Hyperelliptic curves in cryptography

Tanja Lange

ITSC - Information-Security and Cryptography

Ruhr-University of Bochum

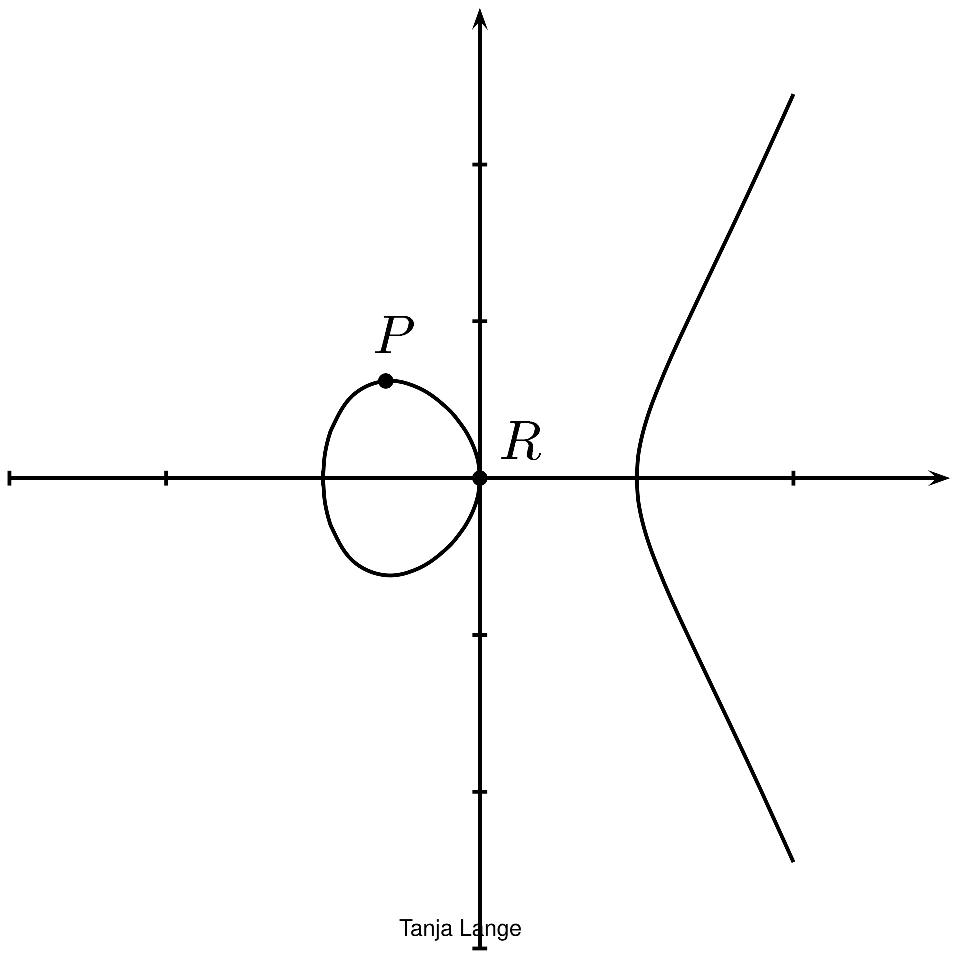
lange@itsc.ruhr-uni-bochum.de

21.12.2004

Elliptic Curve

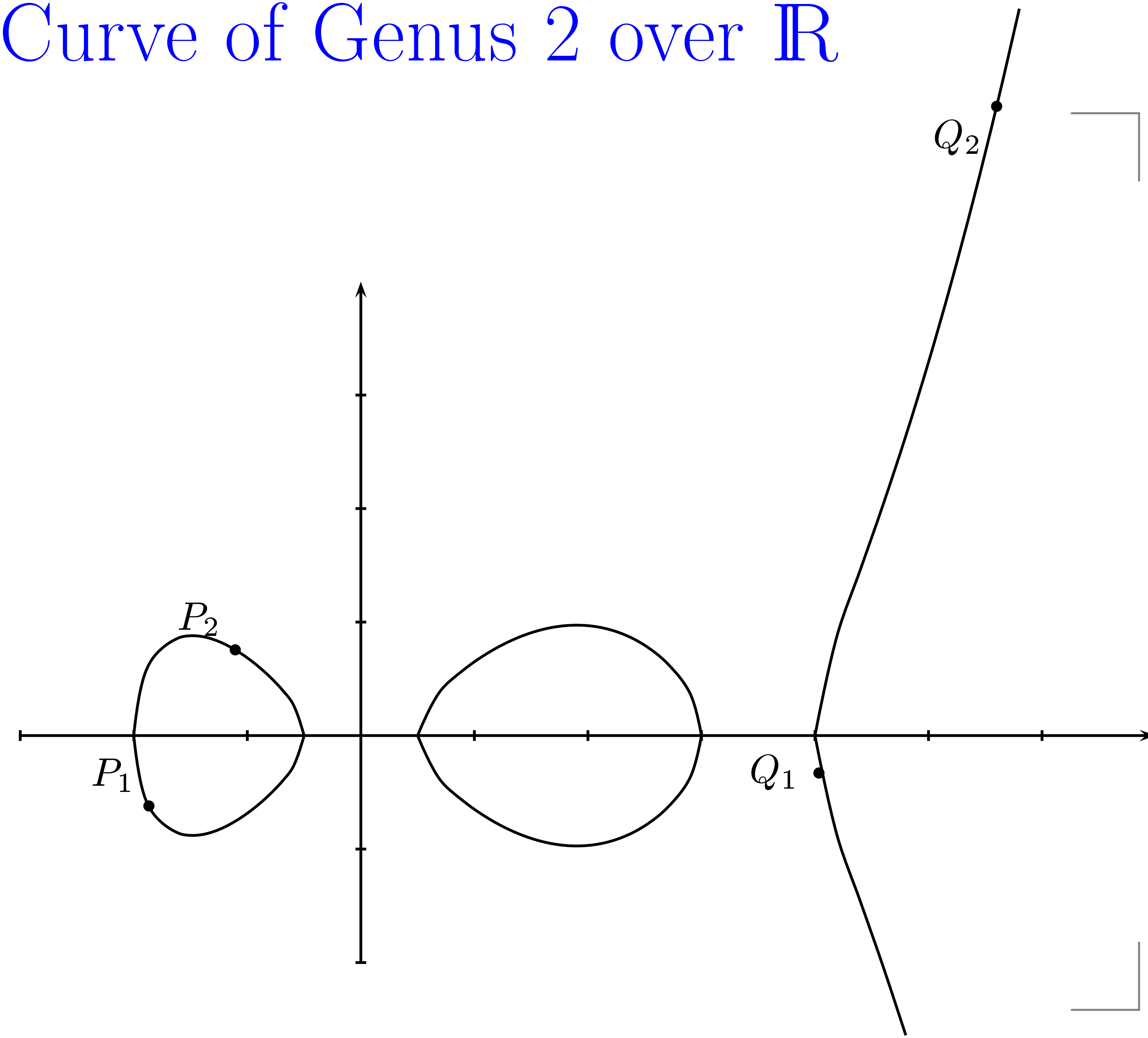
$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}, \quad h, f \in \mathbb{F}_q[x]$$

Group: $E(\mathbb{F}_q) = \{\, (x, y) \in \mathbb{F}_q^2 \,:\, y^2 + h(x)y = f(x) \,\} \cup \{\, P_\infty \,\}$



over $\mathbb{R}$

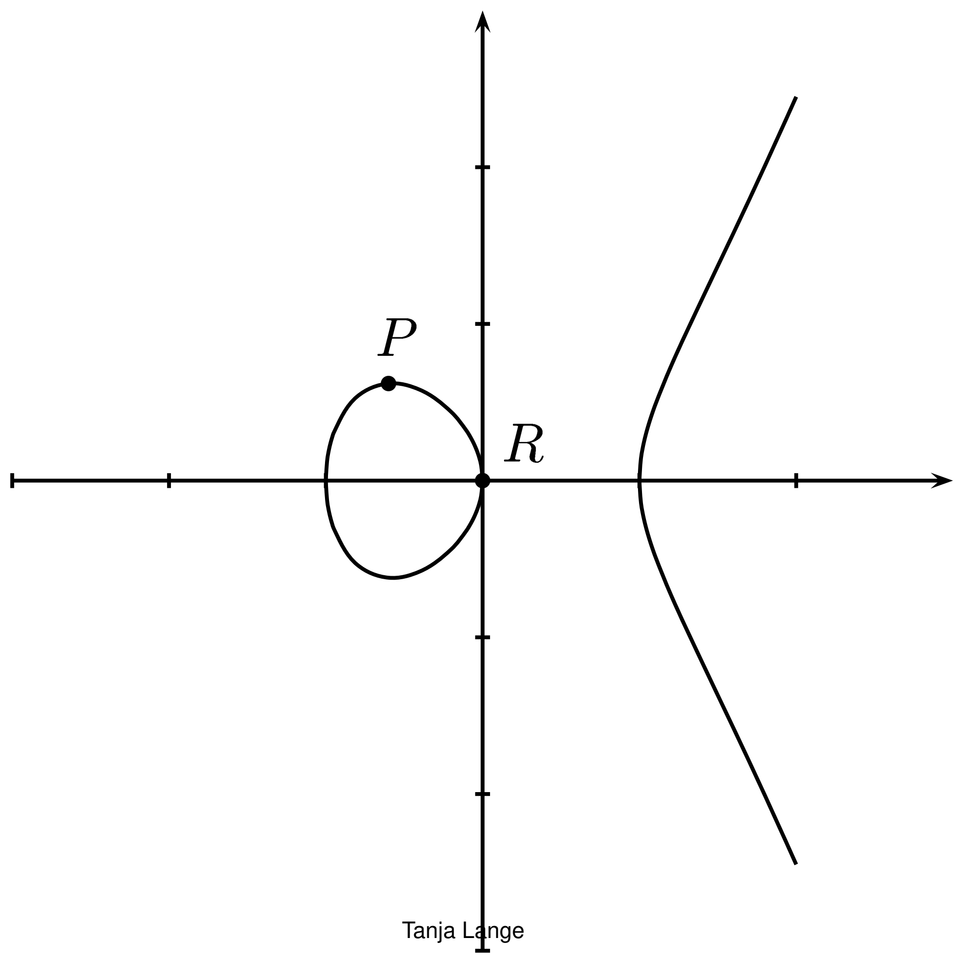
Curve of Genus 2 over $\mathbb{R}$



Elliptic Curve

$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}, \quad h, f \in \mathbb{F}_q[x]$$

Group: $E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \}$

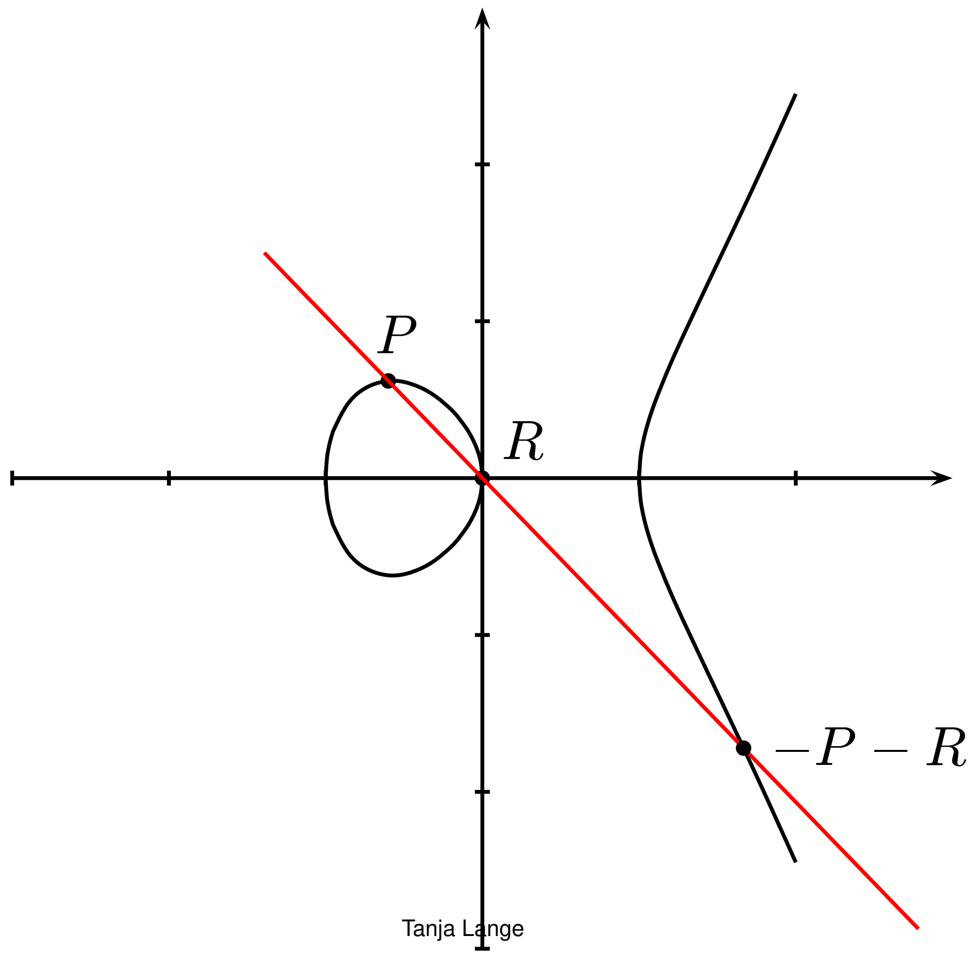


over $\mathbb{R}$

Elliptic Curve

$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}, \quad h, f \in \mathbb{F}_q[x]$$

Group: $E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \}$

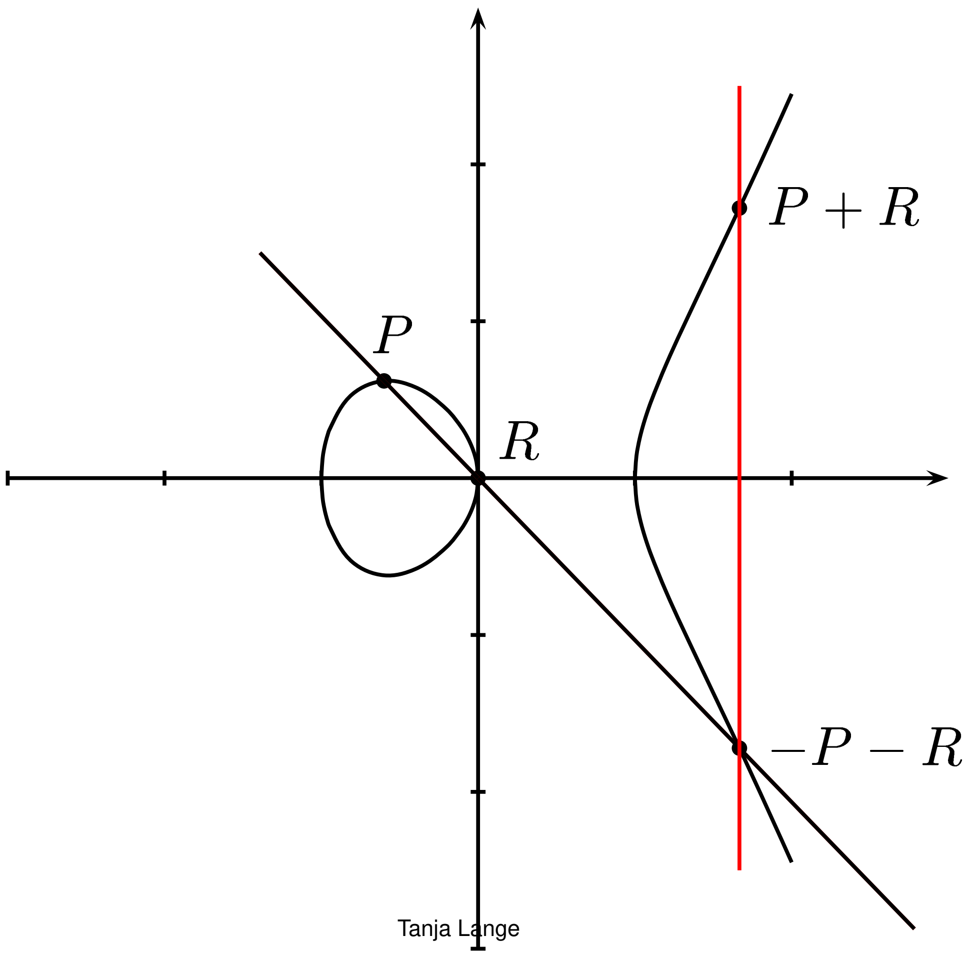


over $\mathbb{R}$

Elliptic Curve

$$E: y^2 + \underbrace{(a_1x + a_3)}_{h(x)}\, y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)}, \quad h, f \in \mathbb{F}_q[x]$$

Group: $E(\mathbb{F}_q) = \{\,(x,y) \in \mathbb{F}_q^2 \;:\; y^2 + h(x)y = f(x)\,\} \cup \{\,P_\infty\,\}$

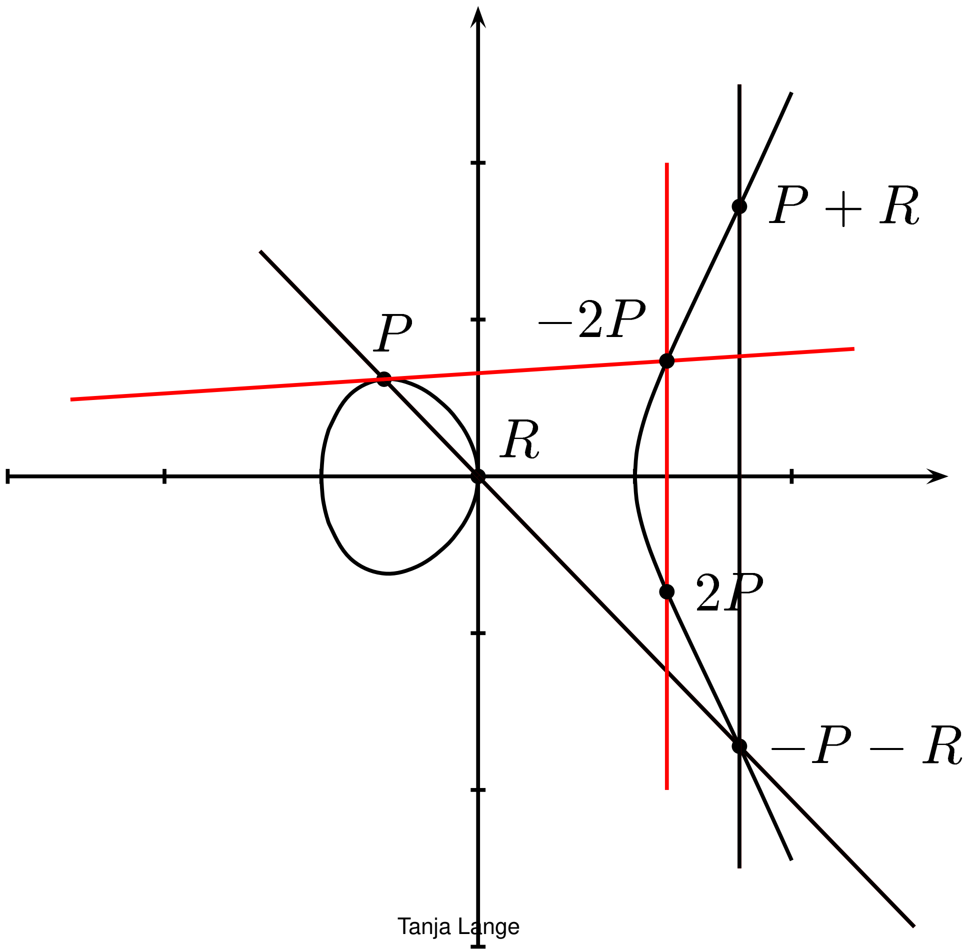


over $\mathbb{R}$

Elliptic Curve

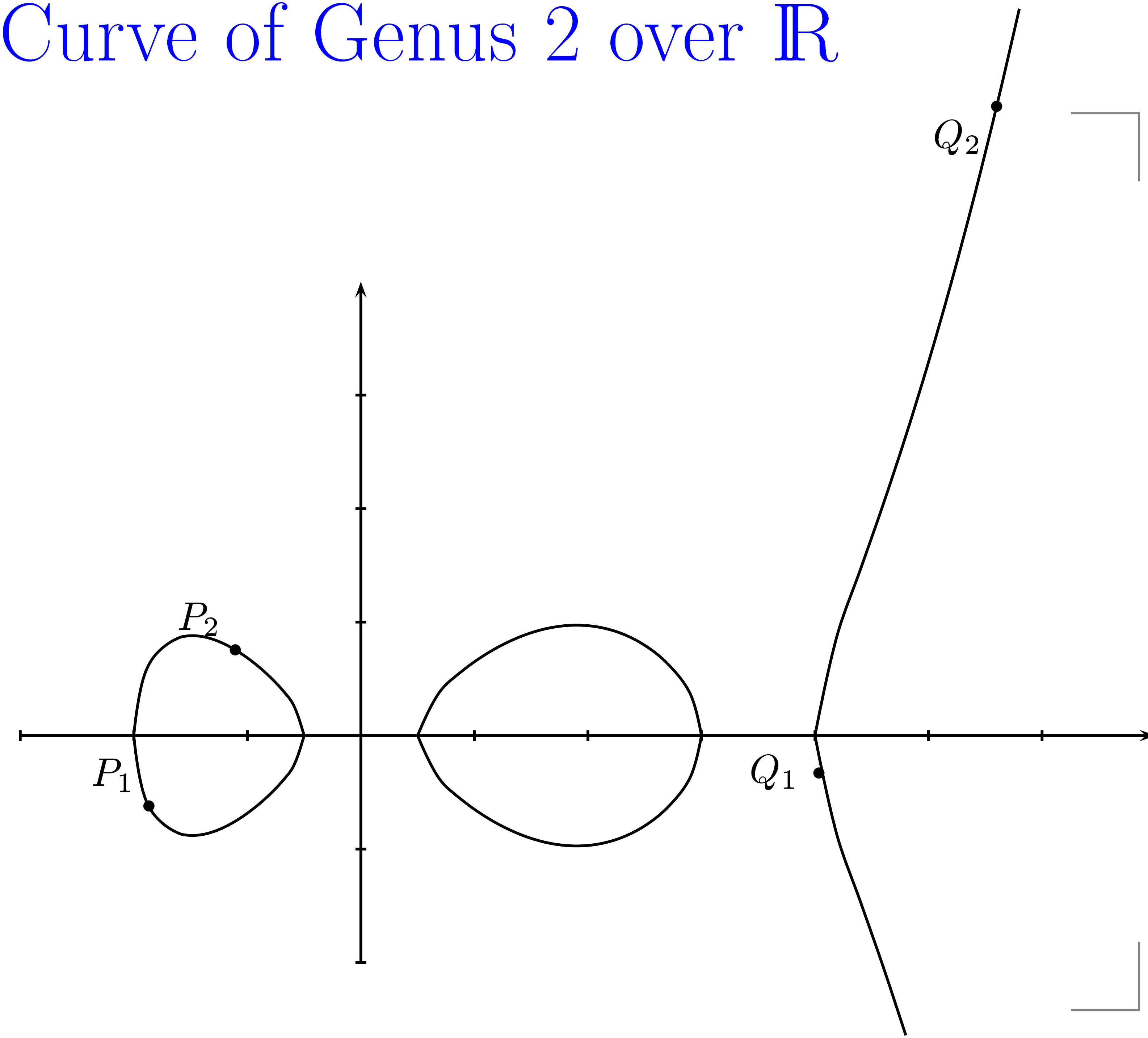
$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}, \quad h, f \in \mathbb{F}_q[x]$$

Group: $E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \}$

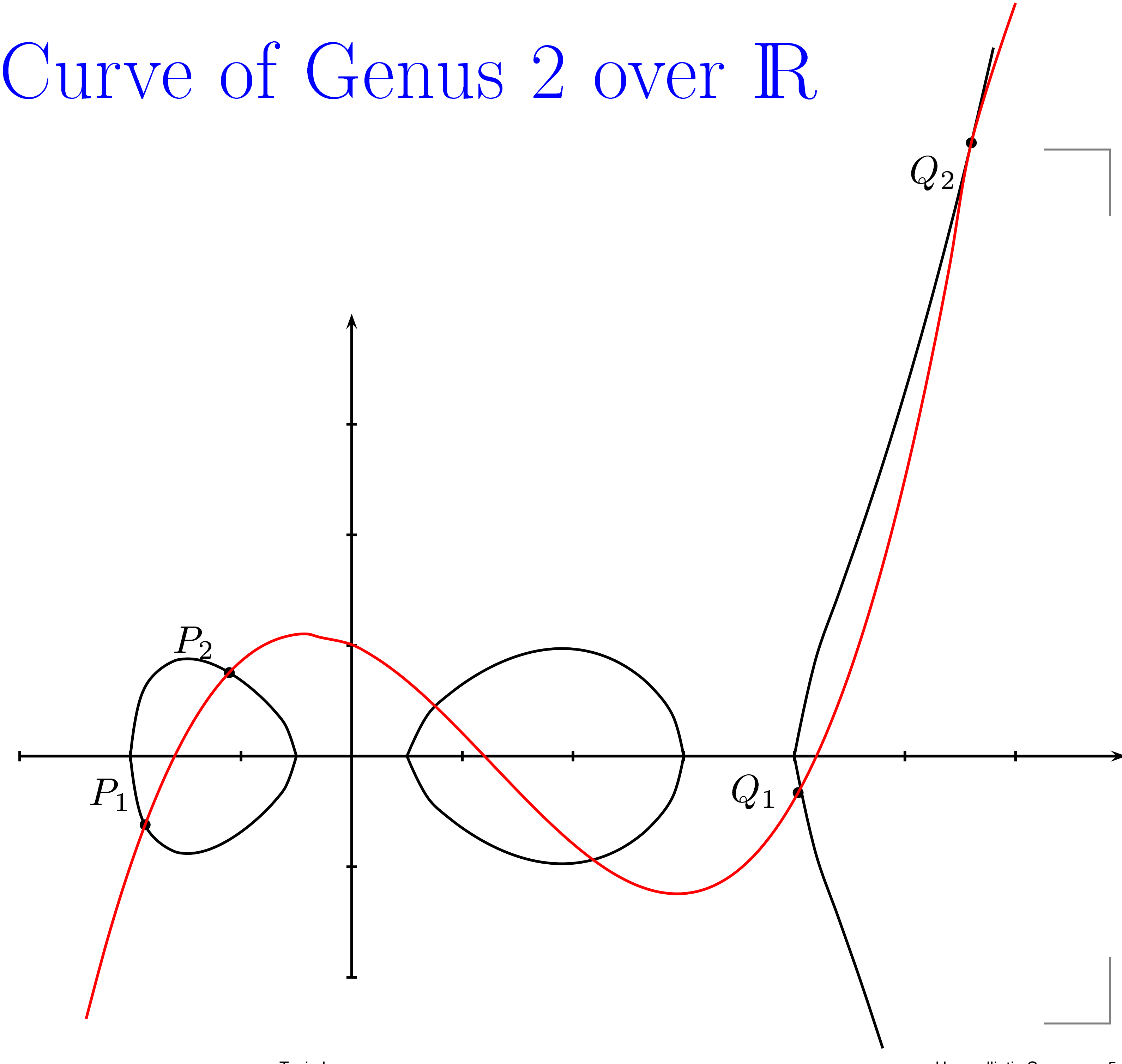


over $\mathbb{R}$

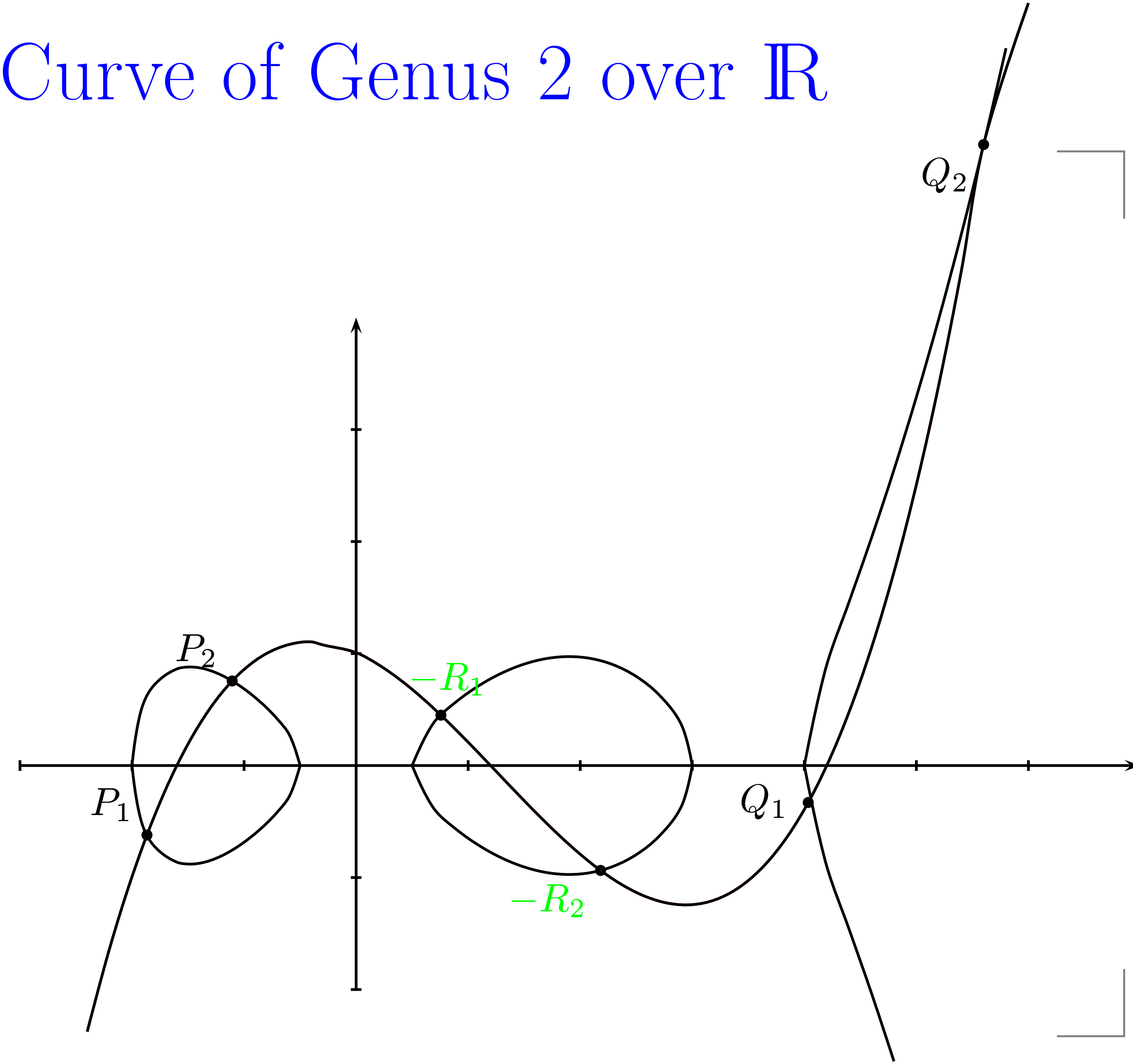
Curve of Genus 2 over $\mathbb{R}$



Curve of Genus 2 over $\mathbb{R}$

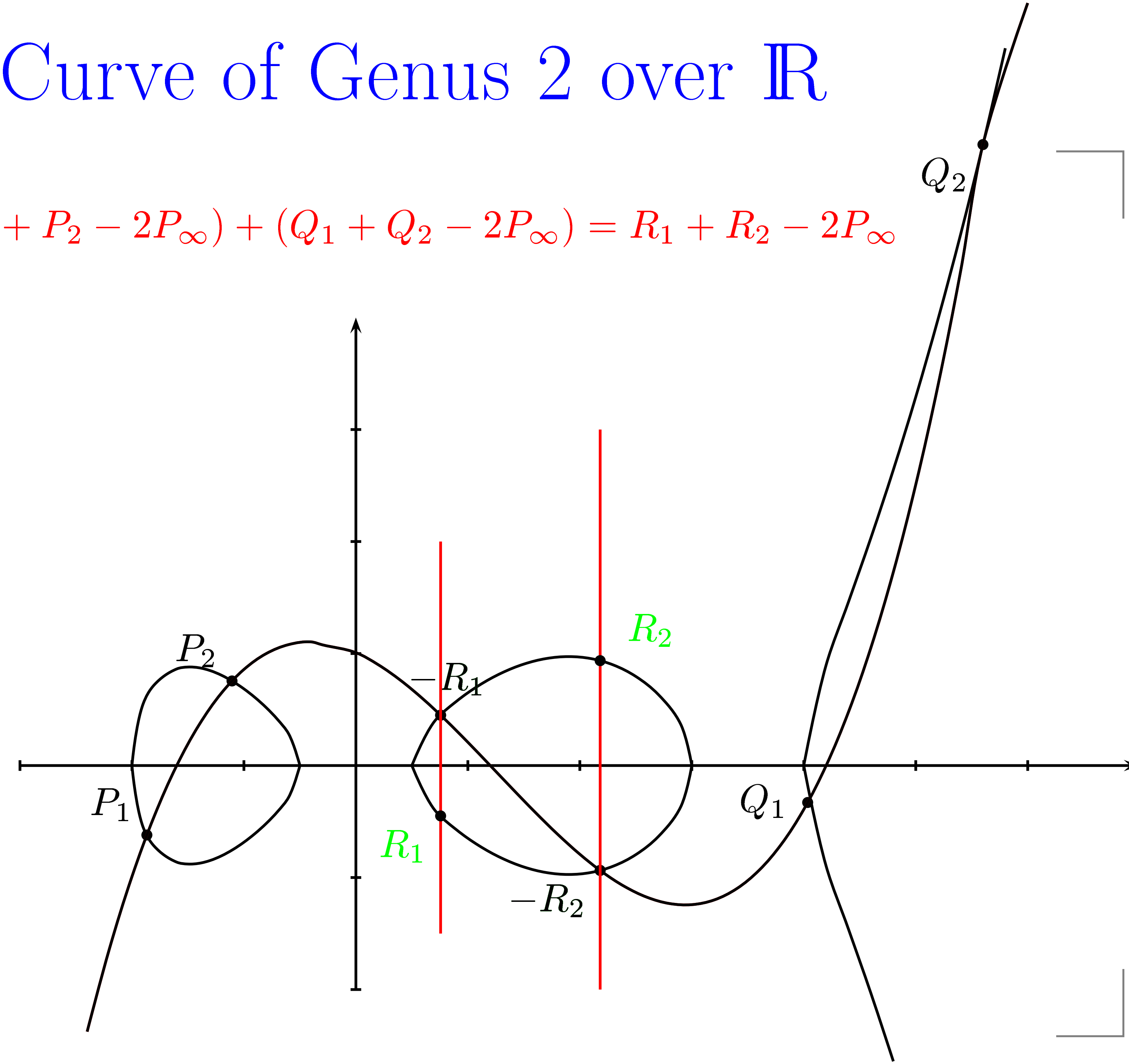


Curve of Genus 2 over $\mathbb{R}$



Curve of Genus 2 over $\mathbb{R}$

$$(P_1 + P_2 - 2P_\infty) + (Q_1 + Q_2 - 2P_\infty) = R_1 + R_2 - 2P_\infty$$



Arithmetic on hyperelliptic curves

Composition & Reduction (Cantor/Koblitz)

`IN:` $D_1 = [u_1, v_1], D_2 = [u_2, v_2], C : y^2 + h(x)y = f(x)$
`OUT:` $D = [u, v]$ reduced with $D \sim D_1 + D_2$

1. compute $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$
2. compute $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2(v_1 + v_2 + h)$
3. let $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$
4. $u = \frac{u_1 u_2}{d^2} \quad v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$
5. let $u' = \frac{f - vh - v^2}{u} \quad b' = (-h - v) \bmod u'$
6. if $\deg u' > g$ put $u := u', v := v'$ goto step 5
7. make u monic

Addition, $g = 2$

Addition, $\deg u_1 = \deg u_2 = 2$		
Input	$[u_1, v_1], [u_2, v_2], u_i = x^2 + u_{i1}x + u_{i0}, v_i = v_{i1}x + v_{i0}$	
Output	$[u', v'] = [u_1, v_1] + [u_2, v_2]$	
Step	Expression	Operations
1	<u>compute resultant r of u_1, u_2:</u> $z_1 = u_{11} - u_{21},\ z_2 = u_{20} - u_{10},\ z_3 = u_{11}z_1 + z_2;$ $r = z_2z_3 + z_1^2u_{10};$	1S, 3M
2	<u>compute almost inverse of u_2 modulo u_1 ($inv = r/u_2 \bmod u_1$):</u> $inv_1 = z_1,\ inv_0 = z_3;$	
3	<u>compute $s' = rs \equiv (v_1 - v_2)inv \bmod u_1$:</u> $w_0 = v_{10} - v_{20},\ w_1 = v_{11} - v_{21},\ w_2 = inv_0w_0,\ w_3 = inv_1w_1;$ $s'_1 = (inv_0 + inv_1)(w_0 + w_1) - w_2 - w_3(1 + u_{11}),\ s'_0 = w_2 - u_{10}w_3;$ if $s'_1 = 0$ see below	5M
4	<u>compute $s'' = x + s_0/s_1 = x + s'_0/s'_1$ and s_1:</u> $w_1 = (rs'_1)^{-1}(= 1/r^2s_1),\ w_2 = rw_1(= 1/s'_1),\ w_3 = {s'}_1^2w_1(= s_1);$ $w_4 = rw_2(= 1/s_1),\ w_5 = w_4^2,\ s''_0 = s'_0w_2;$	I, 2S, 5M
5	<u>compute $l' = s''u_2 = x^3 + l'_2x^2 + l'_1x + l'_0$:</u> $l'_2 = u_{21} + s''_0,\ l'_1 = u_{21}s''_0 + u_{20},\ l'_0 = u_{20}s''_0$	2M
6	<u>compute $u' = (s(l + h + 2v_2) - k)/u_1 = x^2 + u'_1x + u'_0$:</u> $u'_0 = (s''_0 - u_{11})(s''_0 - z_1 + h_2w_4) - u_{10} + l'_1 + (h_1 + 2v_{21})w_4 + (2u_{21} + z_1 - f_4)w_5;$ $u'_1 = 2s''_0 - z_1 + h_2w_4 - w_5;$	3M
7	<u>compute $v' \equiv -h - (l + v_2) \bmod u' = v'_1x + v'_0$:</u> $w_1 = l'_2 - u'_1,\ w_2 = u'_1w_1 + u'_0 - l'_1,\ v'_1 = w_2w_3 - v_{21} - h_1 + h_2u'_1;$ $w_2 = u'_0w_1 - l'_0,\ v'_0 = w_2w_3 - v_{20} - h_0 + h_2u'_0;$	4M
total		I, 3S, 22M

Projective Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P \oplus Q = (X_3 : Y_3 : Z_3)$
on $E : Y^2Z = X^3 + a_4XZ^2 + a_6$

Addition: $P \neq \pm Q$

$A = Y_2Z_1 - Y_1Z_2, B = X_2Z_1 - X_1Z_2,$

$C = A^2Z_1Z_2 - B^3 - 2B^2X_1Z_2$

$X_3 = BC, Z_3 = B^3Z_1Z_2$

$Y_3 = A(B^2X_1Z_2 - C) - B^3Y_1Z_2,$

Doubling $P = Q \neq P$

$A = a_4Z_1^2 + 3X_1^2, B = Y_1Z_1,$

$C = X_1Y_1B, D = A^2 - 8C$

$X_3 = 2BD, Z_3 = 8B^3.$

$Y_3 = A(4C - D) - 8Y_1^2B^2$

No inversion is needed and the computation times are $12M + 2S$ for a general addition and $7M + 5S$ for a doubling.

Jacobian Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P \oplus Q = (X_3 : Y_3 : Z_3)$
on $Y^2 = X^3 + a_4 X Z^4 + a_6 Z^6$ by

Addition: $P \neq \pm Q$

$A = X_1 Z_2^2, B = X_2 Z_1^2, C = Y_1 Z_2^3,$

$D = Y_2 Z_1^3, E = B - A, F = D - C$

$X_3 = -E^3 - 2AE^2 + F^2, Z_3 = Z_1 Z_2 E,$

$Y_3 = -CE^3 + F(AE^2 - X_3),$

Doubling $P = Q \neq P$

$A = 4X_1 Y_1^2, B = 3X_1^2 + a_4 Z_1^4$

$X_3 = -2A + B^2, Z_3 = 2Y_1 Z_1$

$Y_3 = -8Y_1^4 + B(A - X_3).$

No inversion is needed and the computation times are
$12M + 4S$ for a general addition and $4M + 6S$ for a doubling.