COUNTING POINTS ON HYPERELLIPTIC CURVES OVER FINITE FIELDS

FCAS ϟ ϟϟ

Sec 3.1

K = field $\mathrm{char}\, K \neq 2$. (eg. $K = \mathbb{F}_q$ or $\mathbb{Q}$)

$g \geq 1$

C/K = smooth alg. curve assoc. to. affine eqn $y^2 = f(x)$

$f \in K[x]$ squarefree, $\deg f = 2g+1$ or $2g+2$

$$f(x) = f_0 + f_1 x + \cdots + f_{2g+2} x^{2g+2}$$

$f_j \in K$

(allow $f_{2g+2} = 0$)

"Hyperell. curve of genus g over K"

Suppose L/K = finite extn.

Q: describe $C(L)$.

Morphism $x : C \to \mathbb{P}^1$

Induces $x : C(L) \to \mathbb{P}^1(L) = L \cup \{\infty\}$

(map of sets)

Q: given $\alpha \in \mathbb{P}^1(L)$, what are $P \in C(L)$ that map to α?

i) If $\alpha \in L$, just solve $y^2 = f(\alpha)$ in L.

$\Rightarrow$ 0, 1, 2 roots.

ii) $\alpha = \infty$? Need to switch models.

$u = 1/x$ (on $\mathbb{P}^1$)

$x = \infty \Leftrightarrow u = 0$.

$v = y/x^{g+1}$.

$$y^2 = f_0 + f_1 x + \cdots + f_{2g+2} x^{2g+2}$$

$$v^2 = f_0 u^{2g+2} + f_1 u^{2g+1} + \cdots + f_{2g+2}$$

Subst. $u = 0$.

want to solve $v^2 = f_{2g+2} =: "f(\infty)"$

Again: 0 | 1, 2 solutions.

SUMMARY (LEM 3.16)

For each $\alpha \in L \cup \{\infty\}$,

points $P \in C(L)$ such that $x(P) = \alpha$

is $0, 1, 2$ depending on

square roots of $f(\alpha)$ in L.

SEC 3.2 | Now assume $K = \mathbb{F}_q$.

Then $\#C(\mathbb{F}_q) < \infty$.

Goal of course: given $f \in \mathbb{F}_q[x]$,
Compute $\#C(\mathbb{F}_{q^r})$ $r = 1, 2, \ldots$
"quickly".

Enumeration method: try every $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^r})$.
Very slow: Complexity at least q^r.
(exp. in r)

Naive bound: $\#C(\mathbb{F}_{q^r}) \leq 2(q^r+1)$

Hasse–Weil bound:

$$\underbrace{|\#C(\mathbb{F}_{q^r}) - (q^r+1)|}_{\text{main term}} \leq \underbrace{2g \cdot q^{r/2}}_{\text{error term.}} \quad (r \geq 1)$$

Sec 3.3

C/K $y^2 = f(x)$. [1-5] $K = \mathbb{F}_q$

Let $N_r = \#C(\mathbb{F}_{q^r})$. $r \geq 1$.

Zeta fn:

$$Z_C(T) = \exp\left(N_1 T + \frac{N_2}{2} T^2 + \frac{N_3}{3} T^3 + \cdots\right)$$

$$\in \mathbb{Q}[[T]].$$

Weil "Conjectures"

* $Z_C(T)$ is a rational fn.

$$Z_C(T) = \frac{L_C(T)}{(1-T)(1-qT)}$$

$$L_C(T) = 1 + a_1 T + a_2 T^2 + \cdots + a_{2g} T^{2g}$$

$$a_i \in \mathbb{Z}$$

* Functional eqn: $L_C\left(\frac{1}{qT}\right) = (qT^2)^g L_C(T)$.

$$\iff a_{2g-i} = q^{g-i} a_i$$

$$i = 0, \ldots 2g.$$

* Riemann Hypothesis:
roots of $L_C(T)$ have
complex absolute value $q^{-1/2}$.

Goal of course: Compute $L_C(T)$.
$\in \mathbb{Z}[T]$

Using ~~enum. alg and~~ func. eqns,
suffices to compute $N_1, \dots N_g$.

Using enum. alg. complexity $\approx q^g$.

exp in g
$\uparrow$
exp in $\log q$.

Famous unsolved problem:

Given $f \in \mathbb{F}_q[x]$, can we compute
$L_C(T)$ in polynomial time?
input size: $g \cdot \log q$

Schoof-Pila
$(\log q)^{cg}$

Sec 4 | trace formula

From now on $q = p$.

$C/\mathbb{F}_p$ hyp. curve genus $g \geq 1$.

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

Baby trace formula (Prop 4.1.1)

Let $h = f^{\frac{p-1}{2}} \in \mathbb{F}_p[x]$.

Then $\#C(\mathbb{F}_p) \equiv 1 - \sum_{j=1}^{g} h_{j(p-1)} \pmod{p}$

(h_i = coeff of x^i in $h(x)$).