Einführung in die Algebra und Diskrete Mathematik
5.Übungsblatt für den 3. April 2003

1. Sei $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, wobei die p_i lauter verschiedene Primzahlen sind, und sei $s \in \mathbb{N}$. Zeigen Sie, dass für alle $a \in \mathbb{Z}$ gilt:
$$a^{1+s\cdot\prod_{i=1}^{k}(p_i-1)} \equiv a \pmod{n}.$$

2. Für das RSA-Verfahren wählen wir $p = 5, q = 11$ und $k = 13$. Chiffrieren Sie $(01, 22, 03, 08)$ und dechiffrieren Sie das Ergebnis !

3. Frau Huber sendet Herrn Müller mit dem RSA-Verfahren die Nachricht PMOXY. Herr Müller weiß, dass Frau Huber das RSA-Verfahren mit $(n = 35, k = 5)$ verwendet hat (A=0, Z=25). Entschlüsseln Sie die Nachricht!

4. (Mathematica, [1, p. 265]). In einem RSA-System ist
$$n = pq = 32954765761773295963$$
und $k = 1031$. Bestimmen Sie t, und entschlüsseln Sie die Nachricht
$$899150261120482115$$
(A = 0, Z = 25).

5. (a) Sei p eine Primzahl, und sei $a \in \mathbb{Z}$ so, dass $p|a^2 - 1$. Zeigen Sie, dass $a \equiv 1 \pmod{p}$ oder $a \equiv -1 \pmod{p}$ gilt.

   (b) (Mathematica) Wir weisen jetzt mit diesem Satz nach, dass 561 keine Primzahl ist. Nehmen wir an, 561 wäre prim. Dann gilt
   $$2^{560} \equiv 1 \pmod{561}.$$
   Das gilt auch wirklich. Also muss nach Beispiel (5a) gelten: $2^{280} \equiv 1 \pmod{561}$ oder $2^{280} \equiv -1 \pmod{561}$. Gilt das? Wie können Sie das Argument fortsetzen, um herauszubekommen, dass 561 nicht prim ist? *Hinweis:* Verwenden Sie `PowerMod`.

   Diese Überlegungen sind die Basis des *Rabin-Miller*-Primzahlentests [2].

6. Finden Sie aus der Literatur, wie der *Fermat*-Primzahlentest funktioniert, und welche zusammengesetzten Zahlen er nicht als zusammengesetzt erkennt. Geben Sie Ihre Quelle an!

Literatur

[1] R. Lidl and G. F. Pilz. *Applied abstract algebra.* Springer-Verlag, New York, second edition, 1998.

[2] J. Wiesenbauer. Primzahltests and Faktorisierungsalgorithmen. I. (Primality tests and factorization algorithms. I). *Int. Math. Nachr., Wien*, 186:9–23, 2001.