Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2015/16
27. Jan. 2016

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 12

Aufgabe 45

Man zeige: Für eine Primzahl $p \equiv 1 \bmod 4$ haben die elliptischen Kurven

$$E : y^2 = x^3 + x + b \quad \text{und} \quad E' : y^2 = x^3 + x - b$$

über dem Körper $\mathbb{F}_p$ gleich viele Elemente. Was passiert im Fall $p \equiv 3 \bmod 4$?

Aufgabe 46

Sei E eine elliptischen Kurve über dem Körper $\mathbb{F}_p$, (p Primzahl > 3), deren affiner Teil durch eine Gleichung der Gestalt

$$y^2 = a_3x^3 + a_2x^2 + a_1x, \quad a_i \in \mathbb{F}_p,$$

gegeben wird. Man zeige: Die Ordnung von E ist eine gerade Zahl.

Aufgabe 47

Sei p eine Primzahl > 3. Man zeige, dass jede elliptische Kurve $Y^2 = X^3 + AX + B$ über dem Körper $\mathbb{F}_p$ durch eine Transformation $(X, Y) \mapsto (\alpha x, \beta y)$, $\alpha, \beta \in \mathbb{F}_p^*$, isomorph auf eine Kurve abgebildet werden kann, die eine der folgenden drei Gestalten hat:

i) $y^2 = x^3 + b$,

ii) $y^2 = x^3 + x + b$,

iii) $y^2 = x^3 + a_0x + b$.

Dabei ist $a_0 \in \mathbb{F}_p^*$ ein beliebig vorgegebener quadratischer Nichtrest modulo p.

---

b.w.

Aufgabe 48

Alice benutzt eine EC-Variante des ElGamal Public Key Kryptosystems. Die zugrunde liegende elliptische Kurve über dem Körper $\mathbb{F}_p$ mit $p = 85470\,62921$ sei gegeben durch

$$E: \quad Y^2 = X^3 + X + 60.$$

Außerdem sind Punkte

$$P_0 = (10000\,00001, 48575\,61959), \quad P = (68316\,95389, 28678\,59999) \in E$$

gegeben, wobei P_0 Primzahl-Ordnung $q = 85469\,44457$ hat und $P = \omega \cdot P_0$ mit einem geheimen $\omega \in \mathbb{Z}/q$. Alice's Public Key ist nun (E, p, q, P_0, P).

Wenn Bob eine verschlüsselte Nachricht an Alice senden will, teilt er die Nachricht in Blöcke von 4 Bytes. Ein Block (b_0, b_1, b_2, b_3), $(0 < b_\nu < 2^8)$, wird als 32-Bit-Zahl $x = \sum_{\nu=0}^{3} b_\nu \cdot 2^{8\nu}$ interpretiert. Ein solcher Block wird wie folgt verschlüsselt: Bob wählt eine (vom Block abhängige) geheim zu haltende Zufallszahl $\alpha \in (\mathbb{Z}/q)^*$ und berechnet die Punkte

$$A_0 := \alpha \cdot P_0 = (\xi_0, \eta_0), \quad A := \alpha \cdot P = (\xi, \eta) \in E.$$

Die Verschlüsselung von x ist dann

$$y = (\xi_0,\ \eta_0 \bmod 2,\ \xi x \bmod p) \in (\mathbb{Z}/p) \times (\mathbb{Z}/2) \times (\mathbb{Z}/p).$$

Man entschlüssele den folgenden, aus einem 20 Bytes langen ASCII-Klartext entstandenen Geheimtext

$$\begin{aligned}
&(17143\,95687,\ 0,\ 78155\,21784),\\
&\quad (715\,77867,\ 1,\ 84588\,52664),\\
&(84439\,74843,\ 0,\ 60487\,94212),\\
&(43573\,74450,\ 1,\ 82421\,77945),\\
&\quad (7576\,68770,\ 0,\ 56744\,00855),
\end{aligned}$$

indem man das DL-Problem $P = \omega \cdot P_0$ auf der Kurve E für das unbekannte ω löse.