Prime Chapter 11

1. $111,111 = 11 \times 10101$
$= 11 \times 7 \times 1443$
$= 11 \times 7 \times 3 \times 481$
$= 11 \times 7 \times 3 \times 13 \times 37$

3. The positive integers dividing $N = 2^{n-1}p$ are
$1, 2, 2^2, \dots, 2^{n-1}, p, 2p, 2^2p, \dots, 2^{n-1}p.$

Let $D = 1+2+2^2+\dots+2^{n-1}+p+2p+2^2p+\dots+2^{n-2}p$
$= [2^0+2+2^2+\dots+2^{n-1}] + p[2^0+2+2^2+\dots+2^{n-2}]$
$= \dfrac{1(2^n-1)}{2-1} + p\dfrac{(1)(2^{n-1}-1)}{2-1}$
$= (2^n-1) + p(2^{n-1}-1)$
$= 2^n-1 + p2^{n-1} - p$
$= p + p2^{n-1} - p \quad ; \quad p = 2^n-1$
$= 2^{n-1}p$
$= N$ as required.

n	2	3	5	7
$p=2^n-1$	$2^2-1=3$	$2^3-1=7$	$2^5-1=31$	$2^7-1=127$.
$2^{n-1}p$	$2(3)=6$	$4(7)=28$	$16(31)$ $=496$	$2^6(127)=8128$

6, 28, 496, 8128 are four perfect numbers.

4 (i) LHS $= \text{lcm}(a,b)$
$= \text{lcm}(70,120)$
$= 7 \times 120$
$= 840$

RHS $= \dfrac{ab}{\gcd(70,120)}$
$= \dfrac{70 \times 120}{10}$
$= 7 \times 120$
$= 840$
$=$ LHS.

Thus, $\text{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$ holds for $a=70$, $b=120$.

(ii) LHS $= \text{lcm}(5,11)$
$= 5 \times 11$
$= 55$

RHS $= \dfrac{ab}{\gcd(5,11)}$
$= \dfrac{5 \times 11}{1}$
$=$ LHS

Thus, $\text{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$ holds for $a=5$, $b=11$

(iii) LHS $= \text{lcm}(272,1749)$
$= 272 \times 1749$.

RHS $= \dfrac{ab}{\gcd(a,b)}$
$= \dfrac{272 \times 1749}{\gcd(272,1749)}$

Aside: let $\gcd(272,1749) = d$.
$1749 = 6(272) + 117$.
$272 = 2(117) + 38$
$117 = 3(38) + 3$
$38 = 12(3) + 2$.
$3 = 1(2) + 1$.
$2 = 2(1) + 0$.

So $d = 1$.

RHS $= \dfrac{272 \times 1749}{1}$
$=$ LHS.

Thus, $\text{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$ holds for $a=272$, $b=1749$.

4. We want to prove that $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$.

Let $d = \gcd(a,b)$.
Thus, $d \mid a$ and $d \mid b$ and $d \geq 1$.
so $a = dr$ and $b = ds$ for $r, s \in \mathbb{Z}^+$
Let $m = \frac{ab}{d}$ which is really $\frac{ab}{\gcd(a,b)}$

Then $m = \frac{(dr)b}{d}$ and $m = \frac{a(ds)}{d}$

$m = br$ $\quad$ $m = as$

Thus, m is a positive common multiple of a and b.
Now let c be any positive integer multiple of a and b
Thus, $c = au$ and $c = bv$ for some $u, v \in \mathbb{Z}^+$ — ①

Since $d = \gcd(a,b)$, then there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$.

consider $\frac{c}{m} = \frac{c}{\left(\frac{ab}{d}\right)}$

$= \frac{cd}{ab}$

$= \frac{c(ax+by)}{ab}$ $\quad \because d = ax + by$

$= \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y$ and from ① we have

$\frac{c}{m} = vx + uy$

$c = m(vx + uy)$.

Thus, $m \mid c$
So $m \leq c$.
Thus, $m = \operatorname{lcm}(a,b)$

Reversing the steps above will give us if $m = \operatorname{lcm}(a,b)$ then $m = \frac{ab}{\gcd(a,b)}$.

5a) Proof by contradiction

Let $2^{1/3}$ be rational; i.e

$2^{1/3} = \frac{x}{y}$; where $x, y \in \mathbb{Z}$ and $\gcd(x,y) = 1$

so $2 = \frac{x^3}{y^3}$

$2y^3 = x^3$

let $x = 2^a p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

and $y = 2^b q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$

where each p_i and q_j is a prime and each a_i and b_j is an integer with $i \in \{1, 2, \ldots, k\}$ and $j \in \{1, 2, \ldots, l\}$

Then

$2(2^b q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l})^3 \neq (2^a p_1^{a_1} \cdots p_k^{a_k})^3$

By the Fundamental Theorem of Arithmetic

$1 + 3b = 3a$ but this is impossible because both a and b are integers.

Thus, $2^{1/3}$ is irrational.

Same argument can be applied to $3^{1/3}$.

$(\Leftarrow)$

5b) If m is an n^{th} power then $m^{1/n}$ is rational.

i.e $m = c^n$, $c \in \mathbb{Z}$

then $c = m^{1/n}$

since $c \in \mathbb{Z}$ then $m^{1/n}$ is rational.

$(\Rightarrow)$ If $m^{1/n}$ is rational then m is an n^{th} power

Let $m^{1/n} = \frac{x}{y}$, $x, y \in \mathbb{Z}$

then $ym^{1/n} = x$

let p be a prime and let p^a, p^b, p^c be the largest powers of p which divide x, y, m respectively.

Then the power of p dividing x^n is p^{an}, while the power of p dividing my^n is p^{c+bn}.

By the Fundamental Theorem of Arithmetic, we must have

$an = c + bn$

$\Rightarrow c = an - bn$

$= n(a-b)$

so c is divisible by n.

Thus, the power to which each prime divides m is a multiple of n, i.e

$m = p_1^{na_1} p_2^{na_2} \cdots p_k^{na_k}$

for some integers a_i.

Hence $m = (p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k})^n$

and so m is n^{th} power as required.

NO: Prime Chapter 11. DATE:

6. $E = \{2, 4, 6, 8, 10, 12, \ldots, 2n, \ldots\}$; $n \in \mathbb{Z}^+$

$e = \{2, 6, 10, 14, 18, \ldots, 2(2m+1), \ldots\}$ $m \in \{0, 1, 2, \ldots\}$

(i) $6 = 2 \times 3$ but 3 is not even.
Since 3 is not even then $\{3\} \notin E$
Thus, 6 cannot be expressed as a product of two other members of E.
So 6 is a prima.

$4 = 2 \times 2$. 2 is even and $\{2\} \in E$.
Since the definition of prima did not specify the members to be unique then 4 is not a prima.

(ii) The general form of a prima is $2(2m+1)$; $m \in \{0, 1, 2, \ldots\}$

(iii) The general form of an element of E is $2n$; $n \in \mathbb{Z}^+$

We want to prove that every element of E is a product of primas; i.e. $2n = 2(2m+1) \times 2(2p+1)$
where $n \in \mathbb{Z}^+$, $m, p \in \{0, 1, 2, \ldots\}$ and m and p may not be unique.

Case 1: an element e of E is a prima. In this case e is already a product of primas; namely itself

Case 2: an element e of E is not a prima.
$e = \{4, 8, 12, \ldots, 4k, \ldots\}$; $k \in \mathbb{Z}^+$
Any e can be written as
$e = 4k$; $k \in \mathbb{Z}^+$

Case 2.1
Since $4k$ is even then $4k$ can be expressed as the product of two even integers.

$$e = (2a)(2b) \quad ; \; a,b \in \mathbb{Z}^+$$
$$= [2(p+1)] \times [2(q+1)] \quad ; \; p,q \in \{0,1,2,\dots\}$$
$$=$$

Thus, e is a multiple of primas.

Case 2.2 Let $4k$ be a product of an odd integer and an even integer

$$e = (4a)[\;(b+1)] \quad ; \; a,b \in \mathbb{Z}^+$$
$$= 2[2(p+1)][q+2] \quad ; \; p,q \in \{0,1,2,\dots\}.$$
$$= 2(p+1)2(q+1)$$

Thus, e is also a multiple of primas.

(iv) Let $e = 2 \times 10 \times 6 \quad ; \; \{2,6,10\} \in \{\text{primas}\}$
$e = 2 \times 2 \times 30 \quad \{2, 30\} \in \{\text{primas}\}$

Note: $30 = 2(15)$ which is the form of a prima.

Thus, there is no unique prima factorization theorem

NO: Chapter 11 DATE:

7. a) Want $m, n \in \mathbb{Z}^+$ such that $\gcd(m,n) = 50$ and $\text{lcm}(m,n) = 1500$

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

so $1500 = \dfrac{mn}{50}$

so $mn = 1500(50)$

$= (30 \times 50)(2 \times 5^2)$

$= (2 \times 3 \times 5 \times 2 \times 5^2)(2 \times 5^2)$

$= 2^3 \times 3 \times 5^5$

$= (2 \times 5^2)(2^2 \times 3 \times 5^3)$

OR

$= (2 \times 5^2 \times 3)(2^2 \times 5^3)$

OR

$= (2 \times 5^2 \times 5)(2^2 \times 3 \times 5^2)$

OR

$= (2 \times 5^3 \times 3)(2^2 \times 5^2)$

Note that each solution has $\gcd(m,n) = 2 \times 5^2$.

b) Want to prove that if $m, n \in \mathbb{Z}^+$ then $\gcd(m,n) \mid \text{lcm}(m,n)$.

Let $d = \gcd(m,n)$ and $d \mid m$.

Since $d \mid m$ and $\text{lcm}(m,n)$ is a multiple of m then it must be the case $d \mid \text{lcm}(m,n)$

- When does $d = \text{lcm}(m,n)$?

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

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

$\text{lcm}(m,n) = \gcd(m,n)$ when $\text{lcm}(m,n) = m$ and $\gcd(m,n) = m$

or $\text{lcm}(m,n) = n$ and $\gcd(m,n) = n$.

NO: primes. chapter 11 DATE:

7(c) If m, n are positive integers then $\gcd(x,y)=1$ such that $x \mid m$, $y \mid n$ and $xy = \operatorname{lcm}(m,n)$.

Let $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$; $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$

where p_i is a prime for $i \in \{1, 2, \ldots, k\}$, each r_i and s_i is a positive integer.

we let x to be the product of all $p_i^{r_i}$ such that $r_i \geq s_i$ and

y to be the product of all the $p_j^{s_j}$ for which $r_j < s_j$.

Since x and y do not have common primes then $\gcd(x,y)=1$.

Since $m = kx$; where $k \in \mathbb{Z}^+$ then $x \mid m$ and k is the product of all $p_i^{r_i}$ such that $r_i < s_i$

Since $n = ly$; where $l \in \mathbb{Z}^+$ then $y \mid n$ and l is the product of all $p_j^{s_j}$ such that $r_j \geq s_j$

Since $\gcd(x,y)=1$ then there exist integers s and t such that $sx + ty = 1$

specifically $s = k$ and $t = l$.