MAT4003 Assignment 2

1

Assume $x \in \cup_{X\in C} X$. Then $x \in X$ for some $X \in C$. It follows that $x \in [a]$ for some $a \in S$. By definition of an equivalence class, $x \in S$. On the other hand assume $x \in S$. Then by property 1, $x \sim x$, so $x \in [x] \in C$, whence $x \in \cup_{X\in C} X$. This shows $\cup_{X\in C} X = S$.

To show the second equality, assume that some $x \in X \cap Y$ with $X \neq Y$. Suppose $X = [a], Y = [b]$. Then $x \sim a$ and $x \sim b$. By property 2 $x \sim a \implies a \sim x$. Then $a \sim x \wedge x \sim b \implies a \sim b$ by property 3. Similarly $b \sim a$. Now suppose $y \in X$. Then $y \sim a \wedge a \sim b \implies y \in Y$ by property 3 and the definition of Y. Similarly $y \in Y \implies y \sim b \wedge b \sim a \implies y \in X$, which implies $X = Y$, a contradiction. Therefore $X \cap Y = \emptyset$. $\square$

2

Lemma 1. Suppose $(a, b) = 1$. Then $a, b|c \implies ab|c$.

Proof. Let n be the largest integer s.t. p_n, the n^{th} prime, divides either a, b, or c. By FTA, $a = \prod_{i=1}^n p_i^{\alpha_i}; b = \prod_{i=1}^n p_i^{\beta_i}; c = \prod_{i=1}^n p_i^{\theta_i}$. Then $(a, b) = \prod_{i=1}^n p_i^{\min\{\alpha_i,\beta_i\}} = 1 \implies \min\{\alpha_i, \beta_i\} = 0$ for $1 \leq i \leq n$. Therefore $ab = \prod_{i=1}^n p_i^{\alpha_i+\beta_i} = \prod_{i=1}^n p_i^{\max\{\alpha_i,\beta_i\}}$. Also since both a, b divides c, $(a, c) = \prod_{i=1}^n p_i^{\min\{\alpha_i,\theta_i\}} = a$ and $(b, c) = \prod_{i=1}^n p_i^{\min\{\beta_i,\theta_i\}} = b$. Hence $\alpha_i, \beta_i \leq \theta_i$ for $1 \leq i \leq n$. It follows that $(ab, c) = (\prod_{i=1}^n p_i^{\max\{\alpha_i,\beta_i\}}, \prod_{i=1}^n p_i^{\theta_i}) = \prod_{i=1}^n p_i^{\min\{\max\{\alpha_i,\beta_i\},\theta_i\}} = \prod_{i=1}^n p_i^{\max\{\alpha_i,\beta_i\}} = ab$. Therefore $ab|c$. $\square$

"(a) $\implies$ (b)": We prove by induction on r. $r = 1$ is tautology. Assume $x \equiv y \pmod{m_1} \ldots \pmod{m_k} \implies x \equiv y \pmod{m_1 m_2 \ldots m_k}$. Then $x \equiv y \pmod{m_1} \ldots \pmod{m_k} \pmod{m_{k+1}} \implies x \equiv y \pmod{m_1 m_2 \ldots m_k} \pmod{m_{k+1}} \implies m_1 m_2 \ldots m_k, m_{k+1} | (x - y)$.
Since $m_1, \ldots, m_k$ are all pairwise coprime to m_{k+1}, by FTA $(m_1 m_2 \ldots m_k, m_{k+1}) = 1$. Then $m_1 m_2 \ldots m_k m_{k+1} | (x - y)$ by **Lemma 1**, whence $x \equiv y \pmod{m_1 m_2 \ldots m_{k+1}}$.

"(b) $\implies$ (a)": Proceed by induction on r. $r = 1$ is again tautology. Assume $x \equiv y \pmod{m_1 m_2 \ldots m_k} \implies x \equiv y \pmod{m_1} \pmod{m_2} \ldots \pmod{m_k}$. Then $x \equiv y \pmod{m_1 m_2 \ldots m_{k+1}} \implies m_1 m_2 \ldots m_k m_{k+1} | (x - y)$. Therefore $m_1 m_2 \ldots m_k | (x - y)$. By induction hypothesis $x \equiv y \pmod{m_1} \ldots \pmod{m_k}$. Also $m_{k+1} | (x - y)$. So $x \equiv y \pmod{m_{k+1}}$. This completes the proof. $\square$

3

First note that all primes are either of the form $4k + 1$ or $4k + 3$.

Suppose otherwise. Let $p_1 = 3 < p_2 < \ldots < p_n$ be all the primes of the form $4k+3$. Then $N := 4p_2 \ldots p_n + 3 > p_n$ is not such a prime. But $N \not\equiv 1 \pmod 4$ either. Thus N cannot be a prime. By FTA $N = \prod q_i$, where q_i are primes. We claim $q \not\equiv 3 \pmod 4$ for all N's prime factors q. If $q \equiv 3 \pmod 4$ we argue as follows. If $q = 3$, then $3 | 4p_2 \ldots p_n$. By Lemma (1.14), $3|p_i$ with $2 \le i \le n$, which is impossible. If $q \neq 3$, then $q | N \implies q | 3$, which is also impossible. Therefore $q \not\equiv 3 \pmod 4$, whence $q \equiv 1 \pmod 4$. Then $N = \prod q_i \equiv 1 \pmod 4$. However $N \equiv 3 \pmod 4$ by definition, the desired contradiction. $\square$

4

Use proof by contradiction. Suppose there exists some integer n s.t.

$$1 + \frac{1}{2^1} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{5} + \ldots + \frac{1}{2^k} + \ldots + \frac{1}{n} = m \in \mathbb{N} \tag{1}$$

where $2^k \le n < 2^{k+1}$. Multiplying both sides of (1) by 2^{k-1} yields

$$2^{k-1} + 2^{k-2} + \frac{2^{k-1}}{3} + 2^{k-3} + \frac{2^{k-1}}{5} + \ldots + \frac{1}{2} + \ldots + \frac{2^{k-1}}{n} = 2^{k-1}m.$$

Rearranging,

$$\begin{aligned} -\frac{1}{2} &= (2^{k-1} + 2^{k-2} + \ldots + 2 + 1 - 2^{k-1}m) + 2^{k-1}(\frac{1}{3} + \frac{1}{5} + \frac{1}{6} + \ldots + \frac{1}{n}) \\ &= \frac{N}{1} + \frac{2^{k-1}}{3} + \frac{2^{k-1}}{5} + \frac{2^{k-1}}{6} + \ldots + \frac{2^{k-1}}{n}. \end{aligned}$$

where $N = 2^{k-1} + 2^{k-2} + \ldots + 2 + 1 - 2^{k-1}m$ is an integer. All the following terms $\frac{2^{k-1}}{3}, \frac{2^{k-1}}{5}, \frac{2^{k-1}}{6}, \ldots, \frac{2^{k-1}}{n}$ ($\frac{2^{k-1}}{3}, \frac{2^{k-1}}{5}, \frac{2^{k-1}}{6}, \ldots, \frac{2^{k-1}}{n-1}$ in the case $n = 2^k$) can be reduced to $\frac{2^p}{d}$ where the denominator d is odd. Therefore their sum will have an odd denominator in reduced form as well, as
$1 \cdot 1 \cdot \cdots \cdot 1 \equiv 1 \pmod 2$. But then $\frac{1}{2} = \frac{a}{b}$, equivalently $b = 2a$, with b odd. This is clearly absurd. $\square$

5

By FTA $n! = p^\alpha \prod_{i=1}^n p_i^{\alpha_i}$ with $p \neq p_i$ for all i. Since $(p, p_i) = 1, (p^u, \prod_{i=1}^n p_i^{\alpha_i}) = 1$. Hence by Euclid's Lemma $p^u | n! \iff p^u | p^\alpha \iff u \le \alpha$. So $v = \max u = \alpha$.

Assume $n = p^{m+\epsilon}$, with $0 < \epsilon < 1$. Rewrite

$$s := \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = \sum_{i=1}^{m} \left[p^{m+\epsilon-i}\right] = \sum_{i=0}^{m-1} \left[p^{\epsilon+i}\right].$$

We need to prove $\alpha = s$. To find α, consider all terms in $n!$ with prime factor p^i :

$$P_i := \{j \cdot p^i : 1 \le j \le n/p^i = p^{m-i+\epsilon}, p \not| \; j\}.$$

$1 \le j \le p^{m-i+\epsilon}$ gives $[p^{m-i+\epsilon}]$ terms. But we need to rule out terms with $p|j$:

$$i = cp \le p^{m-i+\epsilon} \iff c \le p^{m-i-1+\epsilon} \iff c = 1, 2, \ldots, [p^{m-i-1+\epsilon}].$$

Thus $|P_i| = [p^{m-i+\epsilon}] - [p^{m-i-1+\epsilon}]$. Multiplying all the terms in P_i contribute

$$E_i := i([p^{m-i+\epsilon}] - [p^{m-i-1+\epsilon}])$$

to the exponent α. Adding up E_i for $1 \le i \le m$, we obtain

$$\begin{aligned}\alpha &= \sum_{i=1}^{m} E_i \\ &= \sum_{i=1}^{m} i([p^{m-i+\epsilon}] - [p^{m-i+\epsilon-1}]) \\ &= m[p^{\epsilon+m-1}] - \sum_{i=1}^{m-1} i([p^{\epsilon+i}] - [p^{\epsilon+i-1}]) \\ &= m[p^{\epsilon+m-1}] + \sum_{i=0}^{m-2}[p^{\epsilon+i}] - (m-1)[p^{\epsilon+m-1}] \\ &= \sum_{i=0}^{m-1}[p^{\epsilon+i}] = s. \quad \square\end{aligned}$$

6

By Euler's Theorem, $3^{\phi(100)} = 3^{40} \equiv 1 \pmod{100}$. Therefore $3^{1000} = (3^{40})^{25} \equiv 1^{25} = 1 \pmod{100}$. So the last two digits are 01.

7

The system is equivalent to:

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}.$$

Let $x = 2k+1$. Then $2k+1 = 3t+2$. Thus $2k - 3t = 1$. So $k = 2+3j; t = 1+2j$. It follows that $x = 6j+5$. Then $6j+5 = 5u+3$. So $5u - 6j = 2$, yielding $u = 4+3h; j = 3+5h$. Hence $x = 30h+23$, i.e.,

$$x \equiv 23 \pmod{30}.$$

8

For $m = 1$, there is exactly one solution $x \equiv 0 \pmod 1$.

Assume $m \ge 2$. Let $f(x) := x^2 - x.\, p$ prime. Note that

$$f(0) \equiv f(1) \equiv 0 \pmod p.$$

Also

$$\begin{cases} f'(0) = -1 \\ f'(1) = 1 \end{cases} \not\equiv 0 \pmod p.$$

Applying Hensel's Lemma and induction, solutions $x \equiv 0, 1 \pmod p$ can be uniquely lifted to $x_n \equiv x_1, x_2 \pmod{p^n}$ respectively; in this case, $x_n \equiv 0, 1 \pmod{p^n}$, for all $n \ge 2$. Hence the solutions to the congruence are $x \equiv 0, 1 \pmod{p^n}$ for all $n \in \mathbb{N}$.

Now suppose m has prime factorization $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ with all $\alpha \neq 0$. By CRT solving $f(x) \equiv 0 \pmod{m}$ is equivalent to solving the congruent system

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}} \\ \vdots \\ f(x) \equiv 0 \pmod{p_n^{\alpha_n}} \end{cases}.$$

Based on the previous discussion, the system yields

$$\begin{cases} x \equiv 0, 1 \pmod{p_1^{\alpha_1}} \\ x \equiv 0, 1 \pmod{p_2^{\alpha_2}} \\ \vdots \\ x \equiv 0, 1 \pmod{p_n^{\alpha_n}} \end{cases}.$$

Taking either congruence to 0 or to 1 for each modulo $p_1^{\alpha_1}, \dots, p_n^{\alpha_n}$, we obtain 2^n possible solutions. We claim that these solutions are pairwise incongruent modulo m. For, if $0 \equiv x_1 \not\equiv x_2 \equiv 1 \pmod{p_i^{\alpha_i}}$ for some i, $x_1 \not\equiv x_2 \pmod{m}$ by Lemma (2.6). Therefore,

$$\# \text{ of incongruent solutions} = 2^{\omega(m)}.$$

9

First note that $(a^{-1})^2 \equiv (a^2)^{-1} \pmod{m}$, as

$$a^2 \cdot (a^{-1})^2 = (a \cdot a^{-1})(a \cdot a^{-1}) \equiv 1^2 = 1 \pmod{m}.$$

Since $p \equiv 3 \pmod{4}$, by Theorem (2.14) $x^2 \equiv -1 \pmod{p}$ has no solution. Suppose $x_0^2 \equiv a \pmod{p}$ with $0 < a < p$. Then $y_0^2 \equiv -a \pmod{p}$. It follows that $y_0^2 a^{-1} \equiv y_0^2 (x_0^2)^{-1} \equiv y_0^2 (x_0^{-1})^2 = (y_0 x_0^{-1})^2 \equiv -1 \pmod{p}$. A contradiction. Therefore $x_0^2 \equiv y_0^2 \equiv 0 \pmod{p}$. Since $a^2 \neq p$ for all $0 \leq a < p$, it follows that $x_0 \equiv 0 \pmod{p}$. Similarly $y_0 \equiv 0 \pmod{p}$. $\square$

10

Assume $p, p+2$ both prime greater than 2. Then by Wilson's Theorem,

$$\begin{aligned} (p-1)! &\equiv -1 \pmod{p}; \\ (p+1)! &\equiv -1 \pmod{p+2}. \end{aligned}$$

Note that $(p+1)^{-1} \equiv -1, p^{-1} \equiv (-2)^{-1}$. Therefore

$$\begin{aligned} 4((p-1)!+1) + p &\equiv 0 \pmod{p}; \\ 4((p-1)!+1) + p &\equiv 4(-2)^{-1} + 2 \equiv -2 + 2 \equiv 0 \pmod{p+2}. \end{aligned}$$

Since $(p, p+2) = 1$, by Lemma (2.6)

$$4((p-1)!+1) + p \equiv 0 \pmod{p(p+2)}.$$

Conversely, assume $n > 1$ is odd. And

$$4((n-1)!+1) + n \equiv 0 \pmod{n(n+2)}.$$

Since $(n, n+2) = (n, 2) = 1$, again by Lemma (2.6)

$$4((n-1)!+1)+n \equiv 0 \pmod{n};$$
$$4((n-1)!+1)+n \equiv 0 \pmod{n+2}.$$

Hence

$$(n-1)!+1 \equiv 0 \pmod{n};$$
$$2(n-1)!+1 \equiv 2(n+1)!+2 \equiv (n+1)!+1 \equiv 0 \pmod{n+2}.$$

By Theorem (2.13), n and $n+2$ are both primes. $\square$