Übungen zu Algebra für InformatikerInnen
12. Übungsblatt für den 16./17.6.2011

1. Berechnen Sie mit dem erweiterten euklidschen Algorithmus jeweils den ggT für die Paare (a, b), und bestimmen Sie $(u, v) \in \mathbb{R}^2$ so dass $ggT(a, b) = ua+vb$: $(100, 135)$, $(81, 48)$, $(128, 243)$.

2. Entscheiden Sie ob die folgende (diophantische) Gleichungen über $\mathbb{Z}^2$ lösbar sind. Finden Sie in Falle der Lösbarkeit eine Lösung:

$$128x + 243y = 1 \tag{1}$$
$$81x + 48y = 60 \tag{2}$$
$$100x + 135y = 254 \tag{3}$$

3. Wieviele Lösungen haben die folgenden Gleichungen über $\mathbb{Z}, \mathbb{Z}_6$ und $\mathbb{Z}_7$?

$$2x + 4y = 5 \tag{4}$$
$$2x + 4y = 4 \tag{5}$$

4. Verschlüsseln Sie mit den Parametern p, q, e die folgenden Nachrichten M:

$$p = 7, q = 11, e = 17, M = 8 \tag{6}$$
$$p = 17, q = 31, e = 7, M = 2 \tag{7}$$

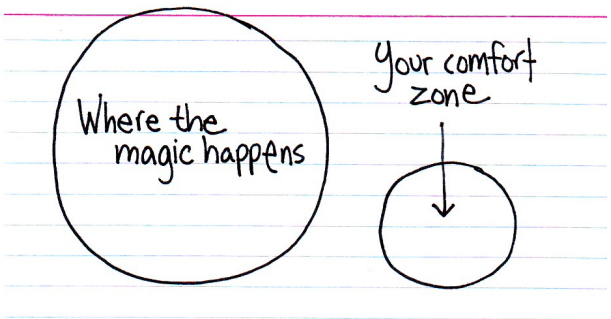
5. Entschlüsseln Sie mit den Parametern p, q, d die kodierte Nachricht C:

$$p = 3, q = 11, d = 7, C = 5 \tag{8}$$
$$p = 7, q = 11, d = 13, C = 11 \tag{9}$$

6. Sei $n = 55$, $e = 7$ mein öffentlicher Schlüssel. Verschlüsseln Sie die Nachricht $M = 10$. Auf eine Meldung von mir antwortet der Bösewicht Karl-Heinz mit einer Nachricht $C = 35$; brechen Sie meine Verschlüsselung (also bestimmen Sie p, q und d) und entschlüsseln Sie seine Nachricht.

7. Alice möchte Bob die Telefonnummer 07041104 schicken und *digital unterschreiben*. Zu diesem Zweck verschlüsselt sie die drei Nummern $07, 04, 11$ mit ihrem privaten Schlüssel $(77, 53)$. Bestimmen Sie die unterschriebene / verschlüsselte Nachricht. Bob empfängt diese Nachricht; entschlüsseln Sie diese mit Alices öffentlichem Schlüssel $(77, 17)$. Bob weißt dann, dass niemand außer Alice die Nachricht hätte schicken können.

Für die Berechnungen von Resten modulo n (Bsp 4–7) dürfen Sie GAP, Mathematica, Maxima oder ähnliche Programme (oder schrieben Sie was!) verwenden.



Courtesy of thisisindexed.com