Index of non-trivial Maple Code for Galois doc PhL 7.11.13

This file includes all Maple items in the exact order they appear in Galois doc. page numbers change, sections are hard to find, I think one can just do a **visual search**. For each non-trivial item below, I will try to identify the **mws file** in which it is located. So if you want to find the code for some item in Galois, find that item below and then note the file name. The Galois mws files are now in a single folder.

Note: Witzend can search mws file for any text, but type it right! That is how I did things here.

```
13*973 - 42*301;          gcd(973,301);
```

7 7 nowhere

```
Quo(3*x^4+4*x^3+2,2*x+3,x) mod 5;
```

$4x^3+x^2+x+1$

```
Rem(3*x^4+4*x^3+2,2*x+3,x) mod 5;
```

4 nowhere

```
for s from 1 to 7 by 2 do
  e1 := (1*s) mod 15:
  e2 := (2*s) mod 15:
  e3 := (4*s) mod 15:
  e4 := (8*s) mod 15:
  print(a^e1,a^e2,a^e3,a^e4);
od:
```

a, a^2, a^4, a^8

a^3, a^6, a^{12}, a^9

a^5, a^{10}, a^5, a^{10}

$a^7, a^{14}, a^{13}, a^{11}$

galois main.mws

```
for s from 1 to 15 by 2 do
  e1 := (1*s)   mod 31:
  e2 := (2*s) mod 31:
  e3 := (4*s) mod 31:
  e4 := (8*s) mod 31:
  e5 := (16*s) mod 31:
  print(a^e1,a^e2,a^e3,a^e4,a^e5);
od:
```

a, a^2, a^4, a^8, a^{16}

$a^3, a^6, a^{12}, a^{24}, a^{17}$

$a^5, a^{10}, a^{20}, a^9, a^{18}$

$a^7, a^{14}, a^{28}, a^{25}, a^{19}$

$a^9, a^{18}, a^5, a^{10}, a^{20}$

$a^{11}, a^{22}, a^{13}, a^{26}, a^{21}$

$a^{13}, a^{26}, a^{21}, a^{11}, a^{22}$

$a^{15}, a^{30}, a^{29}, a^{27}, a^{23}$

galois main.mws

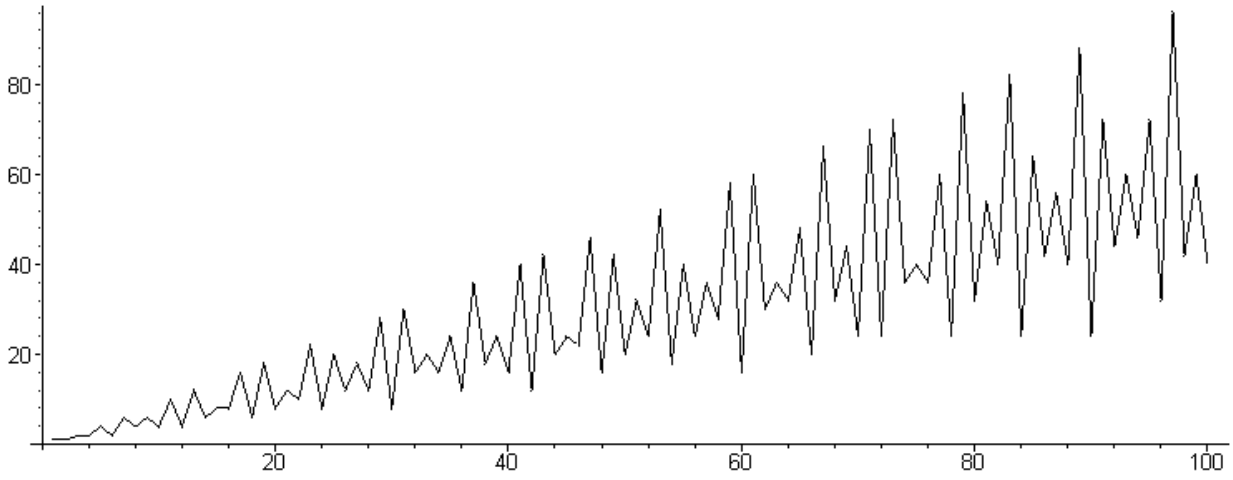
```
for n from 1 to 100 by 10 do
  print(seq([n+i,phi(n+i)],i = 0..9));
od;
```

```
[1, 1], [2, 1], [3, 2], [4, 2], [5, 4], [6, 2], [7, 6], [8, 4], [9, 6], [10, 4]
[11, 10], [12, 4], [13, 12], [14, 6], [15, 8], [16, 8], [17, 16], [18, 6], [19, 18], [20, 8]
[21, 12], [22, 10], [23, 22], [24, 8], [25, 20], [26, 12], [27, 18], [28, 12], [29, 28], [30, 8]
[31, 30], [32, 16], [33, 20], [34, 16], [35, 24], [36, 12], [37, 36], [38, 18], [39, 24], [40, 16]
[41, 40], [42, 12], [43, 42], [44, 20], [45, 24], [46, 22], [47, 46], [48, 16], [49, 42], [50, 20]
[51, 32], [52, 24], [53, 52], [54, 18], [55, 40], [56, 24], [57, 36], [58, 28], [59, 58], [60, 16]
[61, 60], [62, 30], [63, 36], [64, 32], [65, 48], [66, 20], [67, 66], [68, 32], [69, 44], [70, 24]
[71, 70], [72, 24], [73, 72], [74, 36], [75, 40], [76, 36], [77, 60], [78, 24], [79, 78], [80, 32]
[81, 54], [82, 40], [83, 82], [84, 24], [85, 64], [86, 42], [87, 56], [88, 40], [89, 88], [90, 24]
[91, 72], [92, 44], [93, 60], [94, 46], [95, 72], [96, 32], [97, 96], [98, 42], [99, 60], [100, 40]
```

phi.mws

```
p := seq([n,phi(n)],n=1..100):
pointplot([p],style=line);
```

phi.mws



phi.mws

```
Rem(x^15-1,x^4+x^3+x^2+x+1,x) mod 2; #1
```

$$0$$

```
Rem(x^15-1,x^4+x^3+x^2+1,x) mod 2;   #2
```

$$x+1$$

```
Rem(x^15-1,x^4+x^3+x+1,x) mod 2;     #3
```

$$x^3+1$$

```
Rem(x^15-1,x^4+x^2+x+1,x) mod 2;     #4
```

$$x+1$$

```
Rem(x^15-1,x^4+x^3+1,x) mod 2;       #5
```

$$0$$

```
Rem(x^15-1,x^4+x+1,x) mod 2;         #6
```

$$0$$

```
Rem(x^15-1,x^4+x^2+1,x) mod 2;       #7
```

$$x^3+1$$

```
Rem(x^15-1,x^4+1,x) mod 2;           #8
```

$$x^3+1$$

galois main.mws

```
n := 25: found := 0:
for p from 1 to n do
  for m from 1 to n do
    for K from 1 to n do
      for i from 0 to n do
        g := gcd(p^i,(p^m-1)/K);
        if g <> 1 then print(p,m,p^m-1,K,i,g); found := 1 fi;
        # print("p,m,p^m-1,K,i,g = ", p,m,p^m-1,K,i,g);
      od;
    od;
  od;
od;
if found = 0 then print( "no cases found for n = ", n) fi;
```

"no cases found for n = ", 25

test5_35a.mws

```
restart; with(numtheory): # numtheory only for Euler phi use.
PrimID := 1e12:  # use this to mark a prim poly so sorts last in list
p := 2: m:= 6: printf("\n\np = %d, m = %d",p,m);
printf("Number of Primitive Polynomials is %d",phi(p^m-1)/m);
first := true:
for s from 1 to p^m-2 by 1 do  # for each GF(q) element (alpha)^s ...
  # create array e of m conjugate set exponents as shown in sec 5 (c) 3
  for n from 1 to m do e[n] := (p^n*s) mod (p^m-1); od:
  # convert this array to a set so dupe exponents get thrown out (Fig 5.1)
  eset := convert(e,set);
  # test for primitive poly as per (4.32), if yes add PrimID to set
  if gcd(s,p^m-1) = 1 then eset := eset union {PrimID}; fi;
  # first time seta is something like {{3,6,7}}, a set of one set.
  if first then seta := {eset};first := false;
    # otherwise add a new set to set of sets e.g. {{3,6,7},{2,6,PrimID}}
    # this operation removes dupe conjugate sets (!) (Fig 5.2)
    else seta := seta union {eset};
  fi;
od:
# at this point we have seta = {{3,6,7},{2,6,PrimID}, ....}
printf("Number of Minimum Polynomials is %d",nops(seta));
for cs in seta do   # for each conjugate set cs in seta ...
  # convert set to a list so it can be sorted, then sort it
  cs1 := sort(convert(cs,list)):
  L := nops(cs1);  # number of elements in cs1
  if cs1[L] = PrimID then cs1[L] := Prim; L := L-1; fi;
  # construct the polynomial h(x) with exponents in cs1
  first := true;
  for n from 1 to L do
    if first then h := (x-a^cs1[n]); first := false;
    else h := h*(x-a^cs1[n]); fi:
  od:
  print(cs1,h);  # show the exponent list and then the polynomial
od:
```

show conj sets.mws

```
alias(a=RootOf(x^6+x^4+x^3+x+1));
```

$$I, a$$

```
p := (x-a^11)*(x-a^22)*(x-a^25)*(x-a^37)*(x-a^44)*(x-a^50);
```

$$p := (x-a^{11})(x-a^{22})(x-a^{25})(x-a^{37})(x-a^{44})(x-a^{50})$$

```
sort(subs(a=alpha,simplify(p)) mod 2);
```

$$x^6+x^5+x^2+x+1$$

galois main.mws

```
Rem(x^4,1+x^2+x^4,x) mod 2;
```

$$x^2+1$$

galois main.mws

```
mult := proc(n1,n2,m) alpha^(n1+n2 mod (2^m-1)) end:
mult(5,6,3);
```

$$\alpha^4$$

galois main.mws

```
> alpha^3 := 1 + alpha;
Error, invalid lhs of assignment
> alpha := (1 + alpha)^(1/3):
Warning, recursive definition of name
```

cannot find this

```
alias(a = RootOf(z^3-z-1)):
subs(a=alpha,simplify(a^6));
```

$$2\alpha+\alpha^2+1$$

```
subs(a=alpha,simplify(a^6)) mod 2;
```

$$\alpha^2+1$$

galois main.mws

```
t:=array(1..7):
alias(a=RootOf(x^3+x+1)):
for n from 1 to 7 do
  t[n]:=sort(subs(a=alpha,simplify(a^n)) mod 2);
od:
print(t);
```

$$[\alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1, 1]$$

n	α^n
1	α
2	α^2
3	$\alpha+1$
4	$\alpha^2+\alpha$
5	$\alpha^2+\alpha+1$
6	α^2+1
7	1

galois main.mws

```
> t := array(1..15):
> alias(a=RootOf(x^4+x+1)):
> for n from 1 to 15 do
    t[n]:=sort(subs(a=alpha,simplify(a^n)) mod 2);
  od:
> print(t);
```

$$[\alpha, \alpha^2, \alpha^3, \alpha+1, \alpha^2+\alpha, \alpha^3+\alpha^2, \alpha^3+\alpha+1, \alpha^2+1, \alpha^3+\alpha, \alpha^2+\alpha+1,$$
$$\alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1, \alpha^3+\alpha^2+1, \alpha^3+1, 1]$$

galois main.mws

```
> t := array(1..31):
> alias(a=RootOf(x^5+x^3+x^2+x+1)):
> for n from 1 to 31 do
    t[n]:=sort(subs(a=alpha,simplify(a^n)) mod 2);
  od:
> print(t);
```

$$[\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^3+\alpha^2+\alpha+1, \alpha^4+\alpha^3+\alpha^2+\alpha, \alpha^4+\alpha+1, \alpha^3+1, \alpha^4+\alpha, \alpha^3+\alpha+1,$$
$$\alpha^4+\alpha^2+\alpha, \alpha+1, \alpha^2+\alpha, \alpha^3+\alpha^2, \alpha^4+\alpha^3, \alpha^4+\alpha^3+\alpha^2+\alpha+1, \alpha^4+1, \alpha^3+\alpha^2+1,$$
$$\alpha^4+\alpha^3+\alpha, \alpha^4+\alpha^3+\alpha+1, \alpha^4+\alpha^3+1, \alpha^4+\alpha^3+\alpha^2+1, \alpha^4+\alpha^2+1, \alpha^2+1, \alpha^3+\alpha,$$
$$\alpha^4+\alpha^2, \alpha^2+\alpha+1, \alpha^3+\alpha^2+\alpha, \alpha^4+\alpha^3+\alpha^2, \alpha^4+\alpha^2+\alpha+1, 1]$$

galois main.mws

n	α^n
1	α
2	α^2
3	α^3
4	α^4
5	$\alpha^3+\alpha^2+\alpha+1$
6	$\alpha^4+\alpha^3+\alpha^2+\alpha$
7	$\alpha^4+\alpha+1$
8	α^3+1
9	$\alpha^4+\alpha$
10	$\alpha^3+\alpha+1$
11	$\alpha^4+\alpha^2+\alpha$
12	$\alpha+1$
13	$\alpha^2+\alpha$
14	$\alpha^3+\alpha^2$
15	$\alpha^4+\alpha^3$
16	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$
17	α^4+1
18	$\alpha^3+\alpha^2+1$
19	$\alpha^4+\alpha^3+\alpha$
20	$\alpha^4+\alpha^3+\alpha+1$
21	$\alpha^4+\alpha^3+1$
22	$\alpha^4+\alpha^3+\alpha^2+1$
23	$\alpha^4+\alpha^2+1$
24	α^2+1
25	$\alpha^3+\alpha$
26	$\alpha^4+\alpha^2$
27	$\alpha^2+\alpha+1$
28	$\alpha^3+\alpha^2+\alpha$
29	$\alpha^4+\alpha^3+\alpha^2$
30	$\alpha^4+\alpha^2+\alpha+1$
31	1

```
t := array(1..8):
alias(a=RootOf(x^2+x+2)):
for n from 1 to 8 do
  t[n]:=sort(subs(a=alpha,simplify(a^n)) mod 3);
od:

print(t);
```

$$[\alpha, 2\alpha+1, 2\alpha+2, 2, 2\alpha, \alpha+2, \alpha+1, 1]$$

n	α^n
1	α
2	$2\alpha+1$
3	$2\alpha+2$
4	2
5	2α
6	$\alpha+2$
7	$\alpha+1$
8	1

galois main.mws

```
p1 := (x-a)*(x-a^2)*(x-a^4);
```

$$p1 := (x-a)(x-a^2)(x-a^4)$$

```
subs(a=alpha,simplify(p1)) mod 2;
```

$$x^3+x+1$$

```
p3 := (x-a^3)*(x-a^6)*(x-a^5);
```

$$p3 := (x-a^3)(x-a^6)(x-a^5)$$

```
subs(a=alpha,simplify(p3)) mod 2;
```

$$x^3+1+x^2$$

galois main.mws

```
p1 := (x-a)*(x-a^2)*(x-a^4)*(x-a^8);
subs(a=alpha,simplify(p1)) mod 2;
p7 := (x-a^7)*(x-a^14)*(x-a^13)*(x-a^11);
subs(a=alpha,simplify(p7)) mod 2;
m3 := (x-a^3)*(x-a^6)*(x-a^12)*(x-a^9);
subs(a=alpha,simplify(m3)) mod 2;
m5 := (x-a^5)*(x-a^10);
subs(a=alpha,simplify(m5)) mod 2;
```

$$p1 := (x-a)(x-a^2)(x-a^4)(x-a^8)$$

$$x^4+x+1$$

$$p7 := (x-a^7)(x-a^{14})(x-a^{13})(x-a^{11})$$

$$x^4+1+x^3$$

$$m3 := (x-a^3)(x-a^6)(x-a^{12})(x-a^9)$$

$$x^4+x^3+x^2+1+x$$

$$m5 := (x-a^5)(x-a^{10})$$

$$x^2+1+x$$

galois main.mws

```
p1 := (x-a)*(x-a^2)*(x-a^4)*(x-a^8)*(x-a^16);
subs(a=alpha,simplify(p1)) mod 2;
p3 := (x-a^3)*(x-a^6)*(x-a^12)*(x-a^24)*(x-a^17);
subs(a=alpha,simplify(p3)) mod 2;
p5 := (x-a^5)*(x-a^10)*(x-a^20)*(x-a^9)*(x-a^18);
subs(a=alpha,simplify(p5)) mod 2;
p7 := (x-a^7)*(x-a^14)*(x-a^28)*(x-a^25)*(x-a^19);
subs(a=alpha,simplify(p7)) mod 2;
p11 := (x-a^11)*(x-a^22)*(x-a^13)*(x-a^26)*(x-a^21);
subs(a=alpha,simplify(p11)) mod 2;
p15 := (x-a^15)*(x-a^30)*(x-a^29)*(x-a^27)*(x-a^23);
subs(a=alpha,simplify(p15)) mod 2;
```

galois main.mws

```
Factor(x^5+x^3+x^2+x+1,a) mod 2;
```

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

galois main.mws

```
Roots(x^5+x^3+x^2+x+1,a) mod 2;
```

$$[[a^4+a^3+a^2+a+1,\ 1],\ [a^4,\ 1],\ [a,\ 1],\ [a^3+1,\ 1],\ [a^2,\ 1]]$$

galois main.mws

```
Factor(x^5+x^4 +1,a) mod 2;
```

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

galois main.mws

```
Roots(x^5+x^4 +1,a) mod 2;
```

$$[\ ]$$

galois main.mws

```
Factor(x^3+x+1,a) mod 2;
```

$$x^3+1+x$$

```
Roots(x^3+x+1,a) mod 2;
```

$$[\,]$$

galois main.mws

```
Factor(x^4 + x^3 + x + 1) mod 2;
```

$$(x+1)^2(x^2+x+1)$$

galois main.mws

```
expand((x+1)*(x^2+x+1)) mod 2;
```

$$x^3+1$$

galois main.mws

```
Quo(x^31-1,x^5+x^3+x^2+x+1,x) mod 2;
```

$$x^{26}+x^{24}+x^{23}+x^{21}+x^{19}+x^{15}+x^{14}+x^{13}+x^{11}+x^{10}+x^9+x^8+x^7+x^4+x+1$$

```
Rem(x^31-1,x^5+x^3+x^2+x+1,x) mod 2;
```

$$0$$

galois main.mws

```
Quo(x^31-1,x^5+x^4 +1,x) mod 2;
```

$$x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+x^{20}+x^{18}+x^{15}+x^{14}+x^{10}+x^5+x^4+x^3+x^2+x$$

```
Rem(x^31-1,x^5+x^4 +1,x) mod 2;
```

$$x^4+x^3+x^2+x+1$$

galois main.mws

```
alias(a = RootOf(z^4+z+1)):        # appears in the Factor call below
for n from 1 to 2^5-1 by 2 do      # only generate polys of R having a +1
  c := convert(n,base,2):          # for example, n=6 makes c = [0,1,1]
  L := nops(c):                    # L = number of bits in c, eg, 3
  p := sum(c[i]*x^(i-1),i=1..L):   # generate poly p(x) with c as coeffs
  f := Factor(p,a) mod 2:          # attempt to factor p(x) in GF(p,m)
  print(p,"       ",f);            # print p(x) and then its factored form
od:
```

galois main.mws

$1,"\quad ",1$

$1+x,"\quad ",1+x$ **B**

$1+x^2,"\quad ",(1+x)^2$ **B**

$1+x+x^2,"\quad ",(x+a^2+a)(x+a^2+a+1)$ **A**

$1+x^3,"\quad ",(x+1)(x+a^2+a+1)(x+a^2+a)$ **B**

$1+x+x^3,"\quad ",1+x+x^3$ **C**

$1+x^2+x^3,"\quad ",1+x^2+x^3$ **C**

$1+x+x^2+x^3,"\quad ",(x+1)^3$

$1+x^4,"\quad ",(x+1)^4$ **B**

$1+x+x^4,"\quad ",(x+a+1)(x+a)(x+a^2)(x+a^2+1)$ **A**

$1+x^2+x^4,"\quad ",(x+a^2+a+1)^2\ (x+a^2+a)^2$ **E**

$1+x+x^2+x^4,"\quad ",(x+1)(1+x^2+x^3)$ **D**

$1+x^3+x^4,"\quad ",(x+a^3+a^2+1)(x+a^3+a^2+a)(x+a^3+a+1)(x+a^3+1)$ **A**

$1+x+x^3+x^4,"\quad ",(x+1)^2(x+a^2+a+1)(x+a^2+a)$ **B**

$1+x^2+x^3+x^4,"\quad ",(x+1)(x^3+1+x)$ **D**

$1+x+x^2+x^3+x^4,"\quad ",(x+a^3)(x+a^3+a)(x+a^3+a^2)(x+a^3+a^2+a+1)$ **A**

Visio

$$g := x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$$

search for period.mws

```
for n from 0 to 1600 do
  if (n mod 50) = 0 then print("counter",n); fi;
  r := rem(x^n-1,g,x) mod 2;
  if type(r,numeric) and r = 0 then print(n); else print(n, "no go") ;fi
od:
```

search for period.mws

```
m1  := x^5+x^3+x^2+x+1:
m3  := x^5+x^4+x^3+x+1:
m5  := x^5+x^2+1:
m7  := x^5+x^4+x^2+x+1:
m11 := x^5+x^3+1:
m15 := x^5+x^4+x^3+x^2+1:
g2  :=  sort(expand(m1) mod 2);
g4  :=  sort(expand(m1*m3) mod 2);
g6  :=  sort(expand(m1*m3*m5) mod 2);
g10 := sort(expand(m1*m3*m5*m7) mod 2);
g14 := sort(expand(m1*m3*m5*m7*m11) mod 2);
g31 := sort(expand(m1*m3*m5*m7*m11*m15) mod 2);
```

galois main.mws

$$g2 := x^5 + x^3 + x^2 + x + 1$$

$$g4 := x^{10} + x^9 + x^4 + x^3 + 1$$

$$g6 := x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^4 + x^3 + x^2 + 1$$

$$g10 := x^{20} + x^{18} + x^{14} + x^{13} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x + 1$$

$$g14 := x^{25} + x^{21} + x^{20} + x^{19} + x^{17} + x^{15} + x^{12} + x^{10} + x^9 + x^8 + x^7 + x^4 + x^3 + x + 1$$

$$g31 := x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

galois main.mws

(d) Maple program to construct the matrix representation of GF(p^m)

The code is self-documented. The p,m values selected in this code are for GF(2^3).

```
with(linalg): # invoke the linear algebra library
```

matrix rep.mws

```
Procedure to replace elements of mxm matrix M with mod p elements
> matrixp := proc(M::array,m,p)
    local i,j;
    for i from 1 to m do
      for j from 1 to m do
        M[i,j] := M[i,j] mod p;
      od;
    od;
    evalm(M);
  end:
```

matrix rep.mws

```
Enter p, m and the coefficients of a primitive polynomial
>   p := 2: m := 3: d[2] := 0: d[1] := 1: d[0] := 1:
> # p := 3: m := 2:            d[1] := 1 :d[0] := 2:
Cosmetic labels for output
> Xpow := seq(X^k,k=1..p^m-1):
```

matrix rep.mws

Construct the primitive element matrix X using (10.41) and verify the characteristic polynomial

```
> X_ := matrix(m,m):
> for i from 1 to m do
    for j from 1 to m do
      X_[i,j] := delta(i,j+1) - delta(j,m)*d[i-1] mod p;
    od;
  od;
> charpoly(X_,x) mod p;
```

$$x^3 + x + 1$$

matrix rep.mws

Display the entire matrix representation for GF(p^m)

```
>
> for k from 1 to p^m-1 do
     print(Xpow[k],matrixp(evalm(X_^k),m,p));
  od;
  print("0 " ,matrix(m,m,[0$m^2]));

m := 9: d[8] := 0: d[7] := 0: d[6] := 0: d[5] := 0:
p := 2: d[4] := 1: d[3] := 0: d[2] := 0: d[1] := 0:d[0] := 1:

charpoly(X_,x) mod p;
```

$$1 + x^4 + x^9$$

matrix rep.mws

In this case brute force calculation should give $X^{511} = I$. Maple cheerfully does the job:

```
print(Xpow[1],matrixp(evalm(X_^1),m,p));
print(Xpow[511],matrixp(evalm(X_^511),m,p));
```

matrix rep.mws

```
ID := array(1..m,1..m,identity):
for k from 1 to p^m do
  if equal( matrixp(evalm(X_^k),m,p),ID) then print("yes", k) fi;
od;
```

"yes", 511

matrix rep.mws

```
n := 8;
for N from 1 to 2^(n+1)-1 do   # go only as far as needed
 # compute polynomial for this value of N
  c := convert(N,base,2):
  p := sum(c[i]*x^(i-1),i=1..nops(c)):
# see if it has a remainder
  r := Rem(x^n-1,p,x) mod 2;
  if type(r,numeric) and r = 0 then print("N=",N,"degree=",nops(c)-1,"p(x)=",p, r) fi;
od:
```

test2.mws

$$n := 8$$

"N=", 1, "degree=", 0, "p(x)=", 1, 0

"N=", 3, "degree=", 1, "p(x)=", $1+x$, 0

"N=", 5, "degree=", 2, "p(x)=", $1+x^2$, 0

"N=", 15, "degree=", 3, "p(x)=", $1+x+x^2+x^3$, 0

"N=", 17, "degree=", 4, "p(x)=", $1+x^4$, 0

"N=", 51, "degree=", 5, "p(x)=", $1+x+x^4+x^5$, 0

"N=", 85, "degree=", 6, "p(x)=", $1+x^2+x^4+x^6$, 0

"N=", 255, "degree=", 7, "p(x)=", $1+x+x^2+x^3+x^4+x^5+x^6+x^7$, 0

"N=", 257, "degree=", 8, "p(x)=", x^8+1, 0

test2.mws

$$n := 9$$

"N=", 1, "degree=", 0, "p(x)=", 1, 0

"N=", 3, "degree=", 1, "p(x)=", $1+x$, 0

"N=", 7, "degree=", 2, "p(x)=", $1+x+x^2$, 0

"N=", 9, "degree=", 3, "p(x)=", $1+x^3$, 0

"N=", 73, "degree=", 6, "p(x)=", $1+x^3+x^6$, 0

"N=", 219, "degree=", 7, "p(x)=", $1+x+x^3+x^4+x^6+x^7$, 0

"N=", 511, "degree=", 8, "p(x)=", $1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8$, 0

"N=", 513, "degree=", 9, "p(x)=", x^9+1, 0

test2.mws

```
primes := seq(ithprime(i),i=1..20);
```

$primes := 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71$

```
found := false:
for p in [primes] do
  for n from 1 to 1000 do
    if n mod p = 0 then next; fi;   #ignore n being multiple of p
    m := phi(n);
    r := p^m-1 mod n;
    if r <> 0 then found := true; print("exception found", p, m, n) ;fi;
  od;
od;
if found = false then print("no exceptions were found"); fi;
```

"no exceptions were found"

search divisors for n.mws

```
p1 := x^4+x+1:
p7 := x^4+x^3+1:
m3 := x^4+x^3+x^2+x+1:
m5 := x^2+x+1:
m0 := x-1:
mzero := x:
```

search divisors for n.mws

```
period := proc(f,q,p) local per, n;
  per := infinity;
  for n from q by -1 to 1 do if Rem(x^n-1,f,x) mod p = 0 then per := n; fi; od;
  RETURN(per);
end:
```

```
p1 := x^4+x+1:
p7 := x^4+x^3+1:
m3 := x^4+x^3+x^2+x+1:
m5 := x^2+x+1:
m0 := x-1:
mzero := x:
```

search divisors for n.mws

```
period := proc(f,q,p) local per, n;
  per := infinity;
  for n from q by -1 to 1 do if Rem(x^n-1,f,x) mod p = 0 then per := n; fi; od;
  RETURN(per);
end:
```

```
period(p1,15,2);
```

15

```
period(p7,15,2);
```

15

```
period(m3,15,2);
```

5

```
period(m5,15,2);
```

3

```
period(m0,15,2);
```

1

```
period(mzero,15,2);
```

∞

search divisors for n.mws

```
p := 561: ifactor(561);
```

(3) (11) (17)

```
found := false:
for a from 1 to 10000 do
  if (a^p-a) mod p <> 0 then print(a);found := true; fi;
od;
if found = false then print("no exceptions found"); fi;
```

"no exceptions found"

App G.mws