MATH 195: CRYPTOGRAPHY
HOMEWORK #9

Problem F5. *Verify that*

$$X^8 + X^4 + X^3 + X + 1$$

is irreducible in $\mathbb{F}_2[X]$.

Problem F6. *Put* $f = X^8 + X^4 + X^3 + X + 1 \in \mathbb{F}_2[X]$, *and let*

$$a = 00001100 = X^3 + X^2 \in \mathbb{F}_2[X]/(f).$$

Compute a^5. *Can you find an explicit embedding of*

$$\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$$

as a subfield in $\mathbb{F}_2[X]/(f)$*?*

Problem F7. *Let* p *be prime. Prove that in* $\mathbb{F}_p[X]/(X^p - X - 1)$ *one has*

$$X^{p^i} = X + (i \bmod p) = \underbrace{00\ldots00}_{p-2}1(i \bmod p)$$

for i *any positive integer. Deduce that* $X^p - X - 1$ *is irreducible in* $\mathbb{F}_p[X]$.

Date: April 2, 2002.

F5, F6, F7.