M403 Homework 6

Enrique Areyan
October 10, 2012

1. In what follows (a),(b) and (c), to compute gcd use this fact: $gcd(b,a) = gcd(b-a,a)$.

   (a) $gcd(1599,481) = gcd(1118,481) = gcd(637,481) = gcd(481,156) = gcd(325,156) = gcd(169,156) = gcd(156,13) = 13$. In the last step I used the fact that the gcd of a prime and a composite is the prime number. In this case 13 is prime and $156 = 2 \cdot 78$ so is a composite.

   (b) $gcd(3108,1147) = gcd(1961,1147) = gcd(1147,814) = gcd(814,333) = gcd(481,333) = gcd(333,148) = gcd(185,148) = gcd(148,37) = gcd(111,37) = gcd(74,37) = gcd(37,37) = 37$

   (c) $gcd(2460,123) = gcd(2337,123) = gcd(2214,123) = gcd(2091,123) = gcd(1968,123) = gcd(1845,123) = gcd(1722,123) = gcd(1599,123) = gcd(1476,123) = gcd(1353,123) = gcd(1230,123) = gcd(1107,123) = gcd(984,123) = gcd(861,123) = gcd(738,123) = gcd(615,123) = gcd(492,123) = gcd(369,123) = gcd(246,123) = gcd(123,123) = 123$

2. (a) $gcd(2^1 \cdot 3^2 \cdot 5^3, 2^2 \cdot 3^2 \cdot 5^2) = 2^1 \cdot 3^2 \cdot 5^2$ and $lcm(2^1 \cdot 3^2 \cdot 5^3, 2^2 \cdot 3^2 \cdot 5^2) = 2^2 \cdot 3^2 \cdot 5^3$

   (b) $gcd(2^8 \cdot 5^9 \cdot 7^7, 2^3 \cdot 5^7 \cdot 7^2) = 2^3 \cdot 5^7 \cdot 7^2$ and $lcm(2^8 \cdot 5^9 \cdot 7^7, 2^3 \cdot 5^7 \cdot 7^2) = 2^8 \cdot 5^9 \cdot 7^7$

(1.68) (i) **False**. Since both $2^{19} \in \mathbb{Z}$ and $3^{12} \in \mathbb{Z}$, i.e., are integers, then the difference is also going to be an integer. Let $d = |2^{19} - 3^{12}|$. Then $d \in \mathbb{Z}^+$. Therefore, the original question: $d < \frac{1}{2}$, reduces to $d \leq 0$, since it cannot be a rational number. Right away we can see that $d \geq 0$ since d is a positive value (absolute value). So, we only need to check whether $d = 0$ or not. Suppose $d = 0$, then $2^{19} = 3^{12}$, but this is impossible since by the Fundamental Theorem of Arithmetic every number has a unique prime factorization and obviously 2 and 3 are prime, so the above factorization yields different numbers. Therefore, $d > 0$, which implies that $d > \frac{1}{2}$.

(ii) **True**. Suppose that $r = p_1^{g_1} \cdots p_n^{g_n}$, where p_i are distinct primes and g_i are integers. **Proof:** ($\Rightarrow$). Suppose r is an integer. Then by the Fundamental Theorem of Arithmetic there exists a unique factorization of r into primes. By Corollary 1.52, let $r = q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m}$, where $e_1 > 0$ be such a factorization. Then, up to indexing, $q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m} = p_1^{g_1} \cdots p_n^{g_n} \Rightarrow e_i = g_i > 0$.
($\Leftarrow$) Suppose $g_i \in \mathbb{Z}^+$ for all i. Then it is trivially true that r is an integer. Q.E.D.

(iii) **True**. Since $lcm(2^3 \cdot 3^2 \cdot 5 \cdot 7^2, 3^3 \cdot 5 \cdot 13) = lcm(2^3 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13^0, 2^0 \cdot 3^3 \cdot 5 \cdot 7^0 \cdot 13) = 2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 13 = = \frac{2^3 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13}{3^2 \cdot 5} = \frac{2^3 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13}{45}$

(iv) **True**. Let $a, b \in \mathbb{Z}^+$. Suppose that $d = gcd(a,b) \geq 2$. By the Fundamental Theorem of Arithmetic, we can write $d = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}$, where p_i is a distinct prime for all i and $e_i > 0$ for all i, and $n \geq 1$. By definition of gcd, we have that $d|a$ and $d|b$, i.e.,

$$p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n} | a \text{ and } p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n} | b \iff$$

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n} \cdot a' \text{ and } b = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n} \cdot b', \text{ for some } a', b' \in \mathbb{Z}$$

From which we can assert that at least some p_i divides both a and b, since

$$p_i^{e_i} | a \iff a = p_i^{e_i} a'', \text{ where } a'' = p_1^{e_1} \cdot p_2^{e_2} \cdots p_{i-1}^{e_{i-1}} \cdot p_{i+1}^{e_{i+1}} \cdots p_n^{e_n} \cdot a'$$

$$p_i^{e_i} | b \iff b = p_i^{e_i} b'', \text{ where } b'' = p_1^{e_1} \cdot p_2^{e_2} \cdots p_{i-1}^{e_{i-1}} \cdot p_{i+1}^{e_{i+1}} \cdots p_n^{e_n} \cdot b'$$

(v) **True**. Suppose that a and b are relatively prime, i.e., $gcd(a,b) = 1$. If that is the case, then a and b share no common factor. By the Fundamental Theorem of Arithmetic, we can write $a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}$ and $b = q_1^{f_1} \cdot q_2^{f_2} \cdots q_n^{f_n}$; for p_i and q_i prime for all i and all j and $e_i > 0$, $f_i > 0$ for all i. Since a and b are relatively prime, then $p_i \neq q_i$ for all i. Take the squares: $a^2 = (p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n})^2 = p_1^{2e_1} \cdot p_2^{2e_2} \cdots p_n^{2e_n}$. Likewise, $b^2 = (q_1^{f_1} \cdot q_2^{f_2} \cdots q_n^{f_n})^2 = q_1^{2f_1} \cdot q_2^{2f_2} \cdots q_n^{2f_n}$, which shows that a^2 and b^2 have no common factor. Hence, $gcd(a^2, b^2) = 1$

(1.69) (i) $gcd(210,48) = gcd(2 \cdot 3 \cdot 5 \cdot 7, 2^4 \cdot 3 \cdot 5^0 \cdot 7^0) = 2 \cdot 3 \cdot 5^0 \cdot 7^0 = 6$

(ii) Using the fact given in class that $gcd(b,a) = gcd(b - q \cdot a, a)$ for some $q \in \mathbb{Z}$. We can compute: $gcd(5678,1234) = gcd(5678 - 4 \cdot 1234) = gcd(1234,742) = gcd(742,492) = gcd(492,250) = gcd(242,8) = gcd(242 - 30 \cdot 8, 8) = gcd(2,8) = gcd(8 - 4 \cdot 2, 2) = gcd(0,2) = 2$

(1.70) (i) Let $m \geq 2$ be an integer.
($\Rightarrow$) Suppose that m is a perfect square. Then $m = a^2$ for some $a \in \mathbb{Z}$ such that $a \geq 2$. By the Fundamental Theorem of Arithmetic, we can write $a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}$ where p_i is a distinct prime for all i and $e_i > 0$ for all i, and $n \geq 1$. It follows that:

$m = a^2 = (p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n})^2 = p_1^{2e_1} \cdot p_2^{2e_2} \cdots p_n^{2e_n} \Rightarrow$ each of its prime factors occurs an even number of times

($\Leftarrow$) Suppose that each of m's prime factors occurs an even number of times. Then we can write

$$m = p_1^{2e_1} \cdot p_2^{2e_2} \cdots p_n^{2e_n} = (p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n})^2 = b^2 \quad \text{, for some } b \in \mathbb{Z} \Rightarrow \quad m \text{ is a perfect square. Q.E.D.}$$

(ii) Suppose that n is such that $\sqrt{n}$ is a rational number. Then we can write $\sqrt{n} = r \iff n = r^2$ where r is a rational number. Then, by Corollary 1.53, we can factor $r = p_1^{g_1} \cdot p_2^{g_2} \cdots p_n^{g_n}$ where p_i are distinct primes and g_i are nonzero integers. Replacing into the above equation: $n = (p_1^{g_1} \cdot p_2^{g_2} \cdots p_n^{g_n})^2 = p_1^{2g_1} \cdot p_2^{2g_2} \cdots p_n^{2g_n}$, which by above (1.70 (i)), implies that n is a perfect square.
This proves that if $\sqrt{n}$ is a rational number then n is a perfect square. It follows by contraposition that if n is not a perfect square, then $\sqrt{n}$ is not a rational number, i.e., irrational. Q.E.D.

(1.71) **Proof**. Let a and b be positive integers with $gcd(a, b) = 1$ and $a \cdot b$ a square. By the Fundamental Theorem of Arithmetic, we can write $a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdot p_2^{f_2} \cdots p_n^{f_n}$, where p_i are distinct primes and $e_i \geq 0$ and $f_i \geq 0$. Since $a \cdot b$ is a square this means that:

$$c^2 = a \cdot b = (p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n})(p_1^{f_1} \cdot p_2^{f_2} \cdots p_n^{f_n}) = p_1^{e_1+f_1} \cdot p_2^{e_2+f_2} \cdots p_n^{e_n+f_n}$$

Since $gcd(a, b) = 1$ then a and b don't have any common prime divisors. In particular this means that either $e_i = 0$ or $f_i = 0$ for all i, but not both can be greater than zero at the same time. Let $h_i = e_i$ if $f_i = 0$ or $h_i = f_i$ if $e_i = 0$. Then,

$$c^2 = a \cdot b = p_1^{h_1} \cdot p_2^{h_2} \cdots p_n^{h_2}$$

By previous exercise, c^2 (a perfect square) implies that all of its prime factors occur and even number of times. Therefore, $h_i = 2 \cdot k_i$ for all i. If we collect the primes coming from a and primes coming from b, we can conclude that each of these occur an even number of times and thus, both a and b are perfect square. Q.E.D

(1.72) **Proof by Contradiction**. Let $n = p^r m$, where p is prime and p does not divide m. Suppose that $p | \binom{n}{p^r}$. Since $a \cdot b$ is a square, then by the previous exercise

$\binom{n}{p^r}$	$=$	$p \cdot q$	for some $q \in \mathbb{Z}$
$\frac{n!}{(n-p^r)!p^r!}$	$=$	$p \cdot q$	by Pascal's formula
$n!$	$=$	$p \cdot q \cdot (n-p^r)!p^r!$	multiplying both sides by $(n-p^r)!p^r!$
$(p^r m)!$	$=$	$p \cdot q \cdot (n-p^r)!p^r!$	by hypothesis $n = p^r m$
$(p^r m)(p^r m - 1)!$	$=$	$p \cdot q \cdot (n-p^r)!(p^r)(p^r-1)!$	by definition of factorial
$(m)(p^r m - 1)!$	$=$	$p \cdot q \cdot (n-p^r)!(p^r-1)!$	dividing by p^r both sides

Let $q' = q \cdot (n-p^r)!(p^r-1)!$. Then $(m)(p^r m-1)! = p \cdot q' \iff p|(m)(p^r m-1)!$. Since p is prime, by Euclid's Lemma, either $p|m$ or $p|(p^r m-1)$. But, we assume that p does not divide m, therefore it must be the case that $p|(p^r m-1) \iff p|(p^r m-1) \cdot (p^r m-2) \cdots (p^r m - p^r m + 1)$ by definition of factorial.
Applying Euclid's Lemma again, we conclude that there exists a factor of the form $p^r m - i$, where $1 \leq i \leq p^r m - 1$ such that $p|p^r m - i \iff p^r m - i = p \cdot p'$ for some $p' \in \mathbb{Z}$, which is the same as $p^r m = p \cdot p' + i \Rightarrow p \nmid p^r m$. But, $p|p^r m$ since by Euclid's Lemma either $p|m$ or $p|p^r$. By hypothesis, $p \nmid m$ so $p|p^r \iff p^r = p \cdot t$, which is true, for instance just let $t = p^{r-1}$. Therefore, we have a contradiction since we concluded that $p|p^r m$ and $p \nmid p^r m$. It follows that our main assumption was wrong and the case is that $p \nmid \binom{n}{p^r}$.

(1.75) Let $M \geq 0$.

($\Rightarrow$) Suppose M is the least common multiple. Suppose to the contrary that there exists a common multiple of $a_1, a_2, ..., a_n$, call it d, such that $M \nmid d$. Then by the Division algorithm we have that $d = M \cdot q + r$ where $0 < r < M$, it follows that $r = d - M \cdot q$. By property of d, we have that $a_i|d$ for all i. This means that $d = a_i a_i'$. Also, $a_i|M$, meaning that $M = a_i b_i$. Replacing this into our equation for r we have that $r = d - M \cdot q = a_i a_i' - a_i b_i q = a_i(a_i' - b_i q) \Rightarrow a_i|r$ for all i. Hence, r is also a common multiple. However, from the division algorithm we have that $r < M$ but we assumed M to be the least common divisor. This is a contradiction that shows that for any other common divisor d the lcm M is such that $M|d$.

($\Leftarrow$) Suppose M is a common multiple of $a_1, a_2, ..., a_n$ which divides every other common multiple d. Then $M|d \iff d = M \cdot m'$. Take absolute values: $d = |d| = |M| \cdot |m'| \geq 1 \cdot |M| \geq M$, which shows that M is the smallest common multiple. Q.E.D.