Wolfgang K. Seiler
Tel. 2515

A5, C201

12. März 2009

4. Übungsblatt Zahlentheorie

Aufgabe 1: (*4 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 2: (*6 Punkte*)

Der Schlüsselaustausch nach Diffie und Hellman läßt sich nach Burmester und Desmedt folgendermaßen auf mehr als zwei Teilnehmer verallgemeinern: Alle einigen sich auf eine Primzahl p und ein Element $g \in \mathbb{F}_p^\times$ mit möglichst großer Ordnung. Dann wählt sich sich jeder Teilnehmer $i \in \{1, \ldots, N\}$ eine geheime Zufallszahl x_i und schickt $y_i = g^{x_i} \bmod p$ an die anderen. Sodann berechnet er $m_i = (y_{i+1}/y_{i-1})^{x_i} \bmod p$ und verschickt auch diese Zahl. Zum Schluß berechnet er $S_i = y_{i-1}^{Nx_i} \cdot \prod_{j=1}^{N-1} m_{i+j-1}^{N-j}$, wobei jeweils alle Additionen und Subtraktionen im Index modulo N durchgeführt werden, d.h. $m_{N+1} = m_1$, $m_0 = m_N$, *usw.*

a) Zeigen Sie: Die N so berechneten Schlüssel S_i sind gleich.

b) Welche Möglichkeiten hat ein (passiver) Lauscher, um diesen Schlüssel zu finden?

Aufgabe 3: (*3 Punkte*)

a) Mit welchen Exponenten treten die Zwei und die Drei in der Primfaktorzerlegung von 100! auf?

b) Bestimmen Sie die größte natürliche Zahl n, für die 12^n ein Teiler von 100! ist!

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: (*4 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 19. März 2009, um 15.30 Uhr