SS 2010 02.07.2010

Übungen zur Vorlesung Computeralgebra
Blatt 12

Prof. Dr. Klaus Madlener Abgabe bis 19.07.2010

Aufgabe 1:
Betrachten Sie folgenden Spezialfall der polynomialen Faktorisierung: Eingabe ist eine Primzahl p und $f \in \mathbb{F}_p[x]$ vom Grad n und Teiler von $x^p - x$, so dass alle monischen irreduziblen Faktoren von f in $\mathbb{F}_p[x]$ linear und unterschiedlich sind. Finden Sie mit Hilfe der Methode nach Pollard und Strassen einen deterministischen Algorithmus zur Faktorisierung von f mit einer oberen Schranke von $O(n\sqrt{p})$ Operationen in $\mathbb{F}_p$, falls $p^2 > n$.

Aufgabe 2:
Sei $x_0 = 2$ und $x_i = x_{i-1}^2 + 1$ für $i \geq 1$. Für $p \in \mathbb{N}$ sei $e(p) = \min\{i \in \mathbb{N}_{\geq 1} : x_i \equiv x_{2i} \bmod p\}$

1. Berechne $e(p)$ für alle Primzahlen $p \leq 13$
2. Berechne $e(p)$ für alle Primzahlen $p \leq 10^6$. Es sollte $e(p) \leq 3680$ für alle diese p sein. Das vermutete Wachstumsverhalten ist $\sqrt{p \ln p}$
3. Sei N die zu faktorisierende Zahl. Angenommen mit Pollard's ϱ-Methode mit Anfangswert $x_0 = 2$ erhält man $\gcd(x_i - x_{2i}, N) = 1$ für $0 \leq i \leq k$. Zeigen Sie, dass dann $e(p) > k$ für alle Primteiler p von N.
4. Schließen Sie daraus, dass N keine Faktoren bis 10^6 hat, wenn der ggT in 3 in 3680 Schritten trivial ist.

Aufgabe 3:
Sei E eine elliptische Kurve und $P, Q \in E$. Erklären Sie, warum $P + Q = S$, wobei S der dritte Schnittpunkt der Geraden durch P und Q mit E ist, keine Gruppenoperation ist.

Aufgabe 4:
Sei F ein Körper, und $f = x^3 + ax + b \in F[x]$

1. Weisen Sie nach, dass $r = \operatorname{res}(f, f') = 4a^3 + 27b^2$.
2. Folgern Sie, dass f QF genau dann wenn $r \neq 0$.
3. Für welche Werte von b definiert $y^2 = x^3 - x + b$ keine elliptische Kurve über $F = \mathbb{R}$? Wie sieht die Kurve für diese Werte aus?

Aufgabe 5:
Sei $N = 8051 = 97 \cdot 83$.

1. Der öffentliche RSA-Schlüssel ist $K = (N, e) = (8051, 3149)$. Wie lautet der dazu gehörige private Schlüssel?
2. Eine Nachricht x ist mit dem Schlüssel K zu 694 verschlüsselt worden. Was ist x?

Aufgabe 6:
Beweisen Sie den zentralen Satz 7.14 zum RSA-Verfahren aus der Vorlesung. Sei $N = pq$ für zwei unterschiedliche Primzahlen $p, q \in \mathbb{N}$.

1. Zeigen Sie, wie man p, q aus N und $\varphi(N)$ berechnen kann. Hinweis: $(x-p)(x-q) \in \mathbb{Z}[x]$
2. Angenommen es gäbe eine Black-Box, die bei Eingabe $e \in \mathbb{N}$ entscheidet, ob e und $\varphi(N)$ teilerfremd sind, und dann auch ein $d \in \{0, \ldots, \varphi(N) - 1\}$ mit $de \equiv 1 \bmod \varphi(N)$ berechnet. Geben Sie einen Algorithmus an, der diese Black-Box benutzt, und $\varphi(n)$ in Zeit $(\log N)^{\mathrm{O}(1)}$ berechnet. Hinweis: Finde ein kleines e, das teilerfremd zu $\varphi(N)$ ist.