Math 235 (Fall 2009): Assignment 4 Solutions

1.1: Let $m = [a, b]$ and k be an integer such that $a|k$ and $b|k$. Let q and r be integers such that $k = mq + r$ and $0 \leq r < m$. Since $a|k$ and $a|m$, $a|r$. Similarly, $b|r$. But, by definition of m, r has to be zero (why?). Hence, $m|k$.

1.2: Let $d = (a, b)$. We want to prove that $m := \frac{ab}{d}$ is the $lcm(a, b)$. Notice that, since $d|a$, we can write $m = \frac{a}{d}b$ and, hence, $b|m$. Similarly, $a|m$. Clearly $m > 0$.

It remains only to show that if k is a positive integer such that $a|k$ and $b|k$, then $m \leq k$. Let us prove that $m|k$ (i.e., $\frac{k}{m} \in \mathbb{Z}$). $\frac{k}{m} = \frac{kd}{ab}$. We know that $d = ar + bs$, for some $r, s \in \mathbb{Z}$. Thus, $\frac{kd}{ab} = \frac{k(ra+sb)}{ab} = \frac{kr}{b} + \frac{ks}{a} = \frac{k}{b}r + \frac{k}{a}s$. Since $a|k$ and $b|k$, $\frac{k}{b}r + \frac{k}{a}s$ is an integer. Therefore, $m|k$. Hence, $m \leq k$.

2.1: It is easy to see that $d := p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ is a positive divisor of a and b.

Now suppose t is another positive divisor of a and b. Then, $a = tu$. If we use the fundamental theorem of arithmetic we can write $a = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$, $t = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ and $u = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$ (t and u do not contain other primes in their factorizations; why?). Hence, $p_1^{r_1} p_2^{r_2} ... p_k^{r_k} = a = tu = p_1^{\alpha_1+\beta_1} p_2^{\alpha_1+\beta_2} ... p_k^{\alpha_1+\beta_k}$. Now, by the uniqueness part of the fundamental theorem of arithmetic, $r_1 = \alpha_1 + \beta_1$, $r_2 = \alpha_2 + \beta_2$, ... and $r_k = \alpha_k + \beta_k$. Hence, $\alpha_1 \leq r_1$, $\alpha_2 \leq r_2$, ... and $\alpha_k \leq r_k$. Similarly $\alpha_1 \leq s_1$, $\alpha_2 \leq s_2$, ... and $\alpha_k \leq s_k$. Hence, $\alpha_1 \leq min(s_1, r_1) = n_1$, $\alpha_2 \leq min(s_2, r_2) = n_2$, ... and $\alpha_k \leq min(s_k, r_k) = n_k$. Thus, $t \leq d$.

Therefore, $d = (a, b)$.

2.2: This follows from the previous item and 1.2.

3: This is true. The case $n = 3$ is easy. Now suppose there is an integer $n > 3$ such that there is no prime p satisfying $n < p < n!$. This implies that every number m such that $m < n!$ is divisible by a prime $q \leq n$. Consider $m = \prod q + 1$ (where the product is over all primes $q \leq n$). Then $m < n!$ (why?). So m must be divisible by a prime $q_0 \leq n$. Hence, by definition of m, $q_0|1$, contradiction!

4: The prime numbers between 1 and 150 are: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149$. The last prime used to sieve was 11 because $\sqrt{150} \approx 12.2$.

5.1: Suppose it is rational: $\sqrt{2 + \sqrt{3}} = \frac{a}{b}$ for some integers a and b. Then, taking squares, $2 + \sqrt{3} = \frac{a^2}{b^2}$. And, then, $\sqrt{3} = \frac{a^2}{b^2} - 2$ is rational. But $\sqrt{3}$ is irrational (the proof of this is very similar to the proof of proposition 10.1.4).

5.2: Suppose it is rational: $\sqrt{2} + \sqrt{3} = \frac{a}{b}$ for some integers a and b. Then, taking squares, $5 + 2\sqrt{6} = \frac{a^2}{b^2}$. And, then, $\sqrt{6} = \frac{a^2}{2b^2} - \frac{5}{2}$ is rational. But $\sqrt{6}$ is irrational (the proof of this is very similar to the proof of proposition 10.1.4).

5.3: Suppose $\sqrt[3]{p} = \frac{a}{b}$ for some integers a and b. We may assume $(a, b) = 1$. Then, $p = \frac{a^3}{b^3}$. Hence, $b^3 p = a^3$ (equation 1). This implies that $p|a^3$. Since p is a prime,

$p|a$. Thus, $a = pa_0$. Using equation 1, we get $b^3 = a_0^3 p^2$. Therefore, $p|b^3$. Since p is a prime, $p|b$. This contradicts the fact that $(a, b) = 1$ (because clearly $p \nmid 1$).

6: For this exercise, all the relations will be on the set $\mathbb{N}$.

Let $\Gamma = \{(0,1),(1,2)\} \subseteq \mathbb{N} \times \mathbb{N}$. This is a relation that does not satisfy any of the mentioned properties.

Let $\Gamma = \{(n,n)|n \in \mathbb{N}\} \bigcup \{(0,1),(1,2)\} \subseteq \mathbb{N} \times \mathbb{N}$. This is a reflexive relation that is not symmetric nor transitive.

Let $\Gamma = \{(0,1),(1,0)\} \subseteq \mathbb{N} \times \mathbb{N}$. This is a symmetric relation that is not reflexive nor transitive.

Let $\Gamma = \{(n,m)|n,m \in \mathbb{N} \text{ and } n < m\} \subseteq \mathbb{N} \times \mathbb{N}$. This is a transitive relation that is not reflexive nor symmetric.

Let $\Gamma = \{(n,n)|n \in \mathbb{N}\} \bigcup \{(0,1),(1,2),(1,0),(2,1)\} \subseteq \mathbb{N} \times \mathbb{N}$. This is a reflexive symmetric relation that is not transitive.

Let $\Gamma = \{(1,1)\} \subseteq \mathbb{N} \times \mathbb{N}$. This is a symmetric transitive relation that is not reflexive.

Let $\Gamma = \{(n,n)|n \in \mathbb{N}\} \bigcup \{(0,1)\} \subseteq \mathbb{N} \times \mathbb{N}$. This is a reflexive transitive relation that is not symmetric.

Finally, $\Gamma = \mathbb{N} \times \mathbb{N} \subseteq \mathbb{N} \times \mathbb{N}$ is a relation that satisfies all the properties.

7: It is not symmetric (for instance, $1|2$ but $2 \nmid 1$) and is clearly reflexive ($n = 1n$ for every integer n) and transitive ($b = ab_0, c = bc_0$ implies that $c = a(b_0c_0)$).

8.1: Modulo 2, $\overline{1001} = \overline{1}$, $\overline{32} = \overline{0}$, $\overline{35} = \overline{1}$ and $\overline{7921} = \overline{1}$. Hence, $\overline{1001 * 32 + 35 * 7921} = \overline{1} * \overline{0} + \overline{1} * \overline{1} = \overline{1}$.

8.2: Modulo 102, $\overline{101} = \overline{-1}$, $\overline{100} = \overline{-2}$ and $\overline{99} = \overline{-3}$. Thus, $\overline{101} * \overline{100} * \overline{99} - \overline{67} = \overline{-1} * \overline{-2} * \overline{-3} - \overline{67} = \overline{-6} - \overline{67} = \overline{-73} = \overline{29}$.

8.3: Modulo 8, $\overline{7} = \overline{-1}$ and $\overline{9} = \overline{1}$. Therefore, $\overline{7^{23}} - \overline{9^{24}} = \overline{-1} - \overline{1} = \overline{-2} = \overline{6}$.

8.4: $\overline{2^2} = \overline{4}$.
$\overline{2^4} = \overline{(2^2)^2} = \overline{4^2} = \overline{16} = \overline{-3}$.
$\overline{2^8} = \overline{(2^4)^2} = \overline{-3^2} = \overline{9} = \overline{-10}$.
$\overline{2^{16}} = \overline{(2^8)^2} = \overline{-10^2} = \overline{100} = \overline{5}$.
$\overline{2^{32}} = \overline{(2^{16})^2} = \overline{5^2} = \overline{25} = \overline{6}$.
$\overline{2^{64}} = \overline{(2^{32})^2} = \overline{6^2} = \overline{36} = \overline{-2} = \overline{17}$.

8.5: $\overline{2^{66}} = \overline{2^{64} * 2^2} = \overline{(-2) * 4} = \overline{-8} = \overline{11}$.