

**Abgabe: SW6 + SW7**



1. Schreiben Sie auf:

- (a) Der kleine Fermatscher Satz
- (b) Der chinesischer Restsatz
- (c) RSA Verfahren: Ver- und Entschlüsseln

**Lösung:** Seiten 81-85, Skript zur Vorlesung



2. RSA-Code knacken: Wenn man  $N$  und  $\varphi(N)$  kennt, findet man leicht die Faktorisierung von  $N$ . Wie?

**Lösung:**  $N = p \cdot q$

$$\varphi(N) = (p-1)(q-1) = pq - (p+q) + 1 = N - (p+q) + 1 = N - (p + N/p) + 1$$

Auflösen von  $p$ :

$$p^2 - (1+N+\varphi(N))p + N = 0$$

$$p = \frac{1+N-\varphi(N)}{2} \pm \sqrt{\frac{(1+N-\varphi(N))^2}{4} - N} = \frac{p + \frac{N}{p}}{2} \pm \sqrt{\left(\frac{p + \frac{N}{p}}{2}\right)^2 - N}$$

Man nimmt +, wenn  $p$  die größere Primzahl ist und -, wenn  $p$  die kleiner ist.



3. Schreiben Sie den Algorithmus für den Chinesischer Restsatz auf.

**Lösung:** Seite 85



4. Im *Suan-Ching*-Handbuch steht u.a. die folgende Aufgabe: „Wir haben eine gewisse Anzahl von Dingen, wissen aber nicht genau wie viele. Wenn wir sie zu je drei zählen, bleiben zwei übrig. Wenn wir sie zu je fünf zählen, bleiben drei übrig. Wenn wir sie zu je sieben zählen, bleiben zwei übrig. Wieviele Dinge sind es?“

**Lösung:** Seiten 85-86



5. Zeigen Sie für alle  $n \in \mathbb{N}$ :

- a)  $42 \mid n^7 - n$
- b)  $37 \mid 1000^n - 1$

**Lösung:**

- M** 6. **Satz von Euler (Satz von Euler-Fermat).** Er stellt eine Verallgemeinerung des kleinen Fermatschen Satzes dar. Für alle  $n \in \mathbb{N}$  mit  $n \geq 2$  und  $a \in \mathbb{Z} \setminus \{0\}$ , die  $\text{ggT}(a, n) = 1$  erfüllen, gilt:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$\varphi(n)$  bezeichnet die Eulersche  $\varphi$ -Funktion: die Anzahl der natürlichen Zahlen  $k$  von 1 bis  $n$ , die zu  $n$  teilerfremd sind, für die also  $\text{ggT}(k, n) = 1$  ist.

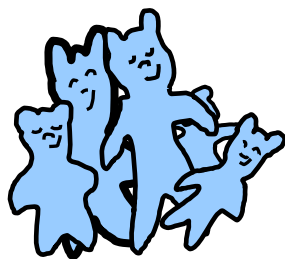
Frage: Wie lautet die letzte Dezimalstelle von  $7^{222}$ , also welche Zahl ist kongruent  $7^{222}$  modulo 10?

Lösung: Seiten 87-88

- M** 7. Finden Sie die letzte Ziffer der Zahlen:  $2156^{43}$ ,  $425^{21}$ ,  $5234^{129}$  und  $17^{80} + 12^{60}$ .

- M** 8. **Wieviele sind es mindestens? (Chinesischer Restsatz)**

Wir haben eine gewisse Anzahl von Gummibärchen, wissen aber nicht,



wieviele es sind. Wenn wir die Bärchen in Tüten verpacken, in die je  $m_1$  Bärchen passen, bleiben  $a_1$  Bärchen übrig. Wenn wir sie in Tüten verpacken, die jeweils eine Kapazität von  $m_2$  Bärchen besitzen, bleiben  $a_2$  übrig. ...

Wenn wir sie in Tüten füllen, die je  $m_k$  Bärchen aufnehmen, bleiben  $a_k$  übrig. Wieviele Gummibärchen sind es mindestens, wenn die  $m_1, m_2, \dots, m_k$  mit  $m_k < 100$  untereinander teilerfremd sind? *Eingabe:* In der Datei *baerchen.in* befinden sich die Paare  $(a_i, m_i)$  mit  $0 \leq a_i < m_i$ ; ein Paar pro Zeile.

*Ausgabe:* Geben Sie die minimale Anzahl der Gummibärchen in die Ausgabedatei *baerchen.out* aus.

Beispiel:

baerchen.in	baerchen.out
2 3	128
3 5	

SS 2008

2 7	
7 11	

**Lösung:** Seite 136. (Umstellen Sie es in Java mit Hilfe der Klasse `java.math.BigInteger!`)



9. Zeigen Sie für alle  $n \in \mathbb{N}$ :

a)  $91 \mid 3^{91} - 3$     b)  $15 \mid 4^{15} - 4$

**Lösung:**



1 Punkt



2 Punkte



3 Punkte

SW = Semester Woche

### Literatur

1. Doina Logofătu, *Algorithmen und Problemlösungen mit C++*, Vieweg Verlag, 2006.