Harbourne M310 Spring 2006 Friday December 15, 2006

Final Exam: Name: Solutions

Instructions: Show all of your work and clearly explain your answers. No books or written notes are allowed during the exam. You may use a calculator. Do any 8 of the 9 problems. If you show work for all 9 problems, clearly cross out the problem you do not want graded. Each problem is worth 25 points, for a total of 200 points.

[1] Prove that there are infinitely many positive integers which are prime numbers.

See p. 55 of the text.

[2] Let n be a positive integer. Prove that $3|n$ if and only if 3 divides the sum of the base 10 digits of n. [Be sure to prove both directions! And give a complete proof; no fair using the trick for divisibility by 9, for example, unless you prove it too.]

See p. 69 of the text.

[3] Use Cardano's method to find a solution to the equation $x^3 - 9x - 12 = 0$. Show every step; find an exact solution.

Recall the identity $(a+b)^3 - 3ab(a^2+b^2) - (a^3+b^3)$. Thus $x = a+b$ is a solution if we can find a and b such that both $-9 = -3ab$ and $-12 = -(a^3+b^3)$. So we just solve these simultaneously: $b = 3/a$ so $12 = a^3 + 27/a^3$, hence $(a^3)^2 - 12(a^3) + 27 = 0$. This is a quadratic equation in a^3, so $a^3 = (12 \pm \sqrt{144 - 4*27})/2$, or, picking a sign, $a = (12 + \sqrt{144 - 4*27})/2)^{1/3} = (12 + \sqrt{36})/2)^{1/3} = 9^{1/3} = 3^{2/3}$. Now $b = 3/a = 3^{1/3}$, so $x = a + b = 3^{2/3} + 3^{1/3}$ is a solution.

[4] Finish each definition. (Note: the R in part (a) has nothing to do with the R in part (c).)

(a) Define the *additive identity* of a ring R. The additive identity of a ring R is that element $r \in R$ such that: $r + a = a$ for every element $a \in R$.

(b) Define the *least common multiple* of positive integers m and n. The least common multiple of m and n is that integer L such that: $0 < L$, $m|L$, $n|L$ and if C is any positive common multiple of m and n, then $L \leq C$.

(c) Define what a *relation* R on a nonempty set S is, and what it means for R to be an *equivalence relation*.
(i) A relation R on S is: a subset of $S \times S$.
(i) We say the relation R is an equivalence relation if: R is reflexive, symmetric and transitive.

(d) Let F be a field. Define what an irreducible polynomial in $F[x]$ is. A polynomial $f(x) \in F[x]$ is said to be irreducible in $F[x]$ if: f has positive degree and whenever f divides a product gh of polynomials, then either f divides g or f divides h. [Alternatively, f is irreducible in $F[x]$ if f has positive degree but has no positive degree factors of degree smaller than the degree of f itself.]

(e) Define what a *field* is. A ring F is said to be a field if: F is commutative, $1 \neq 0$ and every nonzero element is a unit.

[5] Use Euclid's algorithm both to find the gcd of 1610 and 1561 and to solve $1610x + 1561y = \gcd(1610, 1561)$ for x and y. (For full credit, your answer for x and y must be the one that Euclid's algorithm gives.)

Answer: $1610 = 1*1561 + 49$, $1561 = 31*49 + 42$, $49 = 1*42 + 7$, $42 = 6*7 + 0$, so $\gcd(1610, 1561) = 7$. If we take $n = 1610$ and $m = 1561$, this gives $n - m = 49$, $m - 31(n-m) = 42$ or $-31n + 32m = 42$, and $(n-m) - (-31n + 32m) = 7$ so $32*n - 33*m = 7$.

[6] Consider a function $h : R \to S$ of rings.

(a) Finish the definition: the function h is a ring homomorphism if: $h(1) = 1$, and $h(a+b) = h(a) + h(b)$ and $h(ab) = h(a)h(b)$ for all elements $a, b \in R$.

(b) Give an example of rings R and S and a homomorphism $h : R \to S$ which is surjective but not injective. Justify your answer.

Answer: $h : \mathbf{Z}/4\mathbf{Z}$ mapping to $\mathbf{Z}/2\mathbf{Z}$ by $h([m]_4) = [m]_2$. This is well-defined since $2|4$, surjective since $h([0]_4) = [0]_2$ and $h([1]_4) = [1]_2$, but not injective, since $h([0]_4) = h([2]_4)$.

(c) Give an example of rings R and S and a homomorphism $h : R \to S$ which is injective but not surjective. Justify your answer.

Answer: Let $h : \mathbf{Z} \to \mathbf{Q}$ be the inclusion of the integers in the rationals.

(d) Give an example of rings R and S and an isomorphism $h : R \to S$ which is not the identity (i.e., such that either R is not S or if $R = S$, then such that h is not just $h(x) = x$ for all $x \in R$). Justify your answer.

Answer: By the Chinese Remainder Theorem, we have an isomorphism $h : \mathbf{Z}/6\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ given by $h([m]_6) = ([m]_2, [m]_3)$.

[7] Find a single digit base 10 number congruent to 2007^{2006} modulo 10. Explain all of your steps (it is not enough to just get a calculator based answer, although it is OK to use your calculator to check your answer).

Answer: First, $\phi(10) = \phi(2)\phi(5) = 1 * 4 = 4$, and $2006 \equiv 2 \pmod 4$, so $2007^{2006} \equiv 7^{4*501+2} = 7^{4^{501}}7^2 \equiv 1^{501}7^2 \equiv 7^2 \equiv 9 \pmod{10}$. A couple of you noticed a much easier solution: $2007^{2006} \equiv (7^2)^{1003} \equiv (-1)^{1003} \equiv -1 \equiv 9 \pmod{10}$.

[8]
(a) Find $[7]_{39}^{-1}$ in $\mathbf{Z}/39\mathbf{Z}$. Justify your answer.

Answer: $7 * (-11) = -77 = 1 - 2 * 39 \equiv 1 \pmod{10}$, so $[7]_{39}^{-1} = [-11]_{39} = [28]_{39}$.

(b) Give an example of an n such that $[7]_n^{-1}$ does not exist in $\mathbf{Z}/n\mathbf{Z}$. Justify your answer.

Answer: Take any n which is a multiple of $7|n$, say $n = 14$, or even $n = 7$. Then $[7]_n$ is either 0 or a 0-divisor, and hence not a unit.

[9] In each case, determine if the given polynomial is irreducible in the given ring. Justify your answers.
(a) $x^7 - ix + 1$ in $\mathbf{C}[x]$ is not irreducible, since the only irreducible polynomials in $\mathbf{C}[x]$ are the polynomials of degree 1.
(b) $x^8 + x^2 + 1$ in $\mathbf{R}[x]$ is not irreducible, since an irreducible polynomial in $\mathbf{R}[x]$ always has degree 1 or 2.
(c) $x^2 + 3x + 1$ in $\mathbf{R}[x]$ is not irreducible, since $x - a$ divides $x^2 + 3x + 1$, where a is a real root of $x^2 + 3x + 1$, such as $a = (-3 + \sqrt{5})/2$.
(d) $x^2 + 3x + 1$ in $\mathbf{Q}[x]$ is irreducible, since it has degree 2 but has no rational roots (the roots are $(-3 \pm \sqrt{5})/2$, neither of which is rational).
(e) $x^2 + 3x + 1$ in $(\mathbf{Z}/7\mathbf{Z})[x]$ is irreducible, since it has degree 2 but no roots in $\mathbf{Z}/7\mathbf{Z}$.