Wolfgang K. Seiler
Tel. 2515

A5, C201

10. März 2011

4. Übungsblatt Zahlentheorie

Aufgabe 1: *(6 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.

Aufgabe 2: *(6 Punkte)*

a) Berechnen Sie den diskreten Logarithmus von 10 modulo 19 zur Basis 13 !

b) Zeigen Sie, daß es modulo 17 keinen diskreten Logarithmus von 10 zur Basis 13 gibt!

c) p sei eine Primzahl. Für welche $a \in \mathbb{F}_p^\times$ hat jedes $x \in \mathbb{F}_p^\times$ einen diskreten Logarithmus zur Basis a ?

Aufgabe 4: *(3 Punkte)*

a) Runden Sie $\displaystyle\sum_{n=1}^{2\,000\,000} \frac{1}{n}$ zur nächsten ganzen Zahl!

b) Finden Sie ein möglichst kleines N, so daß $\displaystyle\sum_{n=1}^{N} \frac{1}{n} \geq 100$ ist!

Aufgabe 5: *(5 Punkte)*

Die Funktion $f\colon \mathbb{N} \to \mathbb{N}$ sei multiplikativ, d.h. für zwei natürliche Zahlen n, m sei stets $f(nm) = f(n) \cdot f(m)$. Zeigen Sie: Für alle $s \in \mathbb{R}$, für die beide Seiten konvergieren, ist

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \text{ prim}} \frac{1}{1 - \frac{f(p)}{p^s}} !$$

Abgabe bis zum Donnerstag, dem 17. März 2011, um 17.15 Uhr