MATH 302 Assignment 1
May 7, 2009 Solutions

Problem 1. Let a, b, c, j, k be positive integers such that

$$a = cj, \qquad b = ck.$$

(a) Prove the implication: If $\operatorname{lcm}(j,k) = m$, then $\operatorname{lcm}(a,b) = cm$.

(b) Is the converse implication true? Justify your answer.

Proof. Let

$$S = \{x \in \mathbb{Z} : x > 0,\ j|x,\ k|x\}$$

and

$$T = \{y \in \mathbb{Z} : y > 0,\ a|y,\ b|y\}.$$

By Proposition 1.3.9 the set S has a minimum and T has a minimum. By Definition 2.1.6

$$\operatorname{lcm}(j,k) = \min S \qquad \text{and} \qquad \operatorname{lcm}(a,b) = \min T.$$

Proof of (a). Assume that $m = \operatorname{lcm}(j,k) = \min S$. Then $m \in S$, that is m is a positive multiple of j and k. Therefore, there exist integers u, v such that $m = uj$, $m = vk$. Multiplying the last two equations by c we get $mc = ujc$ and $mc = vkc$. Since $a = cj$ and $b = ck$, we get $mc = ua$ and $mc = vb$. Thus mc is a multiple of both a and b. Moreover, since $c > 0$, $mc > 0$. Hence $mc \in T$. Therefore $\operatorname{lcm}(a,b) \le mc$.

I still need to prove $\operatorname{lcm}(a,b) \ge mc$. Here is a proof. To prove this I will use the fact that $m = \min S$. Set $n = \operatorname{lcm}(a,b)$. Then n is a positive common multiple of a and b. Therefore, there exist $w, z \in \mathbb{Z}$ such that $n = aw$, $n = bz$. Since $a = cj$ and $b = ck$, we get $n = cjw$, $n = ckz$. Thus n is a multiple of c and $n = cf$ where $f = jw = kz$. Since both n and c are positive f is positive. Also f is a common multiple of j and k. Therefore $f \in S$. Hence $f \ge m$. Since $c > 0$, we get $fc \ge mc$. Recall that $n = cf$. Thus, $n \ge mc$. So, we proved $\operatorname{lcm}(a,b) \ge mc$.

Proof of (b). The converse implication is true and the proof is similar to the proof of (a).

Assume that $mc = \operatorname{lcm}(a,b) = \min T$. Then $mc \in T$, that is mc is a positive multiple of a and b. Therefore, there exist integers q, r such that $mc = qa$, $mc = rb$. Since $a = cj$ and $b = ck$, we get $mc = qjc$ and $mc = rkc$. Therefore $m = qj = rk$. Thus m is a positive common multiple of j and k. That is, $m \in S$. Therefore $m \ge \operatorname{lcm}(j,k)$.

I still need to prove $\operatorname{lcm}(j,k) \ge m$. Here is a proof. To prove this I will use the fact that $mc = \min T$. Set $o = \operatorname{lcm}(j,k)$. Then o is a positive common multiple of j and k. Therefore, there exist $s, t \in \mathbb{Z}$ such that $o = sj$, $o = tk$. Multiplying the last two equalities by c we get $oc = sjc = tkc$. Since $a = cj$ and $b = ck$, we get $oc = sa = tb$. Thus oc is a common multiple of a and b. Moreover oc is positive. Thus $oc \in T$. Therefore $oc \ge mc$. Since $c > 0$ we conclude that $o \ge m$. Thus $\operatorname{lcm}(j,k) \ge m$ is proved. □

Before before doing remaining problems I will prove two lemmas.

Lemma 1. If a and b are relatively prime and $c > 0$, then $\gcd(ac, bc) = c$.

Proof. Assume that a and b are relatively prime and $c > 0$. Set $d = \gcd(ac, bc)$. Clearly c is a common divisor of both ac and bc. Since d is the greatest common divisor of ac and bc we get $c \leq d$. By Theorem 2.1.3 there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiplying by c we get $acx + bcy = c$. Since d is common divisor of ac and bc, there exist $u, v \in \mathbb{Z}$ such that $ac = du$ and $bc = dv$. Hence $dux + dvy = c$. Thus $d(ux + vy) = c$. Since both d and c are positive, we conclude that $ux + vy$ is positive and consequently $d \leq c$. So, we proved $c \leq d$ and $d \leq c$. Consequently $d = c$. □

Lemma 2. Let $c \in \mathbb{Z}$. If d is a positive integer such that $d|c$ and $d|(c+1)$, then $d = 1$.

Proof. Assume that $d > 0$, $d|c$ and $d|(c+1)$ Consequently $d|(-c)$. By Proposition 1.2.3 we get $d\big|\big((c+1) - c\big)$, that is $d|1$. Since $d > 0$ we deduce that $d = 1$. □

Problem 2. Let $k \in \mathbb{N}$. Let $t_k = \dfrac{k(k+1)}{2}$ be the k-th triangular number. Find the formula for $\gcd(t_k, t_{k+1})$ in terms of k. Prove that your formula is correct.

Proof. If k is even, then $\gcd(t_k, t_{k+1}) = k+1$. Assume that k is even and set $k = 2j$, where $j \in \mathbb{N}$. Then $t_k = j(2j+1)$ and $t_{k+1} = (2j+1)(j+1)$. Since $\gcd(j, j+1) = 1$, by Lemma1, we conclude that $\gcd(t_k, t_{k+1}) = 2j+1 = k+1$. (Here is a proof that $\gcd(j, j+1) = 1$. Set $d = \gcd(j, j+1)$. Then $d|(j+1)$ and $d|j$. By Lemma 2, $d = 1$. Thus $\gcd(j, j+1) = 1$.)

If k is odd, then $\gcd(t_k, t_{k+1}) = (k+1)/2$. Assume that k is odd and set $k = 2j-1$, where $j \in \mathbb{N}$. Then $t_k = (2j-1)j$ and $t_{k+1} = j(2j+1)$. Next I will prove that Since $\gcd(2j-1, 2j+1) = 1$. Set $d = \gcd(2j-1, 2j+1)$. Then $d|(2j-1)$ and $d|(2j+1)$. Consequently, $d\big|\big((2j+1) - (2j-1)$, that is $d|2$. Hence $d = 1$ or $d = 2$. Since $2j+1$ is odd, 2 does not divide $2j+1$. Since $d|(2j+1)$ we conclude $d \neq 2$. Therefore, $d = 1$. By Lemma1, since $\gcd(2j-1, 2j+1) = 1$ we have $\gcd((2j-1)j, (2j+1)j) = j$. Since $t_k = (2j-1)j$, $t_{k+1} = j(2j+1)$ and $j = (k+1)/2$, the claim is proved. □

Problem 3. Let a and b be nonzero integers. Prove that a and b are relatively prime if and only if there exists an integer c such that $a|c$ and $b|(c+1)$.

Proof. Assume that a and b are relatively prime. Then $\gcd(a, b) = 1$. By Theorem 2.1.3 there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Set $c = -ax$. Then, $a|c$. Also, $by = 1 - ax = 1 + c$. Therefore $b|(c+1)$. This proves the existence of $c \in \mathbb{Z}$ such that $a|c$ and $b|(c+1)$.

Assume that there exists $c \in \mathbb{Z}$ such that $a|c$ and $b|(c+1)$. Let $d = \gcd(a, b)$. Then d is a positive number and $d|a$ and $d|b$. Since $a|c$ and $b|(c+1)$, we conclude that $d|c$ and $d|(c+1)$. By Lemma 2 we deduce that $d = 1$. Thus, a and b are relatively prime. □

Problem 4. Let a and b be integers, not both zero. Let $d = \gcd(a, b)$. Prove that $\gcd(a^2, b^2) = d^2$. (Hint: First consider the special case of relatively prime integers a and b.)

Proof. Let a and b be integers, not both zero. Assume that $\gcd(a, b) = 1$. Set $g = \gcd(a^2, b^2)$. I need to prove that $g = 1$. (I will use Michael's brilliant idea here.) By Theorem 2.1.3 there exist integers x and y such that $ax + by = 1$. Now do some algebra

$$1 = 1^3 = (ax+by)^3 = a^3x^3 + 3a^2x^2by + 3axb^2y^2 + b^3y^3 = a^2\big(ax^3 + 3x^2by\big) + b^2\big(3axb^2y^2 + by^3\big).$$

Set $u = ax^3 + 3x^2by$ and $v = 3axb^2y^2 + by^3$. Thus $a^2u + b^2v = 1$. Since $g = \gcd(a^2, b^2)$, there exist $s, t \in \mathbb{Z}$ such that $a^2 = gs$ and $b^2 = gt$. Hence

$$1 = a^2u + b^2v = gsu + gtv = g(su + tv),$$

that is $g|1$. Since $g > 0$ we conclude $g = 1$. This completes the first part of the proof.

Now assume that $d = \gcd(a, b) > 1$. Then there exist $j, k \in \mathbb{Z}$ such that $a = dj$ and $b = dk$. By Proposition 2.2.5 it follows that $\gcd(j, k) = 1$. By the first part of this proof it follows that $\gcd\big(j^2, k^2\big) = 1$. Since $a^2 = d^2 j^2$ and $b^2 = d^2 k^2$ and since j^2 and k^2 are relatively prime, Lemma 1 implies that

$$\gcd(a^2, b^2) = \gcd\big(d^2 j^2, d^2 k^2\big) = d^2.$$

□

Problem 5. Let a and b be positive integers. Prove that $(b^2)|(a^2)$ if and only if $b|a$.

Proof. Assume first that $b|a$. Then there exists $u \in \mathbb{Z}$ such that $a = bu$. Then $a^2 = b^2 u^2$. Since $u^2 \in \mathbb{Z}$ and $b^2 > 0$, this means $(b^2)|(a^2)$.

Now assume that $(b^2)|(a^2)$. Set $d = \gcd(a, b)$. Then by Problem 4, $\gcd(a^2, b^2) = d^2$. But, since $(b^2)|(a^2)$, we know that $\gcd(a^2, b^2) = b^2$. Hence $d^2 = b^2$, that is

$$0 = d^2 - b^2 = (d - b)(d + b).$$

Since $b > 0$ and $d > 0$ we have $d + b > 0$. Therefore, $d - b = 0$, that is $d = b$. Since $d|a$ we conclude that $b|a$. □