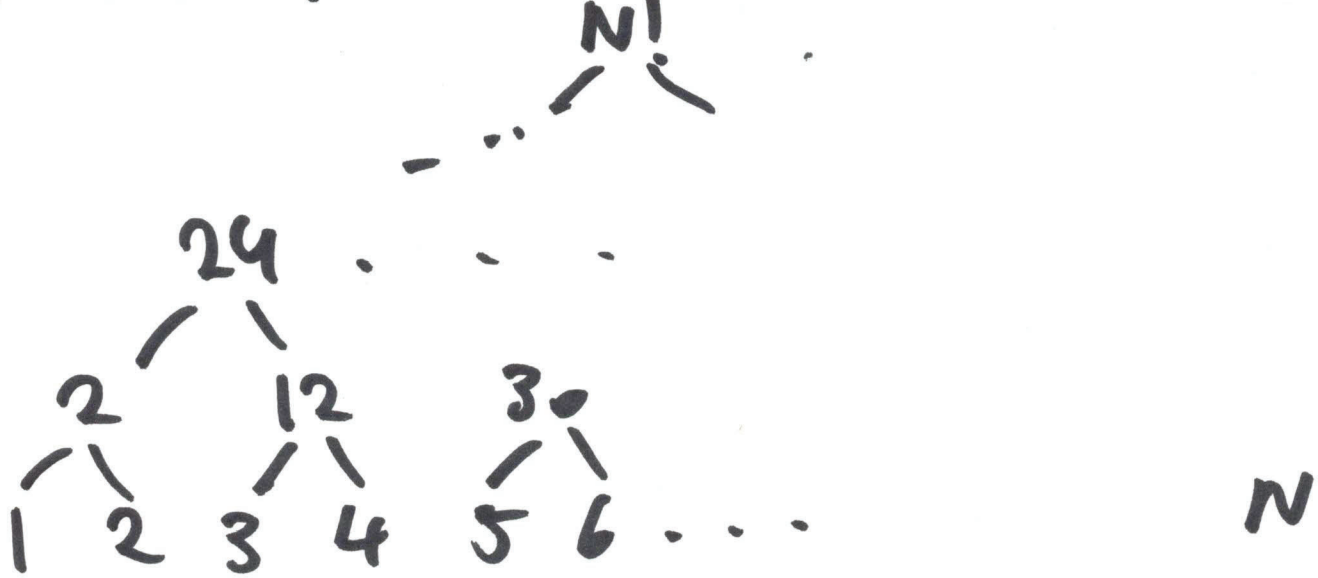


$O(N)$ bits at each level

Cost to build tree: $O(N \log^2 N)$.

Value tree:

product tree on 1, 2, .. N. (Fig 4)

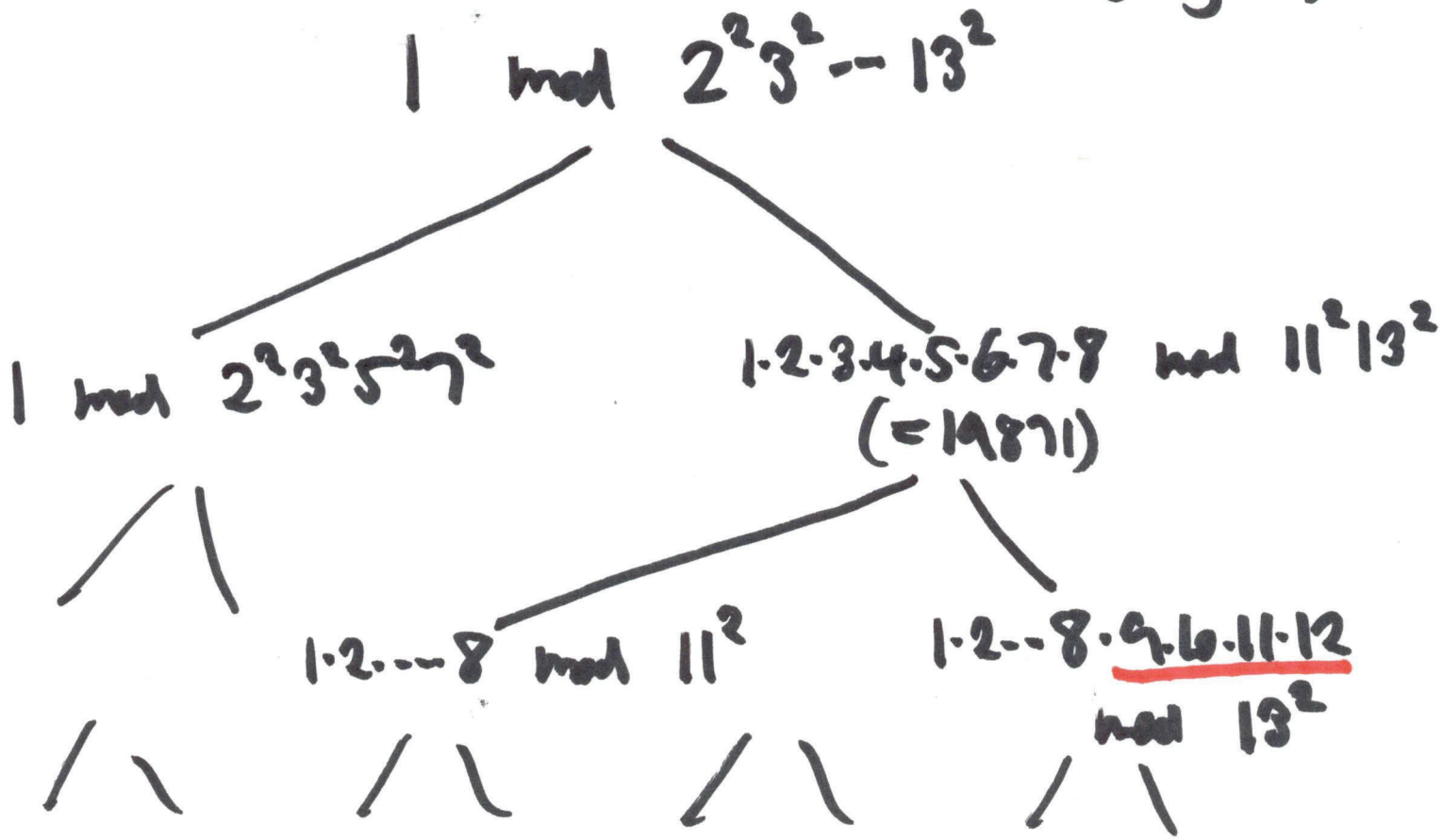


$O(N \log N)$ bits each level

Cost to build is $O(N \log^3 N)$.

Accumulating remainder tree

(Fig 5)



$1 \cdot 2$ mod 3^2 $\quad 1 \cdot 2 \cdot 3 \cdot 4$ mod 5^2 . .

ie. Wilson remainders at bottom of tree

total cost $\Theta(N \log^3 N)$.

Back to point counting.

$T_k^{(p)} \in \mathrm{Mat}_d(\mathbb{Z}/p^2\mathbb{Z})$ for each p.

Want to compute

$i=0$ $T_1^{(p)} \cdots T_{p-1}^{(p)}$

$i=1$ $T_{p+1}^{(p)} \cdots T_{2p-1}^{(p)}$

} want to apply ART, but entries of $T_k^{(p)}$ depend on p!

Solution: work over $\mathbb{Z}[p]/p^2$

$p =$ "generic prime".

$$\overline{T}_j^i(p) = \begin{bmatrix} 0 & & & (d(p+1) \\ 2(ip+j)\overline{F}_0 & & & -2(ip+j))\overline{F}_0 \\ & \ddots & & \\ & & \ddots & ((p+1)-2(ip+j))\overline{F}_1 \\ & & 2(ip+j)\overline{F}_0 & \end{bmatrix}$$

$k = ip+j$ $\quad \in \mathrm{Mat}_d(\mathbb{Z}[p]/p^3)$

$$\overline{T}^{i}_{j}(p) = 2\, T^{(p)}_{ip+j} \pmod{p^2}.$$

Apply ART to

$T^i_1, T^i_2, \ldots$ for each i.