

Solutions to Practice Midterm 1, Fall 2002.

1. We first use the Euclidean algorithm to compute $(15, 42)$ and reverse the algorithm:

$$\begin{aligned}42 &= 15 \cdot 2 + 12, \\15 &= 12 + 3, \\12 &= 3 \cdot 4 + 0.\end{aligned}$$

$$\begin{aligned}3 &= 15 - 12 \\ &= 15 - (42 - 15 \cdot 2) = 15 \cdot 3 - 42.\end{aligned}$$

(a). There are no integer solutions because $3 \nmid 200$.

(b). One solution is given by $(x, y) = (300, -100)$, so all solutions are given by $(300 + 14k, -100 - 5k)$ for $k \in \mathbb{Z}$. In order for this to be positive, we need

$$300 + 14k > 0, \quad -100 - 5k > 0.$$

This is equivalent to

$$\frac{-300}{14} < k < \frac{-100}{5}.$$

The only possibility is $k = -21$. This choice of k gives the solution $(6, 5)$.

2. Let $a, b \in \mathbb{N}^+$. Prove that any common multiple c of a and b is divisible by $[a, b]$. (You may assume any result proved in class.)

Note: All letters denote integers unless otherwise stated. You can prove #2 in more than one way: For the first proof, suppose $a|c$ and $b|c$. Then $c = au = bv$, so dividing through by (a, b) gives

$$\frac{b}{(a, b)} \Big| \frac{a}{(a, b)} u$$

But we showed that if $r|st$ and $(r, s) = 1$ then $r|t$. Applying that here, since

$$\left(\frac{b}{(a, b)}, \frac{a}{(a, b)} \right) = 1,$$

we have

$$\frac{b}{(a, b)} \Big| u.$$

Hence we can write

$$u = \frac{b}{(a, b)} w,$$

and

$$c = \frac{ab}{(a,b)}w,$$

But as we proved in class, $[a,b] = ab/(a,b)$.

The second proof is easier. We showed in class that if $x = p_1^{x_1} \cdots p_k^{x_k}$ and $y = p_1^{y_1} \cdots p_k^{y_k}$ are the prime factorizations of x and y , where p_1, \dots, p_k are distinct primes, then $x|y$ if and only if $x_j \leq y_j$ for every j .

Now suppose that a , b and c have prime factorizations

$$a = p_1^{a_1} \cdots p_k^{a_k}, \quad b = p_1^{b_1} \cdots p_k^{b_k}, \quad c = p_1^{c_1} \cdots p_k^{c_k}.$$

Then

$$\begin{aligned} a|c, \text{ and } b|c &\Leftrightarrow a_j \leq c_j, \quad b_j \leq c_j, \quad \text{for all } j \\ &\Leftrightarrow \max\{a_j, b_j\} \leq c_j, \quad \text{for all } j \\ &\Leftrightarrow p_1^{\max\{a_1, b_1\}} \cdots p_k^{\max\{a_k, b_k\}} \mid p_1^{c_1} \cdots p_k^{c_k}. \end{aligned}$$

We see from this that the least common multiple $[a,b]$ is $p_1^{\max\{a_1, b_1\}} \cdots p_k^{\max\{a_k, b_k\}}$ and this divides c .

3. (a).

$$\left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor = 50 + 25 + 12 + 6 + 3 + 1 = 97.$$

(b).

$$\left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor = 20 + 4 = 24.$$

(c). $100 = 2^2 \cdot 5^2$, and $100^m = 2^{2m} \cdot 5^{2m}$, which divides $100!$ if and only if $2m \leq 97$ and $2m \leq 24$. The largest value of m for which this holds is $m = 12$.

4. Decide whether the following statements are true in general and give a reason or counterexample.

(a). False. Take $b = 1$, $a = c = 2$, then $(a, b, c) = 1$, but $[a, b] = 2$ and $(a, c) = 2$, so $([a, b], (a, c)) = (2, 2) = 2$.

(b). True. Using $(a, b) = (a, b - ca)$, we have $(6k + 1, 8k + 1) = (6k + 1, 2k) = (1, 2k) = 1$.