RUHR UNIVERSITÄT BOCHUM

RUB

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

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 12 / 28. Juni 2013 / Abgabe bis spätestens 8. Juli 2013, 12:00 Uhr in dem Kasten auf NA 02 oder am Anfang der Vorlesung

Geben Sie bitte die Aufgaben zur Vereinfachung der Korrektur folgendermassen nach Aufgaben getrennt ab:

- Aufgabe 1 in Kasten A
- Aufgaben 2,3 in Kasten B
- Aufgaben 4,5 in Kasten C

Die Kästen auf NA 02 sind entsprechend beschriftet. Wenn Sie in der Vorlesung abgeben, machen sie einfach 3 getrennte Stapel. Schreiben Sie auf alle 3 Abgaben jeweils Ihre(n) Namen und/oder Matrikelnummer(n).
Bitte schreiben Sie auf Ihre Abgaben eine Sollrückgabestelle (Übungsgruppe, Zentralübung, persönlich in NA5/74).

AUFGABE 1 (5 Punkte)**:**
Faktorisieren Sie die Zahl $n = 143$ mit Hilfe von Pollards $p-1$ Methode. Nehmen Sie an, dass n ein Primfaktor $p \leq 15$ besitzt, für den $p-1$ 3-glatt ist.

Bemerkung: Sie dürfen in Ihrer Lösung die a's (in der Notation im Skript) dabei nicht so wählen, dass $\mathrm{ggT}(n, a) \neq 1$ ist (in diesem Fall würde die Aufgabenstellung uninteressant).

AUFGABE 2 (4 Punkte)**:**
Berechnen Sie die Lösungen der Gleichung $x^2 \equiv 3 \mod 13$ mit Hilfe des Algorithmus von Cippola.

AUFGABE 3 (4 Punkte)**:**
Sei $n = pp'$ Produkt von 2 Primzahlen $p \neq p'$. Sei q bzw. q' der jeweils größte Primteiler von $p-1$ bzw. $p'-1$.
Zeigen Sie:
Wenn $q = q'$ ist und man in Pollards $p-1$ Methode die Glattheitsschranke $b = q$ wählt (und $C = n$ als obere Schranke für die Primzahl), so ist Pollards $p-1$ Methode nur erfolgreich, wenn $\mathrm{ggT}(a, n) > 1$ (in Schritt 2 in der Notation im Skript) ist.

– bitte wenden

AUFGABE 4 (4 Punkte)**:**
Sei K ein Körper, $D \in K$ kein Quadrat und $\omega = a + b\sqrt{D} \in K[\sqrt{D}] \cong K[X]/(X^2 - D)$ wobei $a, b \in \mathbb{F}_p$
Sei f_ω die Multiplikation mit ω, d.h. $f_\omega : K[\sqrt{D}] \to K[\sqrt{D}]$, $f_\omega(x) = \omega x$.

Zeigen Sie:

(a) f_ω ist K-linear

(b) Geben Sie eine darstellende Matrix (über K) von f_ω an.

(c) $\mathrm{Tr}(f_\omega) = \mathrm{Tr}(\omega)$, $\det f_\omega = N(\omega)$.

(d) Was ist das charakteristische Polynom von f_ω?

Bemerkung: In (c),(d) ist mit $\mathrm{Tr}(f_\omega)$ bzw. charakteristischem Polynom die Spur bzw. das charakteristische Polynom der (K-linearen) Abbildung f_ω im Sinne der linearen Algebra gemeint. $\mathrm{Tr}(\omega) = \omega + \overline{\omega}$ ist hingegen via Konjugation definiert.
Hinweis: Eine darstellende Matrix für f_ω kann man direkt aus Aufgabe 5 von Blatt 5 entnehmen.

AUFGABE 5 (3 Punkte)**:**
Sei p Primzahl, $D, D' \in \mathbb{F}_p^*$ beides keine Quadrate in $\mathbb{F}_p$ und somit $X^2 - D$ und $Y^2 - D'$ irreduzibel in $\mathbb{F}_p[X]$ bzw. $\mathbb{F}_p[Y]$

(a) Zeigen Sie, dass es ein $a \in \mathbb{F}_p$ gibt mit $a^2 = \frac{D}{D'}$.

(b) Geben Sie einen Körperisomorphismus $\phi : \mathbb{F}_p[X]/(X^2 - D) \to \mathbb{F}_p[Y]/(Y^2 - D')$ an.

Hinweis zu (b) Überlegen Sie sich, was $\phi(X)$ sein muss. Präsenzblatt 12 ist hilfreich.