1. Lösung: Man berechnet jeweils mit dem erweiterten euklidischen Algorithmus bzw. mit dem chinesischen Restsatz sowie mit der Teilung mit Rest:

$$\begin{aligned} -26 \cdot 1243 + 27 \cdot 1197 &= 1 \\ 939 \cdot (-26) \cdot 1243 + 847 \cdot 27 \cdot 1197 &= -2972409 \\ -2972409 &= -2 \cdot (1243 \cdot 1197) + \mathbf{3333} \end{aligned}$$

$$\begin{aligned} -634 \cdot 1243 + 361 \cdot 2183 &= 1 \\ 1150 \cdot (-634) \cdot 1243 + 847 \cdot 361 \cdot 2183 &= -238781939 \\ -238781939 &= -88 \cdot (1243 \cdot 2183) + \mathbf{3333} \end{aligned}$$

$$\begin{aligned} 538 \cdot 1197 - 295 \cdot 2183 &= 1 \\ 1150 \cdot 538 \cdot 1197 - 939 \cdot 295 \cdot 2183 &= 135881985 \\ 135881985 &= 52 \cdot (1197 \cdot 2183) + \mathbf{3333} \end{aligned}$$

Der geheime Wert ist 3333.

2. Lösung:

   (a) Für $a, b \in \mathbb{N}$ mit $\mathrm{ggT}(a, b) = 1$ gibt es $u, v \in \mathbb{Z}$ mit $u \cdot a + v \cdot b = 1$. Ist nun $n \in \mathbb{N}$ mit $a|n$ und $b|n$, so ist zu zeigen, daß auch $(a \cdot b)|n$ gilt[1]. Multipliziert man beide Seiten der Gleichung $u \cdot a + v \cdot b = 1$ mit n:

   $$u \cdot a \cdot n + v \cdot b \cdot n = n$$

   so erkennt man, daß beide Summanden der linken Seite durch $a \cdot b$ teilbar sind. Folglich ist auch n durch $a \cdot b$ teilbar. Damit ist die Behauptung aus der Aufgabe für teilerfremde a, b gezeigt.

   (b) Seien $a, b \in \mathbb{N}$ beliebig, $d = \mathrm{ggT}(a, b)$ sowie $m = \mathrm{kgV}(a, b) = a \cdot b/d$. Zu zeigen ist, daß für $n \in \mathbb{N}$ mit $a|n$ und $b|n$ auch $m|n$ gilt. Als Teiler von a (und b) teilt d auch n. Es gibt somit $a_1, b_1, n_1 \in \mathbb{N}$ mit

   $$a = d \cdot a_1, \quad b = d \cdot b_1, \quad \text{und} \quad n = d \cdot n_1$$

   Es folgt dann sofort

   $$a_1 \mid n_1 \quad \text{und} \quad b_1 \mid n_1 \tag{1}$$

   Wie in einer früheren Aufgabe gezeigt wurde, ist $\mathrm{ggT}(a_1, b_1) = 1$. Wie im ersten Teil dieser Aufgabe gezeigt wurde, gilt dann wegen (1)

   $$(a_1 \cdot b_1) \mid n_1 \quad \Leftrightarrow \quad \frac{n_1}{a_1 \cdot b_1} \in \mathbb{N} \tag{2}$$

   Erweitert man den auf der rechten Seite von (2) stehenden (ganzzahlige) Bruch mit d^2, so erhält man weiter

[1] Dieses wurde im Skript bereits gezeigt; der Beweis wird aber hier noch einmal wiederholt

$$\frac{d^2 \cdot n_1}{d^2 \cdot a_1 \cdot b_1} \;=\; \frac{(d \cdot n_1) \cdot d}{(d \cdot a_1) \cdot (d \cdot b_1)} \;=\; \frac{n \cdot d}{a \cdot b} \in \mathbb{N} \tag{3}$$

Der letzte (ganzzahlige) Bruch auf der rechten Seite von (3) läßt sich weiter umformen, damit erhält man

$$\frac{n \cdot d}{a \cdot b} \;=\; \frac{n}{(a \cdot b)/d} \;=\; \frac{n}{m} \in \mathbb{N} \quad \Leftrightarrow \quad m \mid n \tag{4}$$

Mit (4) ist die Behauptung gezeigt.

3. Lösung: Aus der Definition von $\mathcal{R}$ folgt sofort, daß die Nullmatrix und die Einheitsmatrix enthalten sind. Assoziativgesetz und Distributivgesetz sind erfüllt, da sie allgemein für Matrizen gelten. Dieses gilt auch für das Kommutativgesetz der Addition. Weiter folgt sofort aus der Definition von $\mathcal{R}$, daß mit einer Matrix auch deren Negative enthalten ist.

   Addition und Multiplikation zweier solcher Matrizen liefern:

$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} \;=\; \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & a_1 + a_2 \end{pmatrix} \tag{5}$$

$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \circ \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} \;=\; \begin{pmatrix} a_1 \cdot a_2 & a_1 b_2 + b_1 a_2 \\ 0 & a_1 \cdot a_2 \end{pmatrix} \tag{6}$$

   Man erkennt hieran, daß beide Verknüpfungen wieder Matrizen in $\mathcal{R}$ liefern, womit die Abgeschlossenheit bezüglich der Addition und der Multiplikation gezeigt sind. Anhand von (6) erkennt man, daß die Multiplikation für zwei Matrizen der betreffenden Gestalt kommutativ ist.

   Insgesamt folgt damit, daß $\mathcal{R}$ ein kommutativer Ring mit Eins ist, der allerdings Nullteiler besitzt, wie das folgende Beispiel zeigt:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \;=\; \begin{pmatrix} 0 \cdot 0 & 0 \cdot 2 + 1 \cdot 0 \\ 0 & 0 \cdot 0 \end{pmatrix} \;=\; \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

4. Lösung: Diese erste Relation ist eine Äquivalenzrelation. Die zweite Relation ist *keine* Äquivalenzrelation, denn die Transitivität ist nicht gegeben, wie das folgenden Beispiel zeigt:

$$\mathrm{p}_1(x) = x \qquad \mathrm{p}_2(x) = x^2 - x \qquad \mathrm{p}_3(x) = x - 1$$

   Hier ist $\mathrm{p}_1[x] \sim \mathrm{p}_2[x]$, da sie die Nullstelle $x_1 = 0$ gemeinsam besitzen. Ebenso ist $\mathrm{p}_2[x] \sim \mathrm{p}_2[x]$, da sie die Nullstelle $x_2 = 1$ gemeinsam besitzen. Aber es ist $\mathrm{p}_1[x] \not\sim \mathrm{p}_3[x]$, da sie keine gemeinsame Nullstelle besitzen.

5. Lösung: Man berechnet

$$\varphi(42) \;=\; 12$$

Die Multiplikationstabelle von $\mathbb{Z}_{42}^*$ lautet:

$*$	1	5	11	13	17	19	23	25	29	31	37	41
1	1	5	11	13	17	19	23	25	29	31	37	41
5	5	25	13	23	1	11	31	41	19	29	17	37
11	11	13	37	17	19	41	1	23	25	5	29	31
13	13	23	17	1	11	37	5	31	41	25	19	29
17	17	1	19	11	37	29	13	5	31	23	41	25
19	19	11	41	37	29	25	17	13	5	1	31	23
23	23	31	1	5	13	17	25	29	37	41	11	19
25	25	41	23	31	5	13	29	37	11	19	1	17
29	29	19	25	41	31	5	37	11	1	17	23	13
31	31	29	5	25	23	1	41	19	17	37	13	11
37	37	17	29	19	41	31	11	1	23	13	25	5
41	41	37	31	29	25	23	19	17	13	11	5	1

Die Inversen können, wie in der Vorlesung beschrieben, mit Hilfe des erweiterten euklidischen Algorithmus berechnet werden. Steht wie hier die Multiplikationstabelle zur Verfügung, so sucht man in der zur Restklasse $\overline{a} \in \mathbb{Z}_{42}^*$ gehörigen Zeile die $\overline{1}$; der dazu gehörige zweite Faktor ist die Inverse $\overline{a}^{-1}$. Man erhält hier:

$\overline{a}$	1	5	11	13	17	19	23	25	29	31	37	41
$\overline{a}^{-1}$	1	17	23	13	5	31	11	37	29	19	25	41

Die Multiplikationstabelle und $\varphi(42)$ können mit dem folgenden C-Programm berechnet werden:

```
#include <stdio.h>

unsigned long int ggt(unsigned long int a, unsigned long int b){
  while(b>0) {unsigned long int r=a%b; a=b; b=r;}
  return a;
}

int main(){
  unsigned long int n, a, b, phi=0;
  printf("Eine natrliche Zahl >"); scanf("%lu",&n);
  for(a=1;a<n;a++)
    if(ggt(a,n)==1) {
      phi++;
      for(b=1;b<n;b++)
        if(ggt(b,n)==1){
          printf("%lu * %lu =  %lu \n",a,b,(a*b)%n);
        }
      }
  printf("\nphi=%3lu\n\n",phi);
  return 0;
}
```

6. Lösung: Die in $\mathbb{Z}_{22}$ gegebene Gleichung

$$\overline{0} \;=\; \overline{9} \cdot x + \overline{a} \tag{7}$$

ist sicher lösbar, da die Restklasse $\overline{9}$, wie man anhand von $\mathrm{ggT}(9,22) = 1$ erkennt, invertierbar ist. Mit Hilfe des erweiterten euklidischen Algorithmus oder durch Probieren erhält man $\overline{9}^{-1} = \overline{5}$.

Die Lösung der Gleichung (7) berechnet man auf die gewohnte Weise: Man subtrahiert von beiden Seiten $\overline{a}$ und multipliziert anschließend mit $\overline{5} = \overline{9}^{-1}$:

$$x \;=\; -\overline{9}^{-1} \cdot \overline{a} \;=\; -\overline{5} \cdot \overline{a} \tag{8}$$

Die so berechnete Lösung ist eindeutig. Nimmt man nämlich an, es gebe zwei Lösungen

$$\begin{aligned} \overline{0} &= \overline{9} \cdot x_1 + \overline{a} \\ \overline{0} &= \overline{9} \cdot x_2 + \overline{a} \end{aligned} \tag{9}$$

so liefern die Subtraktion beider Gleichungen (9) und die anschließende Multiplikation mit $\overline{5} = \overline{9}^{-1}$

$$\begin{aligned} \overline{5} \cdot \overline{0} &= \overline{5} \cdot \overline{9} \cdot (x_1 - x_2) \\ \Rightarrow \qquad \overline{0} &= x_1 - x_2 \\ \Rightarrow \qquad x_2 &= x_1 \end{aligned}$$

Die Lösungen der Gleichung (7) für alle möglichen $\overline{a} \in \mathbb{Z}_{22}$ erhält man aus (8):

$\overline{a}$	0	1	2	3	4	5	6	7	8	9	10
x	0	17	12	7	2	19	14	9	4	21	16
$\overline{a}$	11	12	13	14	15	16	17	18	19	20	21
x	11	6	1	18	13	8	3	20	15	10	5

Die Gleichung

$$\overline{0} \;=\; \overline{4} \cdot x + \overline{3} \tag{10}$$

ist *nicht* lösbar. Angenommen, es gäbe eine Lösung $x = \overline{u} \in \mathbb{Z}_{22}$, so wäre wegen $\overline{3}^{-1} = \overline{15}$ und wegen

$$\begin{aligned} \overline{3} &= -\overline{4} \cdot \overline{b} \;=\; -\overline{b} \cdot \overline{4} \\ \Rightarrow \quad \overline{1} &= (-\overline{15} \cdot \overline{b}) \cdot \overline{4} \end{aligned}$$

die Restklasse $\overline{4}$ invertierbar, was aber wegen $\mathrm{ggT}(4,22) = 2$ nicht sein kann.

Die Gleichung

$$\overline{0} \;=\; \overline{4} \cdot x + \overline{6} \tag{11}$$

ist *mehrdeutig* lösbar ist. Zwei verschiedene Lösungen sind

$$x_1 \;=\; \overline{4} \quad \text{und} \quad x_2 \;=\; \overline{15}$$

Man beachte, daß die mehrdeutige Lösbarkeit für (9) nur deshalb möglich ist, weil $\overline{4} \in \mathbb{Z}_{22}$ ein Nullteiler ist.