Group Operation on Nodal Curves

Enver Ozdemir

Istanbul Technical University

September 28, 2016

Hyperelliptic Curves

- $H : y^2 = f(x)$ over a field K, $f(x)$ is a square-free polynomial of degree $2g + 1$.

Hyperelliptic Curves

- $H : y^2 = f(x)$ over a field K, $f(x)$ is a square-free polynomial of degree $2g+1$.
- Jacobian group: Ideal class group.

Hyperelliptic Curves

- $H : y^2 = f(x)$ over a field K, $f(x)$ is a square-free polynomial of degree $2g + 1$.
- Jacobian group: Ideal class group.
- Computing in $\mathrm{Jac}(H)$, composition of binary quadratic forms.[M1980][C1988]

Computing in Jacobians: $y^2 = f(x)$

$D = [(u(x), v(x)] \in \mathrm{Jac}(H)$.

- $u(x)$ is a monic polynomial.
- $\deg(v(x)) < \deg(u(x))$.
- $v(x)^2 - f(x)$ is divisible by $u(x)$.

Cantor's Algorithm [C1988]

$D_1 = (u_1, v_1), D_2 = (u_2, v_2)$ and $D = D_1 + D_2 = (u, v)$

- $h = gcd(u_1, u_2, v_1 + v_2)$ with polynomials h_1, h_2, h_3 such that $h = h_1 u_1 + h_2 u_2 + h_3(v_1 + v_2)$
- $u = \dfrac{u_1 u_2}{h^2}$ and $v \equiv \dfrac{h_1 u_1 v_2 + h_2 u_2 v_1 + h_3(v_1 v_2 + f)}{h} \pmod{u}$

  repeat:
- $\widetilde{u} = \dfrac{v^2 - f}{u}$ and $\widetilde{v} \equiv v \pmod{\widetilde{u}}$
- $u = \widetilde{u}$ and $v = -\widetilde{v}$

  until deg $(u) \leq g$
- Multiply u by a constant to make u monic.

Polynomial Factorization

Consider $H : y^2 = f(x)$.

- $(u(x), 0)$.
- Mumford Representation says $0^2 - f(x) = f(x)$ is a multiple of $u(x)$. It means $u(x)$ is a factor.

Singular Curves

A singular curve $H : y^2 = f(x)$ and $f(x)$ can have a multiple roots.

- Generalized Jacobian group $\text{Jac}(H)$. [Ros52,Ros54]
- $(u(x), v(x))$
- For a multiple root a of $f(x)$ if both $u(x)$ and $v(x)$ are divisible by $x - a$ then $v^2(x) - f(x)/u(x)$ is not divisible by $x - a$.

Nodal Curves

$N : y^2 = xf^2(x)$ over finite field $\mathbb{F}_q$. $f(x)$ is irreducible of degree n.

- $\mathrm{Jac}(N) \simeq$ a subgroup of $\mathbb{F}_{q^{2n}}^\times$ [Ros52].
- $q^n + 1$ or $q^n - 1$.

Nodal Curves

$N : y^2 = xf^2(x)$.

- Any polynomial $h(x)$ such that $\gcd(h^2(x) - x, f(x)) = 1$
- Any $D \in \mathrm{Jac}(N)$ uniquely represented by $h(x)$ with $\deg h(x) \leq n$.

Nodal Curves

$N : y^2 = xf^2(x)$.

- Any polynomial $h(x)$ such that $\gcd(h^2(x) - x, f(x)) = 1$
- Any $D \in \mathrm{Jac}(N)$ uniquely represented by $h(x)$ with $\deg h(x) \leq n$.
- $(u(x), v(x))$ such that $\deg v(x) < \deg u(x)$ and $v(x)^2 - xf^2(x)$ is divisible by $u(x)$
- If both $u(x)$ and $v(x)$ are divisible by $f(x)$ then

$$\frac{v(x)^2 - f(x)}{u(x)}$$

  is not divisible by $f(x)$.

- Consider $[f^2(x), h(x)f(x)]$
- $$\frac{h(x)^2 f(x)^2 - x f(x)^2}{f^2(x)} = h^2(x) - x$$

Computing Jacobian of N

$D_1 = h_1(x)$ and $D_2 = h_2(x)$
$D_3 = D_1 + D_2 = h_3(x)$

- Find two polynomials $g_1(x), g_2(x)$ such that

$$g_1(x)f(x) + g_2(x)(h_1(x) + h_2(x)) = 1$$

- Compute

$$h_3(x) \equiv f(x)h_1(x)g_1(x) + g_2(x)(h_1(x)h_2(x) + x) \mod f(x)$$

with $\deg(h_3(x)) < d$

Illustration

- $N : y^2 = x(x+a)^2$
- $f(x) = x + a$ so any $h(x)$ of degree less than 1 represents an element in $\mathrm{Jac}(N)$.
- Any constant $h(x) = t$ as long as $x - t^2 \neq x + a$.
- $h_1 = t$ and $h_2 = r$ then $h_1 + h_2 = \frac{tr-a}{t+r} = h_3$

Summary

- Group structure of Jac(N) [D2006, D2008].
- Each element is a polynomial and each polynomial represents an element.

Thank you very much!