Name: Connor Raymond Stewart
ID: 101041125

MATH 3101 Assignment Two:

1) let $a = 3\cdot 7^2\cdot 11^3\cdot 23$ & $b = 7\cdot 11^2\cdot 23^2$. Compute (a,b) & $[a,b]$:

(a,b):

This can be found by forming the product of all the common prime factors, with each common factor raised to the least power to which it appears in either factorization:

$$a = \cancel{3}\cdot \underline{7}^{\cancel{2}}\cdot \underline{11}^{\cancel{3}}\cdot \underline{23},\ b = \underline{7}\cdot \underline{11^2}\cdot \underline{23}$$

$$\hookrightarrow (a,b) = 7\cdot 11^2\cdot 23$$

$$\boxed{= 19\,481}$$

$[a,b]$:

Can be found by forming the product of all the distinct prime factors that appear in the standard form of either a or b, with each factor raised to the greatest power to which it appears in either factorization:

$$a = \underline{3}\cdot \underline{7^2}\cdot \underline{11^3}\cdot 23,\ b = 7\cdot 11^2\cdot \underline{23^2}$$

$$\hookrightarrow [a,b] = 3\cdot 7^2\cdot 11^3\cdot 23^2 = \boxed{103\,502\,553}$$

$$\boxed{\therefore (a,b) = 19481\ \&\ [a,b] = 103\,502\,553}$$

2) Write out all of the congruence classes of the integers modulo 6. Be sure to explicitly list at least 3 of the numbers in each congruence class:

The equivilence classes for congruence modulo n form a partition of $\mathbb{Z}$; that is, they separate $\mathbb{Z}$ into mutually disjoint subsets. These subsets are called congruence classes:

$$[a] \stackrel{\wedge}{=} \{x\in\mathbb{Z} \mid x \equiv a \pmod n\} = \{x\in\mathbb{Z} \mid x-a = nk,\ k\in\mathbb{Z}\}$$

$$= \{x\in\mathbb{Z} \mid x = a+nk,\ k\in\mathbb{Z}\} = [a+nk,\ k\in\mathbb{Z}]$$

thus, the n distinct congruence classes of modulo n are:

$$[0] = \{\dots, -2n, -n, 0, n, 2n, \dots\}$$
$$[1] = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$$
$$[2] = \{\dots, -2n+2, -n+2, 2, n+2, 2n+2, \dots\}$$
$$\vdots$$
$$[n-1] = \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\}$$

When $n=6$:

$$\left.\begin{aligned}
[0] &= \{\dots, -12, -6, 0, 6, 12, \dots\}\\
[1] &= \{\dots, -11, -5, 1, 7, 13, \dots\}\\
[2] &= \{\dots, -10, -4, 2, 8, 14, \dots\}\\
[3] &= \{\dots, -9, -3, 3, 9, 15, \dots\}\\
[4] &= \{\dots, -8, -2, 4, 10, 16, \dots\}\\
[5] &= \{\dots, -7, -1, 5, 11, 17, \dots\}
\end{aligned}\right\}$$

$\therefore$ These are the congruence classes of the integers ~~of~~ modulo 6.

3) Simplify each of the following expressions. In other words, for each expression, find the least positive integer congruent to the expression modulo 7:

a) $39+44 \pmod 7$:

$39 \equiv 4 \pmod 7$

$44 \equiv 2 \pmod 7$

By Theorm 2.24: (in textbook)

$a+c \equiv b+d \pmod n$

thus:

$39+44 \equiv 4+2 \pmod 7$

$\hookrightarrow \equiv 6 \pmod 7$ where $6 \equiv 6 \pmod 7$

$\therefore 39+44 \pmod 7 \equiv 6 \pmod 7$

So:

$(39+44) \equiv 6 \pmod 7$

b) $82 \cdot 23 \pmod 7$:

$82 \equiv 5 \pmod 7$

$23 \equiv 2 \pmod 7$

By Theorm 2.24: (in textbook)

$ac \equiv bd \pmod n$

Thus:

$82 \cdot 23 \equiv 5 \cdot 2 \pmod 7 = 10 \pmod 7$

$\hookrightarrow 10 \pmod 7 \equiv 3 \pmod 7$

So:

$82 \cdot 23 \pmod 7 \equiv 3 \pmod 7$

c) $79^{24} \pmod 7$:

exponentiation is repeated multiplication:

$\therefore$ theorm 2.24 can be used to evaluate powers of modulo n

$79 \equiv 2 \pmod 7$

So; by theorm 2.24: (in textbook)

$79^{24} \equiv 2^{24} \pmod 7$

expand:

$2^{24} = (2^2)^{12} = 4^{12} = (4^2)^6 = 16^6$

$\hookrightarrow 16 \equiv 2 \pmod 7$ So by theorm 2.24, $16^6 \equiv 2^6$

$2^6 = (2^2)^3 = 4^3 = 4 \cdot 4 \cdot 4 = 16(4) = 64$

$\hookrightarrow 64 \equiv 1 \pmod 7$ So by theorm 2.24, $64 \equiv 1 \pmod 7$

So:

$79^{24} \equiv 1 \pmod 7$

4) Determine whether the following Statements are true or false. Justify your Responses:

a) let $a, b, c, n \in \mathbb{Z}$, with $n > 1$. If $a \equiv b \pmod n$ & $b \equiv c \pmod n$, then $a \equiv c \pmod n$:

Since $a \equiv b \pmod n$, then:

$b < n$ as b is the remainder after integer divison:

If $a \equiv b \pmod n$ then:

$a = nq + r$ where $r = b$ & $q =$ a lower division n

this means r must be less then n Since:

① If $r = n$:

$r \bmod n = 0$

② If $r > n$:

$r \bmod n = r_2$ where $r_2 < r$ & $r_2 < n$

this also means q is $+1$ unit

③ If $r < n$:

$r \bmod n = r$

So, Since $b = r$ & $r < n$:

$b < n$

If $b < n$ & $b \equiv c \pmod n$ then:

$b \bmod n = b$ Since $b < n$ & so all of b is in the remainder r:

If b modulo $n = b$ then $b \equiv c \pmod n$ is Simplified to $b \equiv b \pmod n$ as $b \bmod n = c = b$

So:

$a \equiv b \pmod n$ & $b \equiv c \pmod n$ where $b = c$

If $a \equiv c \pmod n$:

$a \equiv c \pmod n \Rightarrow a \equiv b \pmod n$ which is given

$\therefore$ It's True that $a \equiv c \pmod n$

b) let a & b be nonzero integers. Then $[a,b] \mid (a \cdot b)$ (i.e. the lcm of a & b divides the Product a times b):

$[a,b] = m$ where $m \in \mathbb{Z}^+$, we know by definition:

$a \mid m$

$b \mid m$

$a \mid c$ & $b \mid c$ Such that $m \mid c$

lets assume: Z is a Common multiple of a & b Such that $m \nmid Z$

By Division Theorm:

$Z = Km + r,\ K \in \mathbb{Z},\ 0 < r < m$

Since:

$a \mid Z$ & $a \mid m$, $r = Z - Km$ meaning:

$a \mid r$ & $b \mid r$

thus, r divides both a & b & is $\therefore$ a common multiple of both

however, in the assumption we state $r < m$

this would Contradict the given Claim that m is the lowest Common multiple of a & b

$\therefore$ By Contradiction, we Can Conclude that $m \mid Z$

thus, we Know that the lcm can divide the Common multiple

Since Common multiples are the multiples of two or more numbers, then $m = a \cdot b$ is a Common multiple.

Thus, the lcm of a & b can divide a Common multiple of a & b

& $\therefore$ $[a,b]$ divides $a \cdot b$

$\therefore$ It's true that $[a,b] \mid (a \cdot b)$