

Math 55-2 Midterm 1

Rob Bayer

July 9, 2009

You have until 3:30pm to complete this test. No calculators, books, notes, or consultation with other members of the class are permitted. Your exam should have 3 pages.

Unsupported or improperly supported answers will receive no credit.

Name: _____

1	10	
2	15	
3	15	
4	15	
5	15	
6	15	
7	15	
Total	100	

1. (10 pts) Short answer. You need not show any work for this section

(a) Complete each of the following definitions. Note that there are many possible answers to some of these questions and any mathematically correct definition will receive full credit.

- i. A compound proposition is a tautology iff It is always True
- ii. $f : A \rightarrow B$ is injective (one-to-one) iff $f(x) = f(y) \Rightarrow x = y$
- iii. If $A \subseteq \text{dom}(f)$, then $f(A) = \{y : \exists x \in A f(x) = y\}$
- iv. $f : A \rightarrow B$ is surjective (onto) iff $\forall y \exists x f(x) = y$
- v. $a|b$ (“a divides b”) iff $\exists k \in \mathbb{Z} (b = ak)$
- vi. a, b are relatively prime (coprime) iff $\text{gcd}(a, b) = 1$

(b) Order the following in increasing order of size: $\mathbb{R}, \mathbb{N}, \mathbb{Z}, \mathbb{P}, \mathbb{Q}, \mathbb{R} - \mathbb{N}$ (here \mathbb{P} is the set of all primes). Note that some sets may be the same size as others, and you should be sure to indicate that.

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{P}| = |\mathbb{Q}| < |\mathbb{R}| = |\mathbb{R} - \mathbb{Q}|$$

(c) The linear congruence $ax \equiv b \pmod{m}$ has a solution iff $\text{gcd}(a, m) | b$

(d) If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ (This is Fermat’s Little Theorem)

2. (15 pts)

(a) Determine the truth value for each of the following if the domain for all quantifiers is \mathbb{R} , the set of real number. You must justify your answers

- i. $\forall x \forall y \exists z (x^2 + y^2 = z^2)$
This is true. Since $x^2 + y^2 \geq 0$ for any x, y , we can use $z = \sqrt{x^2 + y^2}$
- ii. $\exists x \forall y (y > x \rightarrow \exists z (y = z^2))$
This is also true. If $y > 0$, then y has a square root and thus $y = \sqrt{y}^2$. So $x = 0, z = \sqrt{y}$ works.
- iii. $\forall x (x > 4 \rightarrow |x - 4| \geq 1)$
This is false. $x = 4.5$ is a counterexample.

(b) Make a truth table for the compound proposition $(p \vee q) \rightarrow (p \wedge q)$

p	q	$p \vee q$	$p \wedge q$	$(p \vee q) \rightarrow (p \wedge q)$
T	T	T	T	T
T	F	T	F	F
F	T	T	F	F
F	F	F	F	T

3. (15 pts) Let $g : A \rightarrow B$ and $f : B \rightarrow C$ be functions.

Show that if $f \circ g$ is bijective, then g is injective and f is surjective.

We’ll show this in two parts.

(g is injective): Here we’ll show that contrapositive: If g is not injective, then $f \circ g$ is not either (and thus isn’t a bijection).

If g is not surjective, then we can find x, y with $x \neq y$ such that $g(x) = g(y)$. Applying f to both sides gives $f(g(x)) = f(g(y))$. Since $x \neq y$, this shows $f \circ g$ is not injective and thus cannot be a bijection.

(f is surjective): Suppose $f \circ g$ is bijective. Then in particular, $f \circ g$ is surjective. Let y be given. Then since $f \circ g$ is surjective, there is some a such that $f(g(a)) = y$. Letting $x = g(a)$, we see that $f(x) = y$ and thus for every y we can find an x such that $f(x) = y$. Therefore, f is surjective.

4. (15 pts) Prove that if x is irrational and y is rational, then $x + 2y^2$ is irrational.

We’ll do this by contradiction. AFSOC that $x + 2y^2$ were rational. In particular, let $p, q \in \mathbb{Z}$ such that $x + 2y^2 = \frac{p}{q}$. Since y is rational, $y = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ and thus $2y^2 = \frac{2m^2}{n^2}$. Then we have:

$$x = (x + 2y^2) - 2y^2 = \frac{p}{q} - \frac{2m^2}{n^2} = \frac{pn^2 - 2qm^2}{qn^2} \in \mathbb{Q}$$

Thus contradicting our hypothesis that x is irrational. Therefore, $x + 2y^2$ must be irrational as well.

5. (15 pts)

- (a) Find $\gcd(382, 97)$ and find integers s, t such that $\gcd(382, 97) = s \cdot 382 + t \cdot 97$

We do the Euclidean Algorithm:

$$382 = 3 \cdot 97 + 91$$

$$97 = 1 \cdot 91 + 6$$

$$91 = 15 \cdot 6 + 1$$

$$6 = 6 \cdot 1 + 0$$

Thus, $\gcd(382, 97) = 1$. (Alternatively: 97 is prime and $97 \nmid 382$ so their gcd must be 1)

To find s, t , we use our equations in the reverse order:

$$\begin{aligned} 1 &= 91 - 15 \cdot 6 \\ &= 91 - 15 \cdot (97 - 1 \cdot 91) \\ &= 16 \cdot 91 - 15 \cdot 97 \\ &= 16(382 - 3 \cdot 97) - 15 \cdot 97 \\ &= 16 \cdot 382 - 63 \cdot 97 \end{aligned}$$

- (b) Find a multiplicative inverse of 97 mod 382 or show that one does not exist.

From our work above, we see that $1 = 16 \cdot 382 - 63 \cdot 97$. Thus, we know $1 \equiv 16 \cdot 382 - 63 \cdot 97 \pmod{382}$. Reducing this, we get:

$$1 \equiv -63 \cdot 97 \pmod{382}$$

So -63 is a multiplicative inverse of 97 mod 382.

(We could also use $382 - 63 = 319$ if you prefer a positive integer)

6. (15 pts) Find all solutions to the system of congruences
$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

The first equation tells us that $x = 1 + 2k$. Plugging in to the second gives $2k + 1 \equiv 2 \pmod{5}$ which is equivalent to $2k \equiv 1 \pmod{5}$. We could either solve this with gcds or by just looking and seeing that $k \equiv 3 \pmod{5}$ is the solution.

So $k = 3 + 5l$ and $x = 1 + 2(3 + 5l) = 7 + 10l$. Plugging this into the last congruence gives $7 + 10l \equiv 3 \pmod{7}$, which is equivalent to $3l \equiv 3 \pmod{7}$ which clearly has solution $l \equiv 1 \pmod{7}$. Thus, $l = 1 + 7m$.

Combining everything, we get $x = 7 + 10(1 + 7m) = 17 + 70m$. That is, x is a solution iff $x \equiv 17 \pmod{70}$

7. (15 pts) Prove that if p is prime and $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

If $x^2 \equiv 1 \pmod{p}$, then from the definition of modular equivalence, we know $p \mid x^2 - 1 = (x + 1)(x - 1)$. Since p is prime and divides the product of two $x + 1$ and $x - 1$ it must divide one of them.

If $p \mid x - 1$, then $x \equiv 1 \pmod{p}$. If $p \mid x + 1$, then $x \equiv -1 \pmod{p}$ (since $x + 1 = x - (-1)$). Thus, we have the desired result.