MAT4003 Assignment 3

1

Given integer a coprime to $561 = 3 \cdot 11 \cdot 17$, it must be that $3, 11, 17 \nmid a$ (otherwise $(a, 561) \geq 3 \neq 1$). Then by Fermat's Little Theorem,

$$\begin{cases} a^2 \equiv 1 \pmod 3 \\ a^{10} \equiv 1 \pmod{11} \\ a^{16} \equiv 1 \pmod{17} \end{cases},$$

which implies

$$\begin{cases} a^{560} \equiv 1 \pmod 3 \\ a^{560} \equiv 1 \pmod{11} \\ a^{560} \equiv 1 \pmod{17} \end{cases}.$$

Therefore by CRT,

$$a^{560} \equiv 1 \pmod{561}. \quad \square$$

2

Test $x \equiv 0, 1, \ldots, 6 \pmod 7$ for the congruence

$$f(x) = x^2 + 4x + 2 \equiv 0 \pmod 7.$$

We obtain solutions

$$x_{1,2} \equiv 1, 2.$$

Now $f'(x) = 2x + 4$. $f'(x_1) \equiv -1 \not\equiv 0 \pmod 7$. By Hensel's Lemma, there exists a unique t in least residue system modulo 7 s.t. $f(x_1 + 7t) \equiv 0 \pmod{49}$, given by

$$t \equiv -\frac{f(x_1)}{7}[f'(x_1)]^{-1} \equiv -(6^{-1}) \equiv 1 \pmod 7.$$

So $t = 1$, and that

$$f(8) \equiv 0 \pmod{49}.$$

Also, $f'(x_2) \equiv 1 \not\equiv 0 \pmod 7$. So by Hensel's Lemma, x_2 can be uniquely lifted to $x_2 + 7t$ with

$$t \equiv -\frac{f(x_2)}{7}[f'(x_2)]^{-1} \equiv (-2)(8^{-1}) \equiv 5 \pmod 7.$$

So $t = 5$, and

$$f(37) \equiv 0 \pmod{49}.$$

Therefore the lifted solutions are given by:

$$\boxed{x \equiv 8 \vee x \equiv 37 \pmod{49}.}$$

3

Note that $1024 = 2^{10}$, we consider the congruence

$$f(x) = x^3 - x - 2 \equiv 0 \pmod{2}$$

The solutions are $x_1 \equiv 0, x_2 \equiv 1$.

First consider x_1. $f'(x) = 3x^2 - 1$; $f'(x_1) \equiv 1 \pmod{2}$. Therefore by Hensel's Lemma, x_1 can be uniquely lifted to $x_1^{(2)} \equiv 0 + (-\frac{-2}{2}) \cdot 2 \equiv 2$ modulo 2^2 s.t. $f(x_1^{(2)}) \equiv 0 \pmod{2^2}$.

Now $f'(x_1^{(2)}) \equiv 1 \pmod{2}$. Again we may uniquely lift it to $x_1^{(3)} \equiv 2 + (-\frac{4}{4}) \cdot 2^2 \equiv 6$ modulo 2^3 s.t. $f(x_1^{(3)}) \equiv 0 \pmod{2^3}$.

In general, if $f(x_1^{(k)}) \equiv 0 \pmod{2^k}$, and that $x_1^{(k)} \equiv 0 \pmod{2}$, it follows that $f'(x_1^{(k)}) \equiv 3 \cdot 0^2 - 1 \equiv 1 \not\equiv 0 \pmod{2}$. So by Hensel's Lemma $x_1^{(k)}$ can be uniquely lifted to $x_1^{(k+1)} \equiv x_1^{(k)} + t \cdot 2^k \pmod{2^{k+1}}$. Notice that again $x_1^{(k+1)} \equiv 0 + t \cdot 2^k \equiv 0 \pmod{2}$. Using induction $x_1^{(k+1)}$ can be further lifted to $x_1^{(k+2)}, x_1^{(k+3)} \dots$ indefinitely. Therefore x_1 can be uniquely lifted to $x_1^{(10)}$ s.t. $f(x_1^{(10)}) \equiv 0 \pmod{1024}$.

Now consider x_2. We set $x_2 = 2t + 1$. Plugging in $f(x) \equiv 0 \pmod{2^2}$, we have $f(x_2) \equiv 6t + 1 - (2t + 1) - 2 \equiv 4t - 2 \equiv 2 \pmod{2^2}$. Hence no odd number x satisfies congruence $f(x) \equiv 0 \pmod{2^2}$. Consequently no odd number x can be a solution to $f(x) \equiv 0 \pmod{2^{10}}$.

Therefore, there exists a $\boxed{\text{unique}}$ $x \equiv x_1^{(10)}$ that satisfies $f(x) \equiv 0 \pmod{2^{10}}$.

4

Since the doors are all close initially, door x is open in the end if and only if the number of changes in the state of the door is $\equiv 1 \pmod{2}$. But the number of changes in the state is exactly the number of Servants in $\{S_1, S_2, \dots, S_{100}\}$ whose indices divide x. In other words, door x is ultimately open if and only if

$$\sigma_0(x) \equiv 1 \pmod{2}.$$

Note that for a non-square x, every positive divisor, d, of x is paired with another distinct positive divisor x/d. Hence $\sigma_0(x) \equiv 0 \pmod{2}$. For a square x, every positive divisor is paired with another distinct divisor, except for $d = \sqrt{x}$, which is paired with itself. In this case $\sigma_0(x) \equiv 1 \pmod{2}$. Therefore, door x is ultimately open if and only if x is a perfect square, i.e., $\boxed{x = 1, 4, 9, \dots, 81, 100}$

5

Suppose $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}, n = p_1^{\beta_1} \dots p_r^{\beta_r}$ with $\alpha, \beta \neq 0$ and p being distinct primes. Since $(m, n) > 1$, we may suppose $D := \{d_1, d_2, \dots, d_i\} \subset \{p_1, \dots, p_r\}$ is the set of all primes that divide both m and n. Now

$$\begin{aligned}\frac{\sigma_k(m)\sigma_k(n)}{\sigma_k(mn)} &= \frac{\prod_j \sigma_k(p_j^{\alpha_j})\sigma_k(p_j^{\beta_j})}{\sigma_k(\prod_j p_j^{\alpha_j+\beta_j})} \\ &= \frac{\prod_{p_j \notin D} \sigma_k(p_j^{\alpha_j})\sigma_k(p_j^{\beta_j})}{\prod_{p_j \notin D} \sigma_k(p_j^{\alpha_j+\beta_j})} \cdot \frac{\prod_{p_j \in D} \sigma_k(p_j^{\alpha_j})\sigma_k(p_j^{\beta_j})}{\prod_{p_j \in D} \sigma_k(p_j^{\alpha_j+\beta_j})} \qquad (*)\end{aligned}$$

where index j ranges over 1 to r. For all j s.t. $p_j \notin D, \min\{\alpha_j, \beta_j\} = 0$. So $\sigma_k(p_j^{\alpha_j+\beta_j}) = \sigma_k(p_j^{\max\{\alpha_j+\beta_j\}}) = \sigma_k(p_j^{\max\{\alpha_j+\beta_j\}})\sigma_k(1) = \sigma_k(p_j^{\alpha_j})\sigma_k(p_j^{\beta_j})$. Thus the first fraction in $(*)$ vanishes:

$$\begin{aligned}\frac{\sigma_k(m)\sigma_k(n)}{\sigma_k(mn)} &= \frac{\prod_{p_j \in D} \sigma_k(p_j^{\alpha_j})\sigma_k(p_j^{\beta_j})}{\prod_{p_j \in D} \sigma_k(p_j^{\alpha_j+\beta_j})} \\ &= \frac{\prod_{p_j \in D}(\sum_{x=1}^{\alpha_j} p_j^{xk} \cdot \sum_{y=1}^{\beta_j} p_j^{yk})}{\prod_{p_j \in D} \sum_{x=1}^{\alpha_j+\beta_j} p_j^{xk}} \qquad (**)\end{aligned}$$

Now, each term in $\sum_{x=1}^{\alpha_j+\beta_j} p_j^{xk}$ can be found in expansion of $\sum_{x=1}^{\alpha_j} p_j^{xk} \cdot \sum_{y=1}^{\beta_j} p_j^{yk}$ (set $y = 1$ and let x ranges over 1 to α_j; then fix x at α_j and traverse y from 1 to β_j). But the coefficient for p_j^{3k} in $\sum_{x=1}^{\alpha_j} p_j^{xk} \cdot \sum_{y=1}^{\beta_j} p_j^{yk}$ is 2 be letting $x, y = 1, 2$ and then $x, y = 2, 1$. So $\sum_{x=1}^{\alpha_j} p_j^{xk} \cdot \sum_{y=1}^{\beta_j} p_j^{yk} > \sum_{x=1}^{\alpha_j+\beta_j} p_j^{xk}$ for all j with $p_j \in D$. It follows that $(**) > 1$, which completes the proof. $\square$

6

(a)

Since ϕ is multiplicative,

$$\frac{\phi^2(n)}{n} = \prod_{p|n} \frac{\phi^2(p^{a_p})}{p^{a_p}} = \prod_{p|n} \frac{[p^{a_p-1}(p-1)]^2}{p^{a_p}} = \prod_{p|n} p^{a_p-2}(p-1)^2 \geq \prod_{p|n} \frac{(p-1)^2}{p}.$$

Note that for all $p \geq 3$, $(p-1)^2/p = p + 1/p - 2 \geq 1 + 1/3 \geq 1$. Therefore

$$\frac{\phi^2(n)}{n} \geq \frac{(2-1)^2}{2} = \frac{1}{2}. \quad \square$$

(b)

Write $n = \prod_{i=1}^r p_i^{a_i}$, where p_i are the primes that divide n. For notational simplicity define $P := \prod_{i=1}^r (a_i + 1)$. By multiplicativity of τ,

$$n^{\tau(n)/2} = n^{[\prod_{i=1}^r (p_i^{a_i})]/2} = n^{P/2}.$$

To compute $\prod_{d|n} d$, note that any divisor d, of n, has the form $d = \prod_{i=1}^{r} p_i^{b_i}$, where $0 \leq b_i \leq a_i$ for all p. (In other words, a divisor d is uniquely determined by choosing the exponents b_i for every prime factor p_i.) Consequently $\prod_{d|n} d$ also has the form $\prod_{i=1}^{r} p_i^{c_i}$. Hence it suffices to find exponents c_i.

To compute c_1, note that for every choice of exponent of p_1, there are $M_1 := (a_2+1)(a_3+1)\dots(a_r+1)$ choices for the exponents of the rest of the primes, producing M_1 distinct divisors. So $c_1 = M_1(0+1+\dots+a_1) = a_1 P/2$. In general, if we define $M_i := P/(a_i+1)$, for every choice of exponent of p_i there are M_i choices for the exponents of prime factors other than p_i. So $c_i = M_i(0+1+\dots+a_i) = a_i P/2$. It follows that

(c)

Since τ is multiplicative, τ^3 is multiplicative. By Theorem (3.10), $\tau * u$ is also multiplicative. It follows that $\mathrm{LHS} = (\tau * u)^2$ multiplicative. Again by Theorem (3.10), $\mathrm{RHS} = \tau^3 * u$ is multiplicative. Thus it suffices to show the equality for prime powers p^a. Indeed,

$$(\tau * u)^2(p^a) = \left(\sum_{i=0}^{a} \tau(p^i)\right)^2 = \left(\sum_{i=1}^{a+1} i\right)^2 = \left[\frac{(a+1)(a+2)}{2}\right]^2$$

$$(\tau^3 * u)(p^a) = \sum_{i=0}^{a} \tau^3(p^i) = \sum_{i=1}^{a+1} i^3 = \left[\frac{(a+1)(a+2)}{2}\right]^2,$$

whence the equality follows. $\square$

(d)

Since μ is multiplicative, LHS is multiplicative by Theorem (3.10). Let a, b are coprime. Then a and b have distinct prime factors. It follows that $2^{\omega(ab)} = 2^{\omega(a)+\omega(b)} = 2^{\omega(a)} \cdot 2^{\omega(b)}$; RHS is also multiplicative. It suffices to show that both sides agree on prime powers p^a, as follows:

$$(\mu^2 * u)(p^a) = \sum_{i=0}^{a} \mu^2(p^i) = 1^2 + (-1)^2 = 2 = 2^{\omega(p^a)}. \quad \square$$

7

By 6(d), $2^{\omega} = u * \mu^2$.

$\implies$: Assume n is not divisible by p^2. Then $\mu(n) = (-1)^{\omega(n)}$, whence $(\mu * 2^{\omega})(n) = (\mu * u * \mu^2)(n) = (I * \mu^2)(n) = \mu^2(n) = 1$.

$\impliedby$: Assume $(\mu * 2^{\omega})(n) = 1$. Then $(\mu * u * \mu^2)(n) = (I * \mu^2)(n) = \mu^2(n) = 1$. So n is not divisible by p^2. $\square$

8

For all $k \geq 4$, $\mu(k!) = 0$ since $2^2 | k!$. Therefore

$$\sum_{k=1}^{\infty}\mu(k!)=\sum_{k=1}^{3}\mu(k!)=2.$$

9

(a)

If f is multiplicative, $f\cdot\mu$ is also multiplicative. Thus by Theorem (3.10), $\mathrm{LHS}=u*(f\cdot\mu)$ is multiplicative. For RHS, assume a,b are coprime. Then a and b have distinct prime factors. It follows that

$$\prod_{p|ab}(1-f(p))=\prod_{q|a}(1-f(q))\cdot\prod_{r|b}(1-f(r))$$

where p,q,r are primes. Thus RHS is also multiplicative. It suffices to show equality for prime powers p^a :

$$[u*(f\cdot\mu)](p^a)=\sum_{i=0}^{a}\mu(p^i)f(p^i)=f(1)-f(p)\overset{f\text{ mult.}}{=}1-f(p).\quad\square$$

(b)

Since τ is multiplicative, it follows from (a) that

$$[u*(\tau\cdot\mu)](n)=\prod_{p|n}(1-\tau(p))=\prod_{p|n}(-1)=(-1)^{\omega(n)}.\quad\square$$

(c)

Since σ is multiplicative, it follows from (a) that

$$[u*(\sigma\cdot\mu)](n)=\prod_{p|n}(1-\sigma(p))=\prod_{p|n}(-p)=(-1)^{\omega(n)}\prod_{p|n}p.\quad\square$$

10

(a)

Write $a=\prod p_i^{a_i}, b=\prod p_i^{b_i}$, where p_i is the i-th prime number.

$$\lambda(ab)=(-1)^{\Omega(ab)}=(-1)^{\sum(a_i+b_i)}=(-1)^{\sum a_i}\cdot(-1)^{\sum b_i}=\lambda(a)\lambda(b).\quad\square$$

(b)

Lemma 1. Let n has prime factorization $p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$. n is a perfect square if and only if $a_1,\dots,a_r$ are all even.

Proof. $\Longleftarrow$ is obvious; $\Longrightarrow$: Suppose $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ is a perfect square. Then $\sqrt{n} = p_1^{a_1/2} p_2^{a_2/2} \dots p_r^{a_r/2} \in \mathbb{N}$. By FTA, $a_1/2, \dots a_r/2$ are all positive integers, whence $a_1, \dots, a_r$ are all even. $\square$

Lemma 2. Let $(a, b) = 1$. Then ab is a perfect square if and only if a and b are both perfect square.

Proof. $\Longleftarrow$ is obvious; $\Longrightarrow$: Assume $(a, b) = 1$. Then a and b have distinct prime factors. We may let $a = p_1^{a_1} \dots p_m^{a_m}$ and $b = q_1^{b_1} \dots q_n^{b_n}$ be their respective prime factorization, where $p_i \neq q_j$ for all i, j. Then by Lemma 1, we have the following chain of equivalence:

$$\begin{aligned} ab = p_1^{a_1} \dots p_m^{a_m} q_1^{b_1} \dots q_n^{b_n} \text{ square} &\iff a_1, \dots, a_m, b_1, \dots, b_n \text{ all even} \\ &\iff a_1, \dots, a_m \text{ all even} \wedge b_1, \dots, b_n \text{ all even} \\ &\iff a \text{ square} \wedge b \text{ square.} \quad \square \end{aligned}$$

We want to show

$$\sum_{d|n} \lambda(d) = p(n) := \begin{cases} 1, & \text{if } n \text{ is square;} \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

Assume $(a, b) = 1$. By Lemma 2, $p(ab) = 1$ if and only if $p(a) = 1$ and $p(b) = 1$. Hence $p(ab) = p(a)p(b)$. p is multiplicative. Since λ is multiplicative, from Theorem (3.11), $\sum_{d|n} \lambda(d)$ is also multiplicative. Thus it suffices to show (1) for prime powers p^a.

$$\sum_{d|p^a} \lambda(d) = \sum_{i=0}^{a} \lambda(p^i) = \sum_{i=0}^{a} (-1)^{\Omega(p^i)} = 1 + \sum_{i=1}^{a} (-1)^i.$$

By Lemma 1, $n = p^a$ is square if and only if a is even. Therefore,

$$\sum_{d|n} \lambda(d) = \begin{cases} 1, & \text{if } a \text{ is even} \iff n \text{ is square} \\ 0, & \text{otherwise.} \end{cases} = p(n). \quad \square$$