Amin Zolfagharian - 610300118

Problem 1.

Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. If $x^2 \overset{n}{\equiv} -1$ then for $1 \leq i \leq k$ we have $x^2 \overset{p_i^{\alpha_i}}{\equiv} -1$, which means we have $x^2 \overset{p_i}{\equiv} -1$. Suppose $p_i \neq 2$. And let x be an answer for this equation:

$$x^2 \overset{p_i}{\equiv} -1 \implies x^4 \overset{p_i}{\equiv} 1$$

This shows that $Ord_{p_i}(x) = 4$. Then we have: $Ord_{p_i}(x) \mid \phi(p_i) = p_i - 1$. Therefore $4 \mid p_i - 1$. Thus $p_i \overset{4}{\equiv} 1$. Now if $p \overset{4}{\equiv} 1$ then we have:

$$\begin{aligned}
-1 = (p-1)! &= (1 \times 2 \times \dots \times \frac{p-1}{2})(\frac{p+1}{2} \times \dots \times (p-1)) \\
&= (1 \times 2 \times \dots \times \frac{p-1}{2})(1 \times 2 \times \dots \times \frac{p-1}{2})(-1)^{(p-1)/2} \\
&= (1 \times 2 \times \dots \times \frac{p-1}{2})^2
\end{aligned}$$

This shows that for prime p_i, $x^2 \overset{p_i}{\equiv} -1$ has an answer iff $p_i \overset{4}{\equiv} 1$ and it has exactly two answers $(1 \times 2 \times \dots \times \frac{p-1}{2})$ and $-(1 \times 2 \times \dots \times \frac{p-1}{2})$. Now suppose r and t are two answers for $x^2 + 1 \overset{p^\alpha}{\equiv} 0$ with $p \overset{4}{\equiv} 1$. Where $p \nmid t - r$ and $p \nmid r, t$. By Hensel's lemma since $p \nmid 2r$ then $x^2 + 1 \overset{p^{\alpha+1}}{\equiv} 0$ has one answer v such that $v \overset{p^\alpha}{\equiv} r$. Similarly for t there exists one answer u such that $u \overset{p^\alpha}{\equiv} t$. And since $p \nmid t - r$ and $p \nmid r, t$ it follows that $p \nmid v - u$ and $p \nmid u, v$. Thus $x^2 + 1 \overset{p^\alpha}{\equiv} 0$ has exactly two answers.
For $p = 2$ we have $x^2 + 1 \overset{2}{\equiv} 0$ has one answer $x = 1$. And for any $\alpha > 1$ by Hensel's lemma $x^2 + 1 \overset{2^\alpha}{\equiv} 0$ doesn't have an answer. Since $x^2 + 1 \overset{4}{\equiv} 0$ doesn't have an answer.
This shows that $x^2 + 1 \overset{p^\alpha}{\equiv} 0$ has 2 answers if $p \overset{4}{\equiv} 1$ and doesn't have an answer if $p \overset{4}{\equiv} 3$, and if $p = 2$ it has one answer if $\alpha = 1$ and doesn't have any answers if $\alpha > 1$. By chinese remainder theorem it is easy to see that the number of answers modulo n is the product of the number of answers for all $1 \leq i \leq k$, $x^2 + 1 \overset{p_i^{\alpha_i}}{\equiv} 0$.

Problem 2.

We know that $26411 = 7^4 \times 11$. $x^2 + x + 47 \overset{7}{\equiv} 0$ has two answers 1 and 5. Now we use Hensel's lemma to lift up these answers modulo 7^4. Let $f(x) = x^2 + x + 47$, then we have $f'(x) = 2x + 1$.

$$\begin{aligned}
1 : f'(1) = 3 \overset{7}{\not\equiv} 0 &\implies t \overset{7}{\equiv} (-f'(1)^* f(1)/7) \implies t = 0 \implies 1 + 7 \times 0 = 1 \\
5 : f'(5) = 11 \overset{7}{\not\equiv} 0 &\implies t \overset{7}{\equiv} (-f'(5)^* f(5)/7) \implies t = 6 \implies 5 + 7 \times 6 = 47
\end{aligned}$$

Thus 1 and 47 are the answers to $x^2 + x + 47 \overset{7^2}{\equiv} 0$. Now for 7^3:

$$1 : f'(1) = 3 \overset{7}{\not\equiv} 0 \implies t \overset{7}{\equiv} (-f'(1)^* f(1)/49) \implies t = 2 \implies 1 + 49 \times 2 = 99$$
$$47 : f'(47) = 95 \overset{7}{\not\equiv} 0 \implies t \overset{7}{\equiv} (-f'(47)^* f(47)/49) \implies t = 4 \implies 47 + 49 \times 4 = 243$$

Thus 99 and 243 are the answers to $x^2 + x + 47 \overset{7^3}{\equiv} 0$. For 7^4:

$$99 : f'(99) \overset{7}{\not\equiv} 0 \implies t \overset{7}{\equiv} (-f'(99)^* f(99)/343) \implies t = 2 \implies 99 + 343 \times 2 = 785$$
$$243 : f'(243) \overset{7}{\not\equiv} 0 \implies t \overset{7}{\equiv} (-f'(243)^* f(243)/343) \implies t = 4$$
$$\implies 243 + 343 \times 4 = 1615$$

Thus 785 and 1615 are the answers to $x^2 + x + 47 \overset{7^4}{\equiv} 0$. Also 5 is the only answer to $x^2 + x + 47 \overset{11}{\equiv} 0$. By Chinese Remainder Theorem we have 10389 and 16021 are the answers to the equation.

Problem 3.

First we prove that τ is multiplicative. Suppose $(m, n) = 1$. Let D_m be the set of divisors of m. We intrudoce a bijection:

$$\pi : D_m \times D_n \to D_{mn}$$
$$\pi(i, j) = ij$$

π is surjective since for any $d \mid mn$ where $(m, n) = 1$ there exists d_1 and d_2 such that $d_1 d_2 = d$ where $d_1 \mid n$ and $d_2 \mid m$. It also is injective since if $\pi(a, b) = \pi(c, d)$. Therefore $ab = cd$. Suppose for prime p such that $p \mid a \mid m$:

$$p \mid a \implies p \mid ab = cd \implies p \mid cd$$
$$p \mid c \text{ or } d$$

If $p \mid d$ then since $d \mid n$, $p \mid n$. which implies $p \mid (m, n) = 1$. Which is a contradiction. Therefore $p \mid c$. This shows that $a \mid c$. Similarly we can show that $c \mid a$. Therefore if $\pi(a, b) = \pi(c, d)$ we would have $a = c$ and $b = d$. Thus π is a bijection. Since $\tau(k)$ is the number of elements in D_k, the bijection π shows that τ is multiplicative and for $(m, n) = 1$ we have $\tau(mn) = \tau(m)\tau(n)$.
We prove this by induction on number of distinct primes in n. First we prove the equation for $k = 1$, $n = p^\alpha$. We know that $\tau(p^\alpha) = \alpha + 1$.

$$[\sum_{d \mid p^\alpha} \tau(d)]^2 = [1 + 2 + \cdots + \alpha + (\alpha + 1)]^2 = 1^3 + 2^3 + \cdots + (\alpha + 1)^3 = \sum_{d \mid p^\alpha} \tau(d)^3$$

Now suppose that for any n with $k - 1$ distinct prime divisors, the equation holds. Now suppose $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, and $n = n_1 p_k^{\alpha_k}$

$$[\sum_{d \mid n} \tau(d)]^2 = [(\sum_{d_1 \mid p_k^{\alpha_k}} \tau(d_1))(\sum_{d_2 \mid n_1} \tau(d_2))]^2$$

Since n_1 has $k-1$ distinct prime divisors, by induction hypothesis for n_1 and $p_k^{\alpha_k}$:

$$[(\sum_{d_1|p_k^{\alpha_k}} \tau(d_1))(\sum_{d_2|n_1} \tau(d_2))]^2 = (\sum_{d_1|p_k^{\alpha_k}} \tau(d_1)^3)(\sum_{d_2|n_1} \tau(d_2)^3)$$
$$= \sum_{d|n} \tau(d)^3$$

Thus the proof is completed.

Problem 4.

We know that ϕ is multiplicative. We prove this by induction on number of distinct prime divisors of d. for $k=0$, we have $d=1$, therefore $(a,b)=1$: $\phi(ab)=\phi(a)\phi(b)\frac{1}{\phi(1)}$ Now suppose that the statement is true for $k-1$. Let $d=p_1^{\alpha_1}\dots p_k^{\alpha_k}=d'p_k^{\alpha_k}$. WLOG suppose $a=p_k^{\alpha_k}a'$ and $b=p_k^{\beta}b'$ where $\beta \geq \alpha_k$.

$$\phi(ab)=\phi(a'b'p_k^{\alpha_k+\beta})=\phi(a'b')\phi(p_k^{\alpha_k+\beta})$$

since $d'=(a',b')$ and has $k-1$ distinct prime divisors, by induction hypothesis we have: $\phi(a'b')=\phi(a')\phi(b')\frac{d'}{\phi(d')}$:

$$\phi(a'b')\phi(p_k^{\alpha_k+\beta})=\phi(a')\phi(b')\frac{d'}{\phi(d')}p_k^{\alpha_k+\beta-1}(p_k-1)$$
$$=\phi(a')\phi(b')\frac{d'}{\phi(d')}p_k^{\alpha_k-1}(p_k-1)p_k^{\beta-1}(p_k-1)\frac{p_k^{\alpha_k}}{p_k^{\alpha_k-1}(p_k-1)}$$
$$=\phi(a')\phi(p_k^{\alpha_k})\phi(b')\phi(p_k^{\beta})\frac{d'}{\phi(d')}\frac{p_k^{\alpha_k}}{\phi(p_k^{\alpha_k})}$$
$$=\phi(a)\phi(b)\frac{d}{\phi(d)}$$

Thus $\phi(ab)=\phi(a)\phi(b)\frac{d}{\phi(d)}$. Now if $d>1$ then $\phi(d)<d$. Therefore $\frac{d}{\phi(d)}>1$. This follows that $\phi(ab)>\phi(a)\phi(b)$.

Problem 5.

The only solutions are prime numbers. For any prime p, we know that $\phi(p)=p-1$ and $\sigma(p)=p+1$. Thus $\phi(p)+\sigma(p)=2p$. Now by induction on the number of distinct divisors of n we show that if n is not a prime number then $\phi(n)+\sigma(n)>2n$. for $k=1$ which means $n=p^\alpha$ with $\alpha>1$ we have:

$$\phi(p^\alpha)+\sigma(p^\alpha)=p^{\alpha-1}(p-1)+p^\alpha+p^{\alpha-1}+\dots+p^1+1$$
$$=2p^\alpha+p^{\alpha-2}+\dots+p^1+1\geq 2p^\alpha+1>2p^\alpha$$

Now suppose the statement is true for $k-1$. Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} = n_1 p_k^{\alpha_k}$:

$$\begin{aligned}\phi(n)+\sigma(n) &= \phi(n_1)\phi(p_k^{\alpha_k})+\sigma(n_1)\sigma(p_k^{\alpha_k})\\ &= \phi(n_1)p^{\alpha_k-1}(p_k-1)+\sigma(n_1)(p_k^{\alpha_k}+\cdots+1)\\ &= \phi(n_1)p_k^{\alpha_k}+\sigma(n_1)p_k^{\alpha_k}-\phi(n_1)p_k^{\alpha_k-1}+\sigma(n_1)(p_k^{\alpha_k-1}+\cdots+1)\\ &\geq p_k^{\alpha_k}(\phi(n_1)+\sigma(n_1))+p_k^{\alpha_k-1}(\sigma(n_1)-\phi(n_1))\end{aligned}$$

Now by induction hypothesis we know that $\phi(n_1)+\sigma(n_1) \geq 2n_1$. We also know that $\phi(n) < n < \sigma(n)$:

$$\begin{aligned}&p_k^{\alpha_k}(\phi(n_1)+\sigma(n_1))+p_k^{\alpha_k-1}(\sigma(n_1)-\phi(n_1))\\ &\geq p_k^{\alpha_k}2n_1+p_k^{\alpha_k-1}(1) \geq 2n+p_k^{\alpha_k-1} > 2n\end{aligned}$$

Thus for any composite n, $\phi(n)+\sigma(n) > 2n$. And only for prime p, $\phi(p)+\sigma(p) = 2p$.

Problem 6.

($\Rightarrow$) If f has an inverse g then we have:

$$f * g = l$$

Where l is the identity function. with $l(1) = 1$ and $l(n) = 0$ for $n \neq 1$. Now if we check input 1:

$$f * g(1) = f(1)g(1) = 1$$

This shows that $f(1) \neq 0$.
($\Leftarrow$) If $f(1) \neq 0$, we find g such that $f * g = l$. We use induction on n. Base case $n = 1$:

$$f * g(1) = f(1)g(1) \implies g(1) = \frac{1}{f(1)}$$

And since $f(1) \neq 1$ then $\frac{1}{f(1)}$ is valid. Now suppose that for all $n \leq k$ we know the value of g such that $f * g(n) = l(n)$. Put $n = k+1$.

$$f * g(n) = \sum_{d|n} f(d)g(\frac{n}{d})$$

For all $\frac{n}{d} < n$ the value of g is already determined, Thus we sum all the values for $d > 1$: $S = \sum_{d|n} f(d)g(\frac{n}{d}) - f(1)g(n)$.

$$\begin{aligned}f * g(n) &= \sum_{d|n} f(d)g(\frac{n}{d}) = S + f(1)g(n)\\ &\implies g(n) = \frac{-S}{f(1)}\end{aligned}$$

Which is valid. Thus we proved that for $n = k+1$ there exists $g(1), \dots, g(k+1)$ such that for all $n \leq k+1$ we have: $f * g(n) = l(n)$. Therefore the funciton g described is the inverse of f.

Problem 7.

(i) We describe f as below:

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is square free} \\ 0 & O.W. \end{cases}$$

Note that $f(1) = 1$. Now $\sum_{d|n} f(d)$ is the number of square free divisors of n. Now let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Free squares divisors of n are all of the form $p_1^{\beta_1} \dots p_k^{\beta_k}$ with $0 \leq \beta_i \leq 1$. And since for any β_i there are two choices, then the number of squares free numbers are $2^k = 2^{\omega(n)}$.

(ii) Note that $\mu(d)$ for any square free d is either +1 or -1 but for any other number is 0. We use induction on the number of distinct primes in n. for $k = 1$ we have $n = p^\alpha$:

$$p^\alpha \sum_{p^\beta | p^\alpha} \frac{|\mu(p^\beta)|}{p^\beta} = p^\alpha(1 + \frac{1}{p} + \frac{0}{p^2} + \dots + \frac{0}{p^\alpha}) = p^\alpha(1 + \frac{1}{p})$$

$$= p^\alpha + \dots + p + 1 - p^{\alpha-2} - \dots - p - 1 = \mu(1)\sigma(p^\alpha) + \mu(p)\sigma(\frac{n}{p^2}) + 0 + \dots + 0$$

$$= \sum_{p^{2\beta} | p^\alpha} \mu(p^\beta)\sigma(\frac{p^\alpha}{p^{2\beta}})$$

Now suppose for $m < k$ the equation holds. Let $m = k$. Thus $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} = n_1 p_k^{\alpha_k}$. We know both μ and σ are both multiplicative, also μ is not zero for square free numbers, which means in $d^2 \mid n$, only square free d numbers are important:

$$n \sum_{d|n} \frac{|\mu(d)|}{d} = n_1 p_k^{\alpha_k} (\sum_{p_k^\beta | p_k^{\alpha_k}} \frac{|\mu(p_k^\beta)|}{p_k^\beta})(\sum_{d_1 | n_1} \frac{|\mu(d_1)|}{d_1}) \overset{I.H}{=} p_k^{\alpha_k}(1 + \frac{1}{p_k})(\sum_{d_1^2 | n_1} \mu(d_1)\sigma(\frac{n_1}{d_1^2}))$$

$$= (p_k^{\alpha_k} + \dots + p_k + 1)(\sum_{d_1^2 | n_1} \mu(d_1)\sigma(\frac{n_1}{d_1^2})) - (p_k^{\alpha_k - 2} + \dots + p_k + 1)(\sum_{d_1^2 | n_1} \mu(d_1)\sigma(\frac{n_1}{d_1^2}))$$

$$= \sum_{d_1^2 | n_1} \mu(d_1)\sigma(\frac{n_1}{d_1^2})\sigma(p_k^{\alpha_k}) + \sum_{d_1^2 | n_1} \mu(d_1)\mu(p_k)\sigma(\frac{n_1}{d_1^2})\sigma(\frac{p_k^{\alpha_k}}{p_k^2})$$

$$= \sum_{d_1^2 | n} \mu(d_1)\sigma(\frac{n}{d_1^2}) + \sum_{p_k^2 d_1^2 | n} \mu(d_1 p_k)\sigma(\frac{n}{p_k^2 d_1^2}) + 0 + \dots + 0$$

$$= \sum_{d^2 | n} \mu(d)\sigma(\frac{n}{d})$$

Note that the last line is because any other square divisor of n, other than d_1^2 and $p_k^2 d_1^2$, is not square free.

Problem 8.

Suppose $(x, m) = 1$. Therefore $(m-x, m) = 1$. And for $m \neq 2$ we know that $x \neq m-x$. Otherwise we would have:

$$x = m - x \implies 2x = m \implies x = \frac{m}{2} \implies x \mid m \implies (x, m) \neq 1$$

Which gives us the contradiction. Therefore for any $m \neq 2$ we can pair all the numbers in $\{c_1, \ldots, c_{\phi(m)}\}$. And sum of all pairs are m since $x + m - x = m$. Therefore $S \overset{m}{\equiv} 0$. For $m = 2$ we have $S = 1$. This concludes the answer.