WOLFGANG K. SEILER
Tel. 2515

A5, C201

5. März 2009

3. Übungsblatt Zahlentheorie

Aufgabe 1: (*5 Punkte)*

a) Beweisen sie die WILSONsche Kongruenz: Für jede Primzahl p ist $(p-1)! \equiv -1 \bmod p$.
Hinweis: Betrachten Sie die Faktoren in $(p-1)!$ als Elemente des Körpers $\mathbb{F}_p$, und beachten Sie, daß mit jedem Element i auch dessen (nicht notwendigerweise von i verschiedenes) Inverses vorkommt.

b) $n \geq 2$ sei eine zusammengesetzte Zahl. Was können Sie über $(n-1)! \bmod n$ sagen?

Aufgabe 2: (*5 Punkte)*

Finden Sie eine primitive Wurzel von $\mathbb{F}_{257}$, d.h. ein Element $a \in \mathbb{F}_{257}$, für das sich alle $x \neq 0$ aus $\mathbb{F}_{257}$ als Potenzen von a schreiben lassen!
Hinweis: Probieren Sie einfach die Elemente $a = 2, 3, 4, \ldots$ durch, bis Sie eine primitive Wurzel gefunden haben!

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 ΕΥΚΛΕΙΔΗΣ 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 ΕΥΚΛΕΙΔΗΣ oHG. Beide Firmen verwenden den öffentlichen Exponenten $e = 3$.

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

b) Berechnen Sie die Primzahlen p, q, r und den privaten Exponenten der ΕΥΚΛΕΙΔΗΣ oHG!

c) Unterschreiben Sie die „Nachricht“ 12345 im Namen der ΕΥΚΛΕΙΔΗΣ 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 der Unterschrift muß dann nicht bestimmt werden.

Abgabe bis zum Donnerstag, dem 16. März 2009, um 15.30 Uhr