Zezhou Alex Liu
AM106 HW1
02/06/2016

(1) $a = \prod_{i=1}^{N_a} p_i^{\alpha_i}, \ \alpha_i > 0$
$b = \prod_{i=1}^{N_b} p_i^{\beta_i}, \ \beta_i > 0$

a) lcm(a, b):

Let us denote $P = \{P_a \cup P_b\}$, so that P is the set of all primes in a and b.

Then for all prime factors $p_i \in P$:

$$\boxed{\operatorname{lcm}(a,b) = \prod_{i=1}^{|P|} p_i^{(\operatorname{Max}(\alpha_i, \beta_i))}}$$

This is to say for each prime factor p_i, it includes the larger exponent in the product.

b) gcd(a, b):

Again, let us use $P = \{P_a \cup P_b\}$, so that P is the set of all primes in a and b. Then for all prime factors $p_i \in P$:

$$\boxed{\gcd(a,b) = \prod_{i=1}^{|P|} p_i^{(\min(\alpha_i, \beta_i))}}$$

This is to say for each prime factor p_i, it includes the smaller exponent in the product.

c) $ab = \operatorname{lcm}(a,b) \cdot \gcd(\operatorname{lcm})$

Consider the set of prime factors $P = \{P_a \cup P_b\}$.

Then for each prime factor p_i, it will be a α_i times "$(p_i^{\alpha_i})$" and in b β_i times $(p_i^{\beta_i})$.

If $\alpha_i \geq \beta_i$, then α_i will be represented in the lcm since it is the max, and β_i will be included in the gcd since it is the min.

If $\alpha_i < \beta_i$, then α_i will be represented in the gcd since it is the min, and β_i will be included in the lcm since it is the max.

This means for each p_i, it will be included a total of $\alpha_i + \beta_i$ times (either α_i in lcm and β_i in gcd, or vice versa). Thus, this is equivalent to the product of $a \cdot b$, and lcm $\cdot$ gcd.

Zezhou Alex Liu
AM106 HW1
02/06/2016

(2) i) $\left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \text{ such that } x, y, z \in \mathbb{R} \right\}$

No, because this violates the invertible property.
The inverse of a matrix in this group is of the form:

$$\frac{1}{xz - 0} \begin{pmatrix} z & -y \\ 0 & x \end{pmatrix} = \frac{1}{xy} \begin{pmatrix} z & -y \\ 0 & x \end{pmatrix}$$

however, xy is not restricted to be nonzero, so this is not guaranteed to be invertible.

ii) $\left\{ \begin{pmatrix} x & u \\ y & z \end{pmatrix} \text{ such that } x, y, z, u \neq 0, \text{ and } x, y, z, u \in \mathbb{R} \right\}$

No, because this violates the identity property

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is not valid in this group since y, u cannot be 0.

iii) $\left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \text{ such that } x \neq 0 \text{ and } x, y \in \mathbb{R} \right\}$

yes because:

(1) multiplication:

$$\begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} = \begin{pmatrix} x^2 & xy + xy \\ 0 & x^2 \end{pmatrix} \text{ is valid } ✓$$

(2) identity

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is valid if $x = \cancel{0}$, $y = 0$

(3) invertible

$$\frac{1}{x^2 - 0} \begin{pmatrix} x & -y \\ 0 & x \end{pmatrix} = \frac{1}{x^2} \begin{pmatrix} x & -y \\ 0 & x \end{pmatrix}, \text{ and } x \neq 0 \text{ so } x^2 \neq 0$$

(2) iv) $\left\{ \begin{pmatrix} z & 0 \\ 0 & w \end{pmatrix} \text{ such that } |z| = |w| = 1 \text{ and } z, w \in \mathbb{C} \right\}$

yes because

(1) multiplication:

$$\begin{pmatrix} z & 0 \\ 0 & w \end{pmatrix}\begin{pmatrix} z & 0 \\ 0 & w \end{pmatrix} = \begin{pmatrix} z^2 & 0 \\ 0 & w^2 \end{pmatrix} \qquad |z| = |z^2| = |w| = |w^2| = 1$$

(2) identity:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \checkmark$$

(3) inverse:

$$\frac{1}{zw}\begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} \checkmark$$

(3) for 3:

$3x = 1 \bmod 199$, solving this gives us $x = 133$.

verify:

$3(133) = 399 \bmod 199 = 1 \bmod 199$ ✓

for 5:

$5x = 1 \bmod 199$, solving this gives us $x = 40$

verify:

$5(40) = 200 \bmod 199 = 1 \bmod 199$ ✓