Übungsblatt 7

Aufgabe 50 ***mündlich***

Sei p eine ungerade Primzahl und $\mathrm{ggT}(a,p)=1$.

(a) Sei $i \geq 2$ und $b^2 \equiv_{p^{i-1}} a$. Zeigen Sie, dass es genau ein $x \in \mathbb{Z}_{p^i}$ gibt mit $x^2 \equiv_{p^i} a$ und $x \equiv_{p^{i-1}} b$. Wie kann x effizient berechnet werden?

(b) Berechnen Sie mit Ihrem Verfahren ausgehend von $6^2 \equiv_{19} 17$ die Wurzeln von 17 modulo 19^2 und modulo 19^3.

(c) Zeigen Sie für jedes $i \geq 1$, dass die Kongruenz $x^2 \equiv_{p^i} a$ entweder 0 oder 2 Lösungen hat.

Aufgabe 51 ***mündlich***

Faktorisieren Sie $n = 256961$ mit der Methode der zufälligen Quadrate. Verwenden Sie die Faktor-Basis

$$\{-1, 2, 3, 5, 7, 11, 13, 17, 19, 29, 31\}$$

und testen Sie die Zahlen $z^2 \bmod n$ mit $z = 500, 501, \ldots$, bis Sie eine Kongruenz der Form $x^2 \equiv_n y^2$ erhalten und die Faktorisierung von n finden.

Aufgabe 52 ***mündlich***

Mit welcher Wahrscheinlichkeit kann eine Zahl n mit der Methode der zufälligen Quadrate erfolgreich faktorisiert werden, wenn als Basis $\mathcal{B} = \{2, 3, 5, \ldots, p_b\}$ verwendet wird und $c > b + 1$ Quadratzahlen $z_i = x_i^2$ über $\mathcal{B}$ faktorisiert werden konnten?

Aufgabe 53 ***mündlich***

Die Punkte der *projektiven Ebene* werden durch die Ursprungsgeraden

$$g(X,Y,Z) = \{(\lambda X, \lambda Y, \lambda Z) \mid \lambda \in \mathbb{R}\},\ (X,Y,Z) \in \mathbb{R}^3 - \{(0,0,0)\}$$

gebildet. Es gilt also $g(X,Y,Z) = g(X',Y',Z')$, falls ein $\lambda \in \mathbb{R} - \{0\}$ existiert mit $X' = \lambda X$, $Y' = \lambda Y$ und $Z' = \lambda Z$.

(a) Überlegen Sie, wie sich die affine Ebene $\mathbb{R}^2$ in die projektive Ebene einbetten lässt. (*Hinweis:* Verwenden Sie nur projektive Punkte der Form $g(X,Y,1)$.)

(b) Zeigen Sie, dass von dieser Einbettung genau die projektiven Punkte der Form $g(X,Y,0)$ nicht erfasst werden. Welche Punkte müsste man zum $\mathbb{R}^2$ hinzunehmen, damit diese Einbettung zu einem Isomorphismus wird? Geben Sie eine geometrische Interpretation dieser Punkte.

(c) Im $\mathbb{R}^2$ sei eine Kurve durch eine Gleichung der Form $F(x,y) = y^2 - x^3 - ax - b = 0$ definiert. Wie lässt sich hieraus eine Kurvengleichung $\tilde{F}(X,Y,Z) = 0$ für die Einbettung $\{g(x,y,1) \mid F(x,y) = 0\}$ dieser Kurve in die projektive Ebene gewinnen?

(d) Welche projektiven Punkte der Form $g(X,Y,0)$ erfüllen ebenfalls die Gleichung $\tilde{F}(X,Y,Z) = 0$?

Aufgabe 54 ***mündlich***

Sei E eine durch die Gleichung $F(x,y) = 0$ im $\mathbb{R}^2$ definierte Kurve, wobei F die Form $F(x,y) = y^2 - x^3 - ax - b$ hat. Zeigen Sie, dass folgende Bedingungen äquivalent sind.

(a) Das Polynom $p(x) = x^3 + ax + b$ hat eine mehrfache Nullstelle.

(b) Es gilt $4a^3 = -27b^2$.

(c) Es ex. ein Punkt $(x_0, y_0) \in E$, für den die partiellen Ableitungen $\frac{\delta F}{\delta x}(x_0,y_0)$ und $\frac{\delta F}{\delta y}(x_0,y_0)$ beide 0 sind. (Ein solcher Punkt heißt *singulär*.)

Aufgabe 55 ***mündlich***

Geben Sie eine geometrische Bedingung dafür an, dass ein Punkt P auf einer elliptischen Kurve über $\mathbb{R}$ die Ordnung 2, 3 oder 4 hat.

Aufgabe 56 ***mündlich***

Zeigen Sie, dass eine über $\mathbb{Z}_p$ mittels

$$y^2 = x^3 + ax + b$$

definierte elliptische Kurve nicht zyklisch ist, wenn das Polynom $x^3 + ax + b$ drei verschiedene Nullstellen in $\mathbb{Z}_p$ hat.

Aufgabe 57 ***mündlich***

Bestimmen Sie die Anzahl der Punkte der durch

$$y^2 = x^3 - 1$$

über $\mathbb{F}_q$ definierten elliptischen Kurve, falls $q \equiv_6 5$ ist.

Aufgabe 58 ***10 Punkte***

Sei E die über $\mathbb{Z}_{71}$ durch

$$y^2 = x^3 - x$$

definierte elliptische Kurve E.

(a) Bestimmen Sie die Anzahl der Punkte von E.

(b) Zeigen Sie, dass E nicht zyklisch ist.

(c) Bestimmen Sie alle Punkte der Ordnung 1, 2, 3 und 4, sowie einen Punkt maximaler Ordnung in E.