MATH 228 Fall 2014

Homework 3

Due in class on Wednesday, October 1^{st}, 2014

NOTE: You will not be allowed to use your calculator during the midterm and the final exams. Therefore, you should not use it to do the homework.

Explain your answers as much as you can. Show your work, not only your answers.

1. (3 points) This is the first part of exercise 2.2 in the textbook. Let m be an integer $\geqslant 2$. Prove that if m is not divisible by any prime p with $p \leqslant \sqrt{m}$, then m is prime.

Use proof by contradiction, so start by assuming that m is not prime, but is not divisible by any prime p with $p \leqslant \sqrt{m}$.

Solution: Suppose that m is not prime and is not divisible by any prime p with $p \leqslant \sqrt{m}$.

By the Fundamental Theorem of Arithmetic, there exist prime numbers $p_1, p_2, \ldots, p_n$ such that $m = p_1 \cdot p_2 \cdots p_n$. Since m is not prime, $n \geqslant 2$, that is, m is the product of at least two prime factors.

$p_1 \mid m$ and $p_2 \mid m$, so $p_1 > \sqrt{m}$ and $p_2 > \sqrt{m}$ because the prime numbers $\leqslant \sqrt{m}$ do not divide m.

Therefore, $p_1 \cdot p_2 > \sqrt{m} \cdot \sqrt{m} = m$. Since $m = p_1 \cdot p_2 \cdots p_n$ and there are at least two prime factors, it follows that $m \geqslant p_1 \cdot p_2 > m$. This is a contradiction because $m > m$ does not make sense.

Since a contradiction has been obtained, the assumption that m is not prime must be rejected, which means that m is prime.

2. (4 points) Write out the addition and multiplication tables for $\mathbb{Z}_6$. (See the notes for Lecture 9 on Monday, September 22.) You don't have to write down all the computations necessary to obtain those tables, you can just give the answer.

Solution:

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

3. (2 points) Let the relation $\sim$ be defined on the set $\mathbb{R}^*$ of nonzero real numbers by: $a \sim b$ exactly when $\frac{a}{b} \in \mathbb{Q}$. Prove that $\sim$ is an equivalence relation. You have to check that this relation $\sim$ satisfies the three properties of an equivalence relation.

Solution: $\sim$ is reflexive: If $a \in \mathbb{R}^*$, then $a \sim a$ since $\frac{a}{a} = 1 \in \mathbb{Q}$.

$\sim$ is symmetric: Let $a, b \in \mathbb{R}^*$. $a \sim b \Longrightarrow \frac{a}{b} \in \mathbb{Q} \Longrightarrow \frac{b}{a} \in \mathbb{Q} \Longrightarrow b \sim a$.

$\sim$ is transitive: Let $a, b, c \in \mathbb{R}^*$. Suppose that $a \sim b$ and $b \sim c$. Then $\frac{a}{b} \in \mathbb{Q}$ and $\frac{b}{c} \in \mathbb{Q}$. Hence $\frac{a}{c} \in \mathbb{Q}$ because $\frac{a}{c} = \frac{a}{b} \cdot \frac{b}{c}$, so $a \sim c$.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

4. (a)(2 points) Find a number r such that $0 \leqslant r < 12$ for which the following congruence holds: $45 \cdot 115 \cdot 77 \cdot 166 \equiv r \pmod{12}$.

Solution: There are different ways to simplify this expression, but of course they all give the same answer.

$$\begin{aligned} 45 \cdot 115 \cdot 77 \cdot 166 &\equiv (-3) \cdot (-5) \cdot 5 \cdot (-2) \pmod{12} \\ &\equiv 15 \cdot (-10) \pmod{12} \\ &\equiv 3 \cdot 2 \pmod{12} \\ &\equiv 6 \pmod{12} \end{aligned}$$

The answer is $r = 6$.

(b)(2 points) What is the remainder upon division by 7 of $5a^3 - 4b^2$ when $a = -31$ and $b = 25$?

Solution:

$$\begin{aligned} 5a^3 - 4b^2 &\equiv 5 \cdot (-31)^3 - 4 \cdot (25)^2 \pmod{7} \\ &\equiv 5 \cdot (-3)^3 - 4 \cdot 4^2 \pmod{7} \\ &\equiv 5 \cdot (-27) - 4 \cdot 16 \pmod{7} \\ &\equiv 5 \cdot 1 - 4 \cdot 2 \pmod{7} \\ &\equiv -3 \equiv 4 \pmod{7} \end{aligned}$$

It follows that the remainder upon division by 7 of $5a^3 - 4b^2$ is 4.

5. (3 points) This is exercise 4.7(i) in the textbook. Show that every nonnegative integer a is congruent mod 11 to the alternating sum of its decimal digits.

For instance, if $a = 538$, then the alternating sum of its digits is $5 - 3 + 8$ and you can check directly that $5 - 3 + 8 = 10$ and $538 \equiv 10 \pmod{11}$ because 11 divides $538 - 10$. If $a = 7852$, the alternating sum of its digits is $-7+8-5+2$. Alternating means that the sign alternates between + and −. *Hint*: Study the proof of Proposition 4.11 in the textbook and read the rest of that page below it.

This provides an easy way to check that a number is divisible by 11. For instance, if $a = 7852$, then $7852 \equiv -7 + 8 - 5 + 2 \equiv -2 \pmod{11}$, so 7852 is not divisible by 11 because $7852 \not\equiv 0 \pmod{11}$. 7854 is divisible by 11 because the alternating sum of its digits is $-7+8-5+4$, which is 0, so $7854 \equiv 0 \pmod{11}$, which means that 7854 is divisible by 11.

Solution: $10 \equiv -1 \pmod{11}$, so $10^i \equiv (-1)^i \pmod{11}$.

The nonnegative integer a can be written as $a = d_k 10^k + d_{k-1}10^{k-1} + \cdots + d_2 10^2 + d_1 10 + d_0$. The digits of a when written in decimal notation are $d_k d_{k-1} \ldots d_2 d_1 d_0$.

Standard properties of congruences imply that

$$a \equiv d_k(-1)^k + d_{k-1}(-1)^{k-1} + \cdots + d_2(-1)^2 + d_1(-1) + d_0 \pmod{11} \tag{1}$$

because $10^i \equiv (-1)^i \pmod{11}$. The expression on the right hand side of the congruence (1) is the alternating sum of the digits of a: when i is even, $(-1)^i = 1$, and $(-1)^i = -1$ when i is odd, so the sign does alternate between + and − as i increases from 0 to k.

****

The following problems are not mandatory and will not be graded, but it is highly recommended that you try to solve them.

6. (a) Let a and b be integers. Prove that if 7 divides $a^2 + b^2$, then $7 \mid a$ and $7 \mid b$. (This is similar to an example done in class at the beginning of Lecture 7 on Wednesday, September 17.)

Solution: By the Division Algorithm, $a = 7q_1 + r_1$ and $b = 7q_2 + r_2$ for certain integers q_1, q_2, r_1, r_2 with $0 \leqslant r_1 \leqslant 6$, $0 \leqslant r_2 \leqslant 6$. Then

$$a^2 + b^2 = 49q_1^2 + 14q_1r_1 + r_1^2 + 49q_2^2 + 14q_2r_2 + r_2^2 = 7(7q_1^2 + 7q_2^2 + 2q_1r_1 + 2q_2r_2) + r_1^2 + r_2^2.$$

Since $7 \mid (a^2 + b^2)$ and $7 \mid 7(7q_1^2 + 7q_2^2 + 2q_1r_1 + 2q_2r_2)$, it must be the case that $7 \mid r_1^2 + r_2^2$.

r_1^2 and r_2^2 are equal to one of the numbers $0, 1, 2^2, 3^2, 4^2, 5^2, 6^2$. Since $3^2 \equiv 2 \pmod{7}$, $4^2 \equiv 2 \pmod{7}$, $5^2 \equiv 4 \pmod{7}$, $6^2 \equiv 1 \pmod{7}$, we see that it is never possible to get $r_1^2 + r_2^2 \equiv 0 \pmod{7}$ unless $r_1 = 0 = r_2$. Therefore, $7 \mid a$ and $7 \mid b$.

(b) Find a counterexample to the following statement: if 5 divides $a^2+b^2+c^2$ and $a, b, c \neq 0$, then $5 \mid a$ and $5 \mid b$ and $5 \mid c$. In other words, find specific non-zero values of a, b and c such that 5 divides $a^2 + b^2 + c^2$ but 5 does not divide at least one of a, b, c.

Solution: $a = 5, b = 1, c = 2$, so $a^2 + b^2 + c^2 = 30$ and 30 is divisible by 5, but $5 \nmid b$ and $5 \nmid c$.

7. Prove that the following relation on the coordinate plane $\mathbb{R}^2$ is an equivalence relation: $(x, y) \sim (u, v)$ if and only if $x - u$ is an integer.

You have to check that this relation $\sim$ satisfies the three properties of an equivalence relation. For the transitivity property, consider three points $(x, y), (u, v)$ and (w, z).

Solution: $\sim$ is reflexive: If $(x, y) \in \mathbb{R}^2$, then $(x, y) \sim (x, y)$ since $x - x = 0 \in \mathbb{Z}$.

$\sim$ is symmetric: Let $(x, y), (u, v) \in \mathbb{R}^2$. $(x, y) \sim (u, v) \implies x - u \in \mathbb{Z} \implies u - x \in \mathbb{Z} \implies (u, v) \sim (x, y)$.

$\sim$ is transitive: Let $(x, y), (u, v), (w, z) \in \mathbb{R}^2$. Suppose that $(x, y) \sim (u, v)$ and $(u, v) \sim (w, z)$. Then $x - u \in \mathbb{Z}$ and $u - w \in \mathbb{Z}$. Since $x - w = (x - u) + (u - w)$, it follows that $x - w$ is also an integer, hence $(x, y) \sim (w, z)$.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

8. This is exercise 4.3 in the textbook. Show that if $a \equiv b \pmod{n}$ and $m \mid n$, then $a \equiv b \pmod{m}$.

Solution: If $a \equiv b \pmod{n}$, then $n \mid (a - b)$, so $a - b = nk$ for some $k \in \mathbb{Z}$.

$m \mid n$, so there exists an integer l such that $n = lm$.

From $a - b = nk$ and $n = lm$, it follows that $a - b = lmk$. Therefore, $m \mid (a - b)$ so $a \equiv b \pmod{m}$.

9. (a) If a is a nonnegative integer, prove that a is congruent to its last digit mod 10. Denoting by d the last digit of a, you have to show that $a \equiv d \pmod{10}$. (For example, $27 \equiv 7 \pmod{10}$.)

Solution: By the Division Algorithm applied to a and 10, there exist $q, r \in \mathbb{Z}$ such that $a = 10q + r$ and $0 \leqslant r \leqslant 9$. r is equal to the last digit d of a, so $a = 10q + d$. This implies that $a \equiv d \pmod{10}$.

(b) Show that no perfect square has $2, 3, 7$, or 8 as its last digit.

Recall that, if a is a perfect square, then there exists $b \in \mathbb{Z}$ such that $a = b^2$. What is the relation between the last digit d of a and the last digit e of b?

Solution: Suppose that $a \in \mathbb{N}$ is a perfect square, so $a = b^2$ for some $b \in \mathbb{N}$. Let d be the last digit of a and let e be the last digit of b. By part (a),

$$e \equiv b \pmod{10}. \tag{2}$$

Since $a = b^2$, by part (a) again,

$$a \equiv b^2 \equiv e^2 \pmod{10}. \tag{3}$$

From (3) and part (a), it follows that

$$d \equiv e^2 \pmod{10}. \tag{4}$$

e can take any integral value between 0 and 9. $0^2 \equiv 0 \pmod{10}$, $1^2 \equiv 1 \pmod{10}$, $2^2 \equiv 4 \pmod{10}$, $3^2 \equiv 9 \pmod{10}$, $4^2 \equiv 6 \pmod{10}$, $5^2 \equiv 5 \pmod{10}$, $6^2 \equiv 6 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $8^2 \equiv 4 \pmod{10}$, $9^2 \equiv 1 \pmod{10}$.

These computations show that $e^2 \not\equiv 2, 3, 7, 8 \pmod{10}$, so $d \not\equiv 2, 3, 7, 8 \pmod{10}$ because of (4). Since $0 \leqslant d \leqslant 9$, this means that $d \neq 2, 3, 7, 8$.