Ringe und Ideale, Primfaktorzerlegung in Hauptidealbereichen, chinesischer Restsatz

Aufgaben: 12

```
> restart;
```

Ringe, Restklassenringe, Ideale

MATH: Im Folgenden werden Ringe immer kommutativ sein und ein Einselement haben. Unter diesen sind die Körper ausgezeichnet. Ein Ring *R* ist genau dann ein Körper, wenn jedes Element ungleich 0 in *R* invertierbar ist, also ein multiplikatives Inverses hat, kurz eine **Einheit** ist.

ÜBUNG [01]:

Was sind die Einheiten in $\mathbb{Z}$, $\mathbb{R}[x]$, $\mathbb{Q}$, $\mathbb{Z}[x]$? Welche dieser Ringe sind Körper? Gib eine Nichteinheit $\neq 0$ an, wenn kein Körper vorliegt.

MATH: Ein interessantes Spiel besteht darin, in einem Ring ein (oder mehrere) Element(e) Null zu setzen, also die Gleichheit durch eine gewisse Äquivalenzrelation zu ersetzen, aber ansonsten genau wie vorher zu rechnen, so dass man wieder einen Ring bekommt. Die Elemente dieses Ringes wären dann die Äquivalenzklassen und die Addition und Multiplikation dieser Klassen dann vertreterweise durchzuführen.

BEISPIELE:

1.) In einem Körper K setzen wir ein Element

$$a \neq 0$$

zu Null, was wir so schreiben:

$$a \equiv 0.$$

Dann folgt

$$1 = a^{-1}a \equiv a^{-1}0 = 0$$

also

$$1 \equiv 0$$

und damit

$$b \equiv 0$$

für alle $b \in K$.

Damit hätte der neue Ring nur ein einziges Element. So etwas betrachten wir nicht . Man verlangt meistens bei einem Ring

$$1 \neq 0.$$

2.) In $\mathbb{Z}$ setzen wir

$$2 \equiv 0$$

und bekommen

$$\mathbb{Z} / 2\mathbb{Z} = \mathbb{F}_2$$

den Körper aus zwei Elementen.

3.) In $\mathbb{R}[x]$ setzen wir

$$x^2 + 1 \equiv 0$$

und bekommen

$$\mathbb{R}[x] / \mathbb{R}[x]\,(x^2 + 1) = \mathbb{C}$$

den Körper der komplexen Zahlen.

ÜBUNG [02]:

Zeige, dass

$$\mathbb{C}[x] / \mathbb{C}[x]\,(x^2 + 1)$$

kein Körper ist.

MATH: Sei R ein Ring (also kommutativ mit Eins, wie oben vereinbart). Eine nicht leere Teilmenge

$$I \subseteq R$$

heißt **Ideal** von R, falls

$$a, b \in I \Rightarrow a + b \in I$$

und

$$a \in I, r \in R \Rightarrow ra, ar \in I$$

gilt.
Schreibweise: $I \trianglelefteq R$.

Diese beiden Regeln sind leicht zu merken, da die Restklasse der 0 ein Ideal bildet, und ebensoleicht motiviert durch

$$0 + 0 = 0$$

und

$$0\,r = r0 = 0.$$

Ist $I \trianglelefteq R$ und $r \in R$, so heißt

$$r + I := \{r + i \mid i \in I\}$$

die **Restklasse** von r nach I.
Die Menge aller Restklassen nach I bilden mit der vertreterweisen Addition und Multiplikation einen Ring, der mit

$$R/I$$

bezeichnet wird.

DENKANSTOSS: Woher kennst du dieses Konzept?

ÜBUNG [03]:

Die ungeraden Zahlen bilden eine Restklasse in $\mathbb{Z}$.
Zeige dies, bestimme das zugehörige Ideal und erinnere dich an die Division mit Rest, um den Namen Restklasse zu motivieren.

DENKANSTOSS: Der Schnitt einer Menge von Idealen eines Ringes ist wieder ein Ideal.

Hauptidealbereiche, Teilbarkeit

MATH: Wichtige Beispiele von Idealen sind Hauptideale. Das von

$$r \in R$$

erzeugte Ideal, also der Schnitt aller Ideale, die *r* enthalten ist, ist gegeben durch

$$rR = Rr := \{ra \mid a \in R\}$$

und heißt das von *r* erzeugte **Hauptideal** von *R*.
Übrigens sind die beiden trivialen Ideal $\{0\}$ und R auch Hauptideale , denn

$$\{0\} = 0\,R \quad \text{und} \quad R = 1\,R.$$

Beachte *R*/*R* ist der bereits oben geschmähte Nullring.

DENKANSTOSS: Die Summe und das Produkt zweier Ideale sind wieder Ideale:

$$I_1, I_2 \trianglelefteq R \;\Rightarrow I_1 + I_2 := \{a + b \mid a \in I_1,\ b \in I_2\} \trianglelefteq R.$$

$$I_1, I_2 \trianglelefteq R \;\Rightarrow I_1 I_2 := \{a_1 b_1 + \ldots + a_n b_n \mid n \in \mathbb{N}, a_i \in I_1,\ b_i \in I_2\} \trianglelefteq R.$$

ÜBUNG [04]:

Zeige, dass in einem Euklidischem Ring jedes Ideal ein Hauptideal ist.
Bestimme den Hauptidealerzeuger von

$$(133412\mathbb{Z} + 33412\mathbb{Z}) \trianglelefteq \mathbb{Z}$$

und

$$((x^{12} + x^8 + 1)\mathbb{F}_2[x] + (x^{15} + x^{10} + 1)\mathbb{F}_2[x]) \trianglelefteq \mathbb{F}_2[x]$$

(Erinnerung: Man hat eine Division mit Rest und kann von dem Rest sagen dass er "kleiner" also der Divisor, sodass man einen Euklidischen Algorithmus hat) .

MATH: Ringe, bei denen das Produkt zweier von Null verschiedener Elemente wieder von Null verschieden ist, heißen **Integritätsbereich**e.
Integritätsbereiche, deren sämtliche Ideale Hauptideale sind heißen **Hauptidealbereich**e.

Offenbar sind Euklidische Ringe Hauptidealbereiche. $\mathbb{Z}$ und $K[x]$, wobei *K* ein Körper ist, sind die wichtigsten Beispiele.

MATH: Sind R und S Ringe, so heißt eine Abbildung

$$\alpha : R \to S$$

Ringhomomorphismus, falls sie additiv und multiplikativ ist, sowie

$$\alpha(1_R) = 1_S$$

erfüllt.

DENKSANSTOSS: Ist ein Ringhomomorphismus bijektiv, so ist sein Inverses auch Ringhomomorphimus. Man spricht von einem **Ringisomorphismus**.

Man überlegt sich leicht:
M ATH: $I \trianglelefteq R \Rightarrow \nu : R \to R/I : r \mapsto r + I$ ist ein **Ringepimorphismus**, also ein surjektiver Ringhomomorphismus.
Umgekehrt:
Ist $\alpha : R \to S$ ein Ringhomomorphismus und $I \trianglelefteq S$ ein Ideal, so folgt $\alpha^{-1}(I) \trianglelefteq R$. Insbesondere ist

$$\text{Kern}(\alpha) := \alpha^{-1}(\{0_S\}) \trianglelefteq R.$$

Weiter:
Ist $\alpha : R \to S$ ein Ringepimorphismus und $I \trianglelefteq R \Rightarrow \alpha(I) \trianglelefteq S$.

ÜBUNG [05]:

Zeige $\mathbb{Z}/100\mathbb{Z}$ ist kein Hauptidealbereich, obwohl seine sämtlichen Ideale Hauptideale sind. Zeige also insbesondere, dass sämtliche Ideale Hauptideale sind.

MATH: Ein Körper *K* hat nur die beiden **trivialen Ideale** $\{0\}$ und *K*.
Offenbar ist ein Ring $K \neq \{0\}$, welcher keine nicht-triviale Ideale enthält, ein Körper (Warum?).
Also: Ist $R \neq \{0\}$ ein Ring und $I \trianglelefteq R$, so folgt:
R/I ist Körper genau dann, wenn *I* **maximales Ideal** von *R* ist.
(Dabei heißt $I \trianglelefteq R$ maximales Ideal, wenn $I \neq R$ gilt und *R* das einzige *I* umfassende Ideal ist.)

BEISPIEL:
$x\mathbb{Z}[x]$ ist kein maximales Ideal von $\mathbb{Z}[x]$, denn $\mathbb{Z}[x]/x\mathbb{Z}[x] \cong \mathbb{Z}$ ist kein Körper.
$2\mathbb{Z}[x]$ ist kein maximales Ideal von $\mathbb{Z}[x]$, denn $\mathbb{Z}[x]/2\mathbb{Z}[x] \cong \mathbb{F}_2[x]$ ist kein Körper.
$x\mathbb{Z}[x] + 2\mathbb{Z}[x]$ ist ein maximales Ideal von $\mathbb{Z}[x]$, denn $\mathbb{Z}[x]/(2\mathbb{Z}[x] + x\mathbb{Z}[x]) \cong \mathbb{F}_2$ ist ein Körper.

DENKANSTOSS: Finde alle Restklassenkörper von $\mathbb{Z}/100\mathbb{Z}$.

MATH: Auf Hauptidealbereiche R und $a \in R$ angewandt bedeutet dies die Äquivalenz der folgenden drei Aussagen:
1.) Ra ist ein maximales Ideal von R.
2.) R/Ra ist ein Körper.

3.) *a* ist **unzerlegbar (= irreduzibel)**, d. h. *a* lässt nur triviale Faktorierungen zu, also solche, in denen ein Faktor eine Einheit ist.

Wir wollen jetzt einen Schritt weitergehen und eine vollständige Teilbarkeitstheorie in Hauptidealbereichen skizzieren, Zunächst eine allgemeine Vorbereitung:

MATH: Sei *R* ein Ring, $a, b \in R$. Man sagt a **teilt** b (kurz $a \mid b$), falls $b \in Ra$ (oder äquivalent $Rb \subseteq Ra$) gilt.
Falls $a \mid b$ und $b \mid a$ gilt, dann heißen a, b **assoziiert**.
Ein Element $p \in R$ heißt **prim**, falls für alle $a, b \in R$ gilt:

$$p \mid ab \Rightarrow p \mid a \text{ oder } p \mid b.$$

Offenbar gilt: Ein primes Element ist irreduzibel.

Die Umkehrung hiervon ist der Kernpunkt bei Hauptidealbereichen

MATH: Sei R ein Hauptidealbereich und $u \in R$ irreduzibel. Dann ist *u* prim.

Beweis: Angenommen $u \nmid a$ und $u \nmid b$. Da Ru ein maximales Ideal ist, folgt dann

$$Ru + Ra = R \text{ und } Ru + Rb = R.$$

Also haben wir $r_i \in R$ mit

$$r_1 u + r_2 a = 1 \text{ und } r_3 u + r_4 b = 1,$$

sodass durch Produktbildung folgt:

$$r_5 u + r_6 ab = 1$$

mit $r_5, r_6 \in R$ geeignet. Das heißt aber $u \nmid ab$.

q.e.d.

ÜBUNG [06]:

Sei *R* ein Hauptidealbereich und $a, b \in R$. Zeige:
$a, b \in R$ sind **teilerfremd**, d. h. haben nur genau dann Einheiten als gemeinsame Teiler, wenn

$$Ra + Rb = R$$

gilt.

Primfaktorzerlegung in Hauptidealbereichen, chinesischer Restsatz

Als Konsequenz aus dem letzten Abschnitt bekommt man nun die eindeutige Primfaktorzerlgung in einem Hauptidealbereich.

MATH: Sei *R* ein Hauptidealbereich und $a \in R$ keine Einheit.
1.) Es gibt ein $n \in \mathbb{N}$ und nicht assoziierte, irreduzible Elemente $p_1, \ldots, p_n \in R$

sowie $k_1, ..., k_n \in \mathbb{N}$
und eine Einheit $e \in R$ mit

$$a = e \cdot p_1^{k_1} \cdot \ldots \cdot p_n^{k_n},$$

kurz eine Primfaktorzerlegung.
2.) Ist

$$a = f \cdot q_1^{l_1} \cdot \ldots \cdot q_m^{l_m}$$

eine zweite Primfaktorzerlegung von *a*, so gilt

$$m = n$$

und nach Umnummerierung der q_i gilt weiter

q_i und p_i sind assoziiert, d. h. sie unterscheiden sich nur um einen Einheitsfaktor, und

$l_i = k_i$ für alle $i = 1, ..., n$.

Es sei angemerkt, dass für die Existenz einer Primfaktorzerlegung nur noch eine kleine Beweisidee fehlt, nämlich die Tatsache, das man nicht unendlich oft Primfaktoren abdividieren kann. Dies würde zu unendlichen aufsteigenden Idealketten führen, die deshalb nicht existieren können, weil die Vereinigung einer solchen Kette wieder ein Hauptideal ist.

ÜBUNG [07]:

Zeige, dass *a* mit der obigen Primfaktorzerlegung $a = e \cdot p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ im Hauptidealbereich *R* genau

$$(k_1 + 1) \cdot \ldots \cdot (k_n + 1)$$

Assoziiertenklassen von Teilern hat. Zeige ferner, dass dies auch die Anzahl der Ideale ist, die *Ra* umfassen.
Bestimme diese Zahl für $a = x^{20} - 1 \in \mathbb{F}_2[x]$ und für $a = x^{20} - 1 \in \mathbb{Q}[x]$.

DENKANSTOSS: (Alles in Hauptidealbereichen!) Wie liest man von der Primfaktorzerlegung zweier Elemente ab, ob sie teilerfrend sind? Zeige *Ra+Rb (= Rab) =Ra∩Rb* für *a,b 2 R* teilerfremd.

Die eindeutige Primfaktorzerlegung der Elemente in Hauptidealbereichen hat eine wichtige Konsequenz für die Struktur der Restklassenringe der Hauptidealbereiche.

MATH: Zwei Ideale *I,J* eines Ringes *R* heißen teilerfremd, falls

I+J=R.

Ist *R* ein Hauptidealbereich, so bedeutet dies, dass die Erzeuger der Ideale teilerfremd sind.
Es gilt der berühmte chinesische Restesatz, welcher besagt, dass man im teilerfremden Fall der Restklassenring

$$R/(I \cap J)$$

aus seinen beiden epimorphen Bildern

$$R/I \text{ und } R/J$$

rekonstruieren kann. Die Art der Rekonstruktion ist sehr einfach:

MATH: Seine R_1, R_2 zwei Ringe mit Einselementen $1_1, 1_2$. Dann heißt

$$R_1 \oplus R_2 := \{ (a, b) \mid a \in R_1,\ b \in R_2 \}$$

die **ringdirekte Summe** von R_1 und R_2, wobei die Verknüpfungen komponentenweise definiert sind:

$$(r_1, r_2) + (s_1, s_2) := (r_1 + s_1, r_2 + s_2)$$

und

$$(r_1, r_2) \cdot (s_1, s_2) := (r_1 \cdot s_1, r_2 \cdot s_2)$$

mit $r_1, s_1 \in R_1, r_2, s_2 \in R_2$.

Damit ist

$$(1_1, 1_2)$$

das Einselement der ringdirekten Summe. Offenbar sind die Projektionen

$R_1 \oplus R_2 \to R_1 : (r_1, r_2) \mapsto r_1$ und $R_1 \oplus R_2 \to R_2 : (r_1, r_2) \mapsto r_2$

Ringepimorphismen, deren Kerne Hauptideale sind, die von

$$(0_1, 1_2) \quad \text{bzw.} \quad (1_1, 0_2)$$

erzeugt werden. Man beachte, dass das von

$$(0_1, 1_2)$$

erzeugte Hauptideal als Ring offenbar wieder isomorph ist zu R_2 und das von

$$(1_1, 0_2)$$

zu R_1.

Ein Ring, welcher zu einer ringdirekten Summe zweier (nicht trivialer) Ringe isomorph ist, heißt auch ringdirekte Summe.

Wie erkennt man ringdirekte Summen?

MATH: Ist R ein Ring und

$$1 = e_1 + e_2$$

eine Zerlgung der Eins in orthogonale Idempotente e_i, d. h.

$$e_1^2 = e_1,\ e_2^2 = e_2,\ e_1 e_2 = 0,$$

so gilt:

$$R \to R\,e_1 \oplus R\,e_1 : r \mapsto (re_1, re_2)$$

ist ein Isomorphismus von Ringen.

DENKANSTOSS: Wie wird man die ringdirekte Summe von n Ringen definieren?

Der chinesische Restsatz besagt nun:

MATH: Sei R ein Ring mit zwei teilerfremden Idealen $I, J \trianglelefteq R$, also $I+J=R$, dann ist

$$R/(I \cap J) \cong R/I \oplus R/J,$$

genauer

$$R/(I \cap J) \to R/I \oplus R/J : r + I \cap J \mapsto (r + I, r + J)$$

ein Ringisomorphismus.
Ist insbesondere R ein Hauptidealbereich mit teilerfremden Elementen $a, b \in R$, dann gilt :

$$R/abR \cong R/aR \oplus R/bR \quad .$$

BEISPIEL: $R := \mathbb{Z}$,

```
> a:=16;b:=9;
```

$$a := 16$$
$$b := 9 \qquad \textbf{(1.3.1)}$$

```
> igcdex(a,b, 's', 't');
```

$$1 \qquad \textbf{(1.3.2)}$$

```
> e2:=a*s;e1:=b*t;
```

$$e2 := 64$$
$$e1 := -63 \qquad \textbf{(1.3.3)}$$

```
> e1 mod 16; e1 mod 9;
```

$$1$$
$$0 \qquad \textbf{(1.3.4)}$$

```
> e2 mod 16; e2 mod 9;
```

$$0$$
$$1 \qquad \textbf{(1.3.5)}$$

Wir können mit dieser Ausgangsinformation nun leicht das lineare Kongruenzensystem

$$x \equiv x_a \pmod{a}, \; x \equiv x_b \pmod{b}$$

lösen, wobei $x_a, x_b \in \mathbb{Z}$ beliebig vorgeben sind. Dies bedeutet,

$$x - x_a \in a\mathbb{Z}, x - x_b \in b\mathbb{Z}.$$

Die Lösungen bilden dann nach dem chinesischen Restsatz eine Restklasse nach $ab\mathbb{Z}$:

$$(x_a + a\mathbb{Z}) \bigcap (x_b + b\mathbb{Z}) = e_1 a + e_2 b + ab\mathbb{Z}$$

ÜBUNG [08]:

Man bestimme alle Polynome $p \in \mathbb{Q}[x]$ mit

$$p \equiv x \pmod{(x^2-1)^2},$$
$$p \equiv x+1 \pmod{(x^2-4)^2},$$
$$p \equiv x+2 \pmod{(x^2-9)^2}.$$

(Hinweis: Jedes der drei Polynome $(x^2-i)^2$ ist teilerfremd zu dem Produkt der beiden anderen.)
Begründe darüberhinaus, dass diese drei Bedingungen äquivalent damit sind, dass p und die Ableitung p' an den Punkten $\pm 1, \pm 2, \pm 3$ bestimmte Werte annehmen. Gib diese Werte an.

Anwendung: RSA-Verfahren in der Kryptografie

```
> restart;
```

Den chinesischen Restesatz kann man anwenden, um die Korrektheit des RSA-Verfahrens zu beweisen, weshalb wir nun einen kleinen Ausflug in die Kryptographie unternehmen.

Wir brauchen folgenden Satz, welchen hier vorerst ohne Beweis akzeptieren wollen:

MATH: Ist M eine endliche abelsche Gruppe, so gilt :

$$|M| \cdot M = \{0\}.$$

Hiermit folgt sofort der berühmte kleine Satz von *Fermat:*

MATH: Ist $a \in \mathbb{Z}$ und $p \in \mathbb{Z}$ prim, so gilt:

$$a^p \equiv a \pmod{p}.$$

ÜBUNG [09]:

Führe diese Folgerung aus. (*Hinweis*: Betrachte die Restklasse von a in $\mathbb{Z}/p\mathbb{Z}$).

Nachdem wir nun die mathematische Vorarbeit geleistet haben kommen wir zum RSA-Verfahren, welches nach seinen Schöpfern Ron Rivest, Adi Shamir und Leonard Adleman benannt wurde.
Das RSA-Verfahren ist ein asymmetrisches Kryptoverfahren (auch Public-Key-Verfahren genannt), das heißt man braucht zwei verschiedene Schlüssel. Einer davon ist privat und nur einem selber bekannt, wohingegen der andere veröffentlicht wird.
Es wird in vielen Bereichen eingesetzt, zum Beispiel zur Signatur von Mails oder deren Verschlüsselung. Ferner wird es im SSL-Protokoll verwendet, also ist jeder der schon mal eine Webseite mit https besucht hat, kam schon mal mit diesem Verfahren in Berührung.

ALGORITHMUS: RSA-Schlüsselerzeugung:
1) Wähle zufällig zwei Primzahlen p und q.
2) Berechne $n = p \cdot q$.
3) Berechne $\varphi(n) = (p-1) \cdot (q-1)$.
4) Wähle $e \in \mathbb{Z}$ mit $1 < e < \varphi(n)$ und $ggT(e, \varphi(n)) = 1$.
5) Berechne $d \equiv e^{-1} \pmod{\varphi(n)}$.

Das Paar $((n, e), (n, d))$ ist das gesuchte Schlüsselpaar. Wir wollen also nun ein solches Paar bestimmen, dafür fragen wir Maple nach Primzahlen:

```
> p:=ithprime(12345);
  q:=ithprime(23456);
```

$$p := 132241$$

(1.4.1)

$$q := 267649 \quad \textbf{(1.4.1)}$$

MAPLE: **ithprime(x)** liefert die x-te Primzahl.

```
> n:=p*q;
```

$$n := 35394171409 \quad \textbf{(1.4.2)}$$

```
> phi_n:=(p-1)*(q-1);
```

$$phi\_n := 35393771520 \quad \textbf{(1.4.3)}$$

```
> e:=rand(2..phi_n-1)():
  while(igcd(e,phi_n)<>1) do
    e:=rand(2..phi_n-1)():
  end do;
  e;
```

$$e := 15235196455$$
$$e := 17988963612$$
$$e := 34344539878$$
$$e := 7412421907$$
$$7412421907 \quad \textbf{(1.4.4)}$$

MAPLE: **rand(2..phi_n-1)()** erzeugt eine zufällige natürliche Zahl aus dem Intervall $[2, \varphi(n)]$.

```
> igcdex(e,phi_n,'d','t'):
  d;
```

$$631864603 \quad \textbf{(1.4.5)}$$

Also erhalten wir das folgende Schlüsselpaar:

```
> public_key:=[n,e];
  private_key:=[n,d];
```

$$public\_key := [35394171409, 7412421907]$$
$$private\_key := [35394171409, 631864603] \quad \textbf{(1.4.6)}$$

ALGORITHMUS: RSA-Verschlüsselung
Input: Public-Key (n, e) , Nachricht m
Output: verschlüsselte Nachricht c
Algorithmus:

$$c := m^e \pmod{n}$$

Wir können dafür natürlich auch eine Maplemethode schreiben:

```
> encrypt:=proc(key::list(posint),m::posint)
    if m < 0 or m > key[1] then
      error("Nachricht m verletzt 0 <= m < n");
    fi;
    if nops(key) <> 2 then
      error("Kein gültiger Schlüssel.");
    fi;
    if key[2]=1 then
      return m;
    end if;
    if irem(key[2],2)=0 then
```

```
    return encrypt([key[1],key[2]/2],m)^2 mod key[1];
   end if;
   return encrypt([key[1],key[2]-1],m)*m mod key[1];
 end proc:
```

ALGORITHMUS: RSA-Verschlüsselung
Input: Private-Key (n, d) , Kryptotext c
Output: Nachricht m
Algorithmus:

$$m := c^d \pmod{n}$$

Auch hier eine Funktion in Maple:

```
> decrypt:=proc(key::list(posint),c::posint)
   if c < 0 or c > key[1] then
    error("Kryptotext c verletzt 0 <= c < n");
   fi;
   if nops(key) <> 2 then
    error("Kein gültiger Schlüssel.");
   fi;
   if key[2]=1 then
    return c;
   end if;
   if irem(key[2],2)=0 then
    return encrypt([key[1],key[2]/2],c)^2 mod key[1];
   end if;
   return encrypt([key[1],key[2]-1],c)*c mod key[1];
 end proc:
```

Wir wollen nun eine Nachricht versenden:

```
> m:=1234567890;
```

$$m := 1234567890 \qquad \textbf{(1.4.7)}$$

```
> c:=encrypt(public_key,m);
```

$$c := 3067791170 \qquad \textbf{(1.4.8)}$$

Nun können wir diese wieder entschlüsseln und testen, ob es sich um die ursprüngliche Nachricht handelt:

```
> m=decrypt(private_key,c);
  is(%);
```

$$1234567890 = 1234567890$$

$$true \qquad \textbf{(1.4.9)}$$

ÜBUNG [10]:
Beweise die Korrektheit des RSA-Verfahrens. (*Hinweis:* Wende den chinesischen Restsatz auf die Situation an.)

Bleibt die Frage: Wie sicher ist das RSA-Verfahren?
Es ist bisher unbekannt wie schwer es ist eine verschlüsselte Nachricht unter

Kenntnis des öffentlichen Schlüsseln zu entschlüsseln. Auf jeden Fall wäre es möglich die Zahl n zu faktorisieren, um dann so den privaten Schlüssel zu berechnen. Zum Glück ist die Faktorisierung ganzer Zahlen (bisher) kein einfaches Problem.

ÜBUNG [11]:

Entschlüssele folgenden Kryptotext

```
> c_2:=462417249216465556509;
```

$$c\_2 := 462417249216465556509 \quad \textbf{(1.4.10)}$$

Hierbei wurde der folgende öffentliche Schlüssel verwendet:

```
> public_key_2:=[105080930338397326003 7,17743887669363763081]
  ;
```

$$public\_key\_2 := [105080930338397326003 7, 17743887669363763081] \quad \textbf{(1.4.11)}$$

Wer nun denkt, dass Entschlüsselung kein Problem sei, der möge sich an folgenden Eingaben versuchen (**ABER NUR AN SEINEM EIGENEM RECHNER UND NUR AUF EIGENE GEFAHR!!!**):

```
> public_key_3:=
  [74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585377011896809828673317327310893090055250511687706329907239638078671008609696253793465056379635 9,
  65665637630314161885353737197235555906318422232283470156237094032552821207253852837617011325408098494204928779466085030181397075423661717908459425773839959881699356825419741845307351885532965717410820210278096419];
```

$$public\_key\_3 := \quad \textbf{(1.4.12)}$$

$$[74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585377011896809828673317327310893090055250511687706329907239638078671008609696253793465056379635 9, 65665637630314161885353737197235555906318422232283470156237094032552821207253852837617011325408098494204928779466085030181397075423661717908459425773839959881699356825419741845307351885532965717410820210278096419]$$

```
> c_3 :=
  174558793054456089214780274632018946387229751252799540604763281526270430116858378881470472234183563803872458181922573039647015877727554436264237978006403134760639999928443984555061036671782997641646315219059714 70;
```

$$c\_3 := 174558793054456089214780274632018946387229751252799540\backslash 60476328152627043011685837888147047223418356380387245818192257303964\backslash 70158777275544362642379780064031347606399999284439845550610366717829976416463152190597147 0 \quad \textbf{(1.4.13)}$$

Es sei hier noch angemerkt, dass die in der Realität verwendeten Schlüsselpaare noch um einiges größer sind. Der obige Schlüssel hat eine Bitlänge von 704, wohingegen man heutzutage problemlos mit Schlüsseln von 2048 oder sogar 4096 Bits arbeitet.

Wer will kann gerne mit dem obigen Schlüssel einige Nachrichten verschlüsseln:

```
> encrypt(public_key_3,1234567890);
```

$$3053424121837317348831809104116156161266046581764896615 02\backslash 68889519053422157468225122572457275927463351471886763 4\backslash 80258121456344553570954156719858951533732416190518514 9\backslash 98228010202018371732421257127137267272335168368 \quad \textbf{(1.4.14)}$$

Man sieht, dass das Rechnen sehr schnell geht, allerdings ist das Knacken ziemlich schwierig.

Ein weiterer Ansatz RSA zu brechen wäre die Berechnung von $\varphi(n)$. Allerdings ist dieser nicht besser als der vorherige wie die nächste Aufgabe zeigt.

ÜBUNG [12]:

Zeige: Die Berechnung von $\varphi(n)$ ist äquivalent zur Bestimmung von p und q.
Hinweis: Bestimme zuerst $p+q$.