Aufgabe 1:

$n = 0$: $(\mathbb{Z}/2^0\mathbb{Z})^\times = (\mathbb{Z}/\mathbb{Z})^\times = \{0\}^\times = \{0\}$, erzeugt von 0 ($ggt(0, 2^0 = 1) = 1$)

$n = 1$: $(\mathbb{Z}/2^1\mathbb{Z})^\times = \{0, 1\}^\times = \{1\}$, erzeugt von 1

$n = 2$: $(\mathbb{Z}/2^2\mathbb{Z})^\times = \{0, 1, 2, 3\}^\times = \{1, 3\}$, erzeugt von 3

$n = 3$: Es sei $a \in (\mathbb{Z}/8\mathbb{Z})^\times, a \in \{1, 3, 5, 7\}$, dann ist $a^2 \in \{1, 9, 25, 49\}$. Immer ist $a^2 \equiv 1 \pmod 8$. Daraus folgt: $(\mathbb{Z}/8\mathbb{Z})^\times$ ist nicht zyklisch, da es kein Element mit Ordnung 4 gibt.

$n \geq 3$: Sei $a \in (\mathbb{Z}/2^n\mathbb{Z})^\times$, also insbesondere ist a ungerade. Wir zeigen dann gilt: $a^{2^{n-2}} \equiv 1 \pmod{2^n}$.

Vollständige Induktion über n: Induktionsanfang $n = 3$: a ist ungerade: $a = 2k + 1$, $a^2 - 1 = 4k^2 + 4k + 1 - 1 = 4(k^2 + k)$. k ist gerade oder ungerade, aber es ist immer $k^2 + k$ gerade. Damit folgt: $8|(a^2 - 1) \Rightarrow a^2 \equiv 1 \pmod 8$, also $(\mathbb{Z}/8\mathbb{Z})^\times$ ist nicht zyklisch, da es kein Element mit Ordnung 4 gibt.

Induktionsschritt $n \Rightarrow (n + 1)$: Es sei $a^{2^{n-2}} \equiv 1 \pmod{2^n} \Rightarrow 2^n|(a^{2^{n-2}} - 1)$ aber auch $2|(a^{2^{n-2}} + 1)$. Es folgt:

$$\begin{aligned} 2^{n+1}|(a^{2^{n-2}} - 1)(a^{2^{n-2}} + 1) = (a^{2^{n-2}})^2 - 1 = a^{2^{n-1}} - 1 \\ \Rightarrow 2^{n+1}|(a^{2^{n-1}} - 1) \end{aligned}$$

Also $a^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$, womit jedes Element in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ eine Ordnung hat, die kleiner als 2^{n-1} ist. Es gibt keinen Erzeuger, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ ist nicht zyklisch.

Alternative für $n > 3$: Die Abbildung $f : (\mathbb{Z}/2^n\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$ mit $a \pmod{2^n} \mapsto a \pmod 8$ ist ein Gruppenhomomorphismus. Damit enthält die Gruppe $(\mathbb{Z}/2^n\mathbb{Z})^\times$ eine nicht-zyklische Untergruppe (nämlich $(\mathbb{Z}/8\mathbb{Z})^\times$, nicht zyklisch, wie oben gezeigt). Dann kann $(\mathbb{Z}/2^n\mathbb{Z})^\times$ nicht zyklisch sein.

Noch zu zeigen: f ist ein Homomorphismus: Sei dazu $a = r_a + q_a 2^n$ und $b = r_b q_b 2^n$ mit $0 \leq r_a, r_b < 2^n$. Es ist zu zeigen, dass $f(ab) = f(a)f(b)$ gilt:

$$\begin{aligned} ab &= r_a r_b + (r_a q_b + r_b q_a + q_a q_b 2^n)2^n \equiv r_a r_b \pmod{2^n} \\ f(ab) &\equiv r_a r_b \pmod 8 \\ &= (r_a)(r_b) \pmod 8 = f(a)f(b) \end{aligned}$$

Die Abbildung f respektiert also die Multiplikation.

Angenommen es gebe eine Primitivwurzel g von $(\mathbb{Z}/2^n\mathbb{Z})^\times$: dann wäre $f(g^n) = f(g)^n$ und $w := f(g)$ wäre eine Primitivwurzel von $(\mathbb{Z}/8\mathbb{Z})^\times$. Widerspruch!

Aufgabe 2:

$n = 1$: $a = 1 : 1 \equiv 5^1 \equiv 1 \pmod 2$

$n = 2$: $a = 1 : 1 \equiv (5)^1 \equiv 1 \pmod 4$
$a = 3 : 3 \equiv (-5)^1 \equiv -1 \equiv 3 \pmod 4$

$n \geq 3$: Wir berechnen zuerst die Ordnung von $5 \pmod{2^n}$. Es ist $\varphi(\mathbb{Z}/2^n\mathbb{Z}) = 2^{n-1}$. Als Ordnung von 5 kommen nur Zweier-Potenzen $2^{n'}$, $n' \leq n - 1$ in Frage. (Elementordnung teilt Gruppenordnung.)

1. Die Ordnung von 5 ist größer als 2^{n-3}: Wir zeigen, dass $5^{2^j} \not\equiv 1 \pmod{2^n}$ ist, für $j = 0, n-3$. Induktion über $n \geq 3$: für den Induktionsanfang $n = 3$ ist alles klar: $5^{2^0} = 5 \not\equiv 1 \pmod 8$.

   Induktionsschritt ($n \Rightarrow n+1$): es sei $5^{2^{n-3}} = 1 + a2^l$ mit a ungerade ($a \not\equiv 0 \pmod 2$) und $1 \leq l < n$ ($5^{2^{n-3}}$ ist eine ungerade Zahl, also (1+ gerade Zahl) aber nach Induktionsvoraussetzung nicht 1 + Vielfaches von 2^n). Wir zeigen nun, dass dann auch $5^{2^{n+1-3}} \not\equiv 1 \pmod{2^{n+1}}$ ist:

$$\begin{aligned} 5^{2^{n-2}} &= (5^{2^{n-3}})^2 = (1 + a2^l)^2 = 1 + a2^{l+1} + a^2 2^{2l} \\ &= 1 + (a + a^2 2^{l-1})2^{l+1} \not\equiv 1 \pmod{2^{n+1}} \end{aligned}$$

   Die letzte Inkongruenz, weil $(a + a^2 2^{l-1})$ ungerade ist und $l + 1 < n + 1$.

   Damit ist auch $5^{2^j} \not\equiv 1 \pmod{2^n}$ für $j = 0, \ldots, n-3$, denn sonst wäre mit $5^{2^j} \equiv 1 \pmod{2^n}$ auch $5^{2^j} 5^{2^j} = 5^{2^{j+1}} \equiv 1 \pmod{2^n}$ und es würde folgen $5^{2^{n-3}} \equiv 1 \pmod{2^n}$.

2. Die Ordnung von 5 ist 2^{n-2}: Wir zeigen nun per Induktion, dass $2^n || (5^{2^{n-2}} - 1)$ ist: Induktionsanfang: $n = 3 : 5^{2^{3-2}} - 1 = 5^2 - 1 = 24 = 3 \cdot 2^3$.

   Induktionsschritt: Es gelte $2^n || (5^{2^{n-2}} - 1)$ also ist $(5^{2^{n-2}} - 1) = a \cdot 2^n$ mit einem ungerade a. Dann ist aber $(5^{2^{n-2}} + 1) = a2^n + 2$. Daraus folgt:

$$\begin{aligned} ((5^{2^{n-2}})^2 - 1) &= (5^{2^{n-2}} + 1)(5^{2^{n-2}} - 1) = (a \cdot 2^n)(2^n \cdot a + 2) \\ &= a^2 2^{2n} + a2^{n+1} \end{aligned}$$

   Insgesamt : $2^{n+1} || ((5^{2^{n-2}})^2 - 1)$ oder $(5^{2^{n-2}})^2 = 5^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$

Die beiden Induktionen zeigen, dass 2^{n-2} die Ordnung von 5 $\pmod{2^n}$ ist. Damit sind die 2^{n-2} Zahlen in $M := \left\{5, 5^2, \ldots, 5^{2^{n-3}}, 5^{2^{n-2}}\right\}$ inkongruent modulo 2^n.

Die 2^{n-2} ungeraden $a \in \mathbb{Z}/2^n\mathbb{Z}$ sind entweder $\equiv 1 \pmod 4$ oder $\equiv -1 \pmod 4$ (jeweils genau 2^{n-2} Stück). Da aber $5 \equiv 1 \pmod 4$ ist, sind die Zahlen in M allesamt $\equiv 1 \pmod 4$.

Für jedes $a \equiv 1 \pmod 4$ gibt es ein x mit $a \equiv 5^x \pmod{2^n}$ (einfach weil M 2^{n-2} verschiedene Elemente hat).

Die 2^{n-2} Elemente in der Menge $\tilde{M} := \left\{-5, -(5)^2, \ldots, -(5)^{2^{n-2}}\right\}$ sind alle $\equiv -1 \pmod 4$ und ebenfalls verschieden modulo 2^n. D.h. für jedes $a \equiv -1 \pmod 4$ gibt es ein x mit $a \equiv 5^x \pmod{2^n}$ (einfach, weil es 2^{n-2} verschiedene Elemente in $\tilde{M}$ gibt).

Aufgabe 3:

```
my_ord(a,m)=
{
    local(o=1, Order=eulerphi(m));

    fordiv(Order,d,
        if(Mod(a,m)^d == 1,
            return(d);
        );
    );

    error("Keine Ordnung gefunden");
}

{
   m=720;

    for(a=1,m,
```

```
        if(gcd(a,m)==1,
            o= my_ord(a,m);
            print(Mod(a,m),": ", o);

            if(o!= znorder(Mod(a,m)), error("Fehler bei "a));
        );
    );
}
```

Aufgabe 4:

```
\\ wie im Skript
p=3058329193;

\\ print(isprime(p));
\\ print(p%4);


{
  x=2;
  while(Mod(-1,p) != Mod(x,p)^((p-1)/2), x++);

  x=lift(Mod(x,p)^((p-1)/4));
  if(x<p/2, x=p-x);

  a=p; b=x;
  while( b > sqrt(p),
    r=a%b;
    a=b;
    b=r;
  );

  v=vecsort([b, sqrtint(p- b*b)]);
  print(v);
  print(v[1]^2+v[2]^2);
/*[16992, 52627]
  3058329193    */
}
```

Aufgabe 5: Eine Abbildung $f : \mathbb{Z}/pZ \to \mathbb{Z}/p\mathbb{Z}$ ordnet jedem Punkt $a_i \in \mathbb{Z}/pZ$ eindeutig einen Punkt $b_i \in \mathbb{Z}/pZ$ zu (f ist Abbildung). Wir haben also eine Menge von Tupeln

$$M = \{(a_1, b_1), \dots (a_p, b_p)\}\,, \quad b_j = f(a_j)$$

Daraus bilden wir das Lagrange-Interpolations-Polynom:

$$g(x) := \sum_{i=1}^{p} f(a_i) l_i(x) \quad \text{mit}$$
$$l_i(x) := \prod_{j=1, j\neq i}^{p} (x - a_j)(a_i - a_j)^{-1}$$

Dabei wird $(a_i - a_j)^{-1}$ als Element von $(\mathbb{Z}/p\mathbb{Z})^{\times}$ betrachtet ($j \neq i$ und alle a_i verschieden, deshalb $\neq 0$) und wieder nach $\mathbb{Z}$ „gelifted“. Dann ist $l_i(x)$ ein Produkt von ganzen Zahlen und $g(x)$ ist eine Summe von ganzen Zahlen. Also hat $g(x)$ ganzzahlige Koeffizienten und Grad $< p$.

Es gilt $g(a_j) = \sum_{i=1}^{n} f(a_j) \cdot 0 + f(a_j) \cdot 1 = b_j$ $(j = 1, \dots, n)$.

Lösung des ersten Rechentestes:

```
print("Aufgabe 1");
p=19;

print("3:");
for(j=1,eulerphi(p),print("   ",j,":\t", Mod(3,p)^j, "\t", -Mod(3,p)^j));
/*
1:      Mod(3, 19)      Mod(16, 19)
2:      Mod(9, 19)      Mod(10, 19)
3:      Mod(8, 19)      Mod(11, 19)
4:      Mod(5, 19)      Mod(14, 19)
5:      Mod(15, 19)     Mod(4, 19)
6:      Mod(7, 19)      Mod(12, 19)
7:      Mod(2, 19)      Mod(17, 19)
8:      Mod(6, 19)      Mod(13, 19)
9:      Mod(18, 19)     Mod(1, 19)
10:     Mod(16, 19)     Mod(3, 19)
11:     Mod(10, 19)     Mod(9, 19)
12:     Mod(11, 19)     Mod(8, 19)
13:     Mod(14, 19)     Mod(5, 19)
14:     Mod(4, 19)      Mod(15, 19)
15:     Mod(12, 19)     Mod(7, 19)
16:     Mod(17, 19)     Mod(2, 19)
17:     Mod(13, 19)     Mod(6, 19)
18:     Mod(1, 19)      Mod(18, 19)


Geschickterweise berechnet man nur 3, 3^2, 3^3, 3^6 und 3^9.
(Als Elementordnung, kommen nur Teiler der Gruppenordnung in Frage.)

3^6 = 3^3 * 3^3  und 3^9 = 3^6*3^3, jeweils Reduzieren modulo 19
nicht vergessen. Man findet heraus: 3^9 = -1 mod 19
=> 3 ist Primitivwurzel.
*/

print("4:");
for(j=1,eulerphi(p),print("   ",j,":\t", Mod(4,p)^j, "\t", -Mod(4,p)^j));
/*
  1:    Mod(4, 19)      Mod(15, 19)
  2:    Mod(16, 19)     Mod(3, 19)
  3:    Mod(7, 19)      Mod(12, 19)
  4:    Mod(9, 19)      Mod(10, 19)
  5:    Mod(17, 19)     Mod(2, 19)
  6:    Mod(11, 19)     Mod(8, 19)
  7:    Mod(6, 19)      Mod(13, 19)
  8:    Mod(5, 19)      Mod(14, 19)
  9:    Mod(1, 19)      Mod(18, 19)
  10:   Mod(4, 19)      Mod(15, 19)
  11:   Mod(16, 19)     Mod(3, 19)
  12:   Mod(7, 19)      Mod(12, 19)
  13:   Mod(9, 19)      Mod(10, 19)
  14:   Mod(17, 19)     Mod(2, 19)
  15:   Mod(11, 19)     Mod(8, 19)
  16:   Mod(6, 19)      Mod(13, 19)
  17:   Mod(5, 19)      Mod(14, 19)
  18:   Mod(1, 19)      Mod(18, 19)

Wieder geschickt rechnen: 4, 4^4, 4^3, 4^6, 4^9 mit
4^6=4^3*4^3, 4^9=4^6 * 4^3. Man findet 4^9 = 1 mod 19
=> 4 ist keine Primitivwurzel.
*/
print("Aufgage2:");
```

```
print("   Lösung: ",chinese([Mod(3,5),Mod(2,11),Mod(1,13)]));
print("  M=",M=5*11*13);
print("    M_i\t\tM_i%m_i  \t  b_i=(M_i)^-1");
print("    ",M1=11*13, "\t\t", M1% 5, "\t\t  ",b1=Mod(M1, 5)^-1);
print("    ",M2= 5*13, "\t\t", M2%11, "\t\t  ",b2=Mod(M2,11)^-1);
print("    ",M3= 5*11, "\t\t", M3%13, "\t\t  ",b3=Mod(M3,13)^-1);
print();
print("    ",T1=3*M1*lift(b1));
print("   ",T2=2*M2*lift(b2));
print("    ",T3=1*M3*lift(b3));
print("   ",S=T1+T2+T3, "\t= ",Mod(S,M));

/*
Aufgage2:
   Lösung: Mod(508, 715)
  M=715
    M_i           M_i%m_i           b_i=(M_i)^-1
    143           3                 Mod(2, 5)
    65            10                Mod(10, 11)
    55            3                 Mod(9, 13)

    858
   1300
    495
   2653  = Mod(508, 715)

*/

print("Aufgabe 3");

ISBN=[0,3,8,7,x,6,3,7,5,8];

Summe = ISBN*vector(10,i,11-i)~;
print(Summe);
/*
    6*x + 221
*/

print(Mod(-221/6,11));
/*
   Mod(9, 11)
*/

print("   -------------");
Summe = ISBN*vector(10,i,i)~;
print(Summe);
print(Mod(-221/6,11));
print(-Mod(6,11), " ",-Mod(221,11));
print(Mod(5,11), " ",Mod(296,11));

/*
   5*x + 296
   Mod(9, 11)
   Mod(5, 11) Mod(10, 11)
   Mod(5, 11) Mod(10, 11)

  Auf die andere Weise kommt das (-1)-fache heraus:
    Sei S := 221. dann ist oben: 6x +S =0,
    hier ist -6x -S = 0 (-6 mod 11 ist 5)
    beide Male ist x = -S * 6^(-1).
```

```
  Vor allem bleibt die Prüfzffer z_10 gleich:
  \sum_{i=1}^{9} z_i (11-i) + 1*z_10 = 0
  z_10 = - \sum_{i=1}^{9} z_i (11-i) =  \sum_{i=1}^{9} z_i (i), (11-i = -i mod 11)
  und
  \sum_{i=1}^{9} z_i (i) + 10*z_10 = 0, (10 = -1 mod 11), also
  \sum_{i=1}^{9} z_i (i) + -1*z_10 = 0, und wieder ist
  z_10 = \sum_{i=1}^{9} z_i (i)
*/
```