Counting pts. on hyperelliptic curves

- The ideas of Adleman–Huang (2001) are:

(1) Compute the $L(t,C)$ polynomial by Chinese Remaindering, i.e. $L \pmod{\ell}$ for the first $(\log q)^{O(g)}$ primes ℓ.

(2) Since, $L(t,C) = |1-Ft; J|$, we have that $L(t,C) \equiv |1-Ft; J[\ell]| \pmod{\ell}$ where $J[\ell]$ are the ℓ-torsion points in the Jacobian variety $J(\bar{C})$ & $\ell \neq p$.

▷ $J[\ell]$ is an $\mathbb{F}_\ell$-vec. space of $\dim = 2g$.

(3) Going over $\mathbb{F}_\ell$ has the advantage that we can now try to find, by brute-force, the irreducible factors of $L \pmod{\ell}$:

Pick an irred. poly. $h \in \mathbb{F}_\ell[t]$ of $\deg \leq 2g$. Let $J[\ell]_h := \{D \in J[\ell] \mid \exists i, (h(F)^i)(D) = 0\}$.

▷ $\dim_{\mathbb{F}_\ell} J[\ell]_h = e \cdot \deg h$, where $h^e \| L$.

- The strategy to compute $L \bmod \ell$ is to try out all power-of-irred. poly. H in $\mathbb{F}_\ell[t]$ of deg $\leq 2g$ & compute $\# \ker(H(F))$ where $H(F) \in \mathrm{End}_{\mathbb{F}_\ell}(J[\ell])$.

Two major issues

I. What kind of an access do we have to $J[\ell]$, given the curve C via the fn. field $K = \overline{\mathbb{F}}_q(x)[y]/(y^2 - f(x))$?

- Any point in $J(\overline{C})$ can be seen as a divisor $D \in Cl_0(\overline{C})$ of the form: $D = \sum_{i=1}^{r} P_i - r P_0$, where $r \leq g$ and P_0 is a fixed $\mathbb{F}_q$-point. (By Riemann-Roch)

- For hyperelliptic C there is an automorphism $i : P = (a,b) \mapsto (a,-b)$. If we fix P_0 to be the "pt. at ∞" then: $P + i(P) - 2P_0 = 0$.
Because $(x-a) = P + i(P) - 2P_0$!

- Thus, each pt. $D \in Cl_0(C)$ has a <u>reduced</u> form $D = \sum_{i=1}^{r} P_i - r P_0$, where: $\begin{cases} r \leq g \\ \forall i \neq j \in [r],\ P_i \neq \iota(P_j) \end{cases}$

- Following Cantor (1987) we can now represent D as a pair of polynomials $(u(X), v(X))$ s.t. $\begin{cases} u(X) := \prod_{i=1}^{r} (X - x(P_i)), \ \& \\ \\ v(x(P_i)) = y(P_i),\ \forall i \leq r. \end{cases}$

▷ $\deg u \leq g$, $\deg v \leq (g-1)$ & $u \mid (v^2 - f(X))$.

▷ Moreover, we get a correspondence of $Cl_0(\overline{C})$ with such (u, v) polynomials in $\overline{\mathbb{F}}_q[X]$.

- But what is (u_1, v_1) "+" (u_2, v_2)?
Cantor (1987) gave an <u>easy</u> way; with almost <u>linear time</u> complexity!

- Thus, we do have a parameterized access to $Cl_0(\overline{C})$ via (u, v) !

- Similarly, we access $J[\ell]$ & get a semi-algebraic description of $H(F)$, for any power-of-irred. poly $H \in \mathbb{F}_\ell[t]$.

II. How do we compute $\#\ker(H(F))$ from the semi-algebraic description?

- The problem here is to count the number of zeros of a semi-algebraic set.

- This is done using Chow forms in time $(\log q)^{\tilde{O}(g^2)}$.

- Details in Adleman & Huang (JSC 2001).
- More practical are p-adic methods!