RUHR UNIVERSITÄT BOCHUM

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

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 9 / 7. Juni 2013 / Abgabe bis spätestens 17. 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 5,6 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)**:**

(a) Bestimmen die die Ordnung von 3 in U_{97}.

(b) Sei x der diskreten Logarithmus von 48 zur Basis 3 in U_{97} ist, dessen Existenz als gegeben vorausgesetzt wird, also $3^x \equiv 48 \mod 97$. Bestimmen Sie $x \mod 4$.

Bemerkung zu (b):
Die Aufgabenstellung in (b) ergibt nur Sinn, weil die Ordnung von 3 durch 4 teilbar ist.
Exponentieren Sie die definierende Gleichung $3^x \equiv 48 \mod 97$, um eine Situation ähnlich des Lemmas „Berechnen des Diskreten Logarithmus modulo 2^s“ aus der Vorlesung herzustellen.
Beachten Sie, dass 3 *kein* Erzeuger von U_{97} ist und Sie daher nicht exakt die Situation aus der Vorlesung vorfinden werden (Dort war $\mathrm{ord}(g) = 2^s$ in dortiger Notation vorausgesetzt).
Die Vorgehensweise ist aber analog. Es ist insbesondere nicht nötig/gewünscht, x komplett zu bestimmen. Die Verwendung eines Taschenrechners ist ratsam.

AUFGABE 2 (3 Punkte)**:**
Zeigen Sie, dass die Kettenbruchentwicklung einer rationalen Zahl eindeutig ist, wenn das letzte Element > 1 ist:
Seien $x = [a_0, \ldots, a_n] = [b_0, \ldots, b_m]$ zwei Kettenbruchentwicklungen, wobei $a_n > 1$, falls $n > 0$ und $b_m > 1$, falls $m = 0$.
Zeigen Sie, dass $m = n$ und $a_i = b_i$ für alle i gilt.

Bemerkung: Die Aussage gilt auch für (unendliche) Kettenbrüche irrationaler Zahlen, wobei in diesem Fall die Bedingung an das letzte Element entfällt.

AUFGABE 3 (3 Punkte)**:**
Berechnen Sie die Lösungsmenge von $x^2 \equiv 12 \mod 97$ mit Hilfe des Tonelli-Shanks-Algorithmus.

AUFGABE 4 (5 Punkte)**:**
Bestimmen Sie jeweils die Lösungsmengen folgender Gleichungen:

(a) $x^3 \equiv 11 \mod 23$

(b) $x^3 \equiv 23 \mod 37$

(c) $x^3 \equiv 17 \mod 37$

Hinweis: Modifizieren Sie den Tonelli-Shanks-Algorithmus. Versuchen Sie bitte nicht, die Aufgabe durch Durchprobieren zu lösen. Sie dürfen verwenden, dass 2 ein Erzeuger von U_{37} ist.

AUFGABE 5 (1 Punkt)**:**
Bestimmen Sie die ersten 5 Elemente $[a_0, a_1, a_2, a_3, a_4]$ der (unendlichen) Kettenbruchentwicklung von $\pi + e$, wobei $a_i \in \mathbb{Z}, a_i > 0$ für $i > 0$. Benutzen Sie hierfür einen Taschenrechner. Geben Sie die Zwischenergebnisse auf 2 Dezimalstellen an. (Sie sollten aber mit mehr als 2 Dezimalstellen rechnen!).

AUFGABE 6 (3 Punkte)**:**
Sei $a \in \mathbb{Z}, n \in \mathbb{N}$ mit $n > 2, \mathrm{ggT}(a, n) = 1$. Sei x das Inverse von a modulon n, d.h. $ax \equiv 1 \mod n$. O.E. wählen wir $0 < a, x < n$. Zeigen Sie, dass x als Nenner in der Kettenbruchentwicklung von $\frac{n}{a}$ auftritt oder $n - x$ als Nenner in der Kettenbruchentwicklung von $\frac{n-a}{a}$ auftritt.

Hinweis: Gehen Sie wie im Beweis des Satzes von Wiener vor.