

MA357, Spring 2008 — Midterm 1

This is a take-home test. It is due by the end of the day on Friday, March 14. This is a firm deadline: no extensions will be given except for medical reasons.

The test contains 11 questions. The number of points for each question is indicated. You should solve enough problems to get at least 100 points. The maximum score you can get, however, is 100, so if you do more problems than necessary you are only buying insurance.

Rules of the Game: While you work on this test, you may consult your textbook and your class notes, but no other reference materials. You may use a calculator or a computer — in fact, you will probably need to. You should work entirely by yourself. You may talk to me (though I don't promise to answer every question you might have), but you may not talk to anyone else. (Complaining and asking for sympathy are ok, but don't discuss the actual content of the test.)

Finally, you should really *write up* (and not just write down) your solutions: they should read as if they were an example in a well-written textbook. Make sure that you explain carefully your line of reasoning at each point; your text should be such that another student at about your level could follow the steps without having to ask you for help. To achieve this goal, be as verbose as necessary — it is better to write too much than too little. Solutions should be written in ink, and be as legible as possible. *Don't turn in first-draft material.*

Together with your test, you should turn in a signed statement saying that you have followed the test rules as stated above.

Good luck!

Number theorists are like lotus-eaters — having once tasted of this food they can never give it up.

– Leopold Kronecker

1. [10 points] Let a and b be integers, and let $d = \gcd(a, b)$. Suppose g is a common divisor of a and b , i.e., that $g|a$ and $g|b$.

a. Prove that $g|d$.

b. Prove that $\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{d}{g}$.

(Hint: to prove something is the greatest common divisor one usually needs to check *two* things. For example, one might show (a) that it is a common divisor, and (b) that it is bigger than any other common divisor.)

2. [10 points] Show that the equation $x^2 + xy - y^2 = 3$ does not have integer solutions. (Hint: if it had integer solutions it'd have solutions (mod n) for any n ; pick the right n ...)

3. [15 points] If p is a prime number, the notation $p^a||n$ (“ p^a exactly divides n ”) is used to mean that $p^a|n$ but $p^{a+1} \nmid n$, so that a is the exact power of p that appears in the factorization of n . Prove that

a. if $n = p^a x$ and $p \nmid x$, then $p^a||n$;

b. if $p^a||n$ and $p^b||m$, then $p^{a+b}||nm$;

c. if $p^a||n$ and $p^b||m$ and $a < b$, then $p^a||(n + m)$;

d. if $p^a||n$ and $p^b||m$ and $a = b$, then $p^a|(n + m)$, but it may or may not be true that $p^a||(n + m)$.

(Hint: Keep in mind that $p^a||n$ asserts *both* that p^a divides n and that p^{a+1} does not.)

4. [10 points] Find all the solutions (if any exist) of each of the following congruences:

a. $375x \equiv 13 \pmod{121}$

b. $36x \equiv 22 \pmod{50}$

c. $87x \equiv 1 \pmod{191}$

d. $19x \equiv 17 \pmod{247}$

5. [10 points] We showed in class that in general we cannot cancel a from a congruence of the form $ax \equiv ab \pmod{m}$. We also showed that it *was* possible to cancel a if $\gcd(a, m) = 1$. Prove the following generalization of that result:

If $ax \equiv ab \pmod{m}$ and $d = \gcd(a, m)$, then $x \equiv b \pmod{\frac{m}{d}}$.

6. [10 points] Solve the congruence $x^{35} + 5x^{19} + 11x^3 \equiv 0 \pmod{17}$. (You should be able to do something more intelligent than “climb every mountain.”)

7. [10 points] For each positive integer k , let M_k be the number whose representation in base 10 is a string of k 9s in a row. So $M_1 = 9$, $M_2 = 99$, $M_8 = 99,999,999$. Let p be a fixed prime, $p > 5$. Show that there exist infinitely many k for which p divides M_k . (Hint: Find a good formula for M_k , then use congruences.)

8. [10 points] A number n is called a *Carmichael number* if it is not prime but nevertheless we have $a^{n-1} \equiv 1 \pmod{n}$ for all numbers a which are relatively prime to n . Show that 6601 is a Carmichael number.

9. [25 points] Let r and s be any two positive integers. Show that there exists a sequence of r consecutive integers each of which is divisible by the s -th power of some integer. For example, the numbers 548, 549, 550 are divisible by 4, 9, and 25, respectively, so they show that there exists a sequence of three consecutive numbers each of which is divisible by some square. This is the case $r = 3$, $s = 2$ of the statement you need to prove. (Hint: use the Chinese Remainder Theorem.)

10. [25 points] For this problem, we have to make or recall several definitions. First, a function $f : \mathbb{Z} \rightarrow \mathbb{R}$ is called *multiplicative* if we have $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$. Second, the μ function is the multiplicative function defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{if } n \text{ is divisible by the square of some prime.} \end{cases}$$

Third, let's define two fairly simple multiplicative functions: $I(n)$ is equal to 1 if $n = 1$ and to 0 otherwise, and $u(n) = 1$ for all n . Finally, if f and g are both multiplicative functions, we define the *convolution* of f and g to be the function $f * g$ defined by

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

- Show that μ is multiplicative.
- Show that if f and g are multiplicative, then $f * g$ is multiplicative.
- Show that $f * g = g * f$ and $(f * g) * h = f * (g * h)$ for all multiplicative functions f, g, h .
- What is $f * I$ equal to?
- What is $\mu * u$ equal to?
- The *Möbius inversion formula* says that if f is a multiplicative function and F is defined by

$$F(n) = \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu(d)F(n/d),$$

and conversely. Prove this.

11. [10 points] Let $\mu(n)$ be the function in the previous problem. Define a function of a real variable $s > 1$ by

$$f(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Show that this is well-defined (i.e., the series converges), and that in fact $f(s)\zeta(s) = 1$, so that $f(s) = 1/\zeta(s)$.