RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 12 / 1.–3. Juli 2013

AUFGABE 1:
Faktorisieren Sie die Zahl $n = 221$ mit Hilfe des Quadratischen Siebs. Wählen Sie als Glattheitsschranke $b = 7$. Für die x_i's im Algorithmus wählen Sie $\sqrt{n} < x_i \leq 23$. Aus didaktischen Gründen führen wir den Algorithmus vollständig durch und brechen nicht ab, sobald wir ausreichend viele Relationen gefunden haben.

Bemerkung: $x^2 \equiv 21 \mod 25$ hat die beiden Lösungen $x \equiv 11 \mod 25$ und $x \equiv 14 \mod 25$.

AUFGABE 2:
Faktorisieren Sie (nochmal) die Zahl $n = 221$ mit Hilfe von Pollard's $p-1$-Methode. Nehmen Sie an, dass für einen der Faktoren p gilt, dass $p - 1$ 2-glatt ist.

AUFGABE 3:
Sei $p > 2$ Primzahl und $D, D' \in \mathbb{F}_p$ beides keine Quadrate in $\mathbb{F}_p$. Zeigen Sie, dass sowohl D als auch D' eine Quadratwurzel in $\mathbb{F}_p[\sqrt{D}]$ besitzen. Besitzt jedes $\omega \in \mathbb{F}_p[\sqrt{D}]$ eine Quadratwurzel in $\mathbb{F}_p[\sqrt{D}]$?

Hinweis zur ersten Frage: Was können Sie über die Quadratwurzel von $D^{-1}D'$ sagen?

AUFGABE 4:
Sei R ein kommutativer Ring, $D \in R$ kein Quadrat. Überlegen Sie sich (nochmal), dass die Abbildung $R[\sqrt{D}] \ni \omega \mapsto \overline{\omega} \in R[\sqrt{D}]$ ein Automorphismus ist.

AUFGABE 5:
Sei p Primzahl und $D \in \mathbb{F}_p$ kein Quadrat. Sei $f : \mathbb{F}_p[\sqrt{D}] \to \mathbb{F}_p[\sqrt{D}]$ ein beliebiger Körperautomorphismus.

(a) Zeigen Sie, dass $f(x) = x$ für alle $x \in \mathbb{F}_p \subset \mathbb{F}_p[\sqrt{D}]$ gilt.

(b) Zeigen Sie, dass f $\mathbb{F}_p$-linear ist.

(c) Zeigen Sie, dass entweder $f(\omega) = \omega$ für alle $\omega \in \mathbb{F}_p[\sqrt{D}]$ gilt oder $f(\omega) = \overline{\omega}$ für alle $\omega \in \mathbb{F}_p[\sqrt{D}]$ gilt.

Hinweis zu (c) Welche Werte kann $f(\sqrt{D})$ nur annehmen?