Übung zu Mathematik I für Informatik

1. Aufgabe: Die Information einer vertraulichen Zahl wird unter drei Personen aufgeteilt. Dabei wird das in der Vorlesung vorgeführte Verfahren verwendet. Die drei Personen A, B und C erhalten jeweils die Information

$$A:\ (29,7), \quad B:\ (31,4), \quad C:\ (23,17)$$

   Wie lautet die geheime Zahl? Geben Sie an, wie jeweils zwei Personen diese gemeinsam ermitteln können.

2. Aufgabe: Betrachten Sie zu der Primzahl $p = 97$ den Restklassenring $\mathbb{Z}_{97}$.

   (a) Finden Sie ein $x \in \mathbb{Z}_{97}^*$ mit

$$x^5 \ = \ \overline{30} \tag{1}$$

   Finden Sie die Lösung von (1) nicht durch Probieren, sondern wenden Sie das in der Vorlesung erläuterte Verfahren an.

   (b) Warum ist die Lösung von (1) eindeutig?

3. (a) Das folgende lineare Gleichungssystem besitzt Koeffizienten aus dem Restklassenkörper $\mathbb{Z}_{23}$:

$$\begin{array}{rcrcrcr} \overline{12}\cdot x_1 & + & \overline{15}\cdot x_2 & + & \overline{4}\cdot x_3 & = & \overline{21} \\ \overline{10}\cdot x_1 & + & \overline{3}\cdot x_2 & + & \overline{20}\cdot x_3 & = & \overline{2} \\ \overline{9}\cdot x_1 & + & \overline{13}\cdot x_2 & + & \overline{21}\cdot x_3 & = & \overline{3} \end{array} \tag{2}$$

   Lösen Sie dieses lineare Gleichungssystem mit Werten aus $\mathbb{Z}_{23}$, indem Sie in gewohnter Weise das Gaußsche Verfahren anwenden. Was sind Rang und Corang dieses Gleichungssystems?

   (b) Sei A die Koeffizientenmatrix des Gleichungssystems (2). Berechnen Sie $\det(A)$, A^2 und, falls $\det(A) \neq \overline{0}$ ist, die Umkehrmatrix A^{-1}.

4. Berechnen Sie in dem Restklassenkörper $\mathbb{Z}_{103}$ die Potenz

$$\overline{5}^{\,1740} \tag{3}$$

   indem Sie die Rechnung zunächst mit Hilfe des Satzes von Euler vereinfachen.

5. Zeigen Sie, daß in dem Restklassenring $\mathbb{Z}_n$ mit $n = 264389$ die beiden Restklassen

$$\overline{u} \ = \ \overline{164790} \quad \text{und} \quad \overline{v} \ = \ \overline{261333} \tag{4}$$

   einerseits dasselbe Quadrat in $\mathbb{Z}_n$ besitzen und andererseits $\overline{u} \neq \pm\overline{v}$ ist.

   Wie kann man daraus schließen, daß $n = 264389$ *keine* Primzahl ist?