

**Übungen zur
Theoretischen Informatik 3
WS 2004/05**

*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 38: Zum Miller-Rabin-Test**

1. Bestimmen Sie für die zusammengesetzte Zahl $n = 21$ die Mengen der Teilbarkeits-, Euklid-, Fermat und Miller-Rabin-Zeugen.
2. Bestimmen Sie für die zusammengesetzte Zahl $n = 105$
 - einen Teilbarkeits-Zeugen
 - einen Euklid-Zeugen, der kein Teilbarkeitszeuge ist
 - einen Fermat-Zeugen, der kein Euklid-Zeuge ist
 - einen Miller-Rabin-Zeugen, der kein Fermat-Zeuge ist

• **Aufgabe 39: Eine Pseudoprimumzahl**

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 Primfaktorisierung 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 40: Verschlüsselung und RSA-System**

In dieser Aufgabe seien die 26 Buchstaben des Alphabets mit den numerischen Werten von 0 bis 25 codiert, also $A \leftrightarrow 00, B \leftrightarrow 01, C \leftrightarrow 02, \dots, Z \leftrightarrow 25$. Je drei Buchstaben einer Text-Nachricht werden zusammengefasst, ergeben also eine sechsstellige Dezimalzahl. Eine Nachricht wird also als Folge von sechstelligigen Zahlen codiert, also z.B. FAU \leftrightarrow 050020. Sollte die Buchstaben-Länge einer Nachricht nicht durch 3 teilbar sein, wird mit ein oder zwei beliebigen Zeichen aufgefüllt.

1. Die Zahl $p = 4578971$ ist eine Primzahl. Weiter werde der Exponent $e = 3317271$ zum Verschlüsseln benutzt, d.h $\mathcal{E} : M \mapsto M^e \pmod{p}$ für Zahlen M mit $0 \leq M < p$. Verschlüsselt werden also jeweils Blöcke von 7 Dezimalzahlen übertragen, die eine Zahl $< p$ darstellen. Entschlüsseln Sie die verschlüsselte Nachricht

4137884 438421 3227477 233970

2. Ein Teilnehmer an einem public-key RSA-Kryptosystem hat seine Systemparameter $p = 1733$, $q = 2347$, also $n = 4067351$ gewählt. Als Verschlüsselungsexponenten gibt er $e = 31$ öffentlich bekannt.

- (a) Welches ist der Entschlüsselungsexponent d ?
- (b) Der Teilnehmer erhält die Nachricht

2721372 3969831 2416419 1795753 2110079 0242624 0889174

Wie lautet der Klartext?

• **Aufgabe 41: Zur Schwierigkeit, den Entschlüsselungsexponenten für RSA zu berechnen (optional)**

Die vorige Aufgabe zeigt, dass man aus der Kenntnis von n und $\phi(n)$ die Faktorisierung von n gewinnen kann, falls n — wie im RSA-Fall — das Produkt von zwei Primzahlen ist. Hier geht es darum, dass man die Faktorisierung von n auch mit Hilfe von e und d bestimmen kann, also ohne $\phi(n)$ zu kennen! Das Verfahren ist probabilistisch und variiert die Idee des Miller-Rabin-Tests.

1. Zeigen sie, ist $n = p \cdot q$ das Produkt von zwei Primzahlen p und q , so hat die Gleichung $x^2 = 1 \pmod n$ genau vier Lösungen.

Hinweis: Chinesischer Restesatz!

2. Zwei der vier erwähnten Lösungen sind $x = \pm 1 \pmod n$, klar! (Hilft aber nichts). Findet man eine der beiden anderen Lösungen, also ein α mit $n \mid (\alpha - 1)(\alpha + 1)$, aber $\alpha \not\equiv \pm 1 \pmod n$, so kann man mittels $\text{ggT}(\alpha - 1, n)$ bzw. $\text{ggT}(\alpha + 1, n)$ Faktoren von n bestimmen.¹

Seien nun e und d mit $e \cdot d \equiv 1 \pmod{\phi(n)}$ bekannt. ($\phi(n)$ selbst braucht nicht bekannt zu sein). Dann ist $e \cdot d - 1 = 2^r \cdot s$ mit ungeradem s . Wie beim Miller-Rabin-Test wird ein Kandidat w mit $0 < w < n$ zufällig gewählt und die Folge

$$z_0 = w^s \pmod n, z_1 = z_0^2 \pmod n, \dots, z_i = z_{i-1}^2 \pmod n, \dots, z_r = z_{r-1}^2 \pmod n$$

durch sukzessiver Quadrieren konstruiert. Es ist also $z_i = w^{2^i s} \pmod n$ und wegen des Satzes von Euler und $\phi(n) \mid e \cdot d - 1 = 2^r \cdot s$ ist $z_r = 1$. Wenn also nicht schon der erste Term der Folge $= 1$ ist (und somit alle folgenden auch), muss eine Stelle geben mit $z_k \not\equiv 1 \pmod n$ und $z_k^2 \equiv 1 \pmod n$. Findet man hierbei ein $z_k \not\equiv -1 \pmod n$, so hat man eine nichttriviale Quadratwurzel gefunden und kann n faktorisieren. Wie beim Miller-Rabin-Test zeigt eine detaillierte Analyse, dass man mindestens mit Wahrscheinlichkeit $1/2$ bei einem Zufallsversuch Glück hat. Das sollen Sie nicht beweisen, sondern vielmehr an einem Beispiel diesen Ansatz nachvollziehen:

Sei $n = 13289$ ein RSA-Modul und $e = 7849$ ein Verschlüsselungsexponent. Irgendwie erfahren Sie, dass $d = 2713$ der zugehörige Entschlüsselungsexponent ist, also $e \cdot d - 1 = 2^r \cdot s$ mit $r = 8$ und $s = 83181$. Wählen Sie zufällige w und finden Sie die beiden Faktoren von n .

• **Aufgabe 42: Zurück zu Fermat (optional)**

1. Die Zahlen der Bauart $F_n = 2^{2^n} + 1$ hat schon Pierre de Fermat (1601–1665) untersucht. Aus der Beobachtung, dass $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ Primzahlen sind, leitete er die Vermutung ab, dass alle F_n Primzahlen seien. Widerlegen Sie ihn, indem Sie nachweisen, dass die Zahlen $F_5 = 4294967297$ und $F_6 = 18446744073709551617$ keine Primzahlen sind.
2. Hätte Fermat Recht gehabt, wäre dies auch ein (weiterer) Nachweis gewesen, dass es unendlich viele Primzahlen gibt. Nun hat Fermat doch garnicht so falsch gelegen: zeigen Sie, dass $F_n = F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1} + 2$ ist und dass daraus die Existenz unendlich vieler Primzahlen folgt.

¹Nebenbei: das ist eine der ältesten Faktorisierungstricks überhaupt.