Wolfgang K. Seiler
Tel. 2515

A5, C201

7. März 2007

3. Übungsblatt Zahlentheorie

Aufgabe 1: (*5 Punkte*)

a) Berechnen Sie im Körper $\mathbb{F}_{1997}$ die folgenden Elemente:

$$x_1 = 3 - 1000, \qquad x_2 = 100 \cdot 100, \qquad x_3 = 11/19, \qquad x_4 = 2^{2007}$$

b) Finden Sie eine primitive Wurzel von $\mathbb{F}_{1997}$!
Hinweis: Die Primfaktorzerlegung von 1996 ist $2^2 \cdot 499$.

Aufgabe 2: (*5 Punkte*)

a) Zeigen Sie: Für jede Primzahl p ist $(\mathbb{Z}/2p)^\times$ zyklisch!

b) Für welche $m \leq 13$ ist die prime Restklassengruppe $(\mathbb{Z}/m)^\times$ zyklisch?

Aufgabe 3: (*5 Punkte*)

a) p sei eine Primzahl, und zu $a \in \mathbb{F}_p^\times$ gebe es ein $x \in \mathbb{F}_p$ mit $x^2 = a$. Zeigen Sie: Dann ist $x^{p+1} = a$.

b) Nun sei $p \equiv 3 \bmod 4$. Zeigen Sie: Wenn es in $\mathbb{F}_p$ eine Lösung x der Gleichung $x^2 = a$ gibt, so ist auch $y = a^{(p-1)/4}$ eine Lösung.

c) Bestimmen Sie im Körper $\mathbb{F}_{127}$ die Lösungsmenge der Gleichung $x^2 = 3$!

d) *Ditto* für $x^2 = 11$!

e) *Ditto* für $x^2 + 2x = 10$!

Aufgabe 4: (*5 Punkte*)

Die Firmen `dot.com` und EYKΛEIΔHΣ oHG beziehen beide ihre RSA-Moduln von der Firma *THRIFTY PRIMES* Inc. Diese erzeugt, getreu ihrem Namen, für beide zusammen nur drei Primzahlen p, q, r und schickt $m = pq = 88051$ an `dot.com` sowie $n = qr = 89197$ an die EYKΛEIΔHΣ oHG. Beide Firmen verwenden den öffentlichen Exponenten $e = 3$.

a) Verschlüsseln Sie die „Nachricht“ 34159 an `dot.com`!

b) Bestimmen Sie den privaten Exponenten der EYKΛEIΔHΣ oHG mit einem Verfahren, das auch funktionieren würde, wenn n und m Produkte hundertstelliger Primzahlen wären.

c) Unterschreiben Sie die „Nachricht“ 12345 im Namen der EYKΛEIΔHΣ oHG!
NB: Alle notwendigen Rechnungen lassen sich auf einem Taschenrechner mit mindestens zehn Stellen ausführen. Falls Sie ohne Computer arbeiten, reicht aber bei *c)* eine Formel; der Zahlenwert muß dann nicht bestimmt werden.

Abgabe bis zum Mittwoch, dem 14. März 2007, um 13.45 Uhr