PARI Exercises

First define the following functions:

1. \( \text{Show}(+) = \text{print}(\text{lift}(\text{lift}(+))) \)

   \( \text{Show}(+) \) can be used to remove all the \( \text{Mod} \)'s that make PARI output so hard to read.

2. \( \text{powerrep}(h, g, g) = \text{for } j=0 \text{ to } g-2, \text{ if } (\text{Mod}(a^j, g) = h, \text{ print}(a^j)) \)

   \( \text{powerrep} \) is used to get the power representation for the input \( h \) over \( \text{GF}(q) \) generated by \( g \).

   This is best illustrated by example:

   \( \Rightarrow g = \text{Mod}(1,2)*(1+a^2 + a^5) \)
\[ h = 1 + a + a^2 + a^3 \]

\[ \text{powerrep}(h, 32, g) \]

23

(Check this with Table 3 of Appendix A!)

Note the following:

1. `factormod(g, p)` factors a polynomial \( g \) over the prime field \( GF(p) \).

Example: The polynomials over \( GF(2) \) of degree 2 are:
\[ X^2, X^2 + 1, X^2 + X, X^2 + X + 1 \]

? `factormod(X^2, 2)`

? `show(%)`

\[ \text{Mat}([X, 2]) \]

\[ \Rightarrow 2 \text{ factors of } X \]

\[ X^2 = X + X \]
? show \( \text{factor mod } (x^2+1, 2) \)
\[
\text{Mat } ([x+1, 2])
\]
\[
\Rightarrow x^2+1 = (x+1)(x+1)
\]

? show \( \text{factor mod } (x^2+ x, 2) \)
\[
[[-1, 1; x+1, 1]]
\]
\[
\Rightarrow x^2+x = (x') (x+1)'
\]

? show \( \text{factor mod } (x^2+ x+1, 2) \)
\[
\text{Mat } ([x^2+ x+1, 1])
\]
\[
\Rightarrow x^2+x+1 \text{ is irreducible}
\]

2. PARI can calculate Euler's \( \Phi \) function

? eulerphi (7)
6

? eulerphi (21)
12
(3) PARI can factor polynomials in $\text{GF}(\mathbb{F}_p^m)$:

```
use factorff ( h, p, q)
```

Example: Consider $(x+2)(x+2)$ over $\text{GF}(32)$ generated by $x^5 + x^2 + 1$

```
? g = Mod(1,2) + (a^5 + a^2 + 1)
```

```
? (x+a^2)*(x+a^3)
   X^2 + (a^3+a^2)x + a^5
```

```
? powerrep (a^3+a^2, 32, g)
   a^20
```

So $(x+2)(x+2) = x^2 + a^20x + a^5$

Check:

```
? factorff( x^2 + a^20*x + a^5, 2, g)
```

```
? show (g)
   [ [x+a^2, 1 ; x+a^3, 1]
```


4. logging your PARI commands & output

```
"backslash" "ell" logfile
```

a file name you make up

Before you exit, do

```
\l
```

to turn logging back off.

5. To quit:

```
? quit
```

6. Division:

In PARI, if division can be done with no remainder, it will be done:

```
\[ \text{Ex}1 \quad ? p = \text{Mod}(1,2) * (a^2 + a + 1) \]
\[ ? p2 = \text{Mod}(1,2) * (a^3 + 1) \]
\[ ? \text{show} (p2/p) \]
\[ a+1 \]
```
To refer to part of a prev. answer, can use matrix notation. For example suppose we wanted to factor \( x^6 + x^5 + \ldots + 1 \) over \( \mathbb{F}_2 \):

\[
\text{gp} \rightarrow \text{factor mod}\left(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, 2\right)
\]

\[
\text{gp} \rightarrow \text{mat size (a)}
\]

\[
Z_2 = \begin{bmatrix} 2 \, 2 \end{bmatrix}
\]

Now, we could loop over all \( Z_2 \) of the factors without knowing ahead of time how many there are:

for \( j = 1, \text{mat size (a)} \),

if \( \text{pol degree (a[j,1])} = 3 \),

print (a[j,1]),

(This will print all of the factors of degree 3.)
Clearly, this isn't too useful for this example, but it could help on the HW!

8. To factor an integer, just do

\[ \text{gp} \gg \text{factor}(3) \]

\[
\begin{align*}
\text{ex} \gg \text{factor}(1386) \\
\begin{bmatrix} 2 & 1 \\ 3 & 2 \\ 7 & 1 \\ 11 & 1 \\
\end{bmatrix} \\
\Rightarrow 1386 = 2 \times 3^2 \times 7 \times 11
\end{align*}
\]

9. It may be useful to check whether one polynomial divides another one (without remainder). The following test might be useful in a loop:

\[
\begin{align*}
\text{ex} \gg \text{p1} &= \text{Mod}(1,2) \times (x^{20} + 1) \\
\text{p2} &= \text{Mod}(42) \times (x^{21} + 1) \\
\text{p3} &= \text{Mod}(1,2) \times (x^{6} + x^{5} + x^{4} + x^{2} + 1) \\
\text{if} (\text{p1} \% \text{p3} == 0, \text{print}("p3|p1")) \\
\text{if} (\text{p2} \% \text{p3} == 0, \text{print}("p3|p2"))
\end{align*}
\]
Exercises

Use PARI. Show your log files.

1) Consider \( GF(2^m) \) for each \( m \in \{2, 3, \ldots, 8\} \). Give a list of the orders that are possible for the elements and the number of elements with that order.

2) Let \( p(x) \) be the generator polynomial for \( GF(32) \) that has the highest overall degree (i.e., if 2 polynomials have the same degree then compare them at the term with the next lowest degree. Ex: choose \( x^3 + x^2 + 1 \) over \( x^3 + x + 1 \)). Find the polynomial representation for:

   a) \( x^{10} \)
   b) \( x^{15} \)
   c) \( x^{21} \)
   d) \( x^{24} \)
   e) \( x^{29} \)
   f) \( x^{30} \)
3) Consider the minimum polynomials for the elements in GF(64), which are tabulated in Appendix B. Using your knowledge of the relationships between the properties of the elements (and their conjugates) and their minimum polynomials, identify which of the polynomials are not primitive.

Using PARI, find $M$ for each of the non-primitive polynomials such that the polynomial divides $X^m + 1$.

4) A $(255, k)$ code exists for every $1 \leq k \leq 255$. Discuss.

5) Does a $(511, k)$ code exist for every $1 \leq k \leq 511$? If not, give the 4 largest $k$ for which no binary cyclic code exists.
6) Design a new homework problem that is easier to solve using PARI than just by hand with tables. The problem should be substantially different than those I have given.