Aufgabe 1: (Siehe `http://hometown.aol.com/jpr2718/ax2p.pdf` für eine ausführliche und systematische Darstellung.)

Hier wird nur ein Beispiel besprochen:

$$\begin{aligned} 0 =& 3 * x^2 + 5 * x * y - 7 * y^2 + x + 2 * y - 8 \\ 0 =& ax^2 + bxy + cy^2 + dx + ey + f \end{aligned} \tag{1}$$

1. b zu 0 machen: B bzw. C werden der Zähler bzw. Nenner von $2 * a/b$, hier also $B = 2 * 3 = 6$ und $C = 5$.

   Mit der Transformation $X = Bx + Cy$, $Y = y$, bzw.

   $$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} 1/B & -C/B \\ 0 & 1 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{bmatrix} 1/6 & -5/6 \\ 0 & 1 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

   wird aus Gleichung (1) die Gleichung

   $$\begin{aligned} 0 =& 1/12 * x^2 - 109/12 * y^2 + 1/6 * x + 7/6 * y - 8, \\ 0 =& ax^2 + cy^2 + dx + ey + f \end{aligned} \tag{2}$$

   eine Gleichung, bei der der Koeefizient von xy Null ist.

2. d zu 0 machen: Unsere Gleichung (2) hat bereits keinen Term mit xy, nun wird der Term mit dem einzelnen x eliminiert:

   B bzw. C werden der Zähler bzw. Nenner von $2 * a/d$, hier also $B = 2 * 6 = 12$ und $C = 12$, wir kürzen aber noch: $B = 1$ und $C = 1$.

   Mit der Transformation $X = Bx + C$, $Y = y$ bzw.:

   $$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} 1/B & 0 \\ 0 & 1 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} -C/B \\ 0 \end{pmatrix} = \begin{bmatrix} 1/1 & 0 \\ 0 & 1 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} -1/1 \\ 0 \end{pmatrix}$$

   wird unsere Gleichung (2) zu:

   $$\begin{aligned} 0 =& 1/12 * x^2 + -109/12 * y^2 + 7/6 * y - 97/12 \\ 0 =& ax^2 + cy^2 + ey + f = 0 \end{aligned} \tag{3}$$

3. e zu 0 machen: den Koeffizienten von y in (3) zu eliminieren geht genauso, bloß die Rollen von X und Y sind vertauscht:

   B bzw. C werden der Zähler bzw. Nenner von $2 * c/e$, hier also $B = 2 * (-109) * 6 = -12 * 109$ und $C = 12 * 7$, wir kürzen aber noch: $B = -109$ und $C = 7$.

   Mit der Transformation $Y = By + C$, $X = y$ bzw.:

   $$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1/B \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} 0 \\ -C/B \end{pmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1/-109 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} 0 \\ -7/(-109) \end{pmatrix}$$

wird unsere Gleichung (3) zu:

$$\begin{aligned} 0 =& 1/12 * x^2 + -1/1308 * y^2 - 877/109 \\ 0 =& ax^2 + cy^2 + +f \end{aligned} \tag{4}$$

```
f(x,y)=3*x^2+5*x*y-7*y^2+x+2*y-8;
print(f(x,y));
g(x,y)=f(1/6*x+-5/6*y,y);
print(g(x,y));
h(x,y)=g(x-1,y);
print(h(x,y));
k(x,y)=h(x,y/(-109)+7/109);
print(k(x,y))
/*
  3*x^2 + (5*y + 1)*x + (-7*y^2 + 2*y - 8)
  1/12*x^2 + 1/6*x + (-109/12*y^2 + 7/6*y - 8)
  1/12*x^2 + (-109/12*y^2 + 7/6*y - 97/12)
  1/12*x^2 + (-1/1308*y^2 - 877/109)
*/
```

Aufgabe 4: Finden Sie eine Formel für die Anzahl der Punkte der projektiven Geraden über $\mathbb{Z}/m\mathbb{Z}$.

Wir betrachten das Problem zuerst für $\mathbb{Z}/p\mathbb{Z}$ mit einer Primzahl p. Die projektive Grade über $\mathbb{P}_1(\mathbb{Z}/p\mathbb{Z})$ ist eine Teilmenge von $(\mathbb{Z}/p\mathbb{Z})^2$ und besteht aus allen Geraden durch den Punkt $(0,0)$. Davon gibt es eine von $(0,0)$ durch $(1,0)$ und p Stück von $(0,0)$ durch die Punkte $(x,1)$ mit $x \in \mathbb{Z}/p\mathbb{Z}$. Das sind also die $p+1$ projektiven Punkte $[1:0]$, $[0:1], \ldots, [p-1:1]$.

Für die projektive Gerade $\mathbb{P}_1(\mathbb{Z}/p^n\mathbb{Z})$ mit eine Primzahlpotenz haben wir zu ermitteln, die Anzahl der Geraden von $(0,0)$ durch Punkte $(x,y) \in (\mathbb{Z}/p^n\mathbb{Z})^2$ für die gilt: $\mathrm{ggT}(x,y,p) = 1$, also eine der beiden Koordinaten ist invertierbar. D.h. sie liegen auf einer der projektiven Geraden $[\cdot:1]$ oder $[1:\cdot]$.

$$\begin{aligned} &\#\left(\left\{(x,y) \in (\mathbb{Z}/(p^n\mathbb{Z}))^2 \middle| \mathrm{ggT}(x,y,p) = 1\right\} / (\mathbb{Z}/p^n\mathbb{Z})^*\right) \\ &= (p^n p^n - p^{n-1}p^{n-1})/(p^n - p^{n-1}) \\ &= p^n + p^{n-1} \end{aligned}$$

$[1:y]$ mit $y \in \mathbb{Z}/(p^n\mathbb{Z})$ und $[x:1]$ mit $x \in \mathbb{Z}/(p^n\mathbb{Z}) \setminus (\mathbb{Z}/(p^n\mathbb{Z}))^*$

Aufgabe 3:

```
BlowUp(L11,L12,m1, L21,L22, m2)=
{
/*
    Vgl Thrm 5.13 in Niven Zuckerman
    f=ax^2+by^2+cz^2
      kong mod m1 zu (L11*[x,y,z])*(L12[x,y,z])
      kong mod m2 zu (L21*[x,y,z])*(L22[x,y,z])

    gibt zurück [a1,b1,c1], [a2,b2,c2] mit
    f kong ([a1,b1,c1]*[x,y,z])*([a2,b2,c2]*[x,y,z])
      mod m1*m2
*/
    local(a1,b1,c1, a2,b2,c2);

    L11=lift(L11); L12=lift(L12);
    L21=lift(L21); L22=lift(L22);

    \\print(L11, " ", m1);
    a1= chinese(Mod(L11[1],m1), Mod(L21[1],m2));
    b1= chinese(Mod(L11[2],m1), Mod(L21[2],m2));
    c1= chinese(Mod(L11[3],m1), Mod(L21[3],m2));

    a2= chinese(Mod(L12[1],m1), Mod(L22[1],m2));
    b2= chinese(Mod(L12[2],m1), Mod(L22[2],m2));
    c2= chinese(Mod(L12[3],m1), Mod(L22[3],m2));

    return([[a1,b1,c1], [a2,b2,c2]]);
}


solveEQ(a,b,c)=
{
\\  Vgl Beweis zu Thrm 5.11 in Niven Zuckerman
    local(T1, T2, t1, t2, t3,
          aInvers, bInvers,cInvers,
          Alpha, Beta, Gamma,
          lx, ly, lz,  x2, y2, z2
          );

    c= -c;
    \\ c z^2 rüberbringen und die Notation
    \\ des Satzes aus der Vorlesung herstellen:
    \\ ax^2+by^2+cz^2=0 \\ mit PLUS und c auf der LINKEN Seite

    if((gcd(a,b)>1) ||
       (gcd(b,c)>1) ||
       (gcd(c,a)>1),
       error("a,b,c nicht paarweise teilerfremd");
    );

    if( !( issquarefree(a) &&
           issquarefree(b) &&
           issquarefree(c)   ),
      error("a,b,c nicht quadratfrei");
    );

    if( !(  (a > 0) &&
            (b > 0) &&
            (c < 0)    ), \\ c ist jetzt negativ
                          \\ c nach aufgabenstellung
                          \\ jedoch positiv
```

```
        \\ eigentlich : nicht alle a,b,c das gleich Vorzeichen
        return(["a,b,c nicht alle >0 ",[0,0]]);
    );

    /* Wenn Lsg existiert, dann existieren diese Wurzeln: */
    \\ wenn diese Wurzeln nicht gibt Pari eine Fehlermeldung:
    trap( ,
        return([0,0]); \\ [0,0] zurückgeben, falls eine der folgenden
                       \\ Wurzeln nicht existiert:
    ,
        t1= sqrt(Mod(-b*c, a));
        t2= sqrt(Mod(-a*c, b));
        t3= sqrt(Mod(-a*b, c));
    );

    aInversC= Mod(a,c)^-1;
    aInversB= Mod(a,b)^-1;
    bInversA= Mod(b,a)^-1;

    /* siehe Niven Zuckerman: pg. 242 ff
    F=ax^2+by^2+cz^2 wird faktoriesiert mod c:
      ax^2+by^2=(1*x - a^(-1)*t3 * y)(a*x + t3*y) mod c
      und mod b und mod a:
    */


    Lc1 = [ 1, -t3*aInversC, 0 ];
    Lc2 = [ a,  t3         , 0 ];

    Lb1 = [ 1, 0, -t2*aInversB ];
    Lb2 = [ a, 0,  t2 ];

    La1 = [ 0, 1, -t1*bInversA ];
    La2 = [ 0, b,  t1 ];

    \\ d.h mod X ist ax^2+by^2+cz^2 kongruent zu
    \\      (LX1*[x,y,z]) * (LX2*[x,y,z]), X \in[a,b,c]
    \\ und L??*[x,y,z])  ist ein Linearfaktor (siehe Beweis von Satz von Legendre
    \\ oder pg. 243 unten)

    \\ die Linearfaktoren mod a und b zu Linearfaktoren mod a*b aufblasen
    T1 = BlowUp(La1,La2, a, Lb1, Lb2, b);
    \\ die Linearfaktoren mod a*b und c zu Linearfaktoren mod a*b*c aufblasen
    T2 = BlowUp(T1[1],T1[2], a*b, Lc1, Lc2, c);

    Alpha= lift(T2[1][1]);
    Beta = lift(T2[1][2]);
    Gamma= lift(T2[1][3]);
    \\ es ist (Alpha*x + Beta*y +Gamma*z) ein Linearfaktor von ax^2+by^2+cz^2 mod abc

\\ ------------------------------------------------------------------------
\\ Der ganze Hokus Pokus bis hierhin, hat den Sinn und Zweck die nächsten drei
\\ for schleifen nur zwischen z.B. 1 und sqrt(ab) statt jeweils 1 und abc laufen zu lassen
\\ (vgl. Thrm 5.12 in Niven Zuckerman)

    for(x1=1,ceil(sqrt(abs(b*c))),
        for(y1=1,ceil(sqrt(abs(a*c))),
            for(z1=1,ceil(sqrt(abs(b*b))),
                \\ Nullstelle des Linearfaktors ist eine Nullstelle des Polynoms
                if(Mod(x1*Alpha + y1*Beta+ z1*Gamma, a*b*c) == 0 ,
                    \\ die Lösung merken, nach dem break sind die Schleifenvariablen weg
                    lx = x1; ly = y1; lz = z1;
```

```
                        \\print("LSG: ",x1, " ", y1, " ", z1);
125                     break(3);
                    );
                );
            );
        );

        s=a*lx^2+b*ly^2+c*lz^2;
        print(s, ": ", [lx,ly,lz]);
        if( s == 0,  \\ kann auch == abc sein
    \\          print("Fall1");
            return([lx,ly,lz]);
        ,\\ else:
            x2= -b*ly + lx*lz;
            y2= a*lx + ly*lz;
            z2= lz^2 + a*b;
            if((x2==0) && (y2==0) && (z2==0 ),
    \\              print("Fall2");
                return([1,-1,0]);
            );
    \\          print("Fall3");
            return([ x2, y2, z2 ]);
        );
    }


a=5; b=7; c=17;

M=solveEQ(a,b,c);

print(M);
print(M[1]^2*a + M[2]^2*b - M[3]^2*c);
print(38^2*5+46^2*(7)-17*36^2)
```