Aufgabe 1: Es bezeichnen $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{C}^2$ die durch folgende Gleichungen beschriebenen affinen Kurven:

$$\mathcal{C}_1 : x^2 + y^2 - 1 = 0, \qquad \mathcal{C}_2 : x^2 + y^2 - 5x = 0.$$

Berechnen Sie den Durchschnitt $\overline{\mathcal{C}}_1 \cap \overline{\mathcal{C}}_2$ ihrer projektiven Abschlüsse.

Der Durchschnitt der projektiven Abschlüssen ist gegeben durch:

$$x^2 + y^2 - z^2 = x^2 + y^2 - 5xz \tag{1}$$

Die beiden Kurven haben Grad 2, deswegen gibt es 4 Punkte im Durchschnitt: $[0:0:0]$ sieht man sofort. Im Fall $z = 0$, haben wir mit $[1 : \pm i : 0]$ zwei weitere Punkte.

Sei nun $z \neq 0$, aus (**??**) folgt die Gleichung $5xz = z^2 \Leftrightarrow 5x = z$, also $x^2 + y^2 = 25x^2 \Leftrightarrow y^2 = 24x^2 \Leftrightarrow y = x2\sqrt{6}, z = 5x$ und $[x : x2\sqrt{6} : 5x] = [\frac{1}{5} : \frac{2}{5}\sqrt{6} : 1]$ ist die vierte Lösung.

Aufgabe 2: Es bezeichne $E \subset \overline{\mathbb{F}}_{17}^2$ die Kurve $E : y^2 = x(x^2 - 1)$. Bestimmen Sie die Ordnung des Punktes $P_1 = (5, 1) \in E$.

Ein kleines Pari-Skript bestimmt schnell die projektiven Punkte $[x : y : z]$, die $y^2z = x^3 - xz^2$ erfüllen:

```
\\ Aufgabe2_EnumPoints.gp

enumPoints(p=17)=
{
    print(" [ 0 : 1 : 0 ]");

    for(x=0,p-1,
        for(y=0,p-1,
            if(Mod(y^2,p)==Mod(x^3-x,p),
                print(" [ ",x," : ",y, " : 1 ] ");
            );
        );
    );
}

enumPoints();

/*
 [  0 :  1 : 0 ]   [  0 : 0 : 1 ]  [  1 :  0 : 1 ]   [ 4 : 3 : 1 ]
 [  4 : 14 : 1 ]   [  5 : 1 : 1 ]  [  5 : 16 : 1 ]   [ 7 : 8 : 1 ]
 [  7 :  9 : 1 ]   [ 10 : 2 : 1 ]  [ 10 : 15 : 1 ]  [ 12 : 4 : 1 ]
 [ 12 : 13 : 1 ]   [ 13 : 5 : 1 ]  [ 13 : 12 : 1 ]  [ 16 : 0 : 1 ]
*/
```

Es gibt 16 Punkte, das ist eine abelsche Gruppe mit 16 Elementen mit der Addition auf der elliptischen Kurve. Es kommt als Ordnung des Punktes P_1 nur ein Teiler von 16, also 2,4,8,16 in Frage.

Für die Addition benutzen wir die Formeln, die in dem Formularium angegeben sind. Eine Rechnung mit Pari/GP zeigt dann, dass P_1 Ordnung 4 hat.

```
\\ Aufgabe2_AddPoints.gp

ECAddition(P, Q, p, q, Modulus)=
/* - P, Q, tupel mit den XYZ-Koordinaten der Punkte
   - gibt das Tupel [XR, YR, 1] mit den Koordinaten des Punktes R = P + Q
     zurück oder [0,1,0] im Fall P + Q = unendlich
   - p,q sind die Koeffizenten der EC: y^2 = x^3 +px +q
   - Modulus ist der Modulus

( Allgemein formuliert, um diese Funktion auch bei Aufgabe 4 zu verwenden. )
*/
```

```
{
    local(s, XR, YR,
       XP=P[1], XQ=Q[1],
       YP=P[2], YQ=Q[2]
    );

    if(Modulus>0,
       XP=Mod(P[1], Modulus);
       XQ=Mod(Q[1], Modulus);
       YP=Mod(P[2], Modulus);
       YQ=Mod(Q[2], Modulus);
    );

    \\ falls Punkte bei Unendlich addiert werden: [0,1,0]
    \\ ist das neutrale Element der Addition, also
    \\ ohne Nachdenken den anderen Punkt zurückgeben:
    if((P[3] == 0), \\ alle nicht unendl. Punkte haben P[3] != 0
       return(Q);
    );
    if((Q[3] == 0),
       return(P);
    );

    \\ ab hier sind P und Q Punkte mit P[3] ==1 && Q[3] ==1
    \\ Berechnung genau, wie im Formularium beschrieben:
    if(XP != XQ,
        s = (YP - YQ)/(XP - XQ);
        XR = s^2 - XP - XQ;
        YR = (YP + s*( XR - XP ));
    );

    \\ else:
    if(XP==XQ,
        if( YP == - YQ, return([0,1, 0]) ); \\ der Punkt bei Unendlich

        if((YP ==  YQ) && YP == 0 , return([0,1, 0]) ); \\ der Punkt bei Unendlich

        \\ weil die Kurve sym. ist, bleibt noch der Fall: gleiche x und
        \\ y-Koordinaten, aber y!=0:

        s = (3*(XP)^2 + p)/(2*YP);
        XR = s^2-2* XP;
        YR = (YP + s*( XR-XP));
     );

    return([lift(XR), lift(-YR), 1]);
}

P1MalEins= [5,1,1];

P1MalZwei = ECAddition(P1MalEins, P1MalEins, -1, 0, 17); \\ == [16,0,1]
P1MalVier = ECAddition(P1MalZwei, P1MalZwei, -1, 0, 17); \\ == [0,1,0],
                                                          \\    also Ordnung 4
/*
  print(P1MalEins);
  print(P1MalZwei);
  print(P1MalVier);
*/
```

Aufgabe 3: Sind 7 und 23 Kongruenzzahlen?

Ein Zahl $n \in \mathbb{N}$ heißt Kongruenzzahl, falls n der Flächeninhalt eines rechtwinkligen Dreiecks mit den

rationalen Seiten a, b, c ist. Es bestehen also die Gleichungen:

$$c^2 = a^2 + b^2, \text{ und } n = \frac{ab}{2}$$

Man kann einen Satz zeigen: n ist eine Kongruenzzahl, genau dann wenn es ein $u \in \mathbb{Q}$ gibt, so dass $u^2 - n$ und $u^2 + n$ rationale Quadratzahlen sind.

Die Verbindung zu den elliptischen Kurven geht nun so: wir haben 3 rationale Quadrate: $u^2, u^2 - n$ und $u^2 + n$, also ist $(u^2 - n)(u^2 + n) = u^4 - n^2 =: v^2$ ebenfalls ein Quadrat.

$$u^2v^2 = u^6 - n^2u^2 \rightsquigarrow u^2v^2 = u^6 - n^2u^2$$
$$y^2 = x^3 - n^2x$$

(Die letzte Zeile legt nahe: $1 = \frac{(x^2-n^2)}{y}\frac{x}{y} = ab'$ aber es muss sein $ab = 2n$, wähle deswegen zu einer Lösung (x, y) der elliptischen Kurve die Seitenlängen $a = \frac{(x^2-n^2)}{y}$, $b = \frac{2nx}{y}$ und $c = \frac{(x^2+n^2)}{y}$.)

Ein Rechnung mit Pari/GP zeigt nun, dass 7 und 23 Kongruenzzahlen sind und es werden aus einem Punkt der Kurve (via `ellgenerators()`) die Dreiecksseiten berechnet:

```
/*
   benötigt pari version 2.3 und höher,
   sowie das elldata Packet, für ellgenerators()
*/

isNCongruent(N=7)=
{
    local(E, GENS, x,y, a,b);

    \\ Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6
    E=ellinit([0,0,0,-N^2,0]);
    GENS=ellgenerators(E);

    print(N," ist", if(#GENS==0, " keine ", " "), "Kongruenzzahl!");

    if(#GENS,
        x=GENS[1][1]; \\ = U^2
        y=GENS[1][2]; \\ = UV

        a= (x^2 - N^2) / y; \\ = ( U^4 - N^2 )/( UV )
        b= (2 * N * x) / y; \\ = ( 2*N * U^2 )/( UV )
                            \\ => c = ( U^4+N^2 ) / ( U V )
        c= (x^2 + N^2)/y;
        \\print(a^2, " ", b^2, " ",c^2, " ", a^2+b^2);

        print("  a="a, ", b=",b, ",\t Flächeninhalt (n):" ,a*b*1/2);
        print("  c=", c);
    );

    return((#GENS>0));
}

isNCongruent(7);
isNCongruent(23);

/*
7 ist Kongruenzzahl!
  a=24/5, b=35/12,        Flächeninhalt (n):7
  c=337/60
```

```
23 ist Kongruenzzahl!
  a=41496/3485, b=80155/20748,    Flächeninhalt (n):23
  c=905141617/72306780
*/
```

Aufgabe 4: bestimmen Sie die Menge L aller Lösungen $(x, y) \in \mathbb{F}_5^2$ der Kurve $E : y^2 = x^3 + x$ und berechnen Sie für jedes Paar P,Q die Summe $P + Q \in \overline{E}$.

Ein Pari/GP-Skript berechnet wieder die Punkte auf der Kurve, sowie die Verknüpfungstabelle (die Additionsfunktion von Aufgabe2 wird benutzt):

```
\r Aufgabe2_AddPoints.gp

enumPoints()=
{   local(T= listcreate(4) );

    listinsert(T, [0, 1, 0 ], #T+1); \\ Unendlich hinzufügen
    for(x=0,4,
        for(y=0,4,
            if(Mod(y^2-x^3-x,5)==0,
                listinsert(T, [ x, y, 1 ], #T+1);
            );
        );
    );

    return(T);
}


VerknuepfungsTabelle(EP)=
{   local(P1, P2, P3);

    for(i=0,#EP-1, print1("P",i,"= ",EP[i+1]));
    print();
    print();

    print1("              ");
    for(i=1,#EP, print1(EP[i], "   ")); print();
    for(i=1,54,print1("-"));print();

    for(i1= 1, #EP,
        P1= EP[i1];
        print1(P1,":   ");
        for(i2= 1, #EP,
            P2= EP[i2];

            P3= ECAddition(P1, P2, +1,0, 5);
            print1(P3, "   ");

        );
        print();
    );
}

ECPoints= enumPoints();

VerknuepfungsTabelle(ECPoints);

/*
P0= [0, 1, 0]P1= [0, 0, 1]P2= [2, 0, 1]P3= [3, 0, 1]

             [0, 1, 0]   [0, 0, 1]   [2, 0, 1]   [3, 0, 1]
```

```
[0, 1, 0]:  [0, 1, 0]  [0, 0, 1]  [2, 0, 1]  [3, 0, 1]
[0, 0, 1]:  [0, 0, 1]  [0, 1, 0]  [3, 0, 1]  [2, 0, 1]
[2, 0, 1]:  [2, 0, 1]  [3, 0, 1]  [0, 1, 0]  [0, 0, 1]
[3, 0, 1]:  [3, 0, 1]  [2, 0, 1]  [0, 0, 1]  [0, 1, 0]
*/
```

Aufgabe 5: Bestimmen Sie alle rationalen Lösungen (x, y) der Gleichung $y^2 = x(x-1)^2$.

Sei $x \neq 1$, die Umformung $x = \frac{y^2}{(x-1)^2}$ legt nahe: $x = \lambda^2$ mit $\lambda = \frac{y}{x-1}$.

Sei (x, y) eine Lösung der Gleichung. Wir bilden Lösungen auf Brüche ab:

$$(x, y) \mapsto \lambda := \begin{cases} 0, & \text{falls } x = 1 \\ \frac{y}{x-1} \end{cases}$$

Durch diese Festlegung ist jeder Lösung eindeutig ein Bruch λ zugeordnet.

Umgekehrt ist $(0, 1)$ sowie $(\lambda^2, (\lambda^2 - 1)\lambda)$ eine Lösung, denn zu $x = \lambda^2$ gehört $y^2 = \lambda^2(\lambda^2 - 1)^2$, also $y = \lambda(\lambda^2 - 1)$.