Aufgabenblatt 3, Aufgabe 8

a) Berechne die quadratfreie Zerlegung von $f(x) := x^{10} + x^6 + x^5 + x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.

Wir suchen eine Zerlegung $f = g_1 g_2^2 \dots g_{10}^{10}$, wobei g_i das Produkt der Primfaktoren ist, die genau i-mal vorkommen.
Berechnung von $g1$:

```
> f:=x^10+x^6+x^5+x^3+x^2+1:
> df:=diff(f,x) mod 2;
```

$$df := x^4 + x^2$$

```
> h1:=Gcd(f,df) mod 2;
```

$$h1 := x^2 + 1$$

```
> Rem(f,h1,x,'f1') mod 2:
> f1;
```

$$x^8 + x^6 + x^3 + 1$$

```
> p1:=Gcd(h1,f1) mod 2;
```

$$p1 := x + 1$$

```
> Rem(f1,p1,x,'g1') mod 2:
> g1:=Factor(g1) mod 2;
```

$$g1 := (x^4 + x + 1)(x^3 + x^2 + 1)$$

Bei unserem Beispiel ist es nun so, dass $h1 = h2$ ist.

```
> dh1:=diff(h1,x) mod 2;
```

$$dh1 := 0$$

```
> h2:=Gcd(h1,dh1) mod 2;
```

$$h2 := x^2 + 1$$

Daher können wir das aus der Vorlesung bekannte Verfahren nicht weiter anwenden. Bisher haben wir die Zerlegung $f = g1 \cdot h1 \cdot p1$. Offensichtlich istquadratfrei und für ein Polynomaus, deren Ableitung gleich 0 ist, gibt es stets eine Funktion, sodassist. In unserem Fall wäre das also $h1 = (x+1)^2$. Womit sich daher $g2 = 1$ und $g3 = x + 1$ ergibt. Die quadratfreie Zerlegung von f lautet also $f = (x^4 + x + 1)(x^3 + x^2 + 1)(x+1)^3$.

b) Zerlege $x^{15} - 1$ aus $\mathbb{Z}_2[x]$ in Primfaktoren mit Hilfe des Berlekamp-Verfahrens für kleine Primzahlen.

```
> p:=2:
> f:=x^15-1:
```

f ist quadratfrei, denn

```
> Gcd(f,diff(f,x)) mod p;
```

$$1$$

Wir wollen die Menge $W = \{ g \in \mathbb{Z}_2[x]_f : g^p = g \}$ berechnen, also die Menge der Fixpunkte des Frobeniusmorphismus. Dazu ermitteln wir zunächst die Matrix Af und ihren Kern. (Wobei im Folgenden $AfE = Af - E$.)

```
> for k from 0 to d-1 do R:=Rem(x^(p*k),f,x) mod p; Z||
k:=[seq(coeff(R,x,k),k=0..d-1)]:od:
> AfE:=map(modp,evalm(concat(seq(Z||k,k=0..d-1))-
array(1..d,1..d,identity)),p);
```

$$AfE := \begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&1&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&1&0&0&0&0 \\ 0&0&0&1&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&1&0&0 \\ 0&0&0&0&0&1&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&1&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&1 \end{bmatrix}$$

> **Bf:=Nullspace(AfE) mod p;**

$$Bf := \{[1,0,0,0,0,0,0,0,0,0,0,0,0,0,0],[0,1,1,0,1,0,0,0,1,0,0,0,0,0,0],$$
$$[0,0,0,0,0,1,0,0,0,0,1,0,0,0,0],[0,0,0,1,0,0,1,0,0,1,0,0,1,0,0],$$
$$[0,0,0,0,0,0,0,1,0,0,0,1,0,1,1]\}$$

Daher lautet die Dimension des Eigenraums zum Eigenwert 1

> **s:=nops(Bf);**

$$s := 5$$

und eine Basis des Kerns ist

> **Bf:=sort(convert(Bf,list),proc(u) global s;local v,k;for k from 2 to s do if not u[k]= 0 then v:= false; return(v);else v:=true; fi;od;v:=true;end);**

$$Bf := [[1,0,0,0,0,0,0,0,0,0,0,0,0,0,0],[0,0,0,0,0,1,0,0,0,0,1,0,0,0,0],$$
$$[0,0,0,0,0,0,0,1,0,0,0,1,0,1,1],[0,0,0,1,0,0,1,0,0,1,0,0,1,0,0],$$
$$[0,1,1,0,1,0,0,0,1,0,0,0,0,0,0]]$$

Die zu den Basisvektoren gehörenden nicht konstanten Lösungen der Kongruenz $g^p = g \bmod f$, also Elemente aus W, lauten:

> **for k to s do gg||k:=add(x^(l-1)*Bf[k][l],l=1..d):od:**

> **g:=[seq(gg||k,k=1..s)]: seq(` g`[k]=g[k],k=1..s);**

$$g_1 = 1,\quad g_2 = x^5 + x^{10},\quad g_3 = x^7 + x^{11} + x^{13} + x^{14},\quad g_4 = x^3 + x^6 + x^9 + x^{12},$$
$$g_5 = x + x^2 + x^4 + x^8$$

Die $g_{1,\dots}, g_5$ bilden eine $\mathbb{Z}_p$ - Basis von W. Nun können wir faktorisieren. Wir beginnen mit dem ersten Schleifendurchlauf (i=2):

> **T:=[f]:**

und die Tabelle der in Frage kommenden ggTs ist

> **GGT:=stackmatrix([` `,seq('r'=k,k=0..p-1)],concat([seq(`ggT mit g`[k]* `-r :`,k=2..s)],map(sort,stackmatrix(seq([seq(Gcd(f,g[k]-r) mod p,r=0..p-1)],k=2..s)),x)));**

$$GGT := \begin{bmatrix} & & r=0 & r=1 \\ ggT\ mit & g_2\text{-}r & : & x^5+1 & x^{10}+x^5+1 \\ ggT\ mit & g_3\text{-}r & : & x^7+x^6+x^4+1 & x^8+x^7+x^6+x^4+1 \\ ggT\ mit & g_4\text{-}r & : & x^3+1 & x^{12}+x^9+x^6+x^3+1 \\ ggT\ mit & g_5\text{-}r & : & x^7+x^3+x+1 & x^8+x^4+x^2+x+1 \end{bmatrix}$$

Somit erhalten wir als neues T:

```
> TT:=[GGT[2,2],GGT[2,3]];
```

$$TT := [x^5+1,\ x^{10}+x^5+1]$$

ggT-Berechnung der neuen Elemente von T:

```
> for m from 2 to s do
> MTT||m:=matrix(nops(TT),p, (k,l)->
> Gcd(TT[k],g[m]-l) mod p);od;
```

$$MTT2 := \begin{bmatrix} 1 & x^5+1 \\ x^{10}+x^5+1 & 1 \end{bmatrix}$$

$$MTT3 := \begin{bmatrix} x^4+x^3+x^2+x+1 & x+1 \\ x^4+x+1 & x^6+x^3+x^2+x+1 \end{bmatrix}$$

$$MTT4 := \begin{bmatrix} x^4+x^3+x^2+x+1 & x+1 \\ x^8+x^7+x^5+x^4+x^3+x+1 & x^2+x+1 \end{bmatrix}$$

$$MTT5 := \begin{bmatrix} x^4+x^3+x^2+x+1 & x+1 \\ x^4+x^3+1 & x^6+x^5+x^4+x^3+1 \end{bmatrix}$$

Der nächste Schleifendurchlauf (i=3) führt zum neuen T:

```
> TTT:=[MTT3[1,1],MTT3[1,2],MTT3[2,1],MTT3[2,2]];
```

$$TTT := [x^4+x^3+x^2+x+1,\ x+1,\ x^4+x+1,\ x^6+x^3+x^2+x+1]$$

ggT-Berechnung der neuen Elemente von T:

```
> for m from 2 to s do
> MTTT||m:=matrix(nops(TTT),p, (k,l)->
> Gcd(TTT[k],g[m]-l) mod p);od;
```

$$MTTT2 := \begin{bmatrix} 1 & x^4+x^3+x^2+x+1 \\ 1 & x+1 \\ x^4+x+1 & 1 \\ x^6+x^3+x^2+x+1 & 1 \end{bmatrix}$$

$$MTTT3 := \begin{bmatrix} x^4+x^3+x^2+x+1 & 1 \\ 1 & x+1 \\ x^4+x+1 & 1 \\ 1 & x^6+x^3+x^2+x+1 \end{bmatrix}$$

$$MTTT4 := \begin{bmatrix} x^4+x^3+x^2+x+1 & 1 \\ 1 & x+1 \\ x^4+x+1 & 1 \\ x^4+x^3+1 & x^2+x+1 \end{bmatrix}$$

$$MTTT5 := \begin{bmatrix} x^4+x^3+x^2+x+1 & 1 \\ 1 & x+1 \\ 1 & x^4+x+1 \\ x^4+x^3+1 & x^2+x+1 \end{bmatrix}$$

Nächster Schleifendurchlauf (i=4):

```
> TTTT:=[TTT[1],TTT[2],TTT[3],MTTT4[4,1],MTTT4[4,2]];
```

$$TTTT := [x^4+x^3+x^2+x+1,\ x+1,\ x^4+x+1,\ x^4+x^3+1,\ x^2+x+1]$$

Nun hat T genau s Elemente und der Algorithmus bricht ab. Maple liefert ebenfalls:

```
> Factor(f) mod p;
```

$$(x^2+x+1)\,(x^4+x^3+1)\,(x^4+x+1)\,(x^4+x^3+x^2+x+1)\,(x+1)$$

c) Berechne die gleichgradige Zerlegung von $g(x) := x^8+x^7+2x^6+3x^5+3x^4+3x^3+2x^2+2x+1$ in $\mathbb{Z}_7[x]$ und zerlege die erhaltenen Faktoren nach dem Verfahren von Cantor und Zassenhaus.

Gesucht ist eine Zerlegung $g = g_1 g_2 \cdots g_8$, wobei g_k das Produkt der Primteiler von g vom Grad k ist.

```
> g:=x^8+x^7+2*x^6+3*x^5+3*x^4+3*x^3+2*x^2+2*x+1:
> p:=7:
```

g ist quadratfrei, denn

```
> Gcd(g,diff(g,x)) mod p;
```

$$1$$

Produkt der Primteiler von g vom Grad 1:

```
> g1:=Gcd(g,x^p-x) mod p;
```

$$g1 := x^5+x^4+x^3+x^2+x+1$$

```
> Rem(g,g1,x,'q') mod p:
> q;
```

$$x^3+x+1$$

Da $q = \frac{g}{g1}$ von 1 verschieden ist, brechen wir nicht ab und fahren weiter fort. Das Produkt der Primteiler von g vom Grad 2 lautet dann:

```
> g2:=Gcd(q,x^(p^2)-x) mod p;
```

$$g2 := 1$$

```
> Rem(g,g1*g2,x,'q1') mod p:
> q1;
```

$$x^3+x+1$$

Produkt der Primteiler von g vom Grad 3:

```
> g3:=Gcd(q,x^(p^3)-x) mod p;
```

$$g3 := x^3+x+1$$

```
> Rem(g,g1*g2*g3,x,'q2') mod p:
> q2;
```

$$1$$

Abbruch, da $q2 = \frac{g}{g1 \cdot g2 \cdot g3} = 1$. Wir erhalten also

```
> g1*g2*g3;
```

$$(x^5+x^4+x^3+x^2+x+1)\,(x^3+x+1)$$

als gleichgradige Zerlegung von g.

Wir wollen nun, die erhaltenen Faktoren $g1$ und $g3$ nach dem Cantor-Zassenhaus Verfahren zerlegen.

$g1$ zerfällt in 5 lineare Faktoren:

```
> d:=degree(g1):
> k:=1:
> T:=[g1]:
```

Wir wählen nun ein zufälliges Polynom aus

```
> f:=sort(randpoly(x,dense,degree=d-1,coeffs=rand(0..p-1)),x);
```

$$f := 2x^3 + 5x^2 + 4x + 3$$

```
> p1:=(p^k-1)/2;
```

$$p1 := 3$$

```
> v:=Gcd(T[1],f^p1-1) mod p;
```

$$v := x^2 + 5x + 4$$

Da v ungleich 1 und ungleich $T[1]$ ist, setzen wir

```
> Rem(T[1],v,x,'a') mod p:
> a;
```

$$x^3 + 3x^2 + 3x + 2$$

```
> T1:=[v,a];
```

$$T1 := [x^2 + 5x + 4, x^3 + 3x^2 + 3x + 2]$$

Da die Mächtigkeit von $T1$ kleiner als 5 ist, fahren wir mit der while-Schleife weiter fort. Wir wählen erneut ein Zufallspolynom.

```
> f1:=sort(randpoly(x,dense,degree=d-1,coeffs=rand(0...p-1)),x);
```

$$f1 := 4x^4 + x^3 + 6x^2 + 2x + 2$$

```
> v1:=Gcd(T1[1],f1^p1-1) mod p;
```

$$v1 := x + 1$$

Da $v1$ ungleich 1 und ungleich $T1[1]$ ist, setzen wir

```
>> Rem(T1[1],v1,x,'a1') mod p:
> a1;
```

$$x + 4$$

```
> T1:=[T1[2],v1,a1];
```

$$T1 := [x^3 + 3x^2 + 3x + 2, x + 1, x + 4]$$

Dritter Durchlauf der while-Schleife:

```
> f2:=sort(randpoly(x,dense,degree=d-1,coeffs=rand(0...p-1)),x);
```

$$f2 := 4x^3 + 5x + 6$$

```
> v2:=Gcd(T1[1],f2^p1-1) mod p;
```

$$v2 := x + 3$$

```
> Rem(T1[1],v2,x,'a2') mod p:
> a2;
```

$$x^2 + 3$$

```
> T1:=[T1[2],T1[3],v2,a2];
```

$$T1 := [x + 1, x + 4, x + 3, x^2 + 3]$$

Vierter Durchlauf der while-Schleife:

```
> f3:=sort(randpoly(x,dense,degree=d-1,coeffs=rand(0...p-1)),x):
```

$$f3 := 4x^3 + 5x^2$$

```
> v3:=Gcd(T1[1],f3^p1-1) mod p;
```

$$v3 := x + 1$$

```
> Rem(T1[1],v3,x,'a3') mod p:
> a3;
```

$$1$$

Da $a3 = 1$ ist, wird die Menge $T1$ nicht verändert (das liegt daran, dass $x + 1$ vom Grad 1 ist und in der Zerlegung von $g1$ vorkommt). Der $T1[2]$ und $T1[3]$ liefern das selbe Ergebnis, daher betrachten wir diese Einträger nicht mehr.

Fünfter Durchlauf der while-Schleife:

```
> f4:=sort(randpoly(x,dense,degree=d-1,coeffs=rand(0...p-1)),x);
```

$$f4 := x^3 + 3x^2 + 6x + 2$$

```
> v4:=Gcd(T1[4],f4^p1-1) mod p;
```

$$v4 := x + 2$$

```
> Rem(T1[4],v4,x,'a4') mod p:
> a4;
```

$$x + 5$$

```
> T1:=[T1[1],T1[2],T1[3],v4,a4];
```

$$T1 := [x + 1, x + 4, x + 3, x + 2, x + 5]$$

Nun ist die Mächtigkeit von $T1$ gleich 5 und der Algorithmus bricht ab. $T1$ Liefert die Elemente der Zerlegung von $g1$.
Kommen wir nun zu $g3$. $g3$ zerfällt nicht weiter, daher ist $k = 3$.

```
> d:=degree(g3):
> k:=3:
> T:=[g3];
```

$$T := [x^3 + x + 1]$$

Da die Mächtigkeit von T gleich 1 ist, bricht der Algorithmus gleich zu Beginn ab und wir sind fertig.
Maple liefert ebenfalls dieselbe Zerlegung:

```
> Factor(g) mod p;
```

$$(x + 3)(x + 4)(x + 5)(x + 2)(x + 1)(x^3 + x + 1)$$