

**Übungen zu
Theoretische Informatik 3
WS 2006/07**

Si fuerit N ad x numerus primes et n numerus partium an N primarum, tum potestas x^n unitate minuta semper per numerum N erit divisibilis.

L. Euler, "Theoremata arithmetica nova methodo demonstrata",
Novi comentarii academiae scientiarum Petropolitanae 8 (1760), 74–104.

• **Aufgabe 43: Zertifikate für Primzahlen**

Berechnen Sie Zertifikate für die Primzahlen $N_1 = 211$ und $N_2 = 311$.

• **Aufgabe 44: Eine Pseudoprimzahl**

Die Zahl $N = 3828001$ ist keine Primzahl ist, obwohl sie die Bedingung der FERMAT-Kongruenz

$$(F) \quad \forall a \in \mathbb{Z} : \text{ggT}(a, N) = 1 \Rightarrow a^{N-1} \equiv 1 \pmod{N}$$

erfüllt.

1. Beschaffen Sie sich die Primfaktorisation von N (woher auch immer, alles ist erlaubt) und weisen Sie nach, dass (F) gilt.
NB: Wie im Fall $N = 561$ (Vorlesung) gilt: wenn Sie glauben, hierfür viel rechnen zu müssen, haben Sie möglicherweise etwas noch nicht verstanden.
2. Bestimmen Sie einen MILLER-RABIN-Zeugen für die Nicht-Primheit von N .

• **Aufgabe 45: Modulare Arithmetik und Miller-Rabin-Test (Klausuraufgabe 2005)**

Die Zahl $N = 1729$ hat $1729 = 7 \cdot 13 \cdot 19$ als Primfaktorisation. Gemäss chinesischem Restesatz ist daher der Ring \mathbb{Z}_{1729} isomorph zu dem Ring $\mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19}$, was man beim Verfahren der modularen Arithmetik ausnutzt.

- a) Die Gleichung $X^2 = 1$ hat in \mathbb{Z}_{1729} genau acht verschiedene Lösungen, nämlich alle diejenigen Elemente, deren Darstellung in $\mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19}$ von der Form $(\pm 1, \pm 1, \pm 1)$ ist. Dabei gelten nach chinesischem Restesatz die Entsprechungen

$$\begin{aligned} \mathbb{Z}_{1729} \ni 1 &\leftrightarrow (+1, +1, +1) \in \mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19} \\ \mathbb{Z}_{1729} \ni -1 = 1728 &\leftrightarrow (-1, -1, -1) = (6, 12, 18) \in \mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19} \end{aligned}$$

Welchem Element von \mathbb{Z}_{1729} entspricht $(+1, -1, +1) \in \mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19}$?

- b) Berechnen Sie die Ordnungen des Elements $a = 2$ in \mathbb{Z}_7^* , in \mathbb{Z}_{13}^* und in \mathbb{Z}_{19}^* .
- c) Verwenden Sie die Resultate von b), um das dem Element $2^{27} \pmod{1729}$ von \mathbb{Z}_{1729} entsprechende Element von $\mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19}$ zu berechnen.
- d) Zeigen Sie, dass $a = 2$ ein MILLER-RABIN-Zeuge dafür ist, dass $N = 1729$ keine Primzahl ist. (Hinweis: es ist $N - 1 = 1728 = 64 \cdot 27$.)

• **Aufgabe 46: RSA-Szenario (Klausuraufgabe 2006)**

Bob möchte sich als Teilnehmer an einem public-key Kryptosystem RSA-verschlüsselte Nachrichten senden lassen. Er wählt zwei Primzahlen p, q mit $p < q$ und berechnet $N = p \cdot q$. Er erhält $N = 55919$. Um einen Verschlüsselungsexponenten e und den dazugehörigen Entschlüsselungsexponenten d festlegen zu können, berechnet Bob $\phi(N)$ und erhält $\phi(N) = 55440$. Bob möchte seinen Partnern das Verschlüsseln möglichst leicht machen und entschliesst sich, die kleinstmögliche dafür geeignete Zahl $e > 1$ zu wählen. Er bestimmt diese Zahl und berechnet den dazugehörigen Entschlüsselungsexponenten d . Dann gibt er das Paar (N, e) öffentlich bekannt.

1. Welche Primzahlen hat Bob gewählt? Bestimmen sie p und q aus den vorhandenen Informationen.
2. Bestimmen Sie die Primfaktorisation von $\phi(N)$. (Das geht auch dann, wenn Sie den ersten Teil nicht gelöst haben).
3. Welches ist der kleinstmögliche Verschlüsselungsexponent e und der dazugehörige Entschlüsselungsexponent d ?
4. Wieviele verschiedene Verschlüsselungsexponenten stehen Bob überhaupt zur Verfügung?
5. Ein Verschlüsselungsexponent e ist auf offensichtliche Weise *riskant*, falls er gleich dem zugehörigen Entschlüsselungsexponenten d ist. Welche Kongruenzbedingung kennzeichnet die riskanten Verschlüsselungsexponenten? Wieviel gibt es davon im vorliegenden Fall?
6. Bestimmen Sie einen riskanten Verschlüsselungsexponenten $\neq \pm 1 \pmod{\phi(n)}$.

