1. Lösung: Person A und B kommen zusammen, wenden den Chinesischen Restsatz an und berechnen damit:

$$\begin{aligned} 15 \cdot 29 - 14 \cdot 31 &= 1 && \text{(erweiterter euklidischer Algorithmus)} \\ 4 \cdot 15 \cdot 29 - 7 \cdot 14 \cdot 31 &= -1298 && \text{(chinesischer Restsatz)} \\ -2 \cdot 29 \cdot 31 + 500 &= -1298 && \text{(Teilung mit Rest)} \end{aligned}$$

In der letzten Zeile erscheint als Divisionsrest der geheime Wert 500. Person A und C berechnen zusammen:

$$\begin{aligned} 4 \cdot 29 - 5 \cdot 23 &= 1 && \text{(erweiterter euklidischer Algorithmus)} \\ 17 \cdot 4 \cdot 29 - 7 \cdot 5 \cdot 23 &= 1167 && \text{(chinesischer Restsatz)} \\ 1 \cdot 29 \cdot 23 + 500 &= 1167 && \text{(Teilung mit Rest)} \end{aligned}$$

Auch hier erscheint in der letzten Zeile erscheint wieder der geheime Wert 500. Person B und C berechnen zusammen:

$$\begin{aligned} 3 \cdot 31 - 4 \cdot 23 &= 1 && \text{(erweiterter euklidischer Algorithmus)} \\ 17 \cdot 3 \cdot 31 - 4 \cdot 4 \cdot 23 &= 1213 && \text{(chinesischer Restsatz)} \\ 1 \cdot 31 \cdot 23 + 500 &= 1213 && \text{(Teilung mit Rest)} \end{aligned}$$

Auch hier erkennt man wieder den geheimen Wert 500.

2. Lösung:

   (a) Mit Hilfe des erweiterten euklidischen Algorithmus oder – wie es in diesem Fall schnell möglich ist – durch Probieren erhält man

$$(-19) \cdot 5 + 1 \cdot 96 = 1 \tag{1}$$

   Nach Vorlesung erhält man damit die Lösung durch

$$x = \overline{30}^{-19} = \overline{30}^{97-1-19} = \overline{30}^{77} \tag{2}$$

   In (2) wurde der Satz von Euler verwendet. Zur Berechnung der Potenz $\overline{30}^{77}$ verwendet man ein geeignetes Rechnerprogramm[1], oder man implementiert das im Skript beschriebene Verfahren zum schnellen Potenzieren, wobei man alle Zwischenergebnisse sofort durch 97 teilen und durch ihren Divisionsrest ersetzen sollte. Eine Implementation in C ist:

[1] z. B. **bc**, den unter Linux und Unix verfügbaren *basic calculator*

```
unsigned long int pot(unsigned long int x,
                      unsigned long int e,
                      unsigned long int n){
  if(e==0) return 1;
  unsigned long int q=e/2, r=e%2;
  unsigned long int y=pot(x,q,n);
  y=(y*y)%n;
  if(r==1) y=(y*x)%n;
  return y;
}
```

Als Ergebnis erhält man $x = \overline{77}$

(b) Die Lösung der Gleichung

$$x^5 = \overline{30} \tag{3}$$

ist eindeutig bestimmt. Um dieses zu zeigen, nimmt man an, es gebe zwei Lösungen $x_1, x_2 \in \mathbb{Z}_{97}^*$:

$$\begin{aligned} x_1^5 &= \overline{30} \\ x_2^5 &= \overline{30} \end{aligned} \tag{4}$$

und zeigt, daß $x_1 = x_2$ ist. Dazu teilt man beide Gleichungen in (4) durcheinander:

$$(x_1 \cdot x_2^{-1})^5 = \overline{1}$$

Mit $y = x_1 \cdot x_2^{-1}$ wird dieses zu

$$y^5 = \overline{1} \tag{5}$$

Nach Vorlesung gilt daher für die Ordnung von y

$$\mathrm{ord}(y) \mid 5 \tag{6}$$

Da y ein Element der Gruppen $\mathbb{Z}_{97}^*$ ist, ist nach Vorlesung die Ordnung von y außerdem ein Teiler der Gruppenordnung:

$$\mathrm{ord}(y) \mid \#\mathbb{Z}_{97}^* = 96 \tag{7}$$

(6) und (7) ergeben zusammen

$$\mathrm{ord}(y) \mid \mathrm{ggT}(96, 5) = 1 \tag{8}$$

Damit bleibt nur die Möglichkeit $\mathrm{ord}(y) = 1$. Das heißt wiederum

$$\begin{aligned} & y = y^1 = \overline{1} \\ \Rightarrow \quad & x_1 \cdot x_2^{-1} = y = \overline{1} \\ \Rightarrow \quad & x_1 = x_2 \end{aligned}$$

Damit wurde $x_1 = x_2$ gezeigt.

3. Lösung:

(a) Zum Lösen des lineare Gleichungssystem

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

über dem Restklassenkörper $\mathbb{Z}_{23}$ mit Hilfe des Gaußschen Verfahrens beginnt man wie üblich mit der Normierung der ersten Zeile. Dazu teilt man hier die erste Zeile durch $\overline{12}$, d. h. man man multipliziert die erste Zeile mit dem inversen Koeffizienten $\overline{12}^{-1}$. Man sieht hier sofort bzw. errechnet mit dem erweiterten Euklidischen Algorithmus $\overline{12}^{-1} = \overline{2}$. Damit liefert die Normierung der ersten Zeile:

$$\begin{array}{rcrcrcr} \overline{1}\cdot x_1 & + & \overline{7}\cdot x_2 & + & \overline{8}\cdot x_3 & = & \overline{19} \\ \overline{10}\cdot x_1 & + & \overline{3}\cdot x_2 & + & \overline{20}\cdot x_3 & = & \overline{2} \\ \overline{9}\cdot x_1 & + & \overline{13}\cdot x_2 & + & \overline{21}\cdot x_3 & = & \overline{3} \end{array} \tag{10}$$

Jetzt subtrahiert man das $\overline{10}$-fache der ersten Zeile von der zweiten Zeile und das $\overline{9}$-fache der ersten Zeile von der zweiten Zeile:

$$\begin{array}{rcrcrcr} \overline{1}\cdot x_1 & + & \overline{7}\cdot x_2 & + & \overline{8}\cdot x_3 & = & \overline{19} \\ & & \overline{2}\cdot x_2 & + & \overline{9}\cdot x_3 & = & \overline{19} \\ & & \overline{19}\cdot x_2 & + & \overline{18}\cdot x_3 & = & \overline{16} \end{array} \tag{11}$$

Jetzt normiert man die zweite Zeile, indem man sie mit $\overline{2}^{-1} = \overline{12}$ multipliziert:

$$\begin{array}{rcrcrcr} \overline{1}\cdot x_1 & + & \overline{7}\cdot x_2 & + & \overline{8}\cdot x_3 & = & \overline{19} \\ & & \overline{1}\cdot x_2 & + & \overline{16}\cdot x_3 & = & \overline{21} \\ & & \overline{19}\cdot x_2 & + & \overline{18}\cdot x_3 & = & \overline{16} \end{array} \tag{12}$$

Jetzt wird das $\overline{19}$-fache der zweiten Zeile von der dritten Zeile abgezogen:

$$\begin{array}{rcrcrcr} \overline{1}\cdot x_1 & + & \overline{7}\cdot x_2 & + & \overline{8}\cdot x_3 & = & \overline{19} \\ & & \overline{1}\cdot x_2 & + & \overline{16}\cdot x_3 & = & \overline{21} \\ & & & & \overline{13}\cdot x_3 & = & \overline{8} \end{array} \tag{13}$$

Man erkennt anhand dieser reduzierten Form des Gleichungssystems, daß der Rang 3 und damit der Corang 0 ist. Wie üblich erhält man die eindeutige Lösung des linearen Gleichungssystems (9):

$$\begin{aligned} x_3 &= \overline{8}\cdot\overline{13}^{-1} = \overline{8}\cdot\overline{16} = \overline{13} \\ x_2 &= \overline{21} - \overline{16}\cdot x_3 = \overline{21} - \overline{16}\cdot\overline{13} = \overline{20} \\ x_1 &= \overline{19} - \overline{7}\cdot x_2 - \overline{8}\cdot x_3 = \overline{19} - \overline{7}\cdot\overline{20} - \overline{8}\cdot\overline{13} = \overline{5} \end{aligned} \tag{14}$$

(b) Die Koeffizientenmatrix des Gleichungssystems (9) lautet:

$$A = \begin{pmatrix} \overline{12} & \overline{15} & \overline{4} \\ \overline{10} & \overline{3} & \overline{20} \\ \overline{9} & \overline{13} & \overline{21} \end{pmatrix} \tag{15}$$

Hier gelten die gewohnten Regeln für die Determinantenberechnung. Mit Verwendung der Koeffizientenmatrix der reduzierten Form (13) liefert dieses:

$$\det A = \det \begin{pmatrix} \overline{12} & \overline{15} & \overline{4} \\ \overline{10} & \overline{3} & \overline{20} \\ \overline{9} & \overline{13} & \overline{21} \end{pmatrix} = \overline{12}\cdot\overline{2}\cdot\det \begin{pmatrix} \overline{1} & \overline{7} & \overline{8} \\ \overline{0} & \overline{1} & \overline{16} \\ \overline{0} & \overline{0} & \overline{13} \end{pmatrix} = \overline{13}$$

Hierbei wurde ausgenutzt, daß man einen vor der Determinanten stehenden Faktor in diese hineinziehen kann, indem man eine einzelne Zeile mit diesem multipliziert. Weiter wurde verwendet, daß sich der Wert der Determinanten nicht ändert, wenn zu einer Zeile das Vielfache einer anderen addiert. Außerdem ist bei einer Diagonalmatrix die Determinante das Produkt der Diagonalelemente.[2]

Auch das Berechnen der inversen Matrix erfolgt in der gewohnten Weise mit dem Gauß(-Jorden)-Verfahren.[3] Man beginnt damit, daß man die Matrix A und die Einheitsmatrix nebeneinander schreibt.

$$\begin{pmatrix} \overline{12} & \overline{15} & \overline{4} \\ \overline{10} & \overline{3} & \overline{20} \\ \overline{9} & \overline{13} & \overline{21} \end{pmatrix} \qquad \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \tag{16}$$

Anschließend führt man das Eliminationsverfahren soweit durch, bis aus A die Einheitsmatrix entstanden ist. Dabei werden alle Zeilenoperationen bei der Matrix A in gleicher Weise auch für die Zeilen der Einheitsmatrix durchgeführt. Die Einheitsmatrix verwandelt sich dann in die inverse Matrix A^{-1}. Es ist nur darauf zu achten, daß anstelle der sonst üblichen Division eine Multiplikation mit der inversen Restklasse des betreffenden Wertes zu erfolgen hat. Die einzelnen Schritte der Inversenberechnung lauten:

$$\begin{pmatrix} \overline{1} & \overline{7} & \overline{8} \\ \overline{0} & \overline{2} & \overline{9} \\ \overline{0} & \overline{19} & \overline{18} \end{pmatrix} \qquad \begin{pmatrix} \overline{2} & \overline{0} & \overline{0} \\ \overline{3} & \overline{1} & \overline{0} \\ \overline{5} & \overline{0} & \overline{1} \end{pmatrix} \tag{17}$$

$$\begin{pmatrix} \overline{1} & \overline{7} & \overline{8} \\ \overline{0} & \overline{1} & \overline{16} \\ \overline{0} & \overline{0} & \overline{13} \end{pmatrix} \qquad \begin{pmatrix} \overline{2} & \overline{0} & \overline{0} \\ \overline{13} & \overline{12} & \overline{0} \\ \overline{11} & \overline{2} & \overline{1} \end{pmatrix} \tag{18}$$

$$\begin{pmatrix} \overline{1} & \overline{7} & \overline{8} \\ \overline{0} & \overline{1} & \overline{16} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \qquad \begin{pmatrix} \overline{2} & \overline{0} & \overline{0} \\ \overline{13} & \overline{12} & \overline{0} \\ \overline{15} & \overline{9} & \overline{16} \end{pmatrix} \tag{19}$$

$$\begin{pmatrix} \overline{1} & \overline{7} & \overline{0} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \qquad \begin{pmatrix} \overline{20} & \overline{20} & \overline{10} \\ \overline{3} & \overline{6} & \overline{20} \\ \overline{15} & \overline{9} & \overline{16} \end{pmatrix} \tag{20}$$

$$\begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \qquad \begin{pmatrix} \overline{22} & \overline{1} & \overline{8} \\ \overline{3} & \overline{6} & \overline{20} \\ \overline{15} & \overline{9} & \overline{16} \end{pmatrix} \tag{21}$$

[2]Siehe Vorlesung bzw. Skript zur Vorlesung „Mathematik 1 für Informatik“.
[3]Siehe auch hier die Vorlesung bzw. Skript zur Vorlesung „Mathematik 1 für Informatik“.

Die rechte Seite von (21) ist die inverse Matrix A^{-1}. Das Matrizenprodukt wird ebenfalls auf die bekannte Art berechnet; dieses liefert:

$$A^2 \;=\; A \circ A \;=\; \begin{pmatrix} \overline{8} & \overline{1} & \overline{18} \\ \overline{8} & \overline{5} & \overline{14} \\ \overline{13} & \overline{10} & \overline{1} \end{pmatrix} \tag{22}$$

Als Beispiel soll hier nur die Berechnung des ersten Elementes der ersten Zeile vorgeführt werden:

$$\overline{12} \cdot \overline{12} \;+\; \overline{15} \cdot \overline{10} \;+\; \overline{4} \cdot \overline{9} \;=\; \overline{330} \;=\; \overline{8}$$

4. Lösung: Da $= 103$ eine Primzahl ist, ist $\varphi(103) = 102$, und nach dem Satz von Euler ist $\overline{a}^{\,102} = \overline{1}$ für alle $\overline{a} \in \mathbb{Z}_{13}^*$. Um dieses hier auszunutzen, teilt man den gegebenen Exponenten mit Rest durch $\varphi(103) = 102$:

$$1740 \;=\; 17 \cdot 102 \;+\; 6 \tag{23}$$

Also hat man

$$\begin{aligned} \overline{5}^{\,1740} \;&=\; \overline{5}^{\,17\cdot 102+6} \;=\; \underbrace{\left(\overline{5}^{\,102}\right)^{17}}_{=\overline{1}} \cdot \overline{5}^{\,6} \;=\; \overline{125}^{\,2} \;=\; \overline{22}^{\,2} \\ &=\; \overline{484} \;=\; \overline{72} \end{aligned}$$

Bemerkung: Auf die Berechnung des ganzzahligen Quotienten 17 in (23) hätte man verzichten können. Es reicht, $6 \equiv 1740 \mod 102$ zu berechnen.

5. Lösung: Zunächst zeigt man durch Nachrechnen

$$\overline{164790}^{\,2} \;=\; \overline{85521} \quad \text{sowie} \quad \overline{261333}^{\,2} \;=\; \overline{85521}$$

Wegen

$$\overline{164790} \;+\; \overline{261333} \;=\; \overline{426123} \;=\; \overline{161734} \;\neq\; \overline{0}$$

ist $\overline{u} \neq \pm\overline{v}$.

Wäre $n = 264389$ eine Primzahl, so wäre $\mathbb{Z}_n$ ein Körper, und ein Polynom zweiten Grades

$$X^2 \;-\; \overline{a}$$

könnte nicht mehr als zwei Nullstellen besitzen. Hier besitzt aber für $\overline{a} = \overline{164790}^{\,2} = \overline{261333}^{\,2} = \overline{85521}$ dieses Polynom die vier Nullstellen $\pm\overline{164790}$, $\pm\overline{261333}$. Daher kann n keine Primzahl sein.

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?