Finding the inverse of a polynomial in the finite field $\mathbb{Z}_p/(f(x))$:

Recall the algorithm from your earlier project or from the slides 8-12 of sec 2.3 to find gcd of two integers.

We write a table with 7 columns. In the first row, the first 4 numbers are always 1, 0, 0, 1 (in that order), while the 5th and 6th numbers are the two numbers for which one seeks the gcd, and the 7th is always zero. Now we choose 5th column a prime number (here 271) and so gcd will be 1.

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	271	192	0

Then we add a new row using the following rules:

- The new q is the greatest integer less than or equal to the quotient of the old u_3 and v_3.
- The new u_i is the old v_i.
- The new $v_i =$ old $u_i -$ (current q)(old v_i)
- We do this multiple times, until we produce a row where $v_3 = 0$

We get **Division Algorithm**:

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	271	192	0
0	1	1	-1	192	79	1
1	-2	-1	3	79	34	2
-2	5	3	-7	34	11	2
5	-17	-7	24	11	1	3
-17	*	24	*	1	0	11

Now $\gcd(271, 192) = 1$ and $(271)(-17) + (192)(24) = 1 \implies (192)^{-1} = 24$ in mod 271.

In order to find the inverse in a finite field, we need to repeat the above algorithm.

For example let us consider the finite filed $\mathbb{Z}_2/(f(x))$ where $f(x) = x^4 + x + 1$.

Suppose that $g(x) = x^3 + x^2 + 1$ which corresponds to the 4-bit 1101. In order to find the inverse of $g(x)$ in this field, we simply repeat above division algorithm starting with f(x) and g(x), but keep in mind that we are dealing with $\mathbb{Z}_2$ and so $-x^n$ is same as x^n and $2x^n = 0$.

Division Algorithm for Polynomials:

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	x^4+x+1	x^3+x^2+1	0
0	1	1	$x+1$	x^3+x^2+1	x^2	$x+1$
1	$x+1$	$x+1$	x^2	x^2	1	$x+1$
$*$	$*$	x^2	$*$	1	0	x^2

Therefore, the inverse of $g(x)$ is x^2. In other words, $(1101)^{-1} = 0100$.

Now let us consider the finite filed $\mathbb{Z}_2/(f(x))$ where $f(x) = x^8 + x^4 + x^3 + x + 1$.

Suppose that $g(x) = x^5 + x^4 + x + 1$. In order to find the inverse of $g(x)$ in this field, we again repeat above division algorithm starting with f(x) and g(x), but keep in mind that we are dealing with $\mathbb{Z}_2$ and so $-x^n$ is same as x^n and $2x^n = 0$.

Division Algorithm for Polynomials:

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	$x^8+x^4+x^3+x+1$	x^5+x^4+x+1	0
0	1	1	x^3+x^2+x+1	x^5+x^4+x+1	x^4+x^3+x	x^3+x^2+x+1
1	x	x^3+x^2+x+1	$x^4+x^3+x^2+x+1$	x^4+x^3+x	x^2+x+1	x
x	x^3+x+1	$x^4+x^3+x^2+x+1$	$x^6+x^5+x^3+x^2$	x^2+x+1	1	x^2+1
$*$	$*$	$x^6+x^5+x^3+x^2$	$*$	1	0	x^2+x+1

For example,

$$\begin{aligned} \text{3rd row } v_2 \; &= \; \text{2nd row } u_2 - (\text{ 3rd row } q)(\text{ 2nd row } v_2) \\ &= 1 - (x)(x^3+x^2+x+1) \\ &= 1 - x^4 - x^3 - x^2 - x \\ &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

Ultimately u_3 will become 1 and the inverse is the u_2 in the corresponding row. So

$$(x^5 + x^4 + x + 1)^{-1} = x^6 + x^5 + x^3 + x^2$$

Exercise: Show that in the above field:

$$(x^6 + x^4 + x + 1)^{-1} = x^7 + x^6 + x^3 + x$$

If you prefer to write a program to find the inverse, see next page.

If you would like to write a program to find the inverse, here is an algorithm:

Extended Euclidean Algorithm to find the inverse of a polynomial a(x) in the finite field $\mathbb{Z}_p/(f(x))$:

INPUT: A nonzero binary polynomial a of degree at most $m-1$.

OUTPUT: $a^{-1} \mod f$.

1. $u \leftarrow a$, $v \leftarrow f$.

2. $g_1 \leftarrow 1$, $g_2 \leftarrow 0$.

3. While $u \neq 1$ do
3.1. $j \leftarrow \deg(u) - \deg(v)$.
3.2. If $j < 0$ then: $u \leftrightarrow v$, $g_1 \leftrightarrow g_2$, $j \leftarrow -j$.
3.3. $u \leftarrow u + z^j v$.
3.4. $g_1 \leftarrow g_1 + z^j g_2$.

4. Return(g_1).

For Python or Perl version of algorithm see section 7.11 of this

lecture note.