RUHR UNIVERSITÄT BOCHUM

RUB

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

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 10 / 14. Juni 2013 / Abgabe bis spätestens 24. Juni 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:

- Aufgaben 1,2 in Kasten A
- Aufgaben 3,4 in Kasten B
- Aufgabe 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 (3 Punkte)**:**
Sei $n = p^k$ mit $p > 2$ prim, $k > 1$. Zeigen Sie, dass die Gleichung

$$x^{n-1} \equiv 1 \mod n$$

höchstens für $p - 1$ viele verschiedene $x \in \mathbb{Z}/(n)$ gilt. Was folgt damit für den Miller-Rabin Test?

AUFGABE 2 (4 Punkte)**:**
Zeigen Sie mittels des Solovay-Strassen Primzahltests, dass 35 und 1105 nicht prim sind.

Bemerkung: 1105 ist eine Carmichael-Zahl (was Sie natürlich in Ihrer Lösung nicht als bekannt voraussetzen dürfen).

AUFGABE 3 (3 Punkte)**:**
Wenden Sie den Rabin-Miller Test auf die Zahl $n = 97$ an.
Wählen Sie $\ell = 2$ und $a_1 = 2, a_2 = 35$.

– bitte wenden –

AUFGABE 4 (6 Punkte)**:**
In dieser Aufgabe wollen wir die Rüchrichtung (n prim $\implies n \mid S_{p-1}$) für den Lucas-Lehmer-Test zeigen:
Sei $n = 2^p - 1$ mit $p \neq 2$, n prim (und damit auch p prim, insbesondere ungerade, vgl. 1. Vorlesung des Semesters). S_k definiert durch $S_1 = 4$ und $S_k = S_{k-1}^2 - 2$. Zeigen Sie:

(a) $(\frac{2}{n}) = +1$

(b) $(\frac{3}{n}) = -1$ und damit $X^2 - 3$ irreduzibel über $\mathbb{F}_n$

(c) In $K = \mathbb{F}_{n^2} = \mathbb{F}_n[X]/(X^2 - 3)$ gilt: $(\overline{a + bX})^n = \overline{a - bX}$ für $a, b \in \mathbb{Z}/(n)$

(d) Für $\omega = \overline{2 + X}$ gilt: $\omega^{-1} = \overline{2 - X} = \omega^n$, $\omega^{2^{k-1}} + \omega^{-2^{k-1}} = \overline{S_k}$.

(e) Für $\eta = \overline{a^{-1}(1 + X)}$ gilt: $\eta^2 = \omega$, wobei $a \in U_n$ mit $a^2 \equiv 2 \mod n$.

(f) $\overline{S_{p-1}} = 0$.

Hinweise/Bemerkungen: Mit $\overline{S_k}$, $\overline{a + bX}$ etc. ist stets die zu $S_k \in \mathbb{Z}$, $a + bX \in \mathbb{F}_n[X]$ etc. gehörige Restklasse in $K = \mathbb{F}_{n^2}$ gemeint (und nicht etwa irgendeine Form von Konjugation). Sie können Teilaufgaben überspringen, falls Sie nicht weiterkommen.
(b) Präsenzblatt 8 ist hilfreich.
(c) Schreiben Sie $\overline{X}^n = (\overline{X}^2)^{\frac{n-1}{2}} \cdot \overline{X}$
(f) Drücken Sie Potenzen von ω als Potenzen von η aus und zeigen Sie, dass $\omega^{2^{p-1}} = \overline{-1}$ gilt.

AUFGABE 5 (4 Punkte)**:**
Sei $x \in \mathbb{R}$ und p_n, q_n die Konvergenten, d.h. $\frac{p_n}{q_n}$ sind die Näherungsbrüche aus der Kettenbruchentwicklung, wobei wir o.E. immer $\mathrm{ggT}(p_n, q_n) = 1$ und $q_n > 0$ wählen. Zeigen Sie, dass die Kettenbruchentwicklung für $n > 1$ eine Bestapproximation liefert, d.h. für die Näherung $\frac{p_n}{q_n}$ an x gilt

$$|x - \frac{p_n}{q_n}| \leq |x - \frac{p}{q}|$$

für alle anderen Näherungen $\frac{p}{q}$ mit Brüchen mit kleinerem Nenner $0 < q < q_n$.

Bemerkung: Es gilt sogar die stärkere Aussage $|q_n \cdot x - p_n| \leq |q \cdot x - p|$ und sie können auch versuchen, zunächst diese zu zeigen.

Hinweis: Es gibt mehrere Möglichkeiten, dies zu zeigen, d.h. Sie können den Hinweis auch ignorieren. Beachten Sie, dass aus dem Beweis der Konvergenz von Kettenbrüchen folgt, dass $|x - \frac{p_n}{q_n}| \leq |x - \frac{p_{n-1}}{q_{n-1}}|$ (warum?). Wenn Sie versuchen, die stärkere Aussage aus der Bemerkung zu zeigen, ist es ratsam $x = [a_0, a_1, \ldots, a_n, r]$ zu schreiben mit $r \in \mathbb{R}$ und $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$ und das Lemma über Näherungsbrüche zu verwenden. Beachten Sie, dass für 2 verschiedene Brüche $\frac{p}{q} \neq \frac{p'}{q'}$ (vollständig gekürzt) stets gilt, dass $|\frac{p}{q} - \frac{p'}{q'}| > \frac{1}{|qq'|}$ (warum?). Benutzen Sie dies, um zu zeigen, dass $\frac{p}{q}$ nicht zwischen $\frac{p_{n-1}}{q_{n-1}}$ und $\frac{p_n}{q_n}$ liegen kann.