

MA357, Spring 2008 — Midterm 1 Solutions

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 $g|d$.

Since d is the gcd, it can be written as a linear combination of a , and b , so $d = ax + by$ with x and y integers. Now notice that $g|a$ and $g|b$, hence $g|(ax + by)$, so $g|d$.

(Done in class, by the way.)

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

The thing to remember here is that proving that something is the gcd requires two steps. For example, we can do it by proving that

- d/g is a common divisor, and
- d/g is bigger than any other common divisor.

The first is easy: we know $a = du$ and $b = dv$, and we just divide both equations by g . For the second, suppose we have

$$\frac{a}{g} = en \quad \text{and} \quad \frac{b}{g} = em$$

for some $e > d/g$. Multiplying by g gives

$$a = egn \quad \text{and} \quad b = egm$$

so that eg is a common divisor. But $eg > d$, contradicting the assumption that d is the gcd.

Another strategy (easier, in this case) is to show that

- d/g is a common divisor, and
- d/g is a linear combination of a/g and b/g .

The first part is done as before. For the second, just write $d = ax + by$ as before and divide through by g .

Notice that just knowing that d/g is a linear combination of a/g and b/g is not enough to show that it is the gcd! What we know is that any linear combination is a *multiple* of the gcd. But if something positive is *both* a linear combination and a common divisor, then it is the gcd.

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 ...)

The easiest method is probably to consider the equation mod 5 and “climb every mountain” to show that there is no pair (a, b) such that $a^2 + ab - b^2 \equiv 3 \pmod{5}$. A slightly fancier method is to notice that

$$x^2 + xy - y^2 \equiv x^2 - 4xy + 4y^2 \equiv (x - 2y)^2 \pmod{5}$$

and use the fact that 3 is not a square (mod 5).

Closely related is the following idea: Let y be a fixed integer and solve the equation

$$x^2 + xy - (y^2 - 3) = 0$$

for x using the quadratic formula to get

$$x = \frac{-y \pm \sqrt{y^2 + 4(y^2 - 3)}}{2} = \frac{-y \pm \sqrt{5y^2 - 12}}{2}.$$

For this to be an integer, $5y^2 - 12$ must be a square, which would make -12 a square (mod 5); but $-12 \equiv 3 \pmod{5}$, which is not a square. (No one did this.)

By the way: The reason both of these methods boil down to considering the equation (mod 5) is that the discriminant of the quadratic $t^2 + t - 1$ is 5.

Next easiest is the method most people used: looking at the equation (mod 3) and climbing mountains, we can quickly see that if x and y satisfy $x^2 + xy - y^2 \equiv 0 \pmod{3}$, then we must have $x \equiv 0 \pmod{3}$ and $y \equiv 0 \pmod{3}$. But if x and y are both divisible by 3, then $x^2 + xy - y^2$ is divisible by 9, and hence can't be equal to 3.

3. [15 points] If p is a prime number, the notation $p^a \parallel n$ (“ p^a exactly divides n ”) is used to mean that $p^a \mid n$ 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 $p^a \parallel n$;

Clearly, $p^a \parallel n$. To see that $p^{a+1} \nmid n$, suppose it did. Then we would have $p^{a+1} \mid p^a x$, and cancelling p^a shows $p \mid x$, which contradicts our assumption.

It's useful to note that the converse is also true: if $p^a \parallel n$, then $n = p^a x$ and $p \nmid x$.

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

Write $n = p^a x$ and $m = p^b y$. The assumption that these are the exact powers means that p does not divide x or y . Now notice that $nm = p^{a+b} xy$. This shows that $p^{a+b} \mid nm$. To show that this is the exact power, we need to show that p does not divide xy . But, since p is a prime, we know that $p \mid xy$ implies that either $p \mid x$ or $p \mid y$, which we know isn't true. So we can conclude that $p \nmid xy$, and therefore that $p^{a+b} \parallel nm$.

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

Again, we can write $n = p^a x$ and $m = p^b y$, with neither x nor y divisible by p . Now

$$n + m = p^a(x + p^{b-a}y),$$

so $p^a \parallel (n + m)$. For the remaining part, notice that if $p \mid (x + p^{b-a}y)$ we would have $p \mid x$, which isn't true. So in fact $p^a \parallel (n + m)$.

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

This time, we have $n = p^a x$ and $m = p^a y$, with neither x or y divisible by p . Now

$$n + m = p^a(x + y),$$

so $p^a \parallel (n + m)$. But the sum of two numbers that are not divisible by p may or may not be divisible by p , which means that we can't decide about exact divisibility in this case. To find examples, just choose x and y appropriately: $p = 5, x = 2, y = 3$ is an example of one possibility, and $p = 5, x = 2, y = 1$ is an example of the other.

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

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

One solution, $x \equiv 112 \pmod{121}$.

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

Two solutions, $x \equiv 2 \pmod{50}$ and $x \equiv 27 \pmod{50}$.

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

One solution, $x \equiv 101 \pmod{191}$.

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

No solutions, because $\gcd(247, 19) = 19$ does not divide 17.

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 $x \equiv b \pmod{\frac{m}{d}}$.

If $ax \equiv ab \pmod{m}$, then $m|a(b-x)$. Since both m and a are divisible by d , we can divide through to get $\frac{m}{d}|\frac{a}{d}(b-x)$. Now note that we can use Problem 2, part b, to conclude that $\gcd(\frac{m}{d}, \frac{a}{d}) = 1$, which allows us to conclude that $\frac{m}{d}|(b-x)$, which is what we want to prove.

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.”)

First of all, if $x \equiv 0 \pmod{17}$ then it clearly is a solution. You need to consider this case separately, because Little Fermat *does not apply* when $x \equiv 0 \pmod{p}$!!!

If not, then we can use Fermat's Little Theorem to conclude that $x^{16} \equiv 1 \pmod{17}$. This allows us to reduce the equation to

$$x^{35} + 5x^{19} + 11x^3 \equiv x^3 + 5x^3 + 11x^3 \equiv 17x^3 \equiv 0 \pmod{17}$$

for any x not divisible by 17. So in fact any x is a solution of this congruence.

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.)

Notice that $M_k = 10^k - 1$, so $p|M_k$ if and only if $10^k \equiv 1 \pmod{p}$. Little Fermat shows that if k is any multiple of $p - 1$ this will be true, so there are infinitely many such k .

Some people had trouble reading the question. It says that for any choice of prime p there should exist infinitely many k with the desired property. It's not enough to exhibit one k for each p !!

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.

Some of you went for huge cannons, but this is actually pretty easy. Notice, first, that $6601 = 7 \times 23 \times 41$. Now notice that

$$7 - 1 = 6 \text{ divides } 6600$$

$$23 - 1 = 22 \text{ divides } 6600$$

$$41 - 1 = 40 \text{ divides } 6600$$

It follows from Fermat's Little Theorem, then, that if $\gcd(a, 6601) = 1$ we have

$$a^{6600} \equiv 1 \pmod{7}$$

$$a^{6600} \equiv 1 \pmod{23}$$

$$a^{6600} \equiv 1 \pmod{41}$$

Those three together say that $a^{6600} \equiv 1 \pmod{6601}$. Since this holds for any a that is relatively prime to 6601, we've shown 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.)

Most of you saw what to do: let p_1, p_2, \dots, p_r be distinct primes. Then $p_1^s, p_2^s, \dots, p_r^s$ are pairwise relatively prime, and the Chinese Remainder Theorem tells us that the system of congruences

$$\begin{aligned} x &\equiv 0 \pmod{p_1^s} \\ x &\equiv -1 \pmod{p_2^s} \\ x &\equiv -2 \pmod{p_3^s} \\ &\dots \\ x &\equiv -(r-1) \pmod{p_r^s} \end{aligned}$$

has a solution. But if x is such a solution then $x, x+1, x+2, \dots, x+(r-1)$ is a sequence of r integers each of which is divisible by an s -th power.

Notice that the problem asked for an existence result, so there was no need to attempt to solve the horrible system of congruences that results.

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

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

- a. Show that μ is multiplicative.

The only problem here was to keep one's head on straight and consider the cases properly.

If either m or n is 1, then, since $\mu(1) = 1$ it's clear that $\mu(mn) = \mu(n)\mu(m)$. If either m or n is divisible by the square of some prime, then so is mn , and so $\mu(mn) = 0 = \mu(m)\mu(n)$. Finally, suppose m is the product of r distinct primes and n is the product of s distinct primes. If m and n are relatively prime, the primes dividing m are different from those that divide n , so that mn is the product of $r + s$ distinct primes. So in this case

$$\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n).$$

Putting it all together, we see that μ is multiplicative.

- b. Show that if f and g are multiplicative, then $f * g$ is multiplicative.

The thing to note is that if $\gcd(m, n) = 1$ then the divisors of mn are exactly the numbers of the form de , where $d|m$ and $e|n$ and $\gcd(d, e) = 1$. (This is clear, for example, by using the prime factorization. Notice that this is a double claim: any divisor looks like that, and does so uniquely.)

Once we see that, it's easy:

$$\begin{aligned} (f * g)(mn) &= \sum_{e,d} f(de)g(mn/de) \\ &= \sum_{d,e} f(d)f(e)g(m/d)g(n/e) \\ &= \left(\sum_{d|m} f(d)g(m/d) \right) \left(\sum_{e|n} f(e)g(n/e) \right) \\ &= (f * g)(m)(f * g)(n). \end{aligned}$$

- c. Show that $f * g = g * f$ and $(f * g) * h = f * (g * h)$ for all multiplicative functions f, g, h .

For both, it's best first to notice that we can rewrite the definition of the

convolution:

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{uv=n} f(u)g(v),$$

where the second sum is taken over all pairs of positive integers u and v such that $uv = n$. Written in this form, it's clear that $f * g = g * f$, and we also see that

$$((f * g) * h)(n) = \sum_{uvw=n} f(u)g(v)h(w) = (f * (g * h))(n).$$

d. What is $f * I$ equal to?

Since $I(n/d) = 1$ only if $d = n$ and is zero otherwise, we get $(f * I)(n) = f(n)$, that is, $f * I = f$. That is, I is the identity element for the convolution operation.

e. What is $\mu * u$ equal to?

Well, note first that $(\mu * u)(1) = \mu(1)u(1) = 1$. Next, if p is a prime then

$$(\mu * u)(p^k) = \mu(1)u(p^k) + \mu(p)u(p^{k-1}) + \mu(p^2)u(p^{k-2}) + \dots + \mu(p^k)u(1) = 1 + (-1)u(p^k) + 0 + \dots + 0 = 0.$$

Since we already know that $\mu * u$ is multiplicative, it follows by factoring any $n > 1$ as a product of prime powers that $(\mu * u)(n) = 0$ unless $n = 1$. Thus, $\mu * u = I$. In other words, μ is the inverse of u with respect to the convolution operation.

f. 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.

In the language of convolutions, we are being asked to prove that $F = f * u$ if and only if $f = F * \mu$. Here we go: If $F = f * u$, then

$$F * \mu = (f * u) * \mu = f * (u * \mu) = f * I = f;$$

conversely, if $f = F * \mu$ then

$$f * u = (F * \mu) * u = F * (\mu * u) = F * I = F.$$

(To see the value of the language of convolutions, try proving this directly!)

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 $f(s) = 1/\zeta(s)$.

To show convergence when $s > 1$, just notice that

$$\left| \frac{\mu(n)}{n^s} \right| \leq \frac{1}{n^s},$$

and use the comparison test for absolute convergence.

Since both series converge absolutely when $s > 1$, we can multiply them and see what we get. So we get something like this:

$$\left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^s} \right) \left(\sum_{e=1}^{\infty} \frac{1}{e^s} \right) = \sum_{d,e=1}^{\infty} \frac{\mu(d)}{d^s e^s} = \sum_{d,e=1}^{\infty} \frac{\mu(d)}{(de)^s}.$$

Now group together all the terms that have the same denominator, i.e., all the terms that have a given n^s in the denominator. Looking at the product above, we see that we get

$$\zeta(s)f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where

$$a_n = \sum_{d|n} \mu(d) = (\mu * u)(n).$$

Now use part (e) of the previous problem.