Homework 4 Solutions

Tim Smits

1. Prove for all integers a, b, n that if $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, that $\gcd(ab, n) = 1$.

Solution: By Bezout, there are integers x_0, y_0, x_1, y_1 such that $ax_0 + ny_0 = 1$ and $bx_1 + ny_1 = 1$. Multiplying these expressions together, we find $(ax_0 + ny_0)(bx_1 + ny_1) = 1$, so $ab(x_0x_1) + n(ax_0y_1 + by_0x_1 + ny_0y_1) = 1$. This says $\gcd(ab, n) \mid 1$, so that $\gcd(ab, n) = 1$.

2. Let $a, b \neq 0$ be integers, let $k \in \mathbb{N}$. Prove that $\gcd(ka, kb) = k \cdot \gcd(a, b)$.

Solution: Let $d' = \gcd(ka, kb)$. By Bezout, there are integers x, y such that $ax + by = d$, where $d = \gcd(a, b)$. Multiplying by k, we see $ka(x) + kb(y) = kd$, so that $d' \mid kd$, which gives $d' \leq kd$. Now, since $d \mid a$ and $d \mid b$, we have $kd \mid ka$ and $kd \mid kb$, so that kd is a common divisor of ka and kb, so by definition we see $kd \leq d'$. This says $d' = kd$ as desired.

3.

(a) Let $S = \{p_1, \ldots, p_n\}$ be a finite set of primes. Prove that $P = p_1 \ldots p_n + 1$ has a prime factor not in S.

(b) Prove there are infinitely many primes.

(c) Let $P_n = p_1 \ldots p_n + 1$ where p_n is the n-th prime. Find n such that P_n is composite.

Solution:

(a) For each prime $p_i \in S$, notice that $p_i \nmid P$, because if $p_i \mid P$, then $p_i \mid (P - p_1 \ldots p_n)$, so $p_i \mid 1$, which is impossible. By the fundamental theorem of arithmetic, P is divisible by some prime number, and the above shows that it cannot be in S.

(b) Start with any finite list of primes, say $p_1, \ldots, p_n$. Then by part a), the number $P = p_1 \ldots p_n + 1$ is divisible by a prime not in this list. Therefore, starting with any finite list of primes we can find a new prime, which shows there must be infinitely many.

(c) Take $n = 6$: $P_6 = 30031 = 53 \cdot 509$.

4. Prove for integers a, b that if $\gcd(a, b) = 1$, then $\text{lcm}(a, b) = ab$.

Solution: Let $\ell = \text{lcm}(a, b)$. Since $a \mid ab$ and $b \mid ab$, by definition we see $\ell \leq ab$. On the other hand, since $a \mid \ell$ and $b \mid \ell$, since $\gcd(a, b) = 1$ we see that $ab \mid \ell$, so that $ab \leq \ell$ gives $\ell = ab$.

5. Prove that for any natural numbers a, b, k that $\text{lcm}(ka, kb) = k \cdot \text{lcm}(a, b)$.

Solution: Set $\ell' = \text{lcm}(ka, kb)$ and $\ell = \text{lcm}(a, b)$. Since $a \mid \ell$ and $b \mid \ell$, we see $ka \mid k\ell$ and $kb \mid k\ell$, so $\ell' \leq k\ell$. By definition, $ka \mid \ell'$ and $kb \mid \ell'$. Write $\ell' = (ka)x$ and $\ell' = (kb)y$ for some integers x, y. In particular, $k \mid \ell'$ so $\ell'' = \ell'/k$ is an integer. Then $\ell'' = ax = by$ is a multiple of both a and b, so $\ell \leq \ell''$ by definition of ℓ. Multiplying by k says $k\ell \leq k\ell'' = \ell'$, so that $k\ell = \ell'$.

6. Let $a, b \in \mathbb{N}$. Prove that $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.

Solution: Set $d = \gcd(a, b)$. Then $a = a'd$ and $b = b'd$ for some relatively prime integers a', b'. By the previous two problems, $\text{lcm}(a, b) = \text{lcm}(a'd, b'd) = d \cdot \text{lcm}(a', b') = d \cdot a'b'$. Multiplying by d says $\gcd(a, b) \cdot \text{lcm}(a, b) = d^2a'b' = ab$.

7. Compute the least common multiple of the following pairs of integers:

(a) $(24, 40)$

(b) $(5754, 7392)$

(c) $(3134376, 1759968)$

Solution: Use the Euclidean algorithm to compute the greatest common divisor and then use the previous result to compute the least common multiple. The details are omitted.

(a) 120

(b) 1012704

(c) 1216137888

8. Let $a, b \in \mathbb{N}$ and write $a = \prod_p p^{e_p}$ and $b = \prod_p p^{f_p}$ where the product is taken over all primes.

(a) Prove that $a \mid b$ if and only if $e_p \leq f_p$ for all prime p.

(b) Find an expression for $\gcd(a, b)$ in terms of the factorization of a and b.

(c) Find an expression for $\text{lcm}(a, b)$ in terms of the factorization of a and b.

Solution:

(a) Suppose that $a \mid b$, so $b = ak$ for some integer k. Write $k = \prod_p p^{k_p}$ as a product of primes, where only finitely many k_p are non-zero. Then equating factorizations, we see $f_p = e_p + k_p$, i.e. $f_p \geq e_p$ for all prime p. Conversely, if $e_p \leq f_p$ for all p, write $f_p = e_p + \varepsilon_p$ where $\varepsilon_p = f_p - e_p \geq 0$. Set $k = \prod_p p^{\varepsilon_p}$ which is an integer, so that $b = ak$ says $a \mid b$.

(b) $\gcd(a, b) = \prod_p p^{\min\{e_p, f_p\}}$. To see this, let $d = \gcd(a, b)$ and write $d = \prod_p p^{d_p}$ into a product of primes where d_p is non-zero for finitely many p. Since $d \mid a$ and $d \mid b$, we see that $d_p \leq e_p$ and $d_p \leq f_p$ for all p, giving $d_p \leq \min\{e_p, f_p\}$ for all p. To get the *greatest* common divisor, maximize the value of d by maximizing the value of d_p in each inequality by setting $d_p = \min\{e_p, f_p\}$. This is still a divisor of a and b by part a), and this forces it to be the largest such common divisor.

(c) $\text{lcm}(a,b) = \prod_p p^{\max\{e_p, f_p\}}$. To see this, let $\ell = \text{lcm}(a,b)$ and write $\ell = \prod_p p^{\ell_p}$ into a product of primes where ℓ_p is non-zero for finitely many p. Since $a \mid \ell$ and $b \mid \ell$, we see that $e_p \leq \ell_p$ and $f_p \leq \ell_p$ for all p, giving $\max\{e_p, f_p\} \leq \ell_p$ for all p. To get the *smallest* common multiple, minimize the value of ℓ by minimizing the value of ℓ_p in each inequality by taking $\ell_p = \max\{e_p, f_p\}$. This still gives a multiple of a and b, and this forces it to be the smallest such common multiple.

9. Compute the following:

(a) $\gcd(2^4 3^8 7^5 19^1, 2^2 3^3 7^4 11^2 13^3)$

(b) $\text{lcm}(2^3 3^2 5^9 13^3, 2^5 5^3 7^2 13^2 17^1)$

Solution: Use the previous problem to take either the minimum/maximum of the exponents on each prime.

(a) $2^2 3^3 7^4$

(b) $2^5 3^2 5^9 7^2 13^3 17$

10. Let $a, b \in \mathbb{N}$. Prove that if $a^2 \mid b^2$, that $a \mid b$.

Solution: Write $a = \prod_p p^{e_p}$ and $b = \prod_p p^{f_p}$ where the product is taken over all primes and only finitely many exponents are non-zero. Then $a^2 = \prod_p p^{2e_p}$ and $b^2 = \prod_p p^{2f_p}$. Since $a^2 \mid b^2$, we have $2e_p \leq 2f_p$ for all p, which says $e_p \leq f_p$ for all p, so $a \mid b$.