Math 104A: Fall 2012
Midterm 1 Solutions and Comments

Instructions: Please write your name on your blue book. Make it clear in your blue book what problem you are working on. Write legibly. This exam is graded out of 100 points. Following these instructions is worth 5 points.

Problem 1: [5+5 points] Let R be a ring. (a) Carefully state what it means for R to be a "domain" and (b) give an example with justification of a ring which is not a domain.

(a) R is a domain if and only if for all $a, b \in R - \{0\}$ we have $ab \neq 0$.

Comments: There were many students who got this definition wrong. Precision is of paramount importance for understanding mathematical definitions.

(b) Let $R = \mathbb{Z} \times \mathbb{Z}$. Then $(0,1), (1,0)$ are nonzero elements of R, but $(1,0)(0,1) = (0,0)$ in R.

Comments: $\mathbb{Z} \times \mathbb{Z}$ was the most common example given. Some students also gave examples involving rings like $\mathbb{Z}_4$, which were fine, although we have yet to cover them in class. (However, $\mathbb{Z}_n$ is not a correct response; this *is* a domain for n prime.)

Problem 2: [15 points] Prove that $\log_3(7)$ is not a rational number.

Suppose $\log_3(7)$ were a rational number. Then there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $\log_3(7) = \frac{a}{b}$. This implies that $3^{\frac{a}{b}} = 7$, or $3^a = 7^b$. By the unique prime factorization theorem for $\mathbb{Z}$, this implies that $a = b = 0$, which is a contradiction.

Comments: This problem appeared on the homework. There were a variety of issues here. Many students did not say *why* the equality $3^a = 7^b$ implies that $a = b = 0$. There is a very, very important theorem which implies this; in a mathematical proof, such key points must be stated. There were also problems with clarity in proof writing here and throughout. Imagine reading your proof aloud to a fellow student; if they cannot follow what you're saying, there's probably a problem.

Problem 3: [15 points] Let $\mathbb{Z}^2 = \{(x, y) : x, y \in \mathbb{Z}\}$ be the integer lattice in the Euclidean plane $\mathbb{R}^2$. Let ℓ_1 and ℓ_2 be the lines with equations $30x + 12y = 9$ and $30x + 12y = 42$. Does ℓ_1 contain any points in $\mathbb{Z}^2$? Does ℓ_2? Justify your answers.

We have that $(30, 12) = 6$. We proved in class that for any $a, b, c \in \mathbb{Z}$, the equation $ax+by = c$ has solutions with $x, y \in \mathbb{Z}$ if and only if $(a, b)|c$. Since $6 \nmid 9$ but $6|42$, we conclude that ℓ_1 does not contain any points in $\mathbb{Z}^2$, but ℓ_2 does.

Comments: Most students got the right idea here. Some used different solution methods, which is fine, but it is very important to understand the reasoning in the solution presented here; linear Diophantine equations in two variables will play a key role for the rest of the quarter.

Problem 4: [10 + 10 points] Let $a, b \in \mathbb{Z}$ be given by $a = 210$ and $b = 45$. (a) Find the greatest common divisor (a, b) and (b) express (a, b) as a linear combination of a and b with integer coefficients.

(a) We apply the Euclidean Algorithm to $(210, 45)$ to get

$$\begin{aligned} 210 &= 4(45) + 30 \\ 45 &= 1(30) + 15. \\ 30 &= 2(15) + 0. \end{aligned}$$

We conclude that $(210, 45) = (15, 0) = 15$.

Comments: Most students got this right.

(b) Reversing the Euclidean Algorithm yields $15 = 45 - 1(30) = 45 - 1(210 - 4(45)) = (-1)(210) + (5)(45)$.

Comments: Most students did well here, too.

Problem 5: [5+15 points] Let D be a domain. (a) Carefully state what it means for D to be a "unique factorization domain (UFD)" (you may take the notions of 'prime' and 'associate' for granted). (b) Let $\mathbb{Z}[2i] = \{a + 2ib : a, b \in \mathbb{Z}\}$. You may assume without proof that $\mathbb{Z}[2i]$ is a domain. Prove that $\mathbb{Z}[2i]$ is *not* a UFD. (Hint: 4.)

(a) D is a UFD if for all $a \in D$ such that a is not zero or a unit, there exist primes $p_1, \ldots, p_r \in D$ such that $a = p_1 \cdots p_r$ and, moreover, if $q_1, \ldots, q_s \in D$ are prime and $a = q_1 \cdots q_s$, then $r = s$ and there exists a reordering of the q_i such that q_i and p_i are associate for $1 \leq i \leq r$.

Comments: There were many problems here. Some students did not state any uniqueness conditions whatsoever. Most students did not stipulate that a cannot be zero. Some students didn't write a definition at all; there was some sort of a 'proof' that some domain is a UFD. Make sure that you understand what questions are asking you to do and, again, be very precise in recapitulating a definition.

Within $\mathbb{Z}[2i]$ we have $4 = (2)(2) = (2i)(-2i)$. We claim that these are distinct factorizations into primes. Indeed, $\frac{\pm 2i}{2} = \pm i \notin \mathbb{Z}[2i]$, so the elements 2 and $\pm 2i$ are not associate in $\mathbb{Z}[2i]$. It remains to show that $2, \pm 2i$ are prime in $\mathbb{Z}[2i]$. To do this, let $N : \mathbb{Z}[2i] \to \mathbb{Z}$ be the function $N(a + 2bi) = a^2 + 4b^2$. Since N is the restriction of the square of the Euclidean distance function on $\mathbb{C}$, we have that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[2i]$ Since $N(2) = N(2i) = N(-2i) = 4$, by uniqueness of prime factorization, if $\alpha \in \{2, \pm 2i\}$ satisfied $\alpha = \beta\gamma$ for $\beta, \gamma \in \mathbb{Z}[2i]$, then $N(\beta), N(\gamma) \in \{1, 2, 4\}$. However, for $a, b \in \mathbb{Z}$, $a^2 + 4b^2 \neq 2$, so without loss of generality we may assume that $N(\beta) = 1$ and $N(\gamma) = 4$.

But since $\beta \in \mathbb{Z}[2i]$ this forces $\beta = \pm 1$, so β is a unit. This implies that α is prime. Since we have exhibited two distinct prime factorizations of 4, we conclude that $\mathbb{Z}[2i]$ is not a UFD.

Comments: This problem also proved challenging. There were some students who thought that $4 = (2)(2) = (4)(1)$ counted as two distinct prime factorizations of 4. This isn't so because 4 isn't prime. There were other students who tried applying a Euclidean algorithm for $\mathbb{Z}[2i]$; since $\mathbb{Z}[2i]$ isn't a UFD, it certainly isn't Euclidean. Among the students who discovered two different prime factorizations for 4 (or, for a few students, 8), there was an overall lack of understanding that it must be shown that (i) these factorizations are factorizations into primes, and (ii) these primes are not associates. Finally, there was an overall lack of clarity in these proofs. If something is difficult for me to follow, it's hard to justify awarding very many points.

Problem 6: [15 points] Recall that for $n \in \mathbb{Z}^+$, $n! := n(n-1)(n-2)\cdots 1$. How many zeros are there at the end of the decimal expansion of $(100!)$?

Let the prime factorization of 100! be $2^a 5^b p_1^{c_1} \cdots p_n^{c_n}$, where $p_1, \ldots, p_n$ are primes other than 2 or 5. The number of zeros in question equals the minimum of a and b. We have that $a = 50 + 25 + 12 + 6 + 3 + 1$ (coming from the integers between 1 and 100 divisible by $2, 4, 8, 16, 32$, and 64) and $b = 20 + 4$ (coming from the integers between 1 and 100 divisible by 5 and 25). We conclude that there are $b = 20 + 4 = 24$ zeros at the end of 100!.

Comments: This proved challenging for most students. I ended up giving full or nearly full credit for the correct answer, regardless of the supporting reasoning.