189-235A: Basic Algebra I

Solutions for the Midterm Exam

1. Let $(u_n)_{n\geq 0}$ be the sequence of real numbers defined recursively by the rule

$$u_0 = 0, \quad u_{n+1} = 2u_n + 1.$$

Show that $u_n = 2^n - 1$ for all $n \geq 0$.
This question was a straight application of induction. Most of you were able to do it correctly.

2. Compute the greatest common divisor of 121 and 77 and express the result as a linear combination of 121 and 77.
Apply the gcd algorithm as explained in class; one finds this greatest common divisor is $11 = 2 \cdot 121 - 3 \cdot 77$.

3. Solve the congruence equation $6x \equiv 10 \pmod{14}$.
There are **two** *distinct solutions to this equation in* $\mathbf{Z}_{14}$*, namely* $x = 4$ *and* $x = 11$*. Most people who lost points on this one did so by only listing one of the solutions.*

4. Show that if $p \in \mathbf{Z}$ is a prime, then the ring $\mathbf{Z}_p$ of congruence classes modulo p is a field.
This proof was done in class: given $[a] \neq 0$ *in* $\mathbf{Z}_p$*, one may consider the* gcd *of the integers* a *and* p*. This gcd divides* p*, so it is either* 1 *or* p*; but it can't be* p *since* a *is not divisible by* p *(because* $[a] \neq 0$*) so* $\gcd(a, p) = 1$*. Now, writing the* gcd *as a linear combination of* a *and* p*, we get* $1 = au + pv$ *for some integers* u *and* v*. The corresponding equation in* $\mathbf{Z}_p$ *becomes* $[1] = [a][u]$*. Hence* $[a]$ *is invertible in* $\mathbf{Z}_p$*, therefore* $\mathbf{Z}_p$ *is a field.*

5. Give an example of two finite rings R_1 and R_2 which have the same cardinality but are not isomorphic. (You should justify your assertion.)
There were two possible solutions here that I came across most often. The first was to take a prime p *and consider the rings* $R_1 = \mathbf{Z}_p \times \mathbf{Z}_p$*, and the*

ring $R_2 = \mathbf{Z}_{p^2}$. These rings are non-isomorphic, because (for example) R_2 contains a non-zero solution of the equation $x^2 = 0$, namely, $[p]$, while R_1 does not—yet an isomorphism from R_2 to R_1 would have to carry a solution to such an equation to a solution of the corresponding equation in R_1. One could also reason on the number of solutions to the equation $px = 0$ (there are p^2 such solutions in R_1, and only p in R_2) or of the equation $x^2 = 1$ (which has four solutions in R_1, and only two solutions in R_2.)

A second solution was to take $R_1 = M_2(\mathbf{Z}_n)$, and $R_2 = \mathbf{Z}_n \times \mathbf{Z}_n \times \mathbf{Z}_n \times \mathbf{Z}_n$, for n and integer > 1. The most immediate way to see that these two rings are not isomorphic is to note that the matrix ring R_1 is not commutative, while R_2 is.

Now that we've seen more about quotient rings, one could also take as a third possible solution, R_1 to be one of the "new" finite fields that we saw in class, having 4 or 8 or p^2 elements, say, and take R_2 to be any ring of the same cardinality that is not a field. I leave you to work out the details...

6. Show that the ring $\mathbf{C}$ of complex numbers is *not* isomorphic to the Cartesian product $\mathbf{R} \times \mathbf{R}$ of the real numbers with itself.

Alot of people lost points on this question by writing down the first bijection f from $\mathbf{C}$ to $\mathbf{R} \times \mathbf{R}$ that came to mind—typically this was $f(a + bi) = (a, b)$—and showing that this function is not a homomorphism because it does not respect the multiplication on $\mathbf{C}$. This is not enough of course (how do you know that $f(a+bi) = (b, a)$, or $f(a+bi) = (a+17b, 3a-187b)$, or any of another myriad functions you could write down, might not be an isomorphism? The key to the solution was to reason as in the previous problem, by finding a ring-theoretic feature of $\mathbf{C}$ that is not shared by $\mathbf{R} \times \mathbf{R}$. There are various ways to do this, here are a few: (1) by noting that every non-zero element of $\mathbf{C}$ is invertible, so that $\mathbf{C}$ is a field, while the same is not true of $\mathbf{R} \times \mathbf{R}$ (try inverting $(0, 1)$, or $(1, 0)$!); (2) focussing on the equation $x^2 + 1 = 0$, which has two solutions in $\mathbf{C}$, but none in $\mathbf{R} \times \mathbf{R}$; (3) by noting that $\mathbf{R} \times \mathbf{R}$ has (infinitely many) zero divisors, while $\mathbf{C}$ has none; (4) by noting that the equation $x^2 - 1$ has two solutions in $\mathbf{C}$, but 4 solutions in $\mathbf{R} \times \mathbf{R}$; and so on and so forth.

The next two problems are Bonus Questions

7. Let f be a polynomial in $\mathbf{Z}[x]$ of degree d and let $p \in \mathbf{Z}$ be a prime

number. Show that the set

$$S = \{n \in \mathbf{Z} \text{ such that } p \text{ divides } f(n)\}$$

is the union of at most d congruence classes modulo p.
Mea culpa! There was a mistake in the wording of this question, which I corrected during the writing of the exam. Of course one had to assume that f is not divisible by p, so that the natural image $\bar{f}$ of f in the ring $\mathbf{Z}_p[x]$ is a non-zero polynomial; its degree, of course, is then ≥ 0 and less than or equal to d. Therefore $\bar{f}$ has at most d roots in $\mathbf{Z}_p$, since $\mathbf{Z}_p$ is a field. (Here is where we use the serious theorem, that a non-zero polynomial of degree d with coefficients in a field F has at most d roots in F.) Each of the roots of $\bar{f}$ is a congruence class modulo p, and the set S is (by definition) the union of these classes, of which there are at most d.

8. Let $p = 2m + 1$ be an odd prime. Show that

$$1^1 \cdot 2^2 \cdot 3^3 \cdots (p-1)^{p-1} \equiv (-1)^{[m/2]} m! \pmod{p}.$$

The idea is to write the expression on the left—a product of $2m$ terms, viewed as an element in $\mathbf{Z}_p$—by grouping together the j-th and the $(p-j)$-th term. Together they give a contribution to the product of

$$j^j (p-j)^{p-j} = j^j (-j)^{p-j} = (-1)^{p-j} j^p = -(-1)^j j,$$

where we've used Fermat's Little theorem to get the last equality. Hence our expression is equal to the product of the terms $-(-1)^j j$, as $j = 1, 2, \ldots, m$. The product of signs gives $(-1)^{[m/2]}$, and the product of the j's from 1 to m is of course just $m!$ (m-factorial).