MATH 195: CRYPTOGRAPHY
HOMEWORK #8

Problem F1. *We let*

$$a_n(p) = \{a_n(p) = \#\{f \in \mathbb{F}_p[X] : \deg f = n, f \text{ monic irreducible}\}.$$

In class it was shown that $a_2(p) = (p^2 - p)/2$. *Prove in the same way that* $a_3(p) = (p^3 - p)/3$.

Problem F2. *Find all monic irreducible polynomials of degree* 2 *in* $\mathbb{F}_3[X]$ *and of degree* 4 *in* $\mathbb{F}_2[X]$.

Problem F3. *Compute* $a_n(2)$ *for* $n = 1, \ldots, 10$.

Problem F4. *Prove that* $X^3 - X - 1$ *is irreducible in* $\mathbb{F}_3[X]$ *and deduce that*

$$\mathbb{F}_3[X]/(X^3 - X - 1)$$

is a field. Recall that we define

$$\mathbb{F}_p[X]/(f(X))$$

to be the set of polynomials of degree $< \deg f$ *in* $\mathbb{F}_p[X]$ *with the usual addition and multiplication after taking the remainder on division by* $f(X)$.

Compute the inverse of X^2 *and of* $X^2 + 1$ *in* $\mathbb{F}_3[X]/(X^3 - X - 1)$.

Date: March 19, 2002.
F1, F2, F3, F4; Updated Friday, March 15, 2002.