Math 335 HW 4 - Due Feb. 27, 2004

1. Problem 2.20, pg. 72 of the text
2. (a) Prove or disprove: $x^3 + x + 2$ is irreducible in $\mathbb{Z}_3[x]$.
   (b) Find $(x^2 + x + 3, x^3 + x^2 + x + 1)$ in $\mathbb{Z}_5[x]$.
   (c) What is the multiplicative inverse of $x^2 + x + 1$ in $\mathbb{Z}_3[x]/(x^3 + 2x^2 + x + 1)$?
3. Consider the following proposed cryptosystem. $\mathcal{P}$ is $\{0, 1, \ldots, 6\}$. Both $\mathcal{C}$ and $\mathcal{K}$ are the non-zero elements of $\mathbb{Z}_2[x]/(x^3 + x^2 + 1)$. The encryption rule is

   $$e_k(x) = k^x.$$

   (By definition, $k^0 = 1$ for any k.)

   Give an example of a key such that this is a valid encryption method. Give an example of a key such that this is NOT a valid encryption method. What happens if we allow 7 in $\mathcal{P}$?
4. Using only the axioms for a field, prove each of the following for a field F.
   (a) If $a, b \in F$ and $ab = 0$, then either $a = 0$ or $b = 0$.
   (b) If $a, b, c \in F, a \neq 0$ and $ab = ac$, then $b = c$.
   (c) The *characteristic* of F is the smallest integer n such that

   $$\underbrace{1 + 1 + \cdots + 1}_{n} = 0.$$

   If there is no such n, then the characteristic of F is zero. Show that the characteristic of F is either zero or a prime.
5. For this exercise we use the following cryptosystem. English plaintext is first translated to $\{1 \ldots 26\}$. Then this number is written in the form $a_2 \cdot 3^2 + a_1 \cdot 3 + a_0$ where each a_i is 0, 1 or 2. For instance, $S \to 19 \to 2 \cdot 3^2 + 0 \cdot 3 + 1$. This expression is now written as a polynomial in $\mathbb{Z}_3[x]$ by replacing 3 with x. So, $S \to 2x^2 + 1$. The key is a monic irreducible polynomial in $\mathbb{Z}_3[x]$ of degree 3 and constant term 2. Call the key $f(x)$. The next step is to write the multiplicative inverse of the previously obtained polynomial in $\mathbb{Z}_3[x]/(f(x))$. Finally, replace x with 3 to obtain an integer in $\{1 \ldots 26\}$. Notice that this is a simple substitution cipher.

   Decrypt the following short message:

   9 10 16 22.