MTH215A : Number Theory: Assignment - 1

Sarthak Rout

October 7, 2020

---

1 Solutions

1.1 Q1

By Euclid's Division Algorithm,

$$\begin{aligned}
5490 &= 4 \cdot 1324 + 194 \\
1324 &= 6 \cdot 194 + 160 \\
194 &= 1 \cdot 160 + 34 \\
160 &= 4 \cdot 34 + 24 \\
34 &= 1 \cdot 24 + 10 \\
24 &= 2 \cdot 10 + 4 \\
10 &= 2 \cdot 4 + 2 \\
4 &= 2 \cdot 2 + 0
\end{aligned} \tag{1}$$

$$\begin{aligned}
24 \cdot 2 &= 5 \cdot 10 - 2 \\
5 \cdot 34 &= 7 \cdot 24 + 2 \\
7 \cdot 160 &= 33 \cdot 34 - 2 \\
33 \cdot 194 &= 40 \cdot 160 + 2 \\
1324 \cdot 40 &= 273 \cdot 194 - 2 \\
2 &= 273 \cdot 5490 - 1132 \cdot 1324
\end{aligned} \tag{2}$$

GCD(5490, 1324) = d = 2. x = -1132 and y = 273

1.2 Q2

On the contrary, let us assume $4 \mid n^2 + 2$, then n^2 must be even as 2 divides 4 and 2 both.
So, let $n = 2 \cdot k$ for some integer k. Then, $4 \mid (2k)^2 + 2 \implies 4 \mid 4k^2 + 2 \implies 4 \mid 2$ which is a contradiction. So, our initial assumption was incorrect and $4 \nmid n^2 + 2$.

1.3 Q3

1.3.1

If n is odd, then $n = 2k + 1$ for some integer k. Then $n^2 - 1 = 4k(k + 1)$.
Now, if k is even, $k(k + 1)$ is even and if k is odd, $k + 1$ is even, hence $k(k + 1)$ is even for all integral values of k. So, $2 \mid k(k + 1) \implies 8 \mid 4k(k + 1) = n^2 - 1$.

1.3.2

$n^3 - n = (n - 1) \cdot n \cdot (n + 1)$. It is product of 3 consecutive numbers.
Lemma: Product of n consecutive numbers is divisible by n.
As there are only n possible remainders when a number is divided by n, n consecutive numbers must give n consecutive remainders in an order, whose product will be 0 as one remainder is definitely 0.
So, the product of 3 consecutive numbers is divisible by 3. But, at the same time, it also has product of 2 consecutive numbers $(n - 1) \cdot n$ or $n \cdot (n + 1)$ as it's factors so, it is also divisible by 2. So, as $(2, 3) = 1$, $2 \cdot 3 = 6 \mid n^3 - n$.

1.4 Q4

Consider binomial expansion of $n^k - 1 = (1 + (n - 1))^k - 1 = 1 + k \cdot (n - 1) + \binom{k}{2} \cdot (n - 1)^2 + W \cdot (n - 1)^2 - 1$.
As higher order terms have higher powers of $(n-1)$ greater than 2, if we take $(n-1)^2$ as common, we will have W as an integral factor.
$(\implies)$ So, $n^k - 1 = k \cdot (n - 1) + W \cdot (n - 1)^2$. If $(n - 1)^2 \mid n^k - 1$, then, $(n - 1)^2 \mid k \cdot (n - 1) \implies (n - 1) \mid k$. Hence, $\implies$ is proved.
$(\impliedby)$ Similarly, if $(n - 1) \mid k \implies (n - 1)^2 \mid k \cdot (n - 1) \implies (n - 1)^2 \mid k \cdot (n - 1) + W' \cdot (n - 1)^2$ for some integer W'. Hence, $\impliedby$ is also proved.

1.5 Q5

For the general statement, let $a \cdot b = c^n$ with $(a, b) = 1$.
Let us assume in general, $a = x^n \cdot s$ and $b = y^n \cdot t$ where s has factors $p_i^{a_i}$ and t has factors $p_j^{a_j}$ where $p_i and p_j$ are primes, such that $0 \le a_1, a_2 < n$. $(s, t) = 1$ as $(a, b) = 1$. $ab = c^n = x^n \cdot y^n \cdot s \cdot t \implies s \cdot t = (\frac{c}{xy})^n$.
This means every p_k which is a factor of $(\frac{c}{xy})^n$ has exponent $z \cdot n$. As s and t are co-prime, p_k must be a factor of either s or t. As described before, all prime factors of s and t have exponent e, $0 \le e < n$. So, z must be zero, which means that there are no prime factors but $s \cdot t = 1$ which implies, $s = t = 1 \implies a = x^n$ and $b = y^n$.
As we have proved the general case, the particular case for $n = 2$ must also be true.

1.6 Q6

Assuming ord$_p$n is the maximum number of times p divides n.
Let $p^{x_1} \mid a$, $p^{x_2} \mid b$ and $p^x \mid a + b$ where the powers are the maximum that divide the corresponding number.
This $\implies x_1 =$ ord$_p$a , $x_2 =$ ord$_p$b and $x =$ ord$_p$(a+b)

$\implies a = k_1 p^{x_1}$, $b = k_2 p^{x_2}$ and $a + b = kp^x$ with $p \nmid k, k_1, k_2$
$\implies k_1 p^{x_1} + k_2 p^{x_2} = kp^x$. WALOG, let $x_1 \leq x_2$
$\implies k_1 + k_2 \cdot p^{x_2 - x_1} = k \cdot p^{x_0 - x_1}$
Case 1: $x_1 \neq x_2 \implies p^{x_0 - x_1} \mid k_1 + k_2 \cdot p^{x_2 - x_1} \implies p^{x_0 - x_1} \mid k_1 \implies x_0 - x_1 = 0 \implies x_0 = x_1 = min(x_1, x_2)(\because p \nmid k_1)$
Case 2: $x_1 = x_2 \implies k_1 + k_2 = k \cdot p^{x_0 - x_1}$. If $x_0 < x_1$, then $k_1 + k_2 = \frac{k}{p^{x_1 - x_0}}$which is not an integer as $p \nmid k$. So , $x \geq x_1 = min(x_1, x_2)$.
Hence, proved.

1.7 Q7

In the proofs below, if a variable is parameterised to be $v = a + b \cdot t$. t_{min} is defined as $t_{min} = \frac{-a}{b}$ the minimum value of t for the variable to achieve a positive value. In this case, b would be positive. Similarly, t_{max} is defined as $t_{max} = \frac{-a}{b}$ maximum value of t for the variable to remain positive. In this case, b would be negative.

1.7.1

GCD(18, 5):

$$\begin{aligned} 18 &= 5 \cdot 3 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \\ \implies 5 &= 2 \cdot 3 - 1 \end{aligned} \tag{3}$$

$GCD(18, 5) = 1$ and $LCM(18, 5) = 90$.
$1 = 2 \cdot 18 - 7 \cdot 5 \implies 48 = 96 \cdot 18 - 336 \cdot 5$
$18x - 90 + 5y + 90 = 1 \implies 18(x - 5) + 5(y + 18) = 1$
$\implies$ if x_0 and y_0 are solutions, $x_0 - 5 \cdot t$ and $y_0 + 18 \cdot t$ are also solutions. So, general solutions are: $x = 96 - 5 \cdot t$, $y = -336 + 18 \cdot t$.
For positive solutions, $t_{max} = 19$ and $t_{min} = 19$ from both equations. So there is only one solution: $x = 96 - 95 = 1$ and $y = -336 + 18 \cdot 19 = 6$.

1.7.2

GCD(54, 21):

$$\begin{aligned} 54 &= 21 \cdot 2 + 12 \\ 21 &= 12 \cdot 1 + 9 \\ 12 &= 9 \cdot 1 + 3 \\ 9 &= 3 \cdot 3 + 0 \\ \implies 21 &= 2 \cdot 12 - 3 \\ 2 \cdot 54 &= 4 \cdot 21 + 21 + 3 \\ 3 &= 2 \cdot 54 - 5 \cdot 21 \end{aligned} \tag{4}$$

$GCD(54, 21) = 3$ and $LCM(54, 21) = 18 \cdot 7 \cdot 3$
$3 = 2 \cdot 54 - 5 \cdot 21 \implies 243 = 162 \cdot 54 - 405 \cdot 21$. $54x - LCM + 21y + LCM = 3 \implies 54(x - 7) + 21(y + 18) = 3$
$\implies$ if x_0 and y_0 are solutions, $(x_0 - 7 \cdot t, y_0 + 18 \cdot t)$ are also solutions. So, general solutions are: $x = 162 - 7 \cdot t, y = -405 + 18 \cdot t$.
For positive solutions, $t_{max} = 23$ and $t_{min} = 23$ from both equations. So, there is only one solution: $x = 1$, $y = 9$.

1.7.3

GCD(158, 57):

$$
\begin{aligned}
158 &= 57 \cdot 2 + 44 \\
57 &= 44 \cdot 1 + 13 \\
44 &= 13 \cdot 3 + 5 \\
13 &= 5 \cdot 2 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2 + 0 \\
\implies 5 &= 3 \cdot 2 - 1 \\
13 \cdot 2 &= 5 \cdot 5 + 1 \\
44 \cdot 5 &= 13 \cdot 17 - 1 \\
57 \cdot 17 &= 44 \cdot 22 + 1 \\
158 \cdot 22 &= 57 \cdot 61 - 1 \\
\implies 1 &= 57 \cdot 61 - 158 \cdot 22 \\
7 &= 57 \cdot 427 - 158 \cdot 154
\end{aligned} \tag{5}
$$

$GCD(158, 57) = 1$ and $LCM(157, 58) = 157 \cdot 58$
$158x - 57y = 7 \implies 158(x + 57) + -57(y + 158) = 1$. The general solutions are $(x = -154 + 57 \cdot t, y = -427 + 158 \cdot t)$ for some integer t.
For positive solutions, $t = \max(\text{ ceil}(\frac{154}{57}), \text{ ceil}(\frac{427}{158})) = 3$. So, the set of positive solutions is $(x = -154 + 57 \cdot t, y = -427 + 158 \cdot t), t \geq 3$ is an integer.

1.8 Q8

Let d be the GCD of $(n! + 1, (n + 1)! + 1)$.
Then, $d \mid n! + 1$, $d \mid (n + 1)! + 1$.
$\implies d \mid (n+1)(n!+1) \implies d \mid (n+1)!+n+1 \implies d \mid (n+1)!+n+1-((n+1)!+1) = n$ $(\because d \mid (n + 1)! + 1)$
$\implies d \mid n! \implies d \mid n! + 1 - (n!) = 1 \implies d = 1$.
Hence, proved.

1.9 Q9

Consider 3 cases : $b > a$, $b = a$ and $b < a$

- Case $b > a$:
  $2^b - 2^a = 2^a \cdot (2^{b-a} - 1) > 2 \cdot 1 (\because a \geq 1 \text{ and } 2^{b-a} - 1 \geq 2 - 1 = 1) \implies 2^b - 1 > 2^a + 1$. Hence, $2^b - 1 \nmid 2^a + 1$ if $b > a$.

- Case $b = a$:
  $k(2^a - 1) = 2^a + 1 \implies 2^a = \frac{k+1}{k-1} = 1 + \frac{2}{k-1}$ This is an integer only for $k = 2$ and $k = 3$ for which $a = b = 1 < 3$. Hence, $2^b - 1 \nmid 2^a + 1$ if $b = a$ and $b \geq 3$.

- Case $b < a$:
  Lemma: $2^b - 1 \nmid 2^b (\because \text{then} 2^b - 1 \mid 1$ which is not possible as $b \geq 3)$
  Assume, $2^b - 1 \mid 2^a + 1 \implies 2^b - 1 \mid 2^a + 2^b = 2^b \cdot (2^{a-b} - 1) \implies 2^b - 1 \mid (2^{a-b} - 1)$. So, if this relation holds for (b, a), it also holds for $(b, a - b)$ and inductively, $(b, a - kb)$ for some integer k. But, at some point, $a - kb \leq b$. Then, we saw in cases 1 and 2 that such as relation doesn't hold if $b \geq a$.
  Hence, the original relation doesn't hold and thus our assumption fails; $2^b - 1 \nmid 2^a + 1$ if $b > a$ too .

Hence, $2^b - 1 \nmid 2^a + 1$ if $b >= 3$.

1.10 Q10

$a^{2^m} - 1 = a^{2^n \cdot 2^{m-n}} - 1 = (a^{2^n})^{2^{m-n}} - 1$. Let $a^{2^n} = r$ and $2^{m-n-1} = s \implies 2^{m-n} = 2s$ be two integers. Then $a^{2^m} - 1 = r^{2s} - 1$.
Hence, $r^2 - 1 \mid (r^2)^s - 1 (\because r^2 = 1$ is a root of the corresponding polynomial $(r^2)^s - 1 = 0)$.
Hence, $a^{2^n} + 1 = r + 1 \mid r^2 - 1 \mid a^{2^m} - 1$.
Let $d = GCD(a^{2^n} + 1, a^{2^m} + 1) \implies d \mid a^{2^n} + 1$, $d \mid a^{2^m} + 1$.
From the above relation, $a^{2^n} + 1 \mid a^{2^m} + 1 - 2 \implies d \mid a^{2^m} + 1 - 2$ and $d \mid a^{2^m} + 1 \implies d \mid 2$.
Only, when a is odd, both $a^{2^n} + 1$ and $a^{2^m} + 1$ are even; d is 2 (maximum value), otherwise, $d \nmid 2$ as both $a^{2^n} + 1$ and $a^{2^m} + 1$ are odd. Then, $d = 1$.
Hence, the original proposition is proved.

1.11 Q11

Let me prove the contrapositive: If n is not a power of 2, $2^n + 1$ is not prime; composite.
If n is not a power of 2 , $n = 2^k \cdot (2 \cdot m + 1)$ where $m > 0$. Then, $2^n + 1 = 2^{2^k \cdot (2 \cdot m + 1)} + 1 = (2^{2^k})^{2 \cdot m + 1} + 1$. This has a proper factor which is not equal to 1 or the number itself, $2^{2^k} + 1$ as $2 \cdot m + 1$ is an odd number greater than 1.

1.12 Q12

Let $GCD(m,n) = k$. Then, $a^m - 1 = a^{kx} - 1$ and $a^n - 1 = a^{ky} - 1$ as $a^k - 1$ is a common factor. WALOG, assuming $m > n$.

$d \mid a^m - 1$ and $d \mid a^n - 1 \implies d \mid a^m - a^n = (a^n - 1)\cdot(a^{m-n} - 1) + a^{m-n} - 1 \implies d \mid a^{m-n} - 1$. Let $x\mathcal{R}y$ on set on $\mathcal{Z}$ if $d \mid a^{|x|} - 1$ and $d \mid a^{|y|} - 1$. So, we have $mRn \implies n\mathcal{R}(m-n)$ and $n\mathcal{R}(n-m)$.

Applying this to itself multiple times, we have $n\mathcal{R}(m-2n), n\mathcal{R}(m-3n)$... and $n\mathcal{R}(2m-n), n\mathcal{R}(3m-n)$. So, by applying this relation multiple times with itself or with other relations, we can generate any linear combination of m and n.

This means, $d \mid a^{|pm+qn|} - 1$ where p, q are arbitrary integers. Since by Euclid's lemma, the minimum positive value of $pm + qn$ is $(m,n) = k$, we have d $= a^k - 1$ as it is smallest value that is a multiple of d that d divides which is itself.

1.13 Q13

By Euclid's division lemma, we have $au + bv = d = 1$ has infinite solutions of the form:

$$(u_0 + \frac{b\cdot t}{d}, v_0 - \frac{a\cdot t}{d}) = (u,v) = (u_0 + b\cdot t, v_0 - a\cdot t)$$

with u_0 and v_0 derived from the division algorithm.
We need $u > 0$ and $v < 0$ so, $u_0 + b\cdot t > 0 \implies t > \frac{-u_0}{b}$ and $v_0 - a\cdot t < 0 \implies t > \frac{v_0}{a}$. So, we can take maximum of these two values and set $t = \max\left(\frac{-u_0}{b}, \frac{v_0}{a}\right)$ to get our required values x and y.

1.14 Q14

Let $x^a = y^b = N$. Let $\text{ord}_p N = z$ for prime factor p of N where $p \mid x$ and $p \mid y$. Let $\text{ord}_p x = z_1$ and $\text{ord}_p y = z_2$. We have $a \cdot z_1 = b \cdot z_2 = z$. As $(a,b) = 1$, $b \mid z_1$ and $a \mid z_2 \implies \frac{z_1}{b} = \frac{z_2}{a} = \frac{z}{a\cdot b} = k_p$ for some integer k and the prime p.
This holds true for all primes that are factors of N and hence, prime factors of x and y. Let us define n to be product of all such primes raised to the power k_p.
We see that, $ord_p n^a = a \cdot k_p = z_2 = ord_p y$ for all prime factors of y and n^a. Hence, $n^a = y$ and similarly, $n^b = x$ as required.

1.15 Q15

Let $\prod\limits_{d|n} d = K$. When, $d \mid n$, we have $\frac{n}{d} \mid n$. So, $\prod\limits_{d|n} \frac{n}{d} = K$ also.

Multiplying, both of these equations and pairing d and $\frac{n}{d}$, we have $\prod\limits_{d|n} d \cdot \frac{n}{d} = K^2$

$$\implies \prod_{d|n} n = K^2 \implies n^{d(n)} = K^2 \implies K = n^{\frac{d(n)}{2}}.$$

1.16 Q16

$\mu^2(d)$ is equal to 1 only when d is square-free else it is 0.
In $\sum_{d|n} \mu^2(d)$, we are counting the number of square-free divisors of n. Let $n = p_1^{a_1} \cdot p_2^{a_2} \dots p_k^{a_k}$. We can equivalently substitute n by $n' = \prod\limits_{1 \le i \le k} p_i$ as μ^2 is nonzero only when d is square-free.
Then, $\sum\limits_{d|n} \mu^2(d) = \sum\limits_{d|n'} \mu^2(d) = 1 + \binom{k}{1} + \binom{k}{2} + \binom{k}{3} \dots \binom{k}{k} = 2^k$ where $\binom{k}{i}$ is number of such divisors which have only i distinct prime factors out of k with exponent 1. As $k = \omega(n)$ (number of prime factors of n), $\sum_{d|n} \mu^2(d) = 2^{\omega(n)}$.

1.17 Q17

We have Mobius Inversion Formula, $\mu * f = g \implies f = u * g$ where μ is the Mobius function.

1.17.1

To prove, $\mu * \tau = u$. We have, $u * u = \sum_{d|n} u(\frac{n}{d}) \cdot u(d) = \sum_{d|n} 1 = \tau(n) =$ number of divisors of $n = d(n)$.
As $u * u = \tau \implies u = \mu * \tau$ by Mobius Inversion Formula as required.

1.17.2

To prove, $\mu * \sigma = E$. We have, $u * E = \sum_{d|n} u(\frac{n}{d}) \cdot E(d) = \sum_{d|n} d = \sigma(n) =$ sum of all divisors of n.
As $u * E = \sigma \implies E = \mu * \sigma$ by Mobius Inversion Formula as required.

1.18 Q18

$d(n)$ is a completely multiplicative function: $d(mn) = d(m).d(n)(\because$ product of factors of m and n is a factor of the product $mn)$.
So, it is sufficient to prove this relation for $n = p^a$.
LHS $= \sum_{k|n} (d(k))^3 = \sum_{0 \le i \le a} (d(p^i))^3 = \sum_{0 \le i \le a} (i+1)^3 = 1^3 + 2^3 + \dots + (a+1)^3 = (\frac{(a+1)(a+2)}{2})^2$.
RHS $= (\sum_{k|n} d(k))^2 = (\sum_{0 \le i \le a} d(p^i))^2 = (\sum_{0 \le i \le a} (i+1))^2 = (\frac{(a+1)(a+2)}{2})^2 =$ LHS.
Hence, proved.

1.19 Q19

We have the base case $\mu * log = \Lambda$, so when n has more than 1 distinct prime factor, it is 0.
As $\mu(n)$ is nonzero only on square-free numbers, it is enough to prove it for $n = p_1 \cdot p_2 \dots p_k$ with $k > m$. Consider, $log(p_i) = a_i$. Then, in $\sum_{d|n} \mu(d) \cdot log^m(d) = \sum_{d|n} \mu(d) \cdot (\sum_t a_i)^m = \sum_{d|n} (-1)^t \cdot (\sum_t a_i)^m$ where t is number of $log(p_i)$ in each term.
Consider the expression, $E = \prod\limits_{1 \le i \le k} (e^{\lambda a_i} - 1) = \prod\limits_{1 \le i \le k} ((\lambda a_i) + \frac{(\lambda a_i)^2}{2!} + \frac{(\lambda a_i)^3}{3!} \dots)$.

The coefficient of $\lambda^m = 0$ because, $m < k$ and we have at least one factor of λ from each term. But if we consider finding a combinatorial expression for λ^m, we get $(-1)^{k-1} \cdot \frac{\lambda^m}{m!} \cdot ((a_1^m) + (a_2^m) + (a_3^m) \ldots (a_k^m) + (-1)^{-1}(a_1+a_2)^m + \cdots + (-1)^{-m+1} \cdot (a_1 + a_2 + a_3 \ldots a_k)^m)$
$= (-1)^{k-1} \cdot \frac{\lambda^m}{m!} \cdot \sum_{d|n} (-1)^{-t} \cdot (\sum_t a_i)^m = (-1)^{k-1} \cdot \frac{\lambda^m}{m!} \cdot \sum_{d|n} (-1)^t \cdot (\sum_t a_i)^m = 0$.
This implies, that our original expression $\sum_{d|n} (-1)^t \cdot (\sum_t a_i)^m$ must be 0.

For Example: Consider $n = p_1 \cdot p_2 \cdot p_3 \implies a = log(p_1), b = log(p_2)$ and $c = log(p_3)$ and $m = 2$. We have to prove $(a^2+b^2+c^2)-(a+b)^2-(b+c)^2-(c+a)^2+(a+b+c)^2 = 0$. Now consider, $E = (e^{\lambda a}-1)\cdot(e^{\lambda b}-1)\cdot(e^{\lambda c}-1)$. The coefficient of λ^2 is the coefficient of λ^2 in $(e^{\lambda a} + e^{\lambda b} + e^{\lambda c} - e^{\lambda(a+b)} - e^{\lambda(b+c)} - e^{\lambda(c+a)} + e^{\lambda(a+b+c)}) = (-1)^2 \cdot \frac{\lambda^2}{2!} \cdot (a^2 + b^2 + c^2) - (a+b)^2 - (b+c)^2 - (c+a)^2 + (a+b+c)^2)$ which is 0 as, in Taylor Expansion of E, we have at least one λ from each factor of E.

1.20 Q20

As $g(n)$ and $f(n)$ are positive, we have LHS $= log(g(n)) = (log(f) * a)(n)$ and RHS $= log(f(n)) = (log(g) * b)(n)$.
We have $(a * b)(n) = I(n)$ by definition.
Multiplying by $log(f(n))$ both sides, we have $((log(f)) * a) * b = log(f) * I \implies (log(g) * b)(n) = log(f)(n)(\because$ LHS $) =$ RHS.
Similarly, multiplying by $log(g(n))$ both sides of $b*a = I$, we have $((log(g))*b)*a = log(g) * I \implies (log(f) * a)(n) = log(g)(n)(\because$ RHS $) =$ LHS. Hence, proved LHS $\iff$ RHS.

1.21 Q21

1.21.1

We have Mobius Inversion Formula $\mu * f = g \implies f = u * g$ where μ is the Mobius function.
So, $F_1 * u = \sum\limits_{d|n}(\sum\limits_{1 \le k \le n, (k,d)=1} f(\frac{k}{d})) = \sum\limits_{qd=n} (\sum\limits_{1 \le k \le n, (qk,n)=q} f(\frac{kq}{n}))$. Now, $(kq, n) = q$ allows all values less than q that have some GCD with n, so that the inner sum sums up all the $k \le n$ that same GCD q. So, the expression is same as F.

1.21.2

Using the above result, we have to prove $(\sum\limits_{1 \le k \le n (k,n)=1} e(\frac{k}{n})) * u = I. \implies \sum\limits_{1 \le k \le n} e(\frac{k}{n})$.
The sum in the expression is a GP. When $n = 1$, the sum $= e^{i2\pi} = 1$, otherwise the sum

$$\frac{e^{\frac{i2\pi}{n}} \cdot e^{i2\pi} - 1}{e^{\frac{i2\pi}{n}} - 1} = 0$$

. So, it is exactly $I(n)$.

1.22 Q22

Observation: $a-1 \leq \sqrt{a^2-1} < a \implies (a-1)^2 \leq a^2-1 < a^2 \implies 2-2a \leq 0 \leq 1 \implies a \geq 1$. So, a can be any natural number.
In the function, $f(n) = \lfloor \sqrt{n} \rfloor - \lfloor \sqrt{n-1} \rfloor$.
Case 1: If n is a perfect square $= a^2 \implies f(n) = a-(a-1) = 1$.
Case 2: If $n = a^2+1, f(n) = a-a = 0$.
Case 3: Otherwise, both n and $n-1$ lie between 2 perfect squares and $f(n) = 0$.
Consider, $0 = f(p_1) \cdot f(p_2) = f(p_1 \cdot p_2) = 0$ where $p_1 \neq p_2$ are primes. But, $0 = f(p_1) \cdot f(p_1) \neq f(p_1^2) = 1$. Hence, $f(n)$ is multiplicative but not completely multiplicative.

1.23 Q23

Consider, $F(p_1) = \prod_{d|p_1} f(d) = f(1) \cdot f(p_1)$ and $F(p_2) = \prod_{d|p_2} f(d) = f(1) \cdot f(p_2)$.
Now, $F(p_1 \cdot p_2) = \prod_{d|p_1 \cdot p_2} f(d) = f(1) \cdot f(p_1) \cdot f(p_2) \cdot f(p_1 \cdot p_2)$ which is not equal to $F(p_1) \cdot F(p_2)$ as $f(p_1)$ and $f(p_2)$ appear twice each in the RHS but once each in the LHS. So, $F(n)$ is not multiplicative.

1.24 Q24

The argument of $f((k,n))$ is $(k,n) = d$ which must divide n. The number of times, $1 \leq k \leq n, (k,n) = d$ is $\phi(n/d)$ as $(k,n) = d \implies (\frac{k}{d}, \frac{n}{d}) = 1$.

So, $\sum_{1 \leq k \leq n} f((k,n)) = \sum_{d|n} f(d) \cdot \phi(n/d) \implies g(n) = \phi(n)$. Hence, such an function $g = \phi$ exists which is multiplicative arithmetic function as required.

Now, in lectures we have proved $\phi = \mu * E$ and E is completely multiplicative by definition. So, if $f = (k,n)\mu(k,n) = \mu E \implies f * g = (\mu E) * \phi = (\mu E) * (\mu * E) = (\mu E * E) * \mu = \mu (\because \mu E$ is the Dirichlet Arithmetic Inverse of 'E' which is completely multiplicative). Hence, proved.

1.25 Q25

In Liouville's function, $\lambda(n) = (-1)^{\omega(n)} \implies \lambda(n) = (-1)^{\sum\limits_{1 \leq i \leq k} a_i}$ where a_i is the exponent of the i^{th} prime p_i in prime factorisation of n.
$\implies \lambda(n) = (-1)^{\sum\limits_{1 \leq i \leq k} a_i \% 2}$ $(\because (-1)^2 = 1))$ where % represents modulo symbol.
Now, consider $n = p^2 \cdot b$ where b is completely square-free. In this representation, a prime p_i is a factor of b if and only if it occurs odd number of times. So, $b = \prod\limits_{1 \leq i \leq k} p_i^{a_i \% 2}$.
Let $\mathcal{S} = \sum\limits_{d^2|n} \mu(\frac{n}{d^2}) = \mu(\frac{p^2 \cdot b}{d^2}$. $\mu(\frac{p^2 \cdot b}{d^2})$ is non zero only when its argument is square free. So, $d = p$ and $\mathcal{S} = \mu(b) = (-1)^{K_b}$ where K_b is the number of prime factors of b and these prime factors occur odd number of times in prime factorisation of n.
As defined above, $K_b = \sum\limits_{1 \leq i \leq k} a_i \% 2$. Hence, $(-1)^{K_b} = \mathcal{S} = \sum\limits_{d^2|n} \mu(\frac{n}{d^2}) = \lambda(n)$.