

## Math 347 – Homework #6 solutions

posted October 18, 2008

### Solutions

1. We observed in class that the greatest common divisor of 0 and 0 does not exist, so we can restrict our attention to nonzero numbers  $n$ . Since every integer divides 0, the greatest common divisor of 0 and  $n$  is just the largest divisor of  $n$ , which is  $|n|$ . So  $\gcd(0, n) = 1$  exactly when  $|n| = 1$ , i.e., when  $n = \pm 1$ .
2. Suppose that  $d$  is a common divisor of  $2n + 5$  and  $3n + 7$ . Then  $d$  divides  $3(2n + 5) = 6n + 15$  and  $2(3n + 7) = 6n + 14$ . Hence  $d$  divides  $(6n + 15) - (6n + 14) = 1$ . Consequently, every common divisor of  $2n + 5$  and  $3n + 7$  is at most 1. Since 1 is a common divisor of  $2n + 5$  and  $3n + 7$ , it follows that 1 is the greatest common divisor of  $2n + 5$  and  $3n + 7$ . That is,  $2n + 5$  and  $3n + 7$  are relatively prime.
3. Let  $S_1 = \{d : d \mid a + b, d \mid a - b\}$ ,  $S_2 = \{d : d \mid 2a, d \mid a - b\}$  and  $S_3 = \{d : d \mid a + b, d \mid 2b\}$ . Then  $\gcd(a + b, a - b)$  is the maximal element of  $S_1$ , while  $\gcd(2a, a - b)$  and  $\gcd(a + b, 2b)$  are the maximal elements of  $S_2$  and  $S_3$ , respectively. So the claim will follow if we show that  $S_1 = S_2 = S_3$ .

First we show that  $S_1 = S_2$ . Suppose  $d \in S_1$ , so that  $d$  divides  $a + b$  and  $d$  divides  $a - b$ . Then  $d$  divides  $(a + b) + (a - b) = 2a$ . Since we were given that  $d$  divides  $a - b$  it follows that  $d \in S_2$ . Thus  $S_1 \subseteq S_2$ . Now suppose  $d \in S_2$ , so that  $d$  divides  $2a$  and  $d$  divides  $a - b$ . Then  $d$  divides  $2a - (a - b) = a + b$ . Since we are given that  $d$  divides  $a - b$ , it follows that  $d \in S_1$ . Hence  $S_2 \subseteq S_1$ . Thus  $S_2 = S_1$ .

We can show similarly that  $S_1 = S_3$ . Suppose  $d \in S_1$ , so that  $d$  divides  $a + b$  and  $d$  divides  $a - b$ . Then  $d$  divides  $(a + b) - (a - b) = 2b$ . Since we are given that  $d$  divides  $a + b$ , it follows that  $d \in S_3$ . Hence  $S_1 \subseteq S_3$ . Now suppose  $d \in S_3$ , so that  $d$  divides  $a + b$  and  $d$  divides  $2b$ . Then  $d$  divides  $(a + b) - 2b = a - b$ . Since we are given that  $d$  divides  $a + b$ , it follows that  $d \in S_1$ . Hence  $S_3 \subseteq S_1$ . Thus  $S_3 = S_1$ .

So  $S_1 = S_2 = S_3$ .

4. Suppose  $k \geq 3$  and that  $k - 2$  divides  $2k$ . In this case we can write  $2k = (k - 2)q$  for some integer  $q$ , and so (since  $k - 2 \neq 0$ ) we have  $2k / (k - 2) = q$ . In particular,

$2k/(k-2)$  is an integer. But

$$\frac{2k}{k-2} = 2 + \frac{4}{k-2}.$$

From this we see that  $2k/(k-2)$  is larger than 2 for every integer  $k \geq 3$ . Moreover, we see that if  $k > 6$ , then  $2k/(k-2) < 2 + 4/4 = 3$ . So if  $k > 6$ , we have that  $2k/(k-2)$  is strictly between 2 and 3, and so cannot be an integer.

So we only have to check the values  $3 \leq k \leq 6$ . Doing so, we find the divisibility relation holds precisely when  $k = 3, 4$ , or  $6$ .

5. Suppose  $c$  is divisible by the relatively prime numbers  $a$  and  $b$ . Since  $b$  divides  $c$ , we can write  $c = bq$  for some integer  $q$ . Since  $a$  divides  $c = bq$ , it follows from Proposition 6.6 that  $a$  divides  $q$ . Hence  $q = am$  for some integer  $m$ . Then  $c = bam = (ab)m$ , so that  $ab$  divides  $c$ , as was to be shown.
6. (a) Yes, either  $a$  or  $b$  must be even. To see this, suppose that  $a^2 + b^2 = c^2$  for integers  $a, b$ , and  $c$  where both  $a$  and  $b$  are odd. Then  $a = 2k + 1$  for some integer  $k$  and  $b = 2l + 1$  for some integer  $l$ , and hence

$$a^2 + b^2 = (4k^2 + 4k + 1) + (4l^2 + 4l + 1) = 4(k^2 + k + l^2 + l) + 2.$$

From this we see that  $a^2 + b^2 = c^2$  is even. Since the square of an odd integer is odd, it must be that  $c$  is even, so we can write  $c = 2m$  for some integer  $m$ . Then writing the equality  $a^2 + b^2 = c^2$  in terms of  $k, l, m$  we find

$$4(k^2 + k + l^2 + l) + 2 = (2m)^2 = 4m^2.$$

Rearranging shows that

$$2(m^2 - (k^2 + k + l^2 + l)) = 1.$$

But this implies that 1 is a multiple of 2, which is false (since  $2 > 1$ ).

- (b) We suppose now that  $a^2 + b^2 = c^2$ , where 3 divides  $c$ . Write  $c = 3k$  for some integer  $k$ , and (using the division algorithm) write  $a = 3q_1 + r_1$  and  $b = 3q_2 + r_2$ , where  $r_1, r_2 \in \{0, 1, 2\}$ . Writing the equality  $a^2 + b^2 = c^2$  in terms of  $k, q_1, q_2, r_1$ , and  $r_2$ , we find

$$9q_1^2 + 6q_1r_1 + r_1^2 + 9q_2^2 + 6q_2r_2 + r_2^2 = 9k^2.$$

Rearranging we find that

$$r_1^2 + r_2^2 = 3(3k^2 - 3q_1^2 - 2q_1r_1 - 3q_2^2 - 2q_2r_2).$$

In particular,  $r_1^2 + r_2^2$  is a multiple of 3. But checking all the possibilities for  $r_1, r_2 \in \{0, 1, 2\}$ , we see that  $r_1^2 + r_2^2$  is a multiple of 3 only when  $r_1 = r_2 = 0$ . Hence  $a = 3q_1$  and  $b = 3q_2$ , so that both  $a$  and  $b$  are multiples of 3, as was to be shown.

7. We begin by recalling that for the values of  $k$  under consideration,  $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ , so that

$$p! = \binom{p}{k} k!(p-k)! = \binom{p}{k} k(k-1) \cdots 2 \cdot 1 \cdot (p-k)(p-k-1) \cdots 2 \cdot 1.$$

Since  $p! = p(p-1)!$  is divisible by  $p$ , it follows from Proposition 6.7 that  $p$  must divide either  $\binom{p}{k}$  or one of the numbers  $k, k-1, \dots, 1$  or one of the numbers  $p-k, p-k-1, \dots, 2, 1$ . Since  $k \leq p-1$ , none of the numbers in the first list can be divisible by  $p$  (since they are all smaller than  $p$ ) and similarly, since  $k \geq 1$ , none of the numbers in the second list can be divisible by  $p$ . So it must be that  $p$  divides  $\binom{p}{k}$ .

8. By unique factorization, the positive divisors of  $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$  are exactly the numbers of the form  $2^{e_1} 3^{e_2} 5^{e_3} 7^{e_4} 11^{e_5} 13^{e_6} 17^{e_7} 19^{e_8}$ , where each  $e_i \in \{0, 1\}$ . Since there are two possibilities for each  $e_i$ , by the rule of product, the total number of positive divisors is  $2^8 = 256$ . Similarly, the positive divisors of  $2^2 3^3 5^5$  are exactly the numbers of the form  $2^{e_1} 3^{e_2} 5^{e_3}$ , where  $e_1 \in \{0, 1, 2\}$ ,  $e_2 \in \{0, 1, 2, 3\}$ , and  $e_3 \in \{0, 1, 2, 3, 4, 5\}$ . Since there are 3 possibilities for  $e_1$ , 4 possibilities for  $e_2$ , and 6 possibilities for  $e_3$ , the number of positive divisors of  $2^2 3^3 5^5$  is  $3 \cdot 4 \cdot 6 = 72$ .

9. We prove the contrapositive: if  $n$  is not prime, then  $2^n - 1$  is not prime. First notice that if  $n = 1$ , then  $2^n - 1 = 1$ , and so is not prime. If  $n > 1$  is not prime, then we can write  $n = ab$ , where  $a$  and  $b$  are integers and  $1 < a, b < n$ . We then substitute  $x = 2^a$  into the algebraic identity

$$x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + \cdots + x + 1) \tag{1}$$

to find that

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1).$$

Notice that both factors on the right hand side are integers, since they are sums and products of integers. Thus  $2^a - 1$  is a divisor of  $2^n - 1$ . Moreover, since  $a > 1$ , we have  $2^a - 1 > 1$ , and since  $a < n$ , we have  $2^a - 1 < 2^n - 1$ . It follows that  $2^a - 1$  is a divisor of  $2^n - 1$  different from 1 and different from  $2^n - 1$ . So  $2^n - 1$  is not prime.

10. Suppose that  $2^n - 1$  is prime. Let  $p$  denote  $2^n - 1$ , and let  $N = 2^{n-1}p$ . We claim that the sum of all the positive divisors of  $N$  is  $2N$ . This implies that the sum of the positive divisors of  $N$  that are less than  $N$  is  $2N - N = N$ , and so proves that  $N$  is perfect (as desired).

To prove the claim we first list the divisors of  $N$ . By unique factorization, the positive divisors of  $N$  are exactly the numbers  $2^{e_1}p^{e_2}$ , where  $e_1 \in \{0, 1, \dots, n-1\}$  and  $e_2 \in \{0, 1\}$ . The divisors for which  $e_2 = 0$  are precisely

$$1, 2, 4, 8, \dots, 2^{n-1}$$

and those for which  $e_2 = 1$  are precisely

$$p, 2p, 4p, 8p, \dots, 2^{n-1}p.$$

So the sum of all the positive divisors of  $N$  is

$$(1 + 2 + \dots + 2^{n-1}) + p(1 + 2 + \dots + 2^{n-1}) = (1 + p)(1 + 2 + \dots + 2^{n-1}).$$

Recalling the definition of  $p$  we see that the first factor on the right hand side here is  $2^n$ . The second factor can be written in closed form as  $2^n - 1$ , as we see by taking  $x = 2$  and  $b = n$  in the identity (1) above. So the sum of all the positive divisors of  $N$  is  $2^n \cdot (2^n - 1)$ , which is exactly  $2N$  by the definition of  $N$ .