

**MATH 4400  
HOMEWORK 3  
COMMENTS AND SOLUTIONS**

**Problem 1:** Let  $\lambda(n) = (-1)^{a_1 + \dots + a_k}$ , where  $n = p_1^{a_1} \dots p_k^{a_k}$ . What is

$$\sum_{d|n} \lambda(d)?$$

If we define  $f(n) = \sum_{d|n} \lambda(d)$ , show that  $f(n)$  is not completely multiplicative (but that it is multiplicative).

**Solution:** We can figure it out first when  $n$  is a prime power, since  $\sum_{d|n} \lambda(d)$  must be a multiplicative function. Well,

$$\sum_{d|p^k} \lambda(d) = 1 + (-1) + 1 + (-1) + \dots + (-1)^k = \begin{cases} 0 & \text{if } k \text{ is odd} \\ 1 & \text{if } k \text{ is even} \end{cases}$$

and so the sum is a product of these over all the different prime powers in the factorization of  $n$ . Clearly, then, this sum is 0 if any prime dividing  $n$  appears an odd number of times, and 1 if all the exponents are even, which happens if and only if  $n$  is a perfect square.

So  $f(n) = 1$  if  $n$  is a square, and 0 otherwise. This is clearly multiplicative (which we already knew), but not completely multiplicative (e.g.  $f(2)f(2) = 0 \neq 1 = f(4)$ ).  $\square$

**Problem 2:** (a) Recall that  $\mathbf{1}(n) = 1$  for all  $n$ . What is  $\mathbf{1} \star \mathbf{1}$ ?

(b) Show that

$$\sigma_1(n) = \sum_{d|n} \varphi(d) \sigma_0\left(\frac{n}{d}\right).$$

(Hint: use part (a), and convolution.)

**Solution:** (a) We see that  $(\mathbf{1} \star \mathbf{1})(n) = \sum_{d|n} 1 \cdot 1 = \sigma_0(n)$ . So  $\mathbf{1} \star \mathbf{1} = \sigma_0$ .

(b) Remembering that  $i(n) = n$ , we have

$$\varphi \star \sigma_0 = \varphi \star (\mathbf{1} \star \mathbf{1}) = (\varphi \star \mathbf{1}) \star \mathbf{1} = i \star \mathbf{1} = \sigma_1,$$

where the last equality is clear if you write it out.  $\square$

**Problem 3:** (a) For which  $n$  is  $\sigma_0(n)$  odd?

(b) A prison with 1000 inmates is overcrowded. The warden decides to let certain prisoners go free, via the following scheme:

The cells, one for each prisoner, are arranged in a circular fashion, with a small gap between cell 1 and 1000. In Step  $n$ , a guard goes to every  $n$ th cell (starting with cell  $n$  and ending with the cell numbered with the largest multiple of  $n$  less than or equal to 1000) and changes its state—if it's locked, he unlocks it; if it's unlocked, he locks it.

The guards start by locking every cell. No prisoner is allowed to leave until the process is completely finished. The guards first execute Step 1, then Step 2, then Step 3, and so on all the way through Step 1000 (which changes the state of cell 1000 but leaves the other

ones unchanged; in fact, Steps 501 through 1000 only change the state of one cell each). Whichever prisoner's cell is unlocked at the end of the process is free to go.

So which prisoners go free? (Hint: use part (a).)

**Solution:** (a) From the formula  $\sigma_0(n) = \prod_{i=1}^k (a_i + 1)$ , where  $n = p_1^{a_1} \cdots p_k^{a_k}$ , we see that  $\sigma_0(n)$  is odd if and only if all the  $a_i$  are even, which happens if and only if  $n$  is a perfect square. (There are, of course, other ways to see this without using the formula.)

(b) Cell  $n$  gets changed by step  $d$  if and only if  $d|n$ . So the total number of changes is clearly  $\sigma_0(n)$ , and a prisoner goes free if and only if  $\sigma_0(n)$  is odd. So exactly 31 prisoners go free, the ones with cell numbers that are perfect squares.  $\square$

**Problem 4:** (a) Show that if  $f$  is an arithmetic function such that  $f(1) \neq 0$ , there exists a function  $g$  such that  $f \star g = \delta$ . (Recall that  $\delta(n) = 1$  if  $n = 1$  and 0 otherwise.)

(b) Show that if  $f$  and  $f \star g$  are multiplicative, then  $g$  is multiplicative. Deduce that if  $f$  is multiplicative, then the function  $g$  defined in part (a) is as well.

**Solution:** (a) We define  $g$  inductively. First,  $g(1) = 1/f(1)$ . Next, suppose we have defined  $g(k)$  for  $k < n$  (note the typo in the hint on the problem set), so that  $(f \star g)(m) = \delta(m)$  for all  $m < n$ . Then define

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d \neq n}} g(d) f\left(\frac{n}{d}\right).$$

From the definition it is clear that  $(f \star g)(n) = \delta(n)$  as well. So we can define  $g$  in such a way that  $(f \star g)(n) = \delta(n)$  for all  $n$ , by induction.

(b) Suppose  $f$  and  $h = f \star g$  are multiplicative but  $g$  is not. Let  $a$  and  $b$  be positive integers with  $ab$  as small as possible such that  $g(a)g(b) \neq g(ab)$ . Note  $ab > 1$ . Now consider

$$\begin{aligned} h(a)h(b) &= \sum_{d|a} f(d)g\left(\frac{a}{d}\right) \sum_{e|b} f(e)g\left(\frac{b}{e}\right) \\ &= \sum_{d|a, e|b} f(d)f(e)g\left(\frac{a}{d}\right)g\left(\frac{b}{e}\right) \\ &= g(ab) + \sum_{\substack{d|a, e|b \\ de \neq 1}} f(de)g\left(\frac{ab}{de}\right) \\ &= g(a)g(b) + \sum_{r|ab, r \neq 1} f(r)g\left(\frac{ab}{r}\right) \\ &= g(a)g(b) + h(ab) - g(ab). \end{aligned}$$

So  $h(a)h(b) - h(ab) = g(a)g(b) - g(ab)$ . But the left side is 0 by assumption, and the right side is nonzero by assumption. This is a contradiction.

Of course it follows that the convolution inverse of a multiplicative function is multiplicative, because  $\delta$  is multiplicative.  $\square$

**Problem 5:** Let  $D_n$  be the set of positive divisors of  $n$ . Show that if  $a$  and  $b$  are relatively prime, the natural map

$$\psi: D_a \times D_b \rightarrow D_{ab}$$

defined by  $\psi(d, e) = de$  is a bijection.

**Solution:** To see that it is injective, suppose  $d_1e_1 = d_2e_2$ . Then  $d_1|d_2e_2$ . But  $d_1$  and  $e_2$  are relatively prime, because any common divisor they have would be a common divisor of  $a$  and  $b$ . So  $d_1|d_2$ . But of course we can make the same argument to prove that  $d_2|d_1$ . So  $d_1 = d_2$ , and hence  $e_1 = e_2$ .

To see that it is surjective, let  $r$  be a divisor of  $ab$ . Then let  $d = \gcd(a, r)$ . Clearly  $d|a$ . Now, since  $(r/d)|(a/d)b$  and  $r/d$  and  $a/d$  are relatively prime (why?), we know that  $(r/d)|b$ . So  $r$  can be written as  $d(r/d)$ , the product of a divisor of  $a$  with a divisor of  $b$ .  $\square$

**Problem 6:** Let  $S_n$  be the set of solutions in  $\mathbb{Z}/n\mathbb{Z}$  to the congruence  $x^2 \equiv 1 \pmod{n}$ . For the rest of the problem, let  $p$  be an odd prime. Of course  $S_2 = \{1\}$  and  $S_p = \{\pm 1\}$ .

(a) Show that  $S_{p^k} = \{\pm 1\}$ .

(b) Show that  $S_{2p^k} = \{\pm 1\}$ .

(c) Show that if  $\gcd(a, b) = 1$ , then the bijection  $(\mathbb{Z}/ab\mathbb{Z})^* \rightarrow (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$  restricts to a bijection  $S_{ab} \rightarrow S_a \times S_b$ .

(d) Show that  $S_4 = \{\pm 1\}$  and  $S_{2^k} = \{\pm 1, \pm 1 + 2^{k-1}\}$  for  $k \geq 3$ .

(e) Now for the punchline: Show that the product

$$\prod_{\substack{1 \leq x \leq m \\ \gcd(x, m) = 1}} x = \prod_{x \in S_m} x,$$

and deduce a formula for this product in terms of the prime factorization of  $m$ .

**Solution:** (a) We do this by induction. Suppose that we have shown that  $S_{p^k} = \{\pm 1\}$ . (The base case was obvious.) Now what is  $S_{p^{k+1}}$ ? Well, anything in  $S_{p^{k+1}}$  has to reduce mod  $p^k$  to something in  $S_{p^k}$ , so it has to be of the form  $\pm 1 + ap^k$ . Squaring this and considering the result mod  $p^{k+1}$ , we get  $1 + 2ap^k$ . For this to be 1, we must have  $p|a$ , so our original element must be  $\pm 1$ .

(b) Something in  $S_{2p^k}$  has to be congruent to  $\pm 1 \pmod{p^k}$ , and congruent to 1 mod 2. The Chinese Remainder Theorem shows that these congruences have only the solutions  $\pm 1 \pmod{2p^k}$ .

(c) Of course, if  $x^2 \equiv 1 \pmod{ab}$ , then  $x^2 \equiv 1 \pmod{a}$  and mod  $b$ , so the image of  $S_{ab}$  lands in  $S_a \times S_b$ . And the restriction of an injective map remains injective. It only remains to show that the restriction is surjective; that is, if  $x^2 \equiv 1 \pmod{a}$  and  $x^2 \equiv 1 \pmod{b}$ , then  $x^2 \equiv 1 \pmod{ab}$  (anything in  $S_a \times S_b$  must come from something in  $(\mathbb{Z}/ab\mathbb{Z})^*$ , because the original map is surjective—we must only show that that something is actually in  $S_{ab}$ ). But this fact follows from the Chinese Remainder Theorem.

(d) Of course  $S_4 = \{\pm 1\}$ . And  $S_8 = \{\pm 1, \pm 1 + 4\}$ . Now we prove the general result by induction. Suppose  $S_{2^k} = \{\pm 1, \pm 1 + 2^{k-1}\}$ . Consider  $x \in S_{2^{k+1}}$ . By considering  $x \pmod{2^k}$ , we get that  $x = \pm 1 + a2^{k-1}$ , where  $a = 0, 1, 2$ , or  $3$ . Squaring this, we get  $1 + a2^k + a^22^{2k-2}$ . Note that  $2k - 2 \geq k + 1$  since  $k \geq 3$ , so this last term disappears mod  $2^{k+1}$ . So we see that  $x \in S_{2^{k+1}}$  if and only if  $a$  is even, so  $a = 0$  or  $2$ . This gives the four elements  $\pm 1, \pm 1 + 2^k$ .

(e) Suppose  $b$  is a prime power that doesn't divide  $a$ . The product  $\prod_{x \in S_{ab}} x$ , when considered mod  $a$ , equals

$$\left( \prod_{y \in S_a} y \right)^{|S_b|}.$$

This follows from the bijection in part (c). (When we look at the bijective image of  $S_{ab}$  in  $S_a \times S_b$ , we get ordered pairs  $(y, z)$ ; when we fix  $y$  there are  $|S_b|$  different  $z$ 's that go with it.)

Suppose that  $n = p_1^{a_1} \cdots p_k^{a_k}$ , and suppose  $k$  is at least 2 (as otherwise we know exactly what  $S_n$  is, and we can compute the product of the elements in  $S_n$  directly; see below). Since  $|S_b|$  is a multiplicative function of  $b$  (this again follows from the bijection in (c)),

$$\prod_{x \in S_n} x = \left( \prod_{y \in S_{p_1^{a_1}}} y \right)^c,$$

where  $c = \prod_{i=2}^k |S_{p_i^{a_i}}|$ .

Now, the product in the above parentheses is clearly either 1 or  $-1$  (it's  $-1$  unless  $p_1 = 2$  and  $a_1 \geq 3$ ). What about the exponent? Well, the only way that  $|S_{p^a}|$  is odd is if  $p^a = 2$  (otherwise, as we have seen, it's 2 if  $p$  is odd or  $p^a = 4$ , and it's 4 if  $p = 2$  and  $a \geq 3$ ). So the product we're trying to compute is almost always 1; the only way it can be  $-1$  if  $k \geq 2$  is if  $p_1$  is odd,  $p_2^{a_2} = 2$ , and  $k = 2$ . In short, the only way it can be  $-1$  when  $n$  is not a prime power is if  $n = 2p_1^{a_1}$ , which we already knew.

So to sum up, we have shown that the product is  $-1$  if  $n$  is a power of an odd prime, twice a power of an odd prime, or 4; otherwise it's 1. (Note that the product is  $-1$  if and only if  $(\mathbb{Z}/n\mathbb{Z})^*$  is cyclic. This is not a coincidence; perhaps you might think about whether you could prove this directly.)  $\square$

**Problem 7:** This exercise is devoted to the proof of the *Erdős-Ginsburg-Ziv Theorem*: Let  $a_1, \dots, a_{2n-1}$  be integers. Then there is some subset  $I$  of  $\{1, \dots, 2n-1\}$  such that  $|I| = n$  and  $\sum_{i \in I} a_i$  is divisible by  $n$ .

(a) First, note that the  $2n-1$  is sharp: find a sequence of  $2n-2$  integers such that no subsequence of  $n$  of them has a sum divisible by  $n$ . (Hint: use 0's and 1's.)

(b) Now let  $p$  be a prime. We will prove the theorem for  $n = p$  next, as follows: Define, in  $\mathbb{F}_p[x_1, \dots, x_{p-1}]$ ,

$$f(x_1, \dots, x_{p-1}) = x_1^{p-1} + \cdots + x_{p-1}^{p-1}, \quad g(x_1, \dots, x_{p-1}) = a_1 x_1^{p-1} + \cdots + a_{p-1} x_{p-1}^{p-1}.$$

Show that  $f$  and  $g$  have a nontrivial common zero.

(c) Explain why the nontrivial common zero you found in part (b) proves the theorem for  $n = p$ .

Now we proceed to prove the theorem for general  $n$  by induction: Let  $n = mp$  for some prime  $p$ , and suppose we have proved the theorem for  $m$ .

(d) Show that we can find  $2m-1$  disjoint subsets  $I_1, \dots, I_{2m-1}$  of  $\{1, \dots, 2n-1\}$  such that each  $I_j$  has  $p$  elements, and  $b_j = \sum_{i \in I_j} a_i$  is divisible by  $p$ .

(e) Now apply the inductive hypothesis to the set  $\{b_1/p, \dots, b_{2m-1}/p\}$ . Finish the proof.

**Solution:** (a) If  $a_1, \dots, a_{2n-2}$  consists of  $n-1$  0's and  $n-1$  1's, then no sum of  $n$  of the terms in this sequence can be divisible by  $n$ .

(b) This is a straightforward application of Chevalley-Waring, since the sum of the degrees of  $f$  and  $g$  is  $2p-2$  and the number of variables is  $2p-1$ . Since the total number of solutions is  $0 \pmod p$ , and there is one trivial solution (where all the  $x_i$  are 0), there must be a nontrivial solution as well.

(c) Suppose  $(c_1, \dots, c_{2p-1})$  is a nontrivial solution of  $f$  and  $g$ . Note that  $0 = f(c_1, \dots, c_{2p-1})$  is congruent mod  $p$  to the number of  $c_i$  that are nonzero. This follows by Fermat's little theorem. So the number of nonzero  $c_i$  is either 0 or  $p$ . It can't be 0 because then we'd be talking about the trivial solution. So exactly  $p$  of the  $c$ 's are nonzero. Let  $I$  be the set of indices  $i \in \{1, \dots, 2p-1\}$  such that  $c_i \neq 0$ .

Again, it follows from Fermat's little theorem that  $g(c_1, \dots, c_{2p-1}) = \sum_{i \in I} a_i$ . Since this sum is 0, it looks like we've constructed the subset we wanted.

(d) This is just a counting argument. Since  $2n-1 \geq 2p-1$ , we can certainly find a set of  $p$  indices such that the sum of the corresponding elements is divisible by  $p$ . (This is because of what we just proved in part (c), the base case for our induction argument.) Now throw out those  $p$  elements of our sequence to get a sequence of  $2n-1-p$  elements. Do the same thing and get a second subsequence of  $p$  integers whose sum is divisible by  $p$ . Throw those out. Keep going; at the end you'll have thrown out  $2m-2$  subsequences and be left with a remaining sequence of  $2n-1-(2m-2)p$  elements. But  $2n-1-(2m-2)p = 2p-1$ , so we have just enough elements left to apply part (c) one more time. This gives us  $2m-1$  subsequences (with disjoint sets of indices) in all.

(e) The inductive hypothesis says that there is some set  $I$  of size  $m$  such that  $\sum_{i \in I} b_i/p$  is divisible by  $m$ . So  $\sum_{i \in I} b_i$  is divisible by  $mp = n$ . But  $\sum_{i \in I} b_i$  is just the sum of the elements in  $m$  of the subsequences we found in part (d), each of size  $p$ . So putting them all together gives a subsequence of length  $mp = n$  whose sum is divisible by  $n$ . Hence the result follows by induction.  $\square$

*Remark:* It is common to reduce the proof of a statement that is supposed to hold for all  $n$  to that of the same statement for primes  $p$  (we saw this already when we discussed Fermat's Last Theorem, although the reduction to the case of prime exponent was much easier in that situation). So the really heavy lifting in this proof is going on in parts (b) and (c), and the reduction to Chevalley-Waring (i.e. the judicious choice of  $f$  and  $g$ ) is what makes this proof so clever and elegant.