ASSIGNMENT 3

MATH 235

QUESTION 1

Let n be a positive integer and $\tau(n)$ be the number of positive divisors of n. The following lemma will be useful in the following proofs:

Lemma Let $r \geq 1$ with $r = p_1...p_k$, primes not necessarily distinct. We then have that all divisors of r can be written as $p_1...p_j$, i.e. some combination of the prime factors of r. Assume otherwise, and choose a divisor $x|r$. Then $xy = r$ for $y \in \mathbb{Z}$.

$$\implies x_1...x_s y_1...y_t = p_1...p_k$$

Since the prime factorization of $r = xy$ is unique, we can group these as follows WLOG:

$$x_1...x_s y_1...y_t = p_1...p_j p_{j+1}...p_k$$

with $x_1 = p_1, ..., x_s = p_j$, and we are done.

Part (1): Suppose p is prime. p^r, then, is its own prime factorization. We can deduce that all divisors of p^r may be written as $\{p^0, p^1, ..., p^r\}$, where, for any divisor p^i, we can write $p^i q = p^r$ with $q = p^{r-i}$.

As shown before, all divisors can be written as a product of prime factors, and so the set $\{p^0, p_1, ..., p^r\}$ is indeed complete, and has $r+1$ elements.

$$\tau(p^r) = r + 1$$

Part (3): Part (2) is done on the next page, since it's lengthy. We borrow its result here, that $\tau(mn) = \tau(m)\tau(n)$. We can then write

$$\tau(a_1 a_2 ... a_n) = \tau(a_1)\tau(a_2...a_n) = \tau(a_1)\tau(a_2)\tau(a_3...a_n) = ... = \tau(a_1)\tau(a_2)...\tau(a_n)$$

Consider $\tau\left(p_1^{a_1}...p_k^{a_k}\right)$. From (2) and above, this is $\prod_{i=1}^{k} \tau(p_i^{a_i})$.

$$\prod_{i=1}^{k} \tau(p_i^{a_i}) = \prod_{i=1}^{k} (a_i + 1)$$

and we are done.

To use our result from (2), note that the GCD of any two expodentiated primes in this list is 1. As proof, for two primes $p_1^{a_1}$ and $p_2^{a_2}$, we have that any two of their divisors, x_1 and x_2, are of the form $p_1^{i_1}$, $p_2^{i_2}$, where $i_1 \leq a_1, i_2 \leq a_2$. Thus we have that $x_1 \neq x_2$ except when $i_1 = i_2 = 0$, i.e. $x_1 = x_2 = 1$ is the only, and thus greatest, common divisor of $p_1^{a_1}$ and $p_2^{a_2}$.

Part (2): Let $\mathcal{D}(i)$ denote the set of all divisors of i. We see that for $m = p_1^{a_1}...p_k^{a_k}$, as before, all divisors can be made up of combinations of these primes and their powers, where no divisors diverge from this form (see lemma):

$$\mathcal{D}(m) = [1, p_1, p_1^2, ..., p_1^{a_1}] \times [1, p_2, p_2^2, ..., p_2^{a_2}] \times ... \times [1, p_k, p_k^2, ..., p_k^{a_k}]$$

Note that this Cartesian product allows for no duplicates, since all p_i are distinct. Pick a prime $p_i^{a_i'}$ in each set $[1, p_i, ..., p_i^{a_i}]$, with $1 \leq a_i' \leq a_i$. Then there are $\sum_{i=1}^{k} \binom{k}{i}$ ways of choosing divisors from $[p_1^{a_1'}] \times ... \times [p_k^{a_k'}]$. Furthermore, let there be $\mathbb{P}_m$ ways of fixing primes, without replacement, as we've just done. Then the total unique combinations are

$$\tau(m) = \left[\sum_{i=1}^{k} \binom{k}{i}\right] \mathbb{P}_m$$

Similarly, for $n = q_1^{b_1}...q_l^{b_l}$, we have

$$\tau(n) = \left[\sum_{i=1}^{l} \binom{l}{i}\right] \mathbb{P}_n$$

Write mn as $p_1^{a_1}...p_k^{a_k} q_1^{b_1}...q_l^{b_l}$. Fixing all $a_1', ..., a_k', b_1', ..., b_l'$ as we did before, we can count $\sum_{i=1}^{k+l} \binom{k+l}{i}$ corresponding divisors. Note that, since $\gcd(m, n) = 1$, they share no common divisors other than 1. This ensures that, in the calculation above, we are not counting duplicate products.

Consider all ways in which $a_1', ..., a_k', b_1', ..., b_l'$ can be chosen uniquely. This is precisely $\mathbb{P}_m\mathbb{P}_n$. Thus:

$$\tau(mn) = \left[\sum_{i=1}^{k+l} \binom{k+l}{i}\right] \mathbb{P}_n\mathbb{P}_m$$

By Binomial theorem, $\tau(m) = 2^k\mathbb{P}_m$, $\tau(n) = 2^l\mathbb{P}_n$, and $\tau(mn) = 2^{k+l}\mathbb{P}_m\mathbb{P}_n = 2^k\mathbb{P}_m 2^l\mathbb{P}_n = \tau(m)\tau(n)$, and we are done.

QUESTION 2

Part (1): Let $c = \text{lcm}(m, n)$. Then $m|c$ and $n|c$. Further, we have that $m|cq$ and $n|cq$ for any q we'd like.

Since we have that $m|k$ and $n|k$, combining with the above equations yields $m|k - cq$, $n|k - cq$. Note that we can write $k = cq + r$ where $0 \leq r < c$, so simplifying we get $m|r$ and $n|r$. Thus, r is a common multiple with $r < c$. But it is given that c is the *least* common multiple, so the only way to satisfy $m|r$ and $n|r$ is to conclude $r = 0$.

$\implies k = cq$, and thus $c|k$

Part (2): Let $m = p_1^{a_1}...p_k^{a_k}$, $n = p_1^{b_1}...p_k^{b_k}$. Denote $\max\{a_i, b_i\}$ as $\max_i$ and $\min\{a_i, b_i\}$ as $\min_i$. The following proof will borrow from the result shown in Q3, i.e. that $\text{lcm}(m, n) = p_1^{\max_1}...p_k^{\max_k}$.

$$\begin{aligned} \text{lcm}(m, n)\,\text{gcd}(m, n) &= p_1^{\max_1}...p_k^{\max_k} p_1^{\min_1}...p_k^{\min_k} \\ &= p_1^{\max_1 + \min_1}...p_k^{\max_k + \min_k} \\ &= p_1^{a_1+b_1}...p_k^{a_k+b_k} \\ &= p_1^{a_1}...p_k^{a_k} p_1^{b_1}...p_k^{b_k} \qquad = mn \end{aligned}$$

Thus, we have

$$\text{lcm}(m, n) = \frac{mn}{\text{gcd}(m, n)}$$

Question 3

Before proving, we'll need to add more construction to our prime factorization of m and n:

Define $m := p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ and $m := p_1^{b_1} p_2^{b_2} ... p_k^{b_k}$ to be factorizations of m and n. Note that, if there is a prime p_i in the unique factorization of m that is not in n, one sets the power $b_i = 0$ (and vise-versa).

Let c be a common multiple of m and n, i.e. $m|c$, $n|c$, and we have

$$\star \quad c = p_1^{a'_1} p_2^{a'_2} ... p_k^{a'_k} \quad \text{and} \quad c = p_1^{b'_1} p_2^{b'_2} ... p_k^{b'_k} \quad \text{with} \quad a'_i \geq a_i, \ b'_i \geq b_i$$

c.f. Proposition 10.2.1.

One normally writes $c = p_1^{a'_1} ... p_k^{a'_k} q_1 ... q_t$ and $c = p_1^{b'_1} ... p_k^{b'_k} r_1 ... r_t$, but, as above, we can take each q_i and r_j to reference particular primes p_i and p_j with their exponents $a_i = b_i = a_j = b_j$ all 0.

Let $l := p_1^{\max\{a_1, b_1\}} ... p_k^{\max\{a_k, b_k\}}$. Denote $\max_i = \max\{a_i, b_i\}$. We can write l in the following two forms:

(1) $l = m \left[p_1^{\max_1 - a_1} ... p_k^{\max_k - a_k} \right] \implies m|l$

(2) $l = n \left[p_1^{\max_1 - b_1} ... p_k^{\max_k - b_k} \right] \implies n|l \implies l$ is a common multiple of m, n.

Note that, since the prime factorization for c is unique, the previous 2 forms are equal.

From $\star$, we can write $c = p_1^{\alpha_1} ... p_k^{\alpha_k}$ with two conditions for α: that $\alpha_i \geq a_i$ and $\alpha_i \geq b_i$. Thus, $\alpha_i \geq \max\{a_i, b_i\}$.

Then, for any common multiple c, we have that $c = p_1^{\alpha_1} ... p_k^{\alpha_k} \geq p_1^{\max_1} ... p_k^{\max_k}$

$c \geq p_1^{\max_1} ... p_k^{\max_k} = l$ is exactly our least common multiple. □

QUESTION 4

Two important facts will be important: $\mathbb{Q}$ is closed under multiplication; for any $i \in \mathbb{Q} \setminus \mathbb{R}$ and $q \in \mathbb{Q}$, $iq \in \mathbb{R} \setminus \mathbb{Q}$. The former is provided since $\mathbb{Q}$ is a ring, and for the latter a proof:

> Let i be irrational. Then, for any choice $a, b \in \mathbb{Z}$, $\frac{a}{b} \neq i$ (it is impossible to express i as a ratio of two integers). Let $q := \frac{c}{d}$
>
> $\implies \ \forall\ a, b \in \mathbb{Z}, \frac{ac}{bd} \neq iq$. Varying a, b only, one can indeed span all of $\mathbb{Q}$: suppose we want $\frac{x}{y}$. Let $a = xd$, $b = yc \implies \frac{xdc}{ycd} = \frac{x}{y}$. Thus, we can rephrase and say $\forall\ x, y \in \mathbb{Q}$, $\frac{x}{y} \neq iq$, i.e. iq is irrational.

Let p, q be rational, and consider $\sqrt{3} = a + b\sqrt{2}$. Then:

$$\implies 3 = a^2 + 2b^2 + 2ab\sqrt{2} \implies \underbrace{3 - a^2 - 2b^2}_{\in \mathbb{Q}} = \underbrace{\underbrace{2ab}_{\in \mathbb{Q}} \cdot \underbrace{\sqrt{2}}_{\in \mathbb{R}\setminus\mathbb{Q}}}_{\in\mathbb{R}\setminus\mathbb{Q} \text{ by lemma} \lightning}$$

Thus, p, q cannot be rational, and we are done.

Question 5

Part (1): Let $N = n_k n_{k-1} \ldots n_1 n_0$, a decimal expansion, where $n_i \in \mathbb{N}\ \forall i$.

($\implies$) Suppose that $N = n_k n_{k-1} \ldots n_1 n_0$ is divisible by 3. Then we have that $N \pmod 3 = 0$, and further $n_0 + 10n_1 + 10^2 n_2 + \ldots + 10^k n_k \pmod 3 = 0$. We can express this sum as:

Note that $3|10^n - 1$. One can show by induction: for $n = 1$, $10 - 1 = 9 = 3(3) \implies 3|9$.

Let $n \rightarrow n+1$. Then $10^{n+1} - 1 \pmod 3 = 10 \cdot 10^n - 1 \pmod 3 = 10 \pmod 3 \cdot 10^n \pmod 3 - 1 \pmod 3 = 1 \cdot [10^n - 1] \pmod 3 = 1(0)$ by ind. hyp. Then, $3|10^{k+1} - 1$, and we are done.

$$n_0 + n_1 + n_2 + \ldots + n_k + 9p_1 + 99p_2 + \ldots + (10^k - 1)p_k$$

Clearly, $3|9$, $3|99$, ..., $3|10^k - 1$, i.e. $(10^i - 1)p_i \pmod 3 = 0\ \forall\ i$.

Using the additive property of congruences, we have:

$$n_0 + n_1 + \ldots + n_k + 9p_1 + 99p_2 + \ldots + (10^k - 1)p_k \pmod 3 = 0$$

$$\implies [n_0 + n_1 + \ldots + n_k \pmod 3] + \underbrace{[9p_1 + 99p_2 + \ldots + (10^k - 1)p_k \pmod 3]}_{=0,\text{ since all divisible by 3}} = 0$$

$$\implies n_0 + n_1 + \ldots + n_k \pmod 3 = 0$$

$$\implies 3|n_0 + n_1 + \ldots + n_k$$

($\impliedby$) Suppose now that $3|n_0 + n_1 + \ldots + n_k$. We know that $3|9$, $3|99$, ..., $3|10^k - 1$, further that $3|9n_1$, $3|99n_2$, ..., $3|(10^k - 1)p_k$, and finally that $3|9n_1 + 99n_2 + \ldots + (10^k - 1)n_k$.

$$\implies 3|n_0 + n_1 + \ldots + n_k + 9n_1 + 99n_2 + \ldots + (10^k - 1)n_k$$

$$\implies 3|n_0 + 10n_1 + \ldots + 10^k n_k \implies 3|N$$

Part (2): *Lemma:* $11|10^{2k}-1$ and $11|10^{2k-1}+1\ \forall k\geq 1$.

We'll show $11|10^{2k}-1$ by induction: let $k=1$. Then $10(2)-1=99=11(9)$, so $11|10^2-1$.

With $k\to k+1$, we have $10^{2(k+1)}-1=10^2\cdot 10^{2k}-1$.

$\implies 10^2\cdot 10^{2k}-1 \pmod{11} = 10^2 \pmod{11}\cdot 10^{2k} \pmod{11} - 1 \pmod{11}$

Since $10^2 \pmod{11} = 1$, this is just

$$10^{2k} \pmod{11} - 1 \pmod{11} = 10^{2k}-1 \pmod{11} = 0$$

by ind. hyp. Thus $11|10^{2(k+1)}-1$, and we conclude $11|10^{2k}-1$.

Now we'll show $11|10^{2k-1}+1$, once again by induction: let $k=1$. Then $10+1=11|11$.

With $k\to k+1$, we have $10^{2(k+1)-1}+1=10^{2k+1}+1=10^2 10^{2k-1}+1$.

As before, $10^2 10^{2k-1}+1 \pmod{11} = \underbrace{10^2 \pmod{11}}_{=1} 10^{2k-1} \pmod{11} + 1 \pmod{11}$

which is $10^{2k-1}+1 \pmod{11} = 0$ by ind. hyp. Thus, $10^{2(k+1)-1}+1 \pmod{11} = 0$, and we conclude that $11|10^{2k-1}+1$.

($\implies$) Assume that $11|N$, and write $N=n_0+10n_1+10^2n_2+\ldots+10^kn_k$.

Rearranging, this is

$$\underbrace{n_0-n_1+n_2-\ldots-n_{k-1}+n_k+\underbrace{(10+1)n_1+(10^2-1)n_2+\ldots+(10^{k-1}+1)n_{k-1}+(10^k-1)n_k}_{\text{(mod 11)=0 from above}}}_{\text{(mod 11)=0 by assumption}}$$

assuming WLOG that k is even.

$\implies n_0-n_1+n_2-\ldots-n_{k-1}+n_k \pmod{11} = 0$, or $11|n_0-n_1+n_2-\ldots-n_{k-1}+n_k$

($\impliedby$) Now assume that $11|n_0-n_1+n_2-\ldots-n_{k-1}+n_k$. We know from lemma that $11|(10^{2k}-1)q_1$ and $11|(10^{2k-1}+1)q_2$ for all $k\geq 1$ and arbitrary $q_1,q_2\in\mathbb{Z}$.

Then we have that $11|(10+1)n_1+(10^2-1)n_2+\ldots+(10^{k-1}+1)n_{k-1}+(10^k-1)n_k$.

Combining our assumption yields:

$11|n_0 - n_1 + n_2 - ... - n_{k-1} + n_k + (10+1)n_1 + (10^2 - 1)n_2 + ... + (10^{k-1} + 1)n_{k-1} + (10^k - 1)n_k$

or $11|N$

Part (3):

$(\implies)$ Suppose $N = n_0 + 10n_1 + ... + 10^k n_k$ is divisible by 7. We'll show that $7|M - 2n_0$, with $M := n_k n_{k-1}...n_1$. We can write

$$
\begin{aligned}
M - 2n_0 &= n_k n_{k-1}...n_1 - 2n_0 \\
&= n_1 + 10n_2 + ... + 10^{k-1} n_k - 2n_0 \\
&= \frac{1}{10}\left(10n_1 + 10^2 n_2 + ... + 10^k n_k\right) - 2n_0 \\
&= \frac{1}{10}\left(n_0 + 10n_1 + ... + 10^k n_k - 21n_0\right)
\end{aligned}
$$

$$
\begin{aligned}
\text{mod 7-ing}: \; & \frac{1}{10}\left(n_0 + 10n_1 + ... + 10^k n_k - 21n_0\right) \bmod 7 \\
&= \left[\frac{1}{10} \bmod 7\right]\left[\underbrace{(n_0 + 10n_1 + ... + 10^k n_k) \bmod 7}_{=0 \text{ by assumption}} \underbrace{-21n_0 \bmod 7}_{=0, \text{ since } 7|21}\right] \\
&= 0, \text{ and thus } 7|M - 2n_0
\end{aligned}
$$

$(\impliedby)$ Now suppose that $M - 2n_0$ is divisible by 7:

$$
\begin{aligned}
7|M - 2n_0 &\implies 7|n_1 + 10n_2 + ... + 10^{k-1} n_k - 2n_0 \\
&\implies 7\left|\frac{1}{10}\left(n_0 + 10n_1 + ... + 10^k n_k - 21n_0\right)\right. \\
&\implies 7|n_0 + 10n_1 + ... + 10^k n_k - 21n_0 \\
&\implies n_0 + 10n_1 + ... + 10^k n_k \underbrace{-21n_0}_{\text{mod } 7=0} \bmod 7 = 0 \\
&\implies n_0 + 10n_1 + ... + 10^k n_k \bmod 7 = 0
\end{aligned}
$$

These are equivelant expressions

And thus $7|n_0 + 10n_1 + ... + 10^k n_k$, or $7|N$

Question 6

We are considering $\frac{3\cdot5-3^3}{2\cdot6+10}$. Simplifying, this is $\frac{-12}{22}$.

In $\mathbb{Z}/5\mathbb{Z}$: Following properties of the inverse, $\frac{1}{22}(22) = 1 \pmod 5$. Setting $\frac{1}{22} = 3$, one sees that $22(3) = 66 = 1 \pmod 5$. Thus, our problem is now $[-12 \pmod 5]\cdot 3 = 3(3) = \boxed{9}$

In $\mathbb{Z}/7\mathbb{Z}$: We require $\frac{1}{22}(22) = 1 \pmod 7$ as before. Setting $\frac{1}{22} = 1$, we have that $1(22) = 1 \pmod 7$. Thus, consider $[-12 \pmod 7]\cdot 1 = 2(1) = \boxed{2}$