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

WS 2018/19
19. Dez. 2018

Übungen zur Vorlesung Kryptographie

Blatt 10

Aufgabe 37

Sei $p > 3$ eine Primzahl und $a \in (\mathbb{Z}/p)^*$. Man beweise:

a) Falls $3 \mid (p-1)$, besitzt a genau dann eine Kubikwurzel (d.h. die Kongruenz $x^3 \equiv a \bmod p$ ist lösbar), wenn

$$a^{(p-1)/3} \equiv 1 \bmod p.$$

Es gibt dann genau 3 Kubikwurzeln von a mod p.
Man bestimme diese im Fall $p = 13$, $a = 5$.

b) Falls $3 \nmid (p-1)$, besitzt jedes $a \in (\mathbb{Z}/p)^*$ genau eine Kubikwurzel. Wie kann man diese effizient berechnen?

Aufgabe 38

Sei p eine Primzahl und $g \in (\mathbb{Z}/p)^*$ eine Primitivwurzel modulo p. Beim Pollardschen Algorithmus zur Berechnung des diskreten Logarithmus $\log_g(x)$ eines Elements $x \in (\mathbb{Z}/p)^*$ entstehe eine Kongruenz

$$g^\mu x^\nu \equiv 1 \bmod p.$$

Falls $\gcd(\nu, p-1) = 1$, erhält man bekanntlich den diskreten Logarithmus als

$$\log_g(x) \equiv -\lambda\mu \bmod (p-1),$$

wobei λ ein Inverses von ν modulo $p-1$ ist.

Sei nun vorausgesetzt, dass $\gcd(\nu, p-1) = d > 1$ mit einer kleinen natürlichen Zahl d. Man zeige, dass dann auch μ durch d teilbar ist, und mit $\nu' := \nu/d$, $\mu' := \mu/d$ gilt in $(\mathbb{Z}/p)^*$

$$g^{\mu'} x^{\nu'} = w,$$

wobei w eine d-te Einheitswurzel modulo p ist (d.h. $w^d \equiv 1 \bmod p$). Wie kann man damit $\log_g(x)$ effizient berechnen?

---

b.w.

Aufgabe 39

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.

Wie verhält sich $\#E(\mathbb{F}_p)$ zu $\#E'(\mathbb{F}_p)$ im Fall $p \equiv 3 \bmod 4$?

Aufgabe 40

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

$$y^2 = a_3x^3 + a_2x^2 + a_1x, \quad a_i \in \mathbb{F}_p,\ a_3 \neq 0,$$

gegeben wird.

a) Welchen Bedingungen müssen die Koeffizienten a_1, a_2, a_3 genügen, damit das Polynom $P(x) = a_3x^3 + a_2x^2 + a_1x$ keine mehrfachen Nullstellen hat?

b) Man zeige: Die Ordnung $\#E(\mathbb{F}_p)$ ist eine gerade Zahl.