Aufgabe 1:

1. $\mathbb{Q}^*$ ist nicht zyklisch: wäre $\mathbb{Q}^*$ zyklisch, so gäbe es ein $g \in \mathbb{Q}^*$ und die beiden Primzahlen 17 und 19 wären Potenzen von g: $g^{n_1} = 17, g^{n_2} = 19$, dann wäre aber g ein gemeinsamer Teiler von der beiden. (g ist $\neq 1$, da 1 kein Erzeuger von $\mathbb{Q}^*$ sein kann.)

2. $(\mathbb{Z}/(35\mathbb{Z}))^*$ ist nicht zyklisch: $\varphi(35) = \varphi(5)\varphi(7) = 4 \cdot 6 = 24$, eine Rechnung mit Pari/GP zeigt, dass alle $x \in (\mathbb{Z}/(35\mathbb{Z}))^*$ die Ordnung 12 haben und deswegen die Gruppe nicht erzeugen können.

3. Es sei

$$M(l) := \begin{bmatrix} \cos(l\pi/6) & -\sin(l\pi/6) \\ \sin(l\pi/6) & \cos(l\pi/6) \end{bmatrix}$$

   Insgesamt hat die Gruppe die Elemente $M(1), M(2), \ldots M(12)$. Denn $M(13) = M(1)$ wegen der Periode 2π von cos und sin: $\cos((l+12)\pi/6) = \cos(l\pi/6 + 2\pi) = \cos(l\pi/6)$ (ebenso für sin).

   Aufgrund der Additionstheoreme von sin und cos gilt $M(x)M(y) = M(x+y)$. Die Additionstheoreme sind :

$$\cos(x \pm y) = \cos(y)\cos(y) \mp \sin(x)\sin(y)$$
$$\sin(x \pm y) = \sin(x)\cos(y) \pm \cos(x)\sin(y)$$

   Wegen der Periodizität ist $M(1)^{13} = M(1)M(1)\ldots M(1) = M(1+12) = M(1)$.

   Die Gruppe ist zyklisch von $M(1)$ erzeugt und hat die Ordnung 12.

Aufgabe 2:

```
ISBN= 3414711517913; temp= factor(ISBN);
/* [1802989  1]
   [1893917  1] */
P = temp[1,1];
Q = temp[2,1];

for(x=0,P, if(Mod(x,P)^2==-1, print(x)));
/*
681159, 1121830
*/

for(x=0,Q, if(Mod(x,Q)^2==-1, print(x)));
/*
735802, 1158115
*/

chinese([Mod(681159,P), Mod(735802,Q)])
chinese([Mod(681159,P), Mod(1158115,Q)])

chinese([Mod(1121830,P), Mod(735802,Q)])
chinese([Mod(1121830,P), Mod(1158115,Q)])

/*
Mod(1054478797809, 3414711517913)
Mod(3446193138, 3414711517913)
Mod(3411265324775, 3414711517913)
Mod(2360232720104, 3414711517913)

ISBN-10: 3446193138
Fermats letzter Satz.
  Die abenteuerliche Geschichte eines  mathematischen Rätsels
  (Gebundene Ausgabe) von Simon Singh (Autor)
*/
```

Theorie: `for(x=1,ISBN-1, ... )` dauert zu lange (viele Stunden).

Anderer Ansatz: $ISBN$ faktorieren $\rightsquigarrow$ $ISBN$ ist das Produkt von 2 Primzahlen: $ISBN = PQ$.

Wenn wir ein $x_1 \pmod P$ und ein $x_2 \pmod Q$ hätten, würden wir mit dem Chinesischen Restsatz ein $x \pmod{ISBN}$ bekommen.

Wie bekommt man ein so ein $x \pmod P$?

Aus der Vorlesung ist der Satz von Euler bekannt: Ist $ggt(y, P) = 1$, dann gilt: $y^{\varphi(P)} \equiv 1 \pmod P$, hier ist $\varphi(P) = P - 1$, also $y^{P-1} \equiv 1 \pmod P$, das heißt aber nichts anderes als $y^{(P-1)/2} \equiv \pm 1 \pmod P$.

Im Fall -1 ist das gesuchte $x := y^{((P-1)/4)}$, dann ist nämlich $x^2 = y^{(P-1)/2}$ was wir als -1 angenommen haben.

So ein y findet durch Probieren:$y = 2, 3, 4, 5, ...$:

```
\\    Für P                                \\    Für Q:
      Mod(2,p)^((p-1)/2)                         Mod(2,q)^((q-1)/2)
      %3 = Mod(1802988, 1802989)                 %19 = Mod(1893916, 1893917)
      x=Mod(2,p)^((p-1)/4)                       Mod(2,q)^((q-1)/4)
      %7 = Mod(1121830, 1802989)                 %20 = Mod(1158115, 1893917)

      Mod(8,p)^((p-1)/2)                         Mod(8,q)^((q-1)/2)
      %15 = Mod(1802988, 1802989)                %28 = Mod(1893916, 1893917)
      Mod(8,p)^((p-1)/4)                         Mod(8,q)^((q-1)/4)
      %16 = Mod(681159, 1802989)                 %29 = Mod(735802, 1893917)

    x11= Mod(681159, 1802989)                  x21=Mod(735802, 1893917)
    x12= Mod(1121830, 1802989)                 x22=Mod(1158115, 1893917)

\\  Das gesuchte x ist in der Menge:
 {  chinese([Mod(681159,P),  Mod(735802,Q)]), chinese([Mod(681159,P),  Mod(1158115,Q)]),
    chinese([Mod(1121830,P), Mod(735802,Q)]), chinese([Mod(1121830,P), Mod(1158115,Q)])
 }
\\  wenn man es als ISBN-Nr interpretiert.
```

Warum findet man so ein y ganz einfach durch Probieren? Wenn man einfach durchprobiert, so ist die Wahrscheinlichkeit ein geeignetes y zu finden $\frac{1}{2}$.

Sei g eine Primitivwurzel modulo P. Dann ist $(\mathbb{Z}/(P\mathbb{Z}))^* = \{g, g^2, g^3, \ldots, g^{P-1}\}$. Wir wenden die Abbildung $x \mapsto x^{(P-1)/2} \pmod P$ an: $g^k \mapsto (g^k)^{(P-1)/2} \equiv \pm 1$, je nachdem, ob k gerade oder ungerade war. Also wird die eine Hälfte auf -1 und die andere Hälfte auf 1 abgebildet.

Aufgabe 3:

```
n=295927; e=1003;
Code=read("/home/lf/ZTUebung/Uebungsblatter/Anhang-Blatt-4.gp");

/*
  Sei x ein Element von Code, also x =Code[i]. x entsteht als c^e mod n, wenn c der i.-te
  Buchstabe der Nachricht ist, bzw. dessen Zahlwert.

  Wie bestimmt man aus x wieder m? Wir wissen, (Euler bzw. Fermat) dass
    c^phi(n) = 1 mod n ist, und damit:
    c^(phi(n) +1 ) = c^(phi(n)) * c = 1 * c = c mod n

  Idee:  c^(phi(n)+1) mittels x= c^e ausdrücken.
```

```
    Suche ein d mit e*d kongruent 1 mod phi(n),d.h. e*d = 1 + q*phi(n),
    dann ist x ^ d = (c^e)^d = (c^phi(n))^q *c =  1^q*c = c mod n.

    Hurra: wir haben gerade RSA geknackt.
    Aber nur, weil n klein war.
    RSA Verschlüsselung geht genau, wie hier. Der geheime Schlüssel ist die Faktorisierung
    von n und die Zahl d. Der öffentliche Schlüssel ist n und e.

    n ist das Produkt von 2 riesigen Primzahlen p,q, so dass eine Faktorisierung praktisch
    unmöglich ist. Und um d zu bestimmen braucht man phi(n) = (p-1)(q-1). (Also die
    Faktorisierung.)

*/

d=bezout(eulerphi(n),e)[2];
\\ 119347
nachricht=vector(#Code, i, lift(Mod(Code[i],n)^d));
print(Strchr(nachricht));
/*
The problem of distinguishing prime numbers from composite numbers and of resolving the
latter into their prime factors is known to be one of the most important and useful in
arithmetic.  It has engaged the industry and wisdom of ancient and modern geometers to
such an extent that it would be superfluous to discuss the problem at length... Further,
the dignity of the science itself seems to require that every possible means be
explored for the solution of a problem so elegant and so celebrated.
(Carl Friedrich Gauss, Disquisitiones Arithmeticae, 1801)
*/
```

Nachtrag RSA: Annahme: Alice möchte Bob eine Nachricht senden.

Vorbereitung:

1. Bob wählt zwei große[1] Primzahlen P und Q.
2. Bob bestimmt $N := P \cdot Q$, sowie $\varphi := (P-1)(Q-1)$.
3. Bob wählt ein zufälliges $e \in (\mathbb{Z}/N\mathbb{Z})^*$ (der Verschlüsselungsexponent)
4. Bob bestimmt (mittels Bezout) eine Zahl d mit $e \cdot d \equiv 1 \pmod{\varphi} \Leftrightarrow ed = q\varphi + 1$ (der Entschlüsselungsexponent).
5. Bob veröffentlich den öffentlichen Schlüssel (N, e) und hält den geheimen Schlüssel d sicher verwahrt.

Verschlüsselung: Alice möchte Bob die Nachricht m senden:

- Alice holt sich den öffentlichen Schlüssel von Bob
- Alice bestimmt $c := m^e \pmod{N}$ und sendet c an Bob.

Entschlüsselung:

- Bob berechnet $c^d = (m^e)^d = m^{(ed)} = m^{(q\varphi+1)} = (m^\varphi)^q m \equiv 1 \cdot m \pmod{N}$

Aufgabe 4: Wir zeigen die Behauptung mittels vollständiger Induktion über n. Dazu prüfen wir zunächst den Induktionsanfang: $n = 1$: Die Behauptung ist für $n = 1$ wahr mit $a_1 := a$, dann ist nämlich $f(a_1) \equiv 0 \pmod{p^1}$ und es ist auch $a_1 \equiv a \pmod{p}$.

Nun für $n = 2$: Wir setzen $a_2 := a + tp$ mit einem $t \in \mathbb{Z}$, also $a_2 \equiv a \pmod{p}$ und wir zeigen dass man t so wählen kann, dass die Bedingungen erfüllt sind.

[1] Die Primzahlen in unserem Beispiel sind winzig.

Die Taylor Entwicklung eines Polynoms f vom Grad N (d.h. $f^{(N+1)} = 0$) um den Punkt a ist:

$$f(x) = \sum_{j=0}^{N} f^{(j)}(a)\frac{(x-a)^j}{j!}$$

für $x = a_2 = a + tp$:

$$\begin{aligned} f(a_2) &= f(a) + f'(a)(a_2 - a) + f''(a)(a_2 - a)^2 + \dots \\ &= f(a) + f'(a)(pt) + f''(a)(pt)^2 + \dots \end{aligned}$$

Das soll $\equiv 0 \pmod{p^2}$ sein:

$$\begin{aligned} 0 &\equiv f(a) + f'(a)(pt) + 0 \pmod{p^2} \\ \Rightarrow -f(a) &\equiv f'(a)(pt) \pmod{p^2} \\ \Rightarrow -f(a)/p &\equiv f'(a)(t) \pmod{p} \end{aligned}$$

$f(a)$ ist ein Vielfaches von p und t bestimmen wir mit dem Satz von Bezout ($xf'(a) + yp = 1$, x ist dann $f'(a)^{-1}$). Damit haben wir unser $a_2 = a + tp = a + (-\frac{f(a)}{p}f'(a)^{-1})p$ bestimmt.

Hierher kommt die Idee zum Induktionsschritt: Es sei a_n wie gefordert. Wir zeigen, dass es ein a_{n+1} mit den gewünschten Eigenschaften gibt: es sei $a_{n+1} := a_n + tp^n$. Wir bestimmen zunächst t, aus der Anforderung, dass $f(a_{n+1)} \equiv 0 \pmod{p^{n+1}}$ sein soll:

$$\begin{aligned} 0 \equiv f(a_{n+1)} &= f(a) + f'(a)(a_{n+1} - a) + f''(a)(a_{n+1} - a)^2 \pmod{p^{n+1}} \\ &\equiv f(a) + f'(a)(tp^n) + f''(a)(tp^n)^2 \pmod{p^{n+1}} \\ -f(a)/p^n &\equiv f'(a)t \pmod{p} \\ -(f(a)/p^n)f'(a)^{-1} &\equiv t \pmod{p} \end{aligned}$$

a_{n+1} hat die gewünschten Eigenschaften.

Aufgabe 5: Wir fassen die Zahl z mit den Zifferen $z_n z_{n-1} \dots z_1 z_0$ auf, als Summe: $(z_0 + 10z_1 + 100z_2) + 1000^1(z_3 + 10z_4 + 100z_5) + \dots$ und berechnen die Kongruenzen modulo 7 der Zehnerpotenzen:

1	10	100	1000	1000^2	1000^n
$1 \pmod 7$	$3 \pmod 7$	$2 \pmod 7$	$-1 \pmod 7$	$(-1 \pmod 7)^2$	$(-1 \pmod 7)^n$

D.h. $z \equiv (z0 + 3z_1 + 2z_2) - (z3 + 3z_4 + 2z_5) + - \dots \pmod 7$ und z ist genau dann durch Sieben teilbar, falls $z \equiv 0 \pmod 7$ oder eben die Summe $\equiv 0 \pmod 7$ also durch 7 teilbar ist.