Peter Cholak and Juan Migliore Math 222 Friday, March 30, 2001
Quiz 5

Be sure to carefully write up your answers. It is suggested that you first write out a draft of your proposed questions and then carefully rewrite that draft to get your final version. You do *not* have to write the answers on this sheet of paper.

Let F be a field. Show that there exist $a, b \in F$ such that $x^2 + 2$ is a divisor of $x^{43} + ax + b$. (Hint: consider the form of the remainder $r(x)$ when x^{43} is divided by $x^2 + 2$. Do not do the actual division. The degree of $r(x)$ is ??)

We can write $x^{43} = q(x)(x^2 + 2) + r(x)$ such that $q(x), r(x) \in F[x]$ and $0 \leq \deg r(x) \leq 1$. So $r(x) = cx + d$ for some $c, d \in F$. Take $a = -c$ and $b = -d$, we get $x^{43} + ax + b = x^{43} - cx - d = q(x)(x^2 + 2)$, which is divided by $x^2 + 2$.

Factor $x^3 + 3x + 1$ over $\mathbb{Z}_5$ into irreducible factors.

By a direct calculation, we see that $x = 1$ and $x = 2$ are solutions of the equation $x^3 + 3x + 1$ mod 5. Dividing $x^3 + 3x + 1$ by $(x - 1)(x - 2)$, we get the quotient $x - 2$. So $x^3 + 3x + 1 = (x - 1)(x - 2)^2$.

Consider the Galois Field $F = GF(3, x^2 + x + 2)$. Let α be the associated Galois imaginary.

(a) Show that α is a primitive element in F. Work out the corresponding cyclic table of F.

(b) Find the inverse of each nonzero element in F. *Hint:* Use part (a).

(c) By definition α is one solution to $x^2 + x + 2 = 0$ over $\mathbb{Z}_3$. There should of course be another solution. It is also an element of F. Find this element. Is it a power of α? *Hint:* Use long division or try the other possibilities.

(a) $\alpha^2 = 2\alpha + 1$, $\alpha^3 = 2\alpha + 2$, $\alpha^4 = 2$, $\alpha^5 = 2\alpha$, $\alpha^6 = \alpha + 2$, $\alpha^7 = \alpha + 1$ and $\alpha^8 = 1$. The order of α is 8. Since α is a primitive element in F, the corresponding cyclic table of F is as follows:

$$\begin{aligned} \alpha^1 &= \alpha \\ \alpha^2 &= 2\alpha + 1 \\ \alpha^3 &= 2\alpha + 2 \\ \alpha^4 &= 2 \\ \alpha^5 &= 2\alpha \\ \alpha^6 &= \alpha + 2 \\ \alpha^7 &= \alpha + 1 \\ \alpha^8 &= 1 \end{aligned} \tag{1}$$

(b) We have $(\alpha^h)^{-1} = \alpha^{-h} = \alpha^{8-h}$ for any integer h. So $\alpha^{-1} = \alpha + 1$, $(2\alpha + 1)^{-1} = \alpha + 2$, $(2\alpha + 2)^{-1} = 2\alpha$, $2^{-1} = 2$, $(2\alpha)^{-1} = 2\alpha + 2$, $(\alpha + 2)^{-1} + 2\alpha + 1$, $\alpha + 1)^{-1} = \alpha$ and $1^{-1} = 1$.