SS 2003 Prof. Dr. Wolfram Koepf Elemente der Arithmetik und Algebra II
Blatt 5 Ausgabe: 26. Mai 2003
Abgabe: 02. Juni 2003, 11 Uhr

1. **(Modulo rechnen)**: Es stehe $m \overset{n}{\equiv} k$ für $m \equiv k (\mathrm{mod}\ n)$

   (a) **(Hohe Potenzen)** Als Beispiel berechnen wir 97^{97} modulo 103 auf dem Papier. Die auftretenden Quadrate werden durch fortwährendes Reduzieren nicht sehr groß, so daß sie sich bequem mit dem Taschenrechner, oft sogar im Kopf berechnen lassen:

   $$\begin{aligned} 97^2 &\overset{103}{\equiv} (-6)^2 &&\overset{103}{\equiv} 36 \\ 97^4 &\overset{103}{\equiv} 36^2 &&\overset{103}{\equiv} 60 \\ 97^8 &\overset{103}{\equiv} 60^2 &&\overset{103}{\equiv} 98 \overset{103}{\equiv} -5 \\ 97^{16} &\overset{103}{\equiv} (-5)^2 &&\overset{103}{\equiv} 25 \\ 97^{32} &\overset{103}{\equiv} 25^2 &&\overset{103}{\equiv} 625 \overset{103}{\equiv} 7 \\ 97^{64} &\overset{103}{\equiv} 7^2 &&\overset{103}{\equiv} 49 \end{aligned}$$

   Nun ist $97 = 64 + 32 + 1$ also $97^{97} = 97^{64} 97^{32} 97^{1}$ und es folgt $97^{97} \overset{103}{\equiv} 49 \cdot 7 \cdot (-6) \overset{103}{\equiv} -2058$ mit $-2058 \overset{103}{\equiv} \overbrace{2060}^{103 \cdot 20} - 2058 = 2$ erhalten wir $97^{97} \overset{103}{\equiv} 2$.

   Berechnen Sie:

   i. modulo 7: 2^{256}, $2^{(4^n)}$, $2^{(2 \cdot 4^n)}, n \in \mathbb{N}$ (3 Punkte)

   ii. modulo 1027: 23^{1026}, 55^{1026} (2 Punkte)

   (b) **(Multiplikationstabellen)**

   i. Erstellen Sie die Multiplikationstabellen für die Restklassenringe $\mathbb{Z}_{10}$ und $\mathbb{Z}_{11}$. (2 Punkte)

   ii. Für jeden der beiden Restklassenringe suchen Sie die multiplikativen Inversen der Elemente 3 und 4. (2 Punkte)

2. **(Fermattest)** Nach dem Satz von Fermat gilt für eine Primzahl p:
   für jedes natürliche $n > 0$ gilt $n^{p-1} \overset{p}{\equiv} 1$ (wir sagen, für n gilt die Fermatbedingung).

   (a) In (1(a)ii) wurde die Fermatbedingung für $n = 23$ und $n = 55$ getestet. Können Sie mittels der Fermatbedingung eine Aussage darüber machen, ob 1027 prim ist? (Probieren sie ggfs. weitere kleine Werte für n) (2 Punkte)

   (b) Wie kann man entscheiden, ob 1031 eine Primzahl ist? Begründung und Ausführung! (2 Punkte)

3. **(Reed-Solomon-Code)**
   Wir betrachten den *Reed-Solomon-Code* modulo der Primzahl 31. Übertragen wurde das Wort "FIBUTTER".

   (a) Die Übertragung war an einer Stelle fehlerhaft: an welcher Position war der Fehler? (3 Punkte)

   (b) Korrigieren Sie den Fehler, wie lautete das ursprüngliche abgesandte Wort? (2 Punkte)