Number Theory Fall 2024 Problem Set 2
Amin Zolfagharian - 610300118

Problem 1.

We can write x as:

$$x \overset{2}{\equiv} 1 \implies x = 2k+1, k \in \mathbb{Z}$$
$$x \overset{3}{\equiv} 1 \implies 2k+1 \overset{3}{\equiv} 1 \implies 2k \overset{3}{\equiv} 0 \implies k = 3t, t \in \mathbb{Z}$$
$$x = 2k+1 = 2(3t)+1 = 6t+1$$
$$x \overset{7}{\equiv} 2 \implies 6t+1 \overset{7}{\equiv} 2 \implies 6t \overset{7}{\equiv} 1 \implies 36t \overset{7}{\equiv} 6$$
$$\implies t \overset{7}{\equiv} 6 \implies t = 7s+6, s \in \mathbb{Z}$$
$$x = 6t+1 = 6(7s+6)+1 = 42s+37, s \in \mathbb{Z}$$
$$\implies x = 42s+37, s \in \mathbb{Z}$$

Problem 2.

Let $p_1, p_2, \ldots, p_k$ be primes and let x be the answer to this system of equations:

$$x \overset{p_1^2}{\equiv} -1$$
$$x \overset{p_2^2}{\equiv} -2$$
$$\vdots$$
$$x \overset{p_k^2}{\equiv} -k$$

By Chinese remainder theorem there exists such x. It is easy to see that none of $x+1, x+2, \ldots, x+k$ are square free since for any $1 \leq i \leq k$ we have: $x \overset{p_i^2}{\equiv} -i$ which implies $p_i^2 \mid x+i$. Therefore for any k there exists k consecutive number where none of them is square free.

Problem 3.

Let $p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2} \dots, p_{R,1}, p_{R,2}$ be distinct primes with product P. And let x be the answer to the system of equations:

$$x \overset{p_{1,1}}{\equiv} 1$$
$$x \overset{p_{2,1}}{\equiv} 2$$
$$\vdots$$
$$x \overset{p_{R,1}}{\equiv} R$$
$$x \overset{p_{1,2}}{\equiv} -1$$
$$x \overset{p_{2,2}}{\equiv} -2$$
$$\vdots$$
$$x \overset{p_{R,2}}{\equiv} -R$$

By Chinese remainder theorem there exists a unique $x \pmod{P}$. This shows that for any $r \in \mathbb{Z}$, $rP + x$ satisfies the equations above. By Dirichlet's theorem there are infinitely many primes with the form $rP + x$. Let y be one of them. It is easy to see that for any $1 \leq i \leq R$, $p_{i,1} \mid y - i$ and $p_{i,2} \mid y + i$. Thus the only prime number in $[y - R, y + R]$ is y. Therefore there are infinitly many prime numbers like p such that any number in $[p - R, p + R]$ except p is a composite number.

Problem 4.

(i) In $\prod_{i=1}^{\phi(m)}$ product of inverses is 1 mod m. So we are left with the elements like x such that $x^2 \overset{m}{\equiv} 1$. Note that $(x, m) = (m - x, m) = 1$ and also since $(m - x)^2 = m^2 - 2mx + x^2 \overset{m}{\equiv}= 1$. So in remaining elements pair each x with $m - x$. We have $x(m - x) = mx - x^2 \overset{m}{\equiv} -1$. So we only have to answer that how many answers are there to the equation $x^2 \overset{m}{\equiv} 1$. It suffices to see how many answers are there to the equation $x^2 \overset{p_i^{\alpha_i}}{\equiv} 1$ where $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. For any odd prime p_i we have:

$$x^2 \overset{p}{\equiv} 1 \implies x = 1, p - 1$$

By Hensel's lemma we can see that if answers to $x^2 - 1 \overset{p^{\alpha-1}}{\equiv} 0$ are 1 and $p^{\alpha-1} - 1$, Since $p \nmid 2x$, Then answers for $x^2 - 1 \overset{p^{\alpha}}{\equiv} 0$ are $1 + 0$ and $p^{\alpha} - 1$. Which shows that for any p^{α} this equation only has two answers. For $p_i = 2$, we have:

$$x^2 - 1 \overset{2}{\equiv} 0 \implies x = 1$$
$$x^2 - 1 \overset{4}{\equiv} 0 \implies x = 1, 3$$
$$x^2 - 1 \overset{8}{\equiv} 0 \implies x = 1, 3, 5, 7$$

And for any other n with $x^2 - 1 \overset{2^n}{\equiv} 0$ we have:

$$2^n \mid (x-1)(x+1) \implies \begin{cases} 2 \mid x+1,\ 2^{n-1} \mid x-1 \\ 2 \mid x-1,\ 2^{n-1} \mid x+1 \end{cases}$$
$$2^{n-1} \mid x-1 \implies x = 2^{n-1}+1 \text{ since } 0 \leq x < 2^n$$
$$2^{n-1} \mid x+1 \implies x = 2^{n-1}-1 \text{ since } 0 \leq x < 2^n$$

This shows that for 2^n with $n > 2$ there are exactly four answers to this equation. Now for any m we just have to multiply the number of answers for each $p_i^{\alpha_i}$. If it is divisible by 4 then $k = 1$ And if not then $k = -1$.

(ii) We just have to find k where $2024^{1403} \overset{100}{\equiv} k$. We know that $\phi(100) = 40$.

$$2024^{1403} \overset{100}{\equiv} 24^{1403} \overset{100}{\equiv} 24^{40\times35+3}$$

And since $2^{40} \overset{100}{\equiv} 1$ we have:

$$(24^{40})^{35}.24^3 \overset{100}{\equiv} 24^3 = 13824 \overset{100}{\equiv} 24$$
$$\implies 2024^{1403} \overset{100}{\equiv} 24$$

Problem 5.

(i) Let $n = (p-1)^{2k+1}$ for some $k \in \mathbb{N}$. It is easy to see that:

$$2^{(p-1)^{2k+1}} \overset{p}{\equiv} (2^{(p-1)})^{(p-1)^{2k}} \overset{p}{\equiv} 1$$
$$\implies (p-1)^{2k+1}2^{(p-1)^{2k+1}} + 1 \overset{p}{\equiv} (p-1)^{2k+1} + 1$$
$$\overset{p}{\equiv} (-1)^{2k+1} + 1 \overset{p}{\equiv} -1 + 1 \overset{p}{\equiv} 0$$
$$\implies p \mid n2^n + 1$$

(ii) Since $(2, n) = 1$ we just have to show that $\phi(n) \mid n!$. First we prove this for $n = p^\alpha$.

$$\phi(p^\alpha) = p^{\alpha-1}(p-1)$$

Since $(p^{\alpha-1}, p-1) = 1$ and $p^{\alpha-1}, p-1 < p^\alpha!$, we have $p^{\alpha-1}(p-1) \mid p^\alpha!$. Now we proceed with induction on number of distinct primes in n. Base case for 1 prime is p^α which is done. Now suppose for any n with N different primes, $\phi(n) \mid n!$. Suppose m is a number with $N+1$ different primes where $m = p_1^{\alpha_1} \dots p_{N+1}^{\alpha_{N+1}}$. We can write $m = km_1$ where $k = p_1^{\alpha_1}$ and m_1 has N primes. By induction hypothesis we know that $\phi(k) \mid k$ and $\phi(m_1) \mid m_1$. And since ϕ is a multiplicative function we have:

$$\phi(m) = \phi(k)\phi(m_1) \mid k!m_1!$$

It only remains to show that $k!m_1! \mid (m_1 k)!$. Since $m_1, k > 1$ we have $m_1 k \geq m_1 + k$ and we know that $k!m_1! \mid (m_1+k)!$ since $\binom{m_1+k}{k}$ is an integer. Therefore we have:

$$\phi(m) \mid k!m_1! \mid (m_1+k)! \mid (m_1 k)! = m!$$

Thus for any $n \in \mathbb{Z}$ we have $\phi(n) \mid n!$. Now we can write $n! = \phi(n)k$:

$$2^{n!} - 1 \overset{n}{\equiv} (2^{\phi(n)})^k - 1 \overset{n}{\equiv} 0$$
$$\implies n \mid 2^{n!} - 1$$

Problem 6.

Suppose number of primes in form of $4k+1$ is finite. And they are all $p_1, p_2, \ldots, p_r$. Let $P = p_1^2 p_2^2 \ldots p_r^2$. $P+4$ is an odd number and is in form of m^2+n^2 where $(n,m) = 1$ since $(P, 4) = 1$. Therefore we know that any divisor of this number is in form of $4k+1$. Then we have $p_i \mid P+4$ for some $1 \le i \le r$.

$$\left.\begin{array}{l} p_i \mid P+4 \\ p_i \mid P \end{array}\right\} \implies p_i \mid 4 \implies p_1 \le 4$$

which is a contradiction since there is no prime in form of $4k+1$ between 1 and 4. This shows that there are infinitely many primes in form of $4k+1$.

Problem 7.

By Wilson's theorem we know that $(p-1)! \overset{p}{\equiv} -1$. This shows that $p \mid (p-1)! + 1$. Now if $(p-1)!+1$ has no other prime factor, then we would have $p^\alpha = (p-1)! + 1$.

$$p^\alpha - 1 = (p-1)!$$
$$(p-1)(p^{\alpha-1} + \cdots + p + 1) = (p-1)!$$
$$p^{\alpha-1} + \cdots + p + 1 = (p-2)!$$

But we know that for any composite n we have: $n \mid (n-1)!$. And since $p-1$ is not a prime then we have: $p-1 \mid (p-2)!$. Thus:

$$p - 1 \mid (p-2)! = p^{\alpha-1} + \cdots + p + 1$$
$$p^{\alpha-1} + \cdots + p + 1 \overset{p-1}{\equiv} 1^{\alpha-1} + \cdots + 1 + 1 \overset{p-1}{\equiv} \alpha$$

And since $\alpha > 1$ then we have $p - 1 \mid \alpha \implies \alpha \ge p-1$. Now we can see that $p^\alpha = (p-1)! + 1$ is not possible since:

$$p^\alpha \ge p^{p-1} = p \times p \times \cdots \times p > (p-1) \times (p-2) \times \cdots \times 2 \times 1 = (p-1)!$$

This shows that $p^\alpha > (p-1)!+1$. Which is a contradiction. This means that $(p-1)!+1$ is not in form of p^α and has another prime factor which completes the proof.