Math 104A: Fall 2012
Midterm 2 Solutions
Monday, 11/19/2012

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: [15 points] Decide whether or not $\overline{17}$ is a unit in $\mathbb{Z}_{30}$. If so, compute $\overline{17}^{-1}$ in $\mathbb{Z}_{30}$. Justify your answers.

Solution: $\overline{17}$ is a unit in $\mathbb{Z}_{30}$ because $(17, 30) = 1$. Applying the Euclidean algorithm yields

$$30 = 17 + 13$$
$$17 = 13 + 4$$
$$13 = 3(4) + 1.$$

Reversing yields $1 = 13 - 3(4) = 13 - 3(17 - 13) = 4(13) - 3(17) = 4(30 - 17) - 3(13)$, and reducing modulo 30 yields $\overline{17}^{-1} = \overline{-7} = \overline{23}$.

Comments: Most students realized that $\overline{17}$ is a unit in $\mathbb{Z}_{30}$, but there were students who didn't know how to go about finding its inverse. This is a key computational skill for this course, so be sure that you understand how to do it.

Problem 2: [5 + 5 points] Let $n \in \mathbb{Z}^+$. (a) Carefully define $\phi(n)$, the Euler ϕ-function evaluated at n and (b) calculate $\phi(128000)$. (You need not use your definition from Part (a) to do Part (b).)

Solution: (a) $\phi(n) = |\{1 \leq i \leq n : (i, n) = 1\}|$.
(b) Recall that if $n = p_1^{e_1} \cdots p_r^{e_r}$ for p_i distinct primes and $e_i \geq 0$, then $\phi(n) = (p_1 - 1)p_1^{e_1 - 1} \cdots (p_r - 1)p_r^{e_r - 1}$. We have that $128000 = 2^{10}5^3$, so that $\phi(128000) = (2 - 1)2^9(5 - 1)(5^2) = 51200$.

Comments: This was an example from class. For Part (a), many students wrote definitions which were somehow related to $\phi(n)$, but incorrect.

Problem 3: [10 points] Give an example (with justification) of a prime $p > 0$ and a nonconstant polynomial $f(x) \in \mathbb{Z}_p[x]$ such that $f(x)$ has no roots in $\mathbb{Z}_p$.

Solution: Let $p = 3$ and $f(x) = x^2 + 1$. We have that $f(0) = 1, f(1) = 2, f(2) = 5 = 2$ in $\mathbb{Z}_3$, so f is nonconstant and does not have a root in $\mathbb{Z}_3$.

Comments: I also accepted polynomials of positive degree that attained the same (nonzero) value for all elements of $\mathbb{Z}_p$ (for example, $p = 2$ and $f(x) = x^2 + x + 1$; I showed you this in class). There were some students who gave answers involving square roots, or said things like 'the roots of $f(x) = x^2 + 1$ are $x = \pm i$. The square root symbol has not yet been defined

in $\mathbb{Z}_p$ (indeed, only half of the nonzero elements of $\mathbb{Z}_p$ have square roots for $p > 2$ and these elements have two distinct square roots). We're also looking for solutions in the finite field $\mathbb{Z}_p$, not the field $\mathbb{C}$ of complex numbers (in fact, $f(x)$ does not even have coefficients in $\mathbb{C}$).

Problem 4: [20 points] Let $p > 0$ be prime and let $a, b \in \mathbb{Z}$. Prove that $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Solution: By the Binomial Theorem, we have that

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}. \tag{1}$$

For $1 \leq i \leq p-1$, we have that $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ and the fact that p is prime implies that $p | \binom{p}{i}$. Moreover, we have that $\binom{p}{p} = \binom{p}{0} = 1$. We conclude that $(a+b)^p \equiv a^p + b^p \pmod{p}$, as desired.

Comments: This appeared on the homework. Most students got it right. As always, write your proofs carefully. For example, some students wrote that $p | \binom{p}{i}$ without any constraints on i (this isn't true for $i = 0, p$).

Problem 5: [20 points] Five pirates find a treasure chest on a desert island containing x golden coins. The pirates, somewhat pressed for time, were not able to count the number of coins in the chest, but estimate that $150 \leq x \leq 250$. When the pirates try to divide up the coins as evenly as possible, one coin is left over. In the vicious fight that ensues, one pirate is killed. The four remaining pirates try to divide up the coins as evenly as possible, but one coin is still left over, and one more casualty results. The three surviving pirates are able to successfully divide up the coins evenly between them. Find x.

Solution: We have the system of congruences:

$$\begin{aligned} x &\equiv 1 (mod 5) \\ x &\equiv 1 (mod 4) \\ x &\equiv 0 (mod 3). \end{aligned}$$

Since $3, 4$, and 5 are relatively prime in pairs, this has a unique solution modulo 60 by the Chinese Remainder Theorem. The first two equations yield $x \equiv 1 \pmod{20}$. Combining this with the last equation yields $x \equiv 21 \pmod{60}$. Since $150 \leq x \leq 250$, we conclude that $x = 201$.

Comments: Most students realized that this is a Chinese Remainder Theorem problem, but a few students set up the system of congruences incorrectly. A few more weren't able to solve this system (another basic computational skill you should take away from this course). Finally, a few left the solution as $x \equiv 21 \pmod{60}$, not answering the question that was asked.

Problem 6: [20 points] Define a sequence of numbers $a_1, a_2, \ldots$ by $a_1 = 1, a_2 = 11, a_3 = 111, a_4 = 1111, \ldots$. Let $m = 539 = 7^2(11)$. Find (with proof) an integer n such that $m|a_n$. You may use the fact that $1 + x + x^2 + \cdots x^{r-1} = \frac{1-x^r}{1-x}$ without proof.

Solution: We have that $a_n = 1 + 10 + \cdots + 10^{n-1} = \frac{1-10^n}{1-10}$. Since $(-9, m) = 1$, we have that $\overline{-9}$ is a unit in $\mathbb{Z}_m$. Therefore, $m|a_n$ if $\overline{10^n} = \overline{1}$ in $\mathbb{Z}_m$. By Euler's Theorem, this holds for $n = \phi(m) = 7(7-1)(11-1) = 420$.

Comments: This was the most difficult problem on the exam. Among the students who 'got the idea', 'off by one' type errors were quite common.