RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Jun.-Prof. Roberto Avanzi
Enrico Thomae

Hausübungen zur Vorlesung

Diskrete Mathematik II

SoSe 2010

Blatt 6 / 29. Juni 2010 / Abgabe bis spätestens 13. Juli 2010, 10:00 Uhr

AUFGABE 45 (8 Punkte)**:**
Sei $\mathbb{F}_5$ der Körper mit 5 Elementen. Verifizieren Sie, dass 2 kein Quadrat in $\mathbb{F}_5$ ist, und konstruieren Sie somit den Körper $\mathbb{F}_{25}$ mit 25 Elementen als die durch das Polynom $z^2 - 2$ definierte Körpererweiterung von $\mathbb{F}_5$.

Betrachten Sie die über $\mathbb{F}_5$ durch folgende Gleichung definierte Kurve

$$E : y^2 = x^3 + x + 2 \ .$$

(a) Zeigen Sie, dass E eine elliptische Kurve ist.

(b) Bestimmen Sie alle Punkte auf E über $\mathbb{F}_5$.

(c) Bestimmen Sie alle Punkte auf E über $\mathbb{F}_{5^2}$, die nicht über $\mathbb{F}_5$ definiert sind.

(d) Geben Sie die Punkte der Ordnung 2 auf $E(\mathbb{F}_5)$ an.

(e) Geben Sie die Punkte der Ordnung 2 auf $E(\mathbb{F}_{5^2})$ an.

(f) Finden Sie einen Punkt P in $E(\mathbb{F}_{5^2})\backslash E(\mathbb{F}_5)$ derart, dass $2 \cdot P \in E(\mathbb{F}_5)$ aber $2 \cdot P \neq 0$.

AUFGABE 46 (5 Punkte)**:**
Sei $p > 3$ eine Primzahl, $a, b \in \mathbb{F}_p$. Zeigen Sie, dass die zu $E : y^2 = x^3 + ax + b$ gehörende Gruppe $(E, +)$ der über $\mathbb{F}_p$ definierten Punkte der Kurve nicht zyklisch ist, falls

$$x^3 + ax + b \equiv 0 \pmod{p} \tag{1}$$

drei verschiedene Lösungen hat.

Hinweis: Betrachten Sie sich die Ordnung, der durch (1) gegebenen Punkte.

AUFGABE 47 (8 Punkte)**:**
Zeigen Sie, dass der in der Vorlesung gegebene Algorithmus zur Berechnung der w-NAF korrekt ist, d.h. der Algorithmus terminiert und liefert die korrekte Ausgabe, wenn eine der zwei dort gegebenen Ziffernmengen verwendet wird. Zeigen Sie auch, dass die erwartete Dichte der w-NAF einer Zufallszahl $\frac{1}{w+1}$ ist. Was ist der Vorteil der 2. Ziffernmenge bei elliptischen Kurven?

AUFGABE 48 (7 Punkte)**:**
Betrachten Sie die elliptische Kurve $E : y^2 = x^3 + ax + b$ über $\mathbb{F}_p$ mit $p > 3$ prim.

(a) Wir wissen, dass ein Punkt $P = (x_1, y_1) \in E$ genau dann die Ordnung 3 besitzt, wenn $2P = -P$. Nutzen Sie dies, um zu zeigen das aus $P = (x_1, y_1) \in E$ von Ordnung 3 folgt, dass

$$3x_1^4 + 6ax_1^2 + 12x_1b - a^2 \equiv 0 \pmod{p}. \tag{2}$$

(b) Schließen Sie aus (2), dass es auf der elliptischen Kurve E höchstens 8 Punkte von Ordnung 3 gibt.

(c) Benutzen Sie (2) um alle Punkte der Ordnung 3 auf der elliptischen Kurve $y^2 \equiv x^3 + 34x \pmod{73}$ zu bestimmen.