

**Übungen zur
Theoretischen Informatik 3
WS 2005/06**

*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 41: Eine Pseudoprимzahl**

Die Zahl $N = 3828001$ ist keine Primzahl, 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 42: 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 43: Simultane Kongruenzen und Inkongruenzen**

1. Um eine beliebiges lösbares Kongruenzensystem in ein äquivalentes System mit teilerfremden Moduln zu transformieren, benötigt man zwei einfache Funktionen `split1` und `split2`, die für Argumente (m, n) , die positive natürliche Zahlen sind, folgendes leisten:
 - `split1` $(m, n) = (u, v)$, wobei u der zu n teilerfremde Teil von m und v der Kofaktor $v = m/u$ ist, d.h. $\text{ggT}(u, n) = 1$, $u \cdot v = m$ und $p|v \rightarrow p|n$ für alle Primzahlen p .
 - `split2` $(m, n) = (u, v)$, wobei u Teiler von m , v Teiler von n , $\text{ggT}(u, v) = 1$ und $\text{kgV}(m, n) = u \cdot v$ ist.

Wie kann man diese beiden Funktionen effizient (also ohne Rückgriff auf die Primfaktorisationen der Argumente m und n , nur mittels ggT-Berechnungen und Divisionen!) realisieren?

2. Betrachten Sie die beiden aussagenlogischen Formeln in 2-CNF:

$$F = (\overline{y_1} \vee y_2) \wedge (y_1 \vee y_3) \wedge (\overline{y_2} \vee y_3) \wedge (y_2 \vee \overline{y_3}) \wedge (\overline{y_2} \vee \overline{y_3})$$
$$G = (\overline{y_1} \vee y_2) \wedge (\overline{y_1} \vee \overline{y_2}) \wedge (y_1 \vee y_3) \wedge (\overline{y_2} \vee y_3) \wedge (y_2 \vee \overline{y_3})$$

Konstruieren Sie für beide Formeln ein System von Inkongruenzen, dessen Lösbarkeit äquivalent zur Erfüllbarkeit der jeweiligen Formel ist. Welche der beiden Formeln ist erfüllbar?

• **Aufgabe 44: 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.