Math 5405
Homework Assignment # 9

The irreducible polynomial:

$$f(x) = x^8 + x^4 + x^3 + x + 1 \pmod 2$$

is mentioned in Trappe-Washington. It may be used to construct:

$$\mathbb{F}_{2^8} = \mathbb{F}_2[x] \pmod{x^8 + x^4 + x^3 + x + 1}$$

via arithmetic of polynomials mod 2 and mod $f(x)$.

1. The polynomials,

$$1, x, x^2, x^4$$

are their own remainders mod $f(x)$, but:

$$x^8, x^{16}, x^{32}, x^{64}$$

are not equal to their remainders. Find the remainders.
(They are polynomials of degree < 8).

2. The group:

$$(\mathbb{F}_{2^8})^\times$$

is a cyclic group with $255 = 3 \cdot 5 \cdot 17$ elements.

(a) Find the order of x in this group. (Hint: it divides 255).

(b) Find a primitive element in the group.

3. Consider the elliptic curve (in the variables (w, y)):

$$y^2 + wy = w^3 + (x^3 + x) \pmod{\mathbb{F}_{2^8}}$$

where $x^3 + x \in \mathbb{F}_{2^8}$, and the point:

$$P = (1, x^4)$$

(a) Verify that P is a point of the elliptic curve.

(b) Find $2P$ and $4P$.