Aufgabe 1: In Stichworten: Eulersches Kriterium anwenden. Bestimmung der Potenz $a^{(p-1)/2}$ auf keinen Fall direkt. Eigentlich sollte eine Funktion zum »Schnellen Potenzieren« geschrieben werden. Mindesten aber sollte es mittels $Mod(a,p)^{(p-1)/2)}$ berechnet werden.

```
PrimUntereGrenze=9593;
\\ prime(PrimUntereGrenze)= 100003

erzeugeZufahlsZahlen(N=10000)=
{   local(a,p,l);
    l=vector(N,i, []);

    for(i=1,N,
        a=100000+random(900000);
        p=prime(random(N)+PrimUntereGrenze);
        l[i]=[a,p]
    );

    write("Blatt6-Aufgabe1-Liste.gp", l);
}

\\ erzeugeZufahlsZahlen();

fastExpo(a,p,potenz)=
{
    local(bisher=1, aPotenz=(a)%p, pot=potenz );

    while( pot > 0,
        if(pot%2==1,
            bisher= (bisher*aPotenz) % p;
            pot--;
        );
        pot/=2;
        aPotenz = (aPotenz)^2 % p;
    );

/*    if(Mod(bisher,p) != (Mod(a,p)^potenz),
        error("Fehler: ",Mod(bisher,p)," ", (Mod(a,p)^potenz));
    );
*/
    return(bisher);
}

myLegendre(a,p)=
{ /* Eulersches Kriterium:
        legendre(a,p)=a^((p-1)/2) mod p
    Es ist a^(p-1)/2 mod p effektiv zu bestimmen.
    Hier mittels der Methode der schnellen Exponentierung */

    if( a%p == 0, return(0));
    potenz=(p-1)/2;
    t=fastExpo(a,p, potenz); \\ so dauern 10000 Rechnungen 1 Sekunde
\\    t=(a^potenz) % p; \\ so dauern 10 Rechnungen 3 Sekunden

    if(t+1==p,
        return(-1),
        return(t));
}

#
{
    Liste=read("Blatt6-Aufgabe1-Liste.gp");
```

```
    t=0;
    gettime();
    for(i=1,#Liste,
        m=myLegendre(Liste[i][1], Liste[i][2]); \\ 840 ms
/*
        k=kronecker(Liste[i][1],Liste[i][2]); \\ 52 ms
        if(m!= k, print(Liste[i]," ",m," ", k));
*/
    );
    t=gettime();
    print("Zeit: ",t ,"ms, ",1.0*(t/#Liste),"ms durchchnittlich");
}

/*
  ein bisschen Testen:
    a=prime(10000); p=prime(20000);
    kronecker(a,p); \\ -1
    n=(p-1)/2;

    Mod(a,p)^n;      \\ time = 0 ms.
    %6 = Mod(224736, 224737)

    \\ keine schnelle Potenzierung,
    \\   (viel zu viele Multiplikationen):
    b=1;
    for(i=1,n,b*=a;b=b%p);
    \\ time = 149 ms.

    \\ mit schneller Potenzierung:
    b=fastExpo(a,p,n);
    \\ time = 0 ms.

    geht gar nicht:
    a^n
    %6 =   ***   user interrupt after 14,837 ms.
*/
```

Aufgabe 2: Wir nutzen die Formel $a(m) = \prod_{p^t||m} a(p^t)$ aus. Sei $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, dann ist $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} a & -b \\ -c & d \end{bmatrix}$.

Zur Bestimmung von $a(p^t)$ machen wir eine Fallunterscheidung:

- Fall 1, $p \nmid \det A$: Der Fall ist einfach, da wir die Matrix (auch mod p^t) invertieren können:

$$A\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^t}$$
$$\Rightarrow \begin{pmatrix} x \\ y \end{pmatrix} \equiv A^{-1}\begin{pmatrix} 0 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^t}$$

  Es gibt also nur die Lösung $x, y \equiv 0 \pmod{p^t}$, $a(p^t) = 1$.

- Fall 2, $p|\det A$: Es gibt (über $\mathbb{Z}$) invertierbare Matrizen M, N, sodass $A = M\begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix} N$ gilt und $\alpha|\delta$ und wegen $\det M = \det N = \pm 1$: $\alpha\delta = \pm \det A$. Das ist die Smith-Normal-Form, α, δ heißen Elementarteiler von A.

Es ist $\alpha := \mathrm{ggT}(a,b,c,d)$ und $\delta = \frac{\det A}{\alpha}$. Wir bestimmen die Anzahl der Lösungen für die Gleichung

$$B\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv 0 \pmod{p^t}, \qquad \text{mit } B := \begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix}.$$

Die Anzahl der Lösungen dieser und der ursprünglichen Gleichung sind identisch.

Es folgt: $\alpha x' \equiv 0 \pmod{p^t}$ und $\delta y' \equiv 0 \pmod{p^t}$, also $x' \equiv 0 \pmod{\frac{p^t}{\mathrm{ggT}(\alpha,p^t)}}$, sowie $y' \equiv 0 \pmod{\frac{p^t}{\mathrm{ggT}(\delta,p^t)}}$. Das bedeutet: $x' = k\frac{p^t}{\mathrm{ggT}(\delta,p^t)}, k = 1,\ldots,\mathrm{ggT}(\delta,p^t)$, das sind $\mathrm{ggT}(\delta,p^t)$ viele Möglichkeiten für x'.

Dann ist $a(p^t) = \mathrm{ggT}(\alpha,p^t)\,\mathrm{ggT}(\delta,p^t)$.

Insgesamt folgt für den Fall $\mathrm{ggT}(m,\det A) > 1$:

$$a(m) = \prod_{p^t||m,p|\det A} \mathrm{ggT}(\alpha,p^t)\,\mathrm{ggT}(\delta,p^t)$$

Aufgabe 3: p ist eine ungerade Primzahl, $0 < a$ und es gelte $p \not| a$. Sei j so wie im Gausschen Kriterium, $0 < j < p/2 \Leftrightarrow 1 \le j \le \frac{p-1}{2}$, so dass $(aj\%p) > \frac{p}{2}$ ist. Daraus folgt $\frac{p}{2} < aj - tp < p$, für ein passendes t.

$$\begin{aligned} &\Rightarrow \quad \frac{p}{2} + tp\frac{2}{2} < aj < p + tp \quad \Rightarrow \quad \frac{p+tp2}{2a} < j < \frac{p+tp}{a}\frac{2}{2} \\ &\Rightarrow \quad \frac{p(1+2t)}{2a} < j < \frac{p(2+2t)}{2a} \quad \Rightarrow \quad \frac{p(2k-1)}{2a} < j < \frac{p(2k+1)}{2a}, \quad k := t+1 \end{aligned}$$

Aufgabe 4: Nach der obigen Aufgabe gilt $\left(\frac{7}{p}\right) = (-1)^N$, wobei $N := \sum_{k=1}^{\lfloor \frac{7}{2} \rfloor} S_k$ und $S_k := \#\left\{\left(\frac{(2k-1)p}{14}, \frac{2kp}{14}\right) \cap \mathbb{Z}\right\}$.

Wir schreiben die Primzahl p als $p = r + 28x$ mit einem ungeraden r, $0 < r < 27$ und $7 \not| r$, da p ja prim ist. (Den Fall $7|p$ bzw. $7|r$ schließen wir aus, da dann das Legendre Symbol 0 ist.)

Wir betrachten den Summand S_1 und versuchen die Anzahl der ganzen Zahlen im Intervall $\left(\frac{(2k-1)p}{14}, \frac{2kp}{14}\right)$ zu bestimmen:

$$\left(\frac{r}{14}, \frac{2r}{14} + 2x\right) \cap \mathbb{Z} = \begin{cases} 2x, & r < 7 \\ 2x+1, & 7 < r < 14 \\ 2x+1, & 14 < r < 21 \\ 2x+2, & 21 < 28 \end{cases}$$

Für die Summanden S_2 und S_3 kann man ähnliche Fallunterscheidungen machen. Dann kann man eine Tabelle mit allen ungeraden Werten von r anlegen und für jede Zeile prüfen, ob

$$(-1)^N = \left(\frac{(-1)^{\frac{p-1}{2}}p}{7}\right) = \left(\frac{(-1)^{\frac{r-1}{2}}p}{7}\right)$$

gilt.

Wir bemühen an dieser Stelle ein Pari-Skript, welches die Formel überprüft:

```
IntervalSchnitt(a,b)=
  /*  a und b sind Polynome von der Form  2x +r1, 4x +r2,
      r1,r2 sind Brüche mit Nenner 14
  */
{   local(l);
    /*  Die Anzahl der ganzen Zahlen dazwischen, wird mittels sum bestimmt, die von
        ceil(a) bis floor(b) läuft, jeweils für x und x^0.
        Bei x läuft die summe z.B. von 2 bis 4 einschliesslich, deswegen wird 1 abgezogen.

        Bei x^0 sind die Brüche so, dass floor und ceil für das "_Innere_ von (a,b)" sorgen.
*/

    l=(sum(k=ceil(polcoeff(a,1)),floor(polcoeff(b,1)),1)-1)*x +
       sum(k=ceil(polcoeff(a,0)),floor(polcoeff(b,0)),1);

    return(l);
}

{   \\ die Primzahl p als r + 28*x darstellen,
    \\ wegen p prim, ist r ungerade:
    forstep(r=1,27,2,
        \\ r=7 würde 7|p bedeuten, deswegen werden Vielfache von 7 übersprungen
        if( (r%7) ==0, next());

        \\ unser p:
        p=r+28.0*x;

        \\ aus dem Gausschen Kriterium:
        S1=[  p/14, 2*p/14];
        S2=[3*p/14, 4*p/14];
        S3=[5*p/14, 6*p/14];

        N= IntervalSchnitt(S1[1],S1[2]) +
           IntervalSchnitt(S2[1],S2[2]) +
           IntervalSchnitt(S3[1],S3[2]);

        \\ eigentlich nur Rest mod 2 für (-1)^N interessant:
        \\ der Koeff von x ist durch 2 teilbar, also gerade und der Koeff von x^0
        \\ bestimmt (-1)^N
        Rest=polcoeff(N,0)%2;
        \\ linke Seite, nach Gausschem Kriterium
        LS= (-1)^Rest;
        \\ p mod 7 == r mod 7:
        \\ (p-1)/2 und (r-1)/2 sind gleich mod 2, da r ungerade
        \\ rechte Seite
        RS= kronecker((r%7)*(-1)^((r-1)/2),7);
        print("r=",r, "\t",LS, "\t",RS," \t",N,"\t ",r%4," ",(r-1)/2 );
        \\print(r,": "kronecker((r%7),7), "\t",(-1)^((r-1)/2), "\t", r %4);
        if(LS != RS, error("Fehler  für ",r,));
    );
}
/*
r=1     1       1       6*x
r=3     1       1       6*x
r=5     -1      -1      6*x + 1
r=9     1       1       6*x + 2
r=11    -1      -1      6*x + 3
r=13    -1      -1      6*x + 3
r=15    -1      -1      6*x + 3
r=17    -1      -1      6*x + 3
r=19    1       1       6*x + 4
r=23    -1      -1      6*x + 5
```

```
r=25    1       1       6*x + 6
r=27    1       1       6*x + 6
*/
```

Aufgabe 5: Ein Dirichletcharakter modulo m ist ein Gruppenhomomorphismus $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$. Sei also $n \in (\mathbb{Z}/m\mathbb{Z})^\times$, d.h. ggT$(n, m) = 1$.

1. Wir zeigen zunächst, dass $\mathbb{D}_m$ eine abelsche Gruppe ist: Zunächst ist $(\chi_1 \cdot \chi_2)(n) := \chi_1(n)\chi_2(n) \in \mathbb{C}^\times$. $(\chi_1 \cdot \chi_2)$ hat die Eigenschaften eines Dirichletcharakters modulo m, da χ_i Dirichletcharaktere modulo m sind.

   kommutativ: zu zeigen: $\chi_1(n)\chi_2(n) = \chi_2(n)\chi_1(n)$: $\chi_i(n) \in \mathbb{C}^\times$, und $\mathbb{C}$ ist kommutativ

   assoziativ: zu zeigen: $\big(\chi_1(n)\chi_2(n)\big)\chi_3(n) = \chi_1(n)\big(\chi_2(n)\chi_3(n)\big)$: $\chi_i(n) \in \mathbb{C}^\times$, und $\mathbb{C}$ ist assoziativ

   neutrales Element: Setze $\chi_0(n) := 1$, dann ist $\forall \chi \in \mathbb{D}_m : \chi_0(n)\chi(n) = \chi(n)$

   inverse Elemente: Für $\chi(n)$ setze $\chi^{-1}(n) := (\chi(n))^{-1}$, dann ist $\chi(n)\chi^{-1}(n) = 1 = \chi_0(n)$

2. Diese Gruppe ist für ungerade Primzahlpotenzen $m = p^t$ zyklisch: Die Gruppe $G := (\mathbb{Z}/m\mathbb{Z})^\times$ ist zyklisch, da m eine ungerade Primzahlpotenz ist. Sei also w eine Primitivwurzel von G und $\chi \in \mathbb{D}_m$ ein beliebiger Charakter. Es ist einerseits $\chi(w^{\varphi(m)}) = \chi^{\varphi(m)}(w)$, andererseits ist $\chi(w^{\varphi(m)}) = \chi(1) = 1$. Sei $r := \varphi(m)$, also ist $\epsilon := \chi(w)$ eine r-te Einheitswurzel: $\epsilon \in \boldsymbol{\mu_r} := \big\{e^{2\pi ik/r} \big| k = 0, \ldots, r-1\big\}$.

   Es sei nun $\tilde{\chi}$ derjenige Charakter, für den $\tilde{\chi}(w) = e^{2\pi i/r}$ ist. Wegen $\tilde{\chi}^k(w) = e^{2\pi ik/r}$ sind die Charaktere $\tilde{\chi}^r = \chi_0, \tilde{\chi}, \tilde{\chi}^2, \ldots, \tilde{\chi}^{r-1}$ alle verschieden und das sind schon alle Gruppencharaktere von G, (weil es schon alle r-ten Einheitswurzeln sind). Es ist $\mathbb{D}_m$ zyklisch, erzeugt z.B. von $\tilde{\chi}$ oder einem anderen Charaktere, der w auf einen Erzeuger von $\boldsymbol{\mu_m}$ abbildet.

3. Die Elemente der Ordnung 2: Für ein $\chi \in \mathbb{D}_p$ mit Ordnung 2 gilt für eine Primitivwurzel w von $(\mathbb{Z}/p\mathbb{Z})^\times$ (Ordnung von w ist $\varphi(p) = p - 1$) :

$$\begin{aligned} \chi(w) &= -1 \\ \chi(w^2) = \chi^2(w) &= (-1)^2 = 1 \\ \chi(w) &= e^{2\pi it/(p-1)} \quad \text{für ein passendes } t \end{aligned}$$

   Daraus folgt: $\chi(w) = \left(\frac{w}{p}\right)$