

MATH 521A EXAM 1 SOLUTIONS  
Sep 24, 2007

1. (10 pts) Let  $a, b \in \mathbb{Z}$  and  $d = \gcd(a, b)$ . If  $a = da'$  and  $b = db'$ , show that  $\gcd(a', b') = 1$ .

Let  $d' = \gcd(a', b')$ . If  $d = \gcd(a, b)$  then there exist  $s, t \in \mathbb{Z}$  such that  $d = sa + tb = sda' + tdb' = d(sa' + tb')$ . Hence  $1 = sa' + tb'$ . Since  $d'|a'$  and  $d'|b'$ ,  $d'|sa' + tb' = 1$ . Being a greatest common divisor,  $d' \in \mathbb{Z}^+$ . The only positive integer which divides 1 is 1. So  $d' = 1$ .

2. (10 pts) Let  $a$  and  $b$  be positive integers and let  $m = \text{lcm}(a, b)$ . If  $s$  is a multiple of both  $a$  and  $b$ , prove that  $s$  is a multiple of  $m$ .

Let  $s$  be a common multiple of  $a$  and  $b$ . By the Division Algorithm,  $s = qm + r$  for some  $q, r \in \mathbb{Z}$  with  $0 \leq r < m$ . Since  $a|s$  and  $a|m$ ,  $a|s - qm = r$ . Similarly,  $b|r$ . But  $r < m$  and  $m$  is the smallest positive integer which is a common multiple of  $a$  and  $b$ . Hence  $r$  must be 0 and  $m|s$ .

3. (10 pts) Show that  $5n + 3$  and  $7n + 4$  are relatively prime for all  $n \in \mathbb{Z}$ .

Let  $d = \gcd(5n + 3, 7n + 4)$ . Notice that  $7(5n + 3) - 5(7n + 4) = 35n + 21 - 35n - 20 = 1$ . Since  $d|5n + 3$  and  $d|7n + 4$ ,  $d|1$ . But the only positive divisor of 1 is 1. So  $d = 1$ .

4. (10 pts) Use the Euclidean Algorithm to find  $\gcd(238, 850)$ .

$$850 = 3 \cdot 238 + 136$$

$$238 = 136 + 102$$

$$136 = 102 + 34$$

$$102 = 3 \cdot 34 + 0$$

By the Euclidean Algorithm,  $\gcd(238, 850) = 34$ .

5. (10 pts) Let  $a, b \in \mathbb{Z}$ . Euclid's Lemma says that if  $p$  is a prime and  $p|ab$ , then  $p|a$  or  $p|b$ . Give a proof.

If  $p|a$ , we are done. If  $p \nmid a$ , then  $\gcd(a, p) = 1$ , since 1 is the only other positive divisor of  $p$ . Hence there exist  $s, t \in \mathbb{Z}$  such that  $1 = sa + tp$ . Multiply both sides by  $b$  to get  $b = sab + tpb$ . Since  $p|ab$ ,  $p$  divides each term on the right-hand side. Therefore  $p|b$ .

6. (10 pts) **Extra credit problem.** Let  $a, b \in \mathbb{Z}^+$ . Prove that  $\gcd(a, b)\text{lcm}(a, b) = ab$ . (Hint: Look at  $ab/\gcd(a, b)$ . First prove that it is a common multiple of  $a, b$  then that it is the least common multiple.)

You may use the result of problem 2 if you need it.

Let  $d = \gcd(a, b)$  and

$$m = \frac{ab}{d} = a \frac{b}{d} = \frac{a}{d} b.$$

Since  $d|b$ ,  $b/d \in \mathbb{Z}$ , hence  $m$  is a multiple of  $a$ . Similarly,  $m$  is a multiple of  $b$ .

Let  $l = \text{lcm}(a, b)$ . By the result of problem 2 above,  $l|m$ . Let  $m = ql$ . So  $qld = ab$ . Then

$$(qd) \frac{l}{b} = a \quad (qd) \frac{l}{a} = b.$$

Since  $l/a$  and  $l/b$  are integers,  $qd$  divides both  $a$  and  $b$ . But  $d$  is the greatest common divisor of  $a, b$ , hence  $q$  must be 1. This shows that  $m = l$ . Hence  $ab = dm = dl$ , which is what we wanted to prove.