Math 114 Professor K. A. Ribet

Midterm Exam February 19, 2004

This exam was an 80-minute exam. It began at 3:40PM. There were 4 problems, for which the point counts were 6, 8, 9 and 7. The maximum possible score was 30.

Please put away all books, calculators, electronic games, cell phones, pagers, .mp3 players, PDAs, and other electronic devices. You may refer to a single 2-sided sheet of notes. Please write your name on each sheet of paper that you turn in; don't trust staples to keep your papers together. Explain your answers in full English sentences as is customary and appropriate. Your paper is your ambassador when it is graded.

1. *Let n be a positive integer and let p be a prime number. Suppose that x is an integer with $\gcd(x, n) = 1$. Show that there is an integer y such that $\gcd(y, pn) = 1$ and such that $y \equiv x$ mod n.*

In class, we discussed the surjectivity of the natural map $(\mathbf{Z}/n\mathbf{Z})^* \to (\mathbf{Z}/d\mathbf{Z})^*$ when d is a divisor of n. This took most of a period(!); it was related to a homework problem. With mildly different notation, you have to prove surjectivity of the map $(\mathbf{Z}/nm\mathbf{Z})^* \to (\mathbf{Z}/n\mathbf{Z})^*$ when $n, m \geq 1$. In class, I did this in an ugly way by writing out the prime factorizations of n and m. A nicer technique would have been to note that, by induction, if you can do this for m prime, you can do it for all m. The problem at hand is about the case where $m = p$ is prime.

In this situation, two things can happen. The first is where p is a divisor of n. In that case, x is prime to pn because it is prime to n and we take simply $y = x$. The more interesting situation is that where p does not divide n. Then using the Chinese Remainder Theorem, we can find y so that y is congruent to x mod n and y is congruent to 1 (or some other unit that we might like better) mod p. This y fits the bill.

Students have come up with the following efficient way of doing the problem: Start with x, n and p as in the problem. If $\gcd(x, pn) = 1$, choose $y = x$. Otherwise, x has a common factor with np. The only possibility is that p divides x, but note that p cannot then divide n because $\gcd(x, n) = 1$. We set $y = x + n$, and this choice works. Indeed, y is clearly congruent to x mod n. Also, p cannot divide y because it divides x but not n.

Find such a y if $n = 15$, $p = 7$ and $x = 7$.

My purpose is asking you about this example was to get you to think about the abstract problem in a concrete situation. The point is that we can't take $y = x$ because x is not prime to p. We have to take a y that is congruent to 7 mod 15 and is prime to 7. We could certainly take $y = 22$.

2. *Let p be a prime number. Prove that the polynomial*

$$1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^p}{p!}$$

is irreducible over $\mathbf{Q}$.

The presence of a prime number in the problem suggests that we might want to use Eisenstein's criterion. Multiply the polynomial by $p!$ to get a monic polynomial with integer coefficients. The coefficients of the resulting polynomial are 1, p, $p(p-1)$, and so on; the constant coefficient is $p!$. Eisenstein's criterion applies beautifully; note that $p!$ is divisible by p but not by p^2.

Prove that $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbf{Z}/2\mathbf{Z}$ (the field of integers mod 2) and that $1234567x^4 - 98765x^3 + 357x^2 - x + 17$ is irreducible over $\mathbf{Q}$.

The polynomial $x^4 + x^3 + x^2 + x + 1$ has no root in $\mathbf{Z}/2\mathbf{Z}$: plug in 0 or 1 and you get 1 as the value. This does not imply that the polynomial is irreducible; it could plausibly factor as a product of two irreducible quadratics. In fact, the only irreducible quadratic over $\mathbf{Z}/2\mathbf{Z}$ is $x^2 + x + 1$; all others have 0 or 1 as a root. The only possible factorization, then is $x^4 + x^3 + x^2 + x + 1 = (x^2 + x + 1)^2$. However, when $2 = 0$, the square of a sum is the sum of the squares, so $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, which is not $x^4 + x^3 + x^2 + x + 1$. We conclude that $x^4 + x^3 + x^2 + x + 1$ is indeed irreducible over $\mathbf{Z}/2\mathbf{Z}$. The statement about $1234567x^4 - 98765x^3 + 357x^2 - x + 17$ follows when you combine two facts. The first is that a polynomial over $\mathbf{Z}$ factors over $\mathbf{Z}$ if it factors over $\mathbf{Q}$; this is Gauss's lemma. The second is that a polynomial that factors over $\mathbf{Z}$ factors over $\mathbf{Z}/p\mathbf{Z}$ for every p; this is completely obvious. Thus a polynomial over $\mathbf{Z}$ is irreducible if there is a prime modulo which it is irreducible. We mentioned this in class several times, and now here it is on an exam.

3. *Let $\alpha \approx -2.9196$ be the real root of the polynomial $f(x) := x^3 + 2x^2 - 2x + 2$. Write $\dfrac{1}{\alpha + 3}$ as a polynomial in α.*

There are presumably several ways to do this problem. Here's how I did it while we were setting in the exam room. If $\delta = \alpha + 3$, then $f(\delta - 3) = 0$. If you plug $\delta - 3$ in to f and expand, you get that $0 = \delta^3 - 7\delta^2 + 13\delta - 1$, so that $1/\delta = \delta^2 - 7\delta + 13$. If you remember that $\delta = \alpha + 3$ and you expand, you get that $1/\delta = \alpha^2 - \alpha + 1$.

Let β be a complex root of the polynomial $f(x - 7) = x^3 - 19x^2 + 117x - 229$. Show that the fields $\mathbf{Q}(\alpha)$ and $\mathbf{Q}(\beta)$ are isomorphic.

Let $\gamma = \beta + 7$. Then γ and α are roots of the same polynomial, namely f. This polynomial is irreducible by Eisenstein's criterion. Hence $\mathbf{Q}(\alpha)$ and $\mathbf{Q}(\gamma)$ are isomorphic to each other; each is isomorphic to $\mathbf{Q}[x]/(f(x))$. On the other hand, the fields $\mathbf{Q}(\beta)$ and $\mathbf{Q}(\gamma)$ are visibly equal. Hence $\mathbf{Q}(\beta)$ and $\mathbf{Q}(\alpha)$ are isomorphic.

4. *For the cubic polynomial $y^3 + py + q = 0$, Cardano's formula reads*

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

When $p = -1$ and $q = 0$, the polynomial is $y^3 - y$, which you can solve without the formula (I hope!). Exhibit choices of roots in the formula that lead to the three values -1, 0 and $+1$ for the expression

$$\sqrt[3]{\sqrt{\frac{-1}{27}}} + \sqrt[3]{-\sqrt{\frac{-1}{27}}}.$$

Cardano tells us that every root of $y^3 - y$ may be written in the form $\sqrt[3]{\sqrt{\frac{-1}{27}}} + \sqrt[3]{-\sqrt{\frac{-1}{27}}}$. Thus each of 0, 1 and -1 may be written in this form. The question is to explain how this is possible. First of all, in the formula, the quantities $\sqrt{\frac{-1}{27}}$ and $-\sqrt{\frac{-1}{27}}$ are supposed to represent the two different square roots of $-1/27$. There is no way to distinguish between them. The two square roots are $\pm\frac{i}{3\sqrt{3}}$. When we take the cube roots of these numbers, we get $\frac{1}{\sqrt{3}}$ times the cube roots of $\pm i$. One cube root of $-i$ is clearly i. The others are $i\frac{-1 \pm i\sqrt{3}}{2} = \frac{\mp\sqrt{3} + i}{2}$. One cube root of i is $-i$. The others are $\frac{\mp\sqrt{3} - i}{2}$. Now we are in good shape. We can take the cube roots of $\pm\frac{i}{3\sqrt{3}}$ to be $\frac{-i}{\sqrt{3}}$ and $\frac{+i}{\sqrt{3}}$, which sum to 0. We can take the cube roots to be $\frac{-\sqrt{3} + i}{2\sqrt{3}}$ and $\frac{-\sqrt{3} - i}{2\sqrt{3}}$, which sum to -1. Finally, if we take the cube roots to be $\frac{\sqrt{3} + i}{2\sqrt{3}}$ and $\frac{\sqrt{3} - i}{2\sqrt{3}}$, their sum will be 1.