Summer School on Elliptic and Hyperelliptic Curve Cryptography
Exercises for lectures on Friday, 15.09.2006

Parings-II exercises

[PII1] Let $E/\mathbb{F}_{2^n}$ be supersingular. Investigate which embedding degrees can appear. If that feels to hard, consider the question over $\mathbb{F}_2, \mathbb{F}_4, \ldots$.

[PII2] Let $E/\mathbb{F}_{3^n}$ be supersingular. Investigate which embedding degrees can appear. If that feels to hard, consider the question over $\mathbb{F}_3, \mathbb{F}_9, \ldots$.

Parings-frienly-curves exercises

[PFC1] Let $\phi_d(X)$ be the d-th cyclotomic polynomial. That means that the roots of ϕ_d are exactly the primitive d-th roots of unity. Show $\deg(\phi_d) = \varphi(d)$.

[PFC2] One has

$$X^k - 1 \prod_{d|k} \phi_d(X).$$

Show that k minimal with $\ell \mid q^k - 1$ is equivalent to

$$\ell \mid \phi_k(q), \text{ and } \ell \nmid \phi_d(q) \text{ for } d < k.$$

Index-calculus-HEC-II exercises

[ICH1] Solve this again, now with the knowledge of today's lecture:
Given an elliptic curve $E/\mathbb{F}_q : y^2 = x^3 + ax + b$, we could try a substitution $\tilde{x} = x^d$ to embed E into a hyperelliptic curve C and then solve the discrete logarithm problem in the group $\mathrm{Pic}^0_C(\mathbb{F}_q)$ using index calculus. Why doesn't that give a faster attack for the ECDLP?
Hint: What genus would you need for C?