

Math 109 Winter 2007 Exam 2

February 28, 2007

NAME: Answers

Problem 1 /20	
Problem 2 /35	
Problem 3 /25	
Problem 4 /20	
Total /100	

Problem 1 (20 pts)

1a. (10 pts) Calculate $\gcd(59, 44)$ using the Euclidean algorithm (you may be able to find it by guessing, but I want you to use the Euclidean algorithm anyway.) Show your work.

$$59 = (1)(44) + 15$$

$$44 = (2)(15) + 14$$

$$15 = (1)(14) + 1$$

$$14 = (14)(1) + 0.$$

Thus $\gcd(59, 44) = 1$.

1b. (10 pts) Find some pair of integers x, y such that $59x + 44y = 5$. Show your work. (Note you are asked only to find any solution, you don't have to find all solutions.)

Since $\gcd(59, 44) = 1$ divides 5, we know there are solutions. Using the calculation from the preceding page, we write each number appearing in the algorithm as an integral linear combination of 59 and 44.

$$59 = (1)(59) + (0)(44)$$

$$44 = (0)(59) + (1)(44)$$

$$15 = 59 - 44 = (1)(59) + (-1)(44)$$

$$14 = 44 - 2(15) = (-2)(59) + (3)(44)$$

$$1 = 15 - 14 = (3)(59) + (-4)(44).$$

Multiplying by 5 we have

$$5 = (15)(59) + (-20)(44)$$

and so we can take $x = 15, y = -20$.

Problem 2 (35 pts)

2a.(15 pts). Let A, B, C be sets, and let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions. Suppose that f and g are injective functions. Prove that the composition $g \circ f : A \rightarrow C$ is also injective.

Suppose that $g \circ f(a_1) = g \circ f(a_2)$ for some elements $a_1, a_2 \in A$. By definition of composition this means $g(f(a_1)) = g(f(a_2))$. Now since g is injective, this implies that $f(a_1) = f(a_2)$. Then using that f is injective, this implies $a_1 = a_2$.

Altogether we have shown that $g \circ f(a_1) = g \circ f(a_2) \implies a_1 = a_2$ and so the function $g \circ f$ is injective.

2b.(10 pts) Give an explicit example of a function $f : \mathbb{R} \rightarrow \mathbb{R}$ (so the domain and codomain are both the set of real numbers) which is not injective and not surjective. Justify your answer. (If you use the graph, you have to say what properties of the graph you are using as justification. It is not enough to just draw the graph.)

There are lots of possible examples, but one of the easiest is $f(x) = x^2$. To see that f is not injective, just note that $f(1) = f(-1) = 1$. To see that f is not surjective, just note that if $f(x) = -1$ for some $x \in \mathbb{R}$ then $x^2 = -1$ which is impossible since squares of real numbers are always nonnegative. Thus -1 is not in the image of f and f is not surjective.

2c.(10 pts) Write out the following statement in words. Then prove or disprove it.

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^2 < x^2.$$

In words, this says “For all real numbers x , there exists a real number y such that $y^2 < x^2$ ”.

This statement is false, and to show this we just need to give a counterexample. If $x = 0$, then there does not exist any real number y such that $y^2 < 0^2 = 0$, because squares of real numbers are nonnegative.

Problem 3 (25 pts)

3a.(15 pts) Find r with $0 \leq r < 20$ such that $3^{250} \equiv r \pmod{20}$. Prove your answer is correct.

We start by calculating some small powers of 3 modulo 20. We have

$$3 \equiv 3 \pmod{20},$$

$$3^2 \equiv 9 \equiv 9 \pmod{20},$$

$$3^3 \equiv 27 \equiv 7 \pmod{20},$$

$$3^4 \equiv (7)(3) \equiv 21 \equiv 1 \pmod{20}.$$

Once we get a 1 things get easier: Every 3^n where n is a multiple of 4 will be congruent to 1. In particular, we have

$$3^{248} \equiv (3^4)^{62} \equiv 1^{62} \equiv 1 \pmod{20}$$

and so

$$3^{250} \equiv (3^2)(3^{248}) \equiv (9)(1) \equiv 9 \pmod{20}.$$

So $r = 9$.

3b.(10 pts) Let $m = 20$ and let $\mathbb{Z}_{20} = \{[0], [1], [2], \dots, [19]\}$ be the set of congruence classes mod 20, with the operations of addition and multiplication of congruence classes. Suppose that the equation $[a][b] = [1]$ holds for the two congruence classes $[a]$ and $[b]$ in \mathbb{Z}_{20} . Prove that $\gcd(a, 20) = 1$.

By definition of multiplication of congruence classes, $[a][b] = [1]$ means that $[a][b] = [ab] = [1]$. In particular, since $1 \in [1]$, $1 \in [ab]$ which means by definition that $ab \equiv 1 \pmod{20}$.

The definition of congruence now gives $ab - 1 = 20q$ for some $q \in \mathbb{Z}$. Rearranging, we have $ab - 20q = 1$. Now we may quote the theorem on the solutions of diophantine equations which we proved in class: Since $x = b, y = -q$ is a solution to the diophantine equation $ax + 20y = 1$, the criterion for the existence of such a solution gives $\gcd(a, 20) = 1$.

If we wish not to quote this theorem, we can easily prove this fact directly. Suppose that d is a positive integer such that $d|a$ and $d|20$. Then $a = md$ and $20 = nd$ for some integers m, n . Then $ax + 20y = mdx + ndy = d(mx + ny) = 1$. So $d|1$. This forces $d = 1$. Thus $\gcd(a, 20) = 1$.

Problem 4 (20 pts)

4a.(10 pts) Complete the following statement of the division theorem.

Let a and b be integers with $b > 0$. Then there are unique integers q and r satisfying the following properties: ...

$$a = bq + r \text{ and } 0 \leq r < b.$$

4b.(10 pts) Recall that a *perfect square* is an integer of the form m^2 for some integer m . Prove that 255342343 is not a perfect square. (Hint: consider what perfect squares look like mod 4.)

Given an integer m , then one of the four possibilities $m \equiv 0 \pmod{4}$, $m \equiv 1 \pmod{4}$, $m \equiv 2 \pmod{4}$, $m \equiv 3 \pmod{4}$ holds. Squaring, we get $m^2 \equiv 0 \pmod{4}$, $m^2 \equiv 1 \pmod{4}$, $m^2 \equiv 4 \equiv 0 \pmod{4}$, or $m^2 \equiv 9 \equiv 1 \pmod{4}$. So if $n = m^2$ is a perfect square, then there are only two possibilities, $n \equiv 0 \pmod{4}$ or $n \equiv 1 \pmod{4}$.

Now notice that $255342343 = 2553423(100) + 43 \equiv 43 \equiv 3 \pmod{4}$. Since every integer is congruent to modulo 4 to a unique $r \in \{0, 1, 2, 3\}$, this proves that 255342343 is not a perfect square by the previous paragraph.