Math 228: Solutions for Problem Set Ten

Isaac Levy – ilevy.web.wesleyan.edu

April 4, 2007

1. *Suppose a and b are relatively prime. Prove that* $gcd(a + 2b, a - 3b)$ *is either 5 or 1, and give examples to show both possibilities occur.*

   Let the $d = gcd(a + 2b, a - 3b)$. We know d divides $a + 2b$ and d divides $a - 3b$. So then d divides any linear combination $m(a + 2b) + n(a - 3b)$ where m and n are integers. In particular, d divides $(a + 2b) - (a - 3b)$ and d divides $3(a + 2b) + 2(a - 3b)$. So d divides $5a$ and d divides $5b$.

   We know a and b are relatively prime, so $gcd(a, b) = 1$. That means we can find integers l, k such that $l \cdot a + k \cdot b = 1$. If we multiply this equation by 5 and rearrange, we get:

   $$l \cdot (5a) + k \cdot (5b) = 5$$

   Since $d \mid 5a$ and $d \mid 5b$, d divides any linear combination of 5a and 5b, including $l \cdot (5a) + k \cdot (5b)$. So d divides the entire left half of the equation. Thus d divides 5.

   But 5 is prime, so its only divisors are 1 and itself. Hence $d = 1$ or $d = 5$.

   Examples

   (a) $gcd(a + 2b, a - 3b) = 1$
   Let $a = 2$ and $b = 3$. Then $a + 2b = 8$ and $a - 3b = -7$.

   (b) $gcd(a + 2b, a - 3b) = 5$
   Let $a = 1$ and $b = 2$. Then $a + 2b = 5$ and $a - 3b = -5$.

2. *Suppose we have two integers a, b with $d = gcd(a, b)$. Prove that $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

Since $d = gcd(a, b)$, we know that $d \mid a$ and $d \mid b$, so $\frac{a}{d}$ and $\frac{b}{d}$ are integers. We also know there exist integers m, n such that $m \cdot a + n \cdot b = d$. If we divide this equation by d, we get $m \cdot \frac{a}{d} + n \cdot \frac{b}{d} = 1$.

Define $h = gcd(\frac{a}{d}, \frac{b}{d})$. Since $h \mid \frac{a}{d}$ and $h \mid \frac{b}{d}$, from Proposition 4.2.3, h divides any linear combination of $\frac{a}{d}$ and $\frac{b}{d}$. So then h divides $m \cdot \frac{a}{d} + n \cdot \frac{b}{d}$. So h divides 1. So $h = 1$.

Note that using Proposition 4.2.3, if $c = gcd(f, g)$, where f and g are integers, then $c \mid x \cdot f + y \cdot g$ where x and y are arbitrary integers.

3. *Suppose x is an integer. Prove that x is divisible by 9 if and only if the sum of its digits is divisible by 9. [Hint: $10,000 = 9999 + 1$].*

Suppose x is a n-digit integer. Then x can be expressed as a series of digits $x = a_{n-1}a_{n-2}\ldots a_2a_1a_0$, where a_i are digits between 0 and 9. We can convert x into "expanded form."
$x = 10^{n-1} \cdot a_{n-1} + 10^{n-2} \cdot a_{n-2} + \ldots + 10^2 \cdot a_2 + 10^1 \cdot a_1 + 10^0 \cdot a_0$. Using the hint we will now perform some algebraic manipulation.

$$
\begin{aligned}
x &= 10^{n-1} \cdot a_{n-1} + 10^{n-2} \cdot a_{n-2} + \ldots + 10^2 \cdot a_2 + 10^1 \cdot a_1 + 10^0 \cdot a_0 \\
&= 1\overbrace{000\ldots00}^{n-1} \cdot a_{n-1} + \ldots + 100 \cdot a_2 + 10 \cdot a_1 + 1 \cdot a_0 \\
&= (1 + \overbrace{999\ldots99}^{n-1}) \cdot a_{n-1} + \ldots + (1 + 99) \cdot a_2 + (1 + 9) \cdot a_1 + 1 \cdot a_0 \\
&= \overbrace{999\ldots99}^{n-1} \cdot a_{n-1} + \ldots + 99 \cdot a_2 + 9 \cdot a_1 + 1 \cdot (a_{n-1} + \ldots + a_1 + a_0) \\
&= 9 \cdot (\overbrace{111\ldots11}^{n-1} \cdot a_{n-1} + \ldots + 11 \cdot a_2 + 1 \cdot a_1) + (a_{n-1} + \ldots + a_1 + a_0) \\
&= 9 \cdot (m) + (a_{n-1} + \ldots + a_1 + a_0) \quad \text{for some integer } m
\end{aligned}
$$

The first term on the right side is divisible by 9. But the second term is just the sum of all the digits of x. If the sum of the digits is divisible by 9, then the entire right-hand side of the equation is divisible by 9, and thus so is x.

On the other hand, suppose x is divisible by 9. We can subtract $9m$ from the both sides of the equation.

$$x - 9 \cdot m = (a_{n-1} + \ldots + a_1 + a_0)$$

$x - 9m$ is divisible by 9. So the sum of the digits are also divisible by 9.

Hence x is divisible by 9 if and only if the sum of its digits are divisible by 9.

4. **Page 113 number 33**

   (a) Let $g_1 = gcd(a, b, c)$, $g_2 = gcd(a, b)$ and $g_3 = gcd(gcd(a, b), c)$. First we will prove that $g_3 \leq g_1$.

   We know $g_2 \mid a$ and $g_2 \mid b$. But $g_3 \mid g_2$. So $g_3 \mid a$ and $g_3 \mid b$. We also know $g_3 \mid c$. By definition 4.2.14 of the n-integer gcd, $g_3 \leq g_1$.

   $g_1 \mid a$ and $g_1 \mid b$. By Corollary 4.2.11, $g_1 \mid gcd(a, b)$. But g_1 also divides c. So by definition of gcd, $g_1 \leq gcd(gcd(a, b), c) = g_3$.

   Thus $g_1 = g_3$.

   (b) From part (a) we know $gcd(a, b, c) = gcd(gcd(a, b), c)$.
   Let $g_1 = gcd(gcd(a, b), c)$ and $g_2 = gcd(a, b)$. Since g_2 is the gcd of a and b, we can find two integers, m and n, such that $m \cdot a + n \cdot b = g_2$. Since g_1 is the gcd of g_2 and c, we can find two integers, k and l such that $k \cdot g_2 + l \cdot c = g_1$. Substituting in the first equation we have: $k \cdot (m \cdot a + n \cdot b) + l \cdot c = g_1$.

   Thus $(km) \cdot a + (kn) \cdot b + l \cdot c = g_1 = gcd(a, b, c)$

   (c) We will solve this problem using parts (a) and (b). From part (a) we know $gcd(105, 231, 165) = gcd(gcd(105, 231), 165)$. Using the Euclidean Algorithm, $gcd(105, 231) = 21$. One linear combination is $231 - 2 \cdot 105 = 21$. Again using the Euclidean Algorithm, $gcd(21, 165) = 3$ and a linear combination is $8 \cdot 21 - 165 = 3$. Thus $gcd(105, 231, 165) = 3$. We can substitute our linear combination from our first gcd into our second linear combination equation. $8 \cdot (231 - 2 \cdot 105) - 165 = 3$.

   So $8 \cdot 231 - 16 \cdot 105 - 165 = 3$.

5. *Similarly to the previous problem, we can define* $lcm(a, b, c)$ *to be the least common multiple of all three of* a, b, *and* c. *Prove that* $lcm(a, b, c) = lcm(lcm(a, b), c)$. *However, give an example to show that it is NOT always true that* $lcm(a, b, c) = \frac{abc}{gcd(a,b,c)}$.

Lemma *If* $a \mid c$ *and* $b \mid c$ *then* $lcm(a, b) \mid c$.

We will prove this with prime decompositions, though this was proved differently in class. $a = \prod_n {p_n}^{a_n}$ and $b = \prod_n {p_n}^{b_n}$, $c = \prod_n {p_n}^{c_n}$ where p_i are primes and a_j, b_j, c_j are the unique exponents for each decomposition. Since $a \mid c$ and $b \mid c$, $c_j \geq a_j$ and $c_j \geq b_j \forall j \in n$. So then $c_j \geq Max\{a_j, b_j\}\ \forall j$.
Thus $lcm(a, b) = \prod_n {p_n}^{Max\{a_n, b_n\}} \mid c$.

Let $l_1 = lcm(a, b, c)$, $l_2 = lcm(a, b)$ and $l_3 = lcm(lcm(a, b), c)$. First we will prove that $l_1 \leq l_3$.

We know $a \mid l_2$ and $b \mid l_2$. But $l_2 \mid l_3$. So $a \mid l_3$ and $b \mid l_3$. We also know $c \mid l_3$. By definition of the n-integer lcm, $l_1 \leq l_3$.

$a \mid l_1$ and $b \mid l_1$. From the lemma, we know $lcm(a, b) \mid l_1$. But c also divides l_1. So by definition of lcm, $lcm(lcm(a, b), c) = l_3 \leq l_1$.

Thus $l_1 = l_3$.

Example

Let $a = 4, b = 6$ and $c = 8$. Then $lcm(a, b, c) = 24$ but $\frac{abc}{gcd(a,b,c)} = 96$.

Note: A generalization to three variables is: $lcm(ab, ac, bc) = \frac{abc}{gcd(a,b,c)}$