Summer School on Elliptic and Hyperelliptic Curve Cryptography
Exercises for lectures on Tuesday, 12.09.2006

Hyperelliptic-curves exercises
Here is the condition on the derivatives of v:
Let $D = \sum_{i=1}^{m} P_i - mP_\infty$, with P_i affine, $P_i \neq \iota P_j$ for $i \neq j$ and $m \leq g$. Put $P_i = (x_i, y_i)$. Then the corresponding polynomials are defined by $u = \prod_{i=1}^{m}(x - x_i)$ and the property that if P_i occurs n_i times then

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 + v(x)h(x) - f(x)\right]_{|x=x_i} = 0, \quad \text{for } 0 \leq j \leq n_i - 1.$$

[HEC1] Consider $C : y^2 = x^5 + 4x^3 + 3x^2 + 11x + 5$ over $\mathbb{F}_{17}$. Find at least one divisor class defined over $\mathbb{F}_{17}$ where in the Mumford representation u is irreducible of degree 2.

[HEC2] Show that for elliptic curves every divisor class can be represented in the form $P_1 - P_\infty$ or as 0. Explain how the computation modulo principal divisors translates to the chord and tangent method (i.e. why do we work with points rather than classes, how do we get intersecting lines or tangents rather than more general functions.

[HEC3] Show by direct computation that for $g = 2$ each class can be represented with at most 2 affine points, i.e. start with a degree zero divisor of arbitrary length and show how to reduce it.

[HEC4] Let C be a hyperelliptic curve of genus g. For $D, E \in \mathrm{Div}_C$ define a partial order $D \geq E$ iff $D - E$ is effective. Let $\mathrm{L}(D) := \{f \in K(C) \mid \mathrm{div}(f) \geq -D\}$. One sees that $L(D)$ is a K-vector space of some dimension $\ell(D)$. The *Theorem of Riemann-Roch* says:
For every divisor $D \in \mathrm{Div}_C$ one has

$$\ell(D) \geq \deg(D) - g + 1.$$

For all $D \in \mathrm{Div}_C$ with $\deg(D) > 2g - 2$ one even has equality $\ell(D) = \deg(D) - g + 1$.

Use this or direct calculation (and hand-waving) to show that each divisor class can be uniquely represented by a reduced divisor.

[HEC5] An elliptic curve E/K is defined to be a smooth genus 1 curve with at least 1 K-rational point. Use this definition and the Riemann-Roch Theorem to prove that each elliptic curve can be represented by a Weierstrass equation.
What is different if you consider curves of larger genus?

Index-calculus exercise

[IC1] Let $p = 5387$. In that case $\mathbb{F}_p^* = \langle 2 \rangle$ is generated by 2. We want to solve the DLP $h = 2^x = 2909$ in $\mathbb{F}_p^*$ using the factor base $\mathcal{F}(11) = \{2, 3, 5, 7, 11\}$.

Hints:
1. To find relations try arbitrary exponents – or use 2^r for
$r \in \{1067, 3721, 4409, 1619, 2072, 4200, 4806\}$.
2. Compute the discrete logarithm $x(q)$ for all elements q in the factor base $q = 2^{x(q)}$. E.g. the exponent 1619 directly gives the discrete logarithm of 7 to the base 2.
3. Finally find a power y of 2 so that $h \cdot 2^y$ is B-smooth. If you are desperate, try $y = 145$.

Elliptic-curves-2 exercises

[EC21] Let p be prime, and let $\mathbb{F}_p$ be the finite field with p elements.

a Let $\alpha, \beta \in \mathbb{F}_p^*$ be non-squares. Prove that the product $\alpha\beta$ is a square.

b Let $E/\mathbb{F}_p$ be the elliptic curve defined by the Weierstraß equation $Y^2 = X^3 + aX + b$, and let $t = p + 1 - \#E(\mathbb{F}_p) \in \mathbb{Z}$ be the trace of the Frobenius morphism of E. For a non-square $g \in \mathbb{F}_p^*$, define the curve $E_g : Y^2 = X^3 + g^2aX + bg^3$. Prove that the trace of Frobenius of E_g is $-t$, i.e., that E_g has $p + 1 + t$ points.
('The' curve E_g is called the *quadratic twist* of E.)

[EC22] Let q be a prime power, and let $\mathbb{F}_q$ be the finite field with q elements. Let E be an *ordinary* elliptic curve over $\mathbb{F}_q$. Prove that the endomorphism ring $\mathrm{End}(E)$ is *not* isomorphic to $\mathbb{Z}$. (NB: as mentioned in class, this statement also holds for supersingular curves.)

[EC23] The goal of this exercise is to prove Hasse's theorem on the number of points of $E/\mathbb{F}_q$ using the machinery developed in class. You are allowed to use

- the involution $\bar{\cdot}$ on $\mathrm{End}(E)$
- $\deg(F_q) = q$
- degrees are non-negative.

Let $t = F_q + \overline{F}_q \in \mathbb{Z}$ be the trace of Frobenius. Compute $\deg(t - 2F_q)$ and conclude $|t| \leq 2\sqrt{q}$.

Background-CM exercises

[BCM1] a Do the *odd* numbers form an ideal of $\mathbb{Z}$?

b Prove that we have $\mathbb{Z}[i]/(1 + i) \cong \mathbb{F}_2$, and $\mathbb{Z}[i]/(3) \cong \mathbb{F}_9$.

[BCM2] Let $\mathcal{O}_K$ be the maximal order of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D}) \subset \mathbb{C}$.

a Prove that the invertible elements of $\mathcal{O}_K$ lie on the unit circle, i.e., are roots of unity.

b Prove that the only invertible elements of $\mathcal{O}_K$ are $+1$ and -1, except for $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\sqrt{-3})$. What are the invertible elements in these two exceptional cases?

[BCM3] Define the *norm* $N : \mathbb{Z}[i] \to \mathbb{Z}$ by $N(a + bi) = a^2 + b^2$.

a Let α, β be elements of $\mathbb{Z}[i]$ with $\beta \neq 0$. Prove that there exist $q, r \in \mathbb{Z}[i]$ with $\alpha = q\beta + r$ and with $N(r) < N(\beta)$. (Hint: draw in a picture what this condition means for the quotient $\frac{\alpha}{\beta} \in \mathbb{Q}(i) \subset \mathbb{C}$.)

b Let I be an ideal in $\mathbb{Z}[i]$, and let x be an element of I of *minimal* norm. Prove that we have $I = (x)$. Conclude that $\mathbb{Z}[i]$ has class number 1.