Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Dr. Peter Ullrich

WS 2004/05
Übungsblatt 6
25. November 2004

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 1.12.04

Aufgabe 1

Zeigen Sie die Korrektheit der Verifikationsprozedur im ElGamal-DS- und DSA-Verfahren.

Aufgabe 2

Sei K ein Körper und $f \in K[X]$ ein normiertes, irreduzibles Polynom vom Grad $d > 0$. Es bezeichne x die Restklasse von X in $K[X]/(f)$. Zeigen Sie, dass $1, x, x^2, \ldots, x^{d-1}$ eine K-Vektorraumbasis von $K[X]/(f)$ ist.

Aufgabe 3

(a) Zeigen Sie, dass die Polynome $X^2 + 1$ und $X^2 \pm X - 1$ irreduzibel in $\mathbb{F}_3[X]$ sind.

(b) Sei $f(X) = X^2 + 1$. Dann ist $\mathbb{F}_9 = \mathbb{F}_3[X]/(f)$ und nach Aufgabe 2 ist $1, x$ ($x =$ Restklasse von X in $\mathbb{F}_2[X]/(f)$) eine $\mathbb{F}_3$-Vektorraumbasis von $\mathbb{F}_9$. Bestimmen Sie alle Potenzen von x. Ist x ein Generator von $\mathbb{F}_9^*$? Berechnen Sie zudem $(2+2x)^2$, $(2+x)(1+x)$ und $(1 + x)(1 - 2x)$ in $\mathbb{F}_9$.

(c) Wie (b) mit $f(X) = X^2 - X - 1$ anstelle von $X^2 + 1$.

Aufgabe 4

Sei $q = p^d$ eine Primzahlpotenz. Für jeden Teiler e von d sei I_e die Menge aller normierten, irreduziblen Polynome in $\mathbb{F}_p[X]$ vom Grad e und $n_e = \#I_e$. Zeigen Sie:

(a) $X^q - X = \prod_{e|d} \prod_{f \in I_e} f$.

(b) $q = \sum_{e|d} e n_e$.