Proofs of the Exercises in Chapter 1

Vincent Tran

June 14, 2022

Exercise 1. *Proof.* Let $a, b, c, d, e, f \in \mathbb{Z}$ and $x, y, z \in \mathbb{Z}/m$ such that $(b, m) = (d, m) = (f, m) = 1$ and $xb \equiv a, yd \equiv c, zf \equiv e \pmod{m}$. Then we can show that $\frac{a}{b} + \frac{c}{d} = \frac{e}{f} \implies x + y \equiv z$:

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{e}{f} \\ adf + cbf &= ebd \\ xbdf + ybdf &\equiv zbdf \\ x + y &\equiv z \end{aligned}$$

Furthermore, if $\frac{ac}{bd} = \frac{e}{f}$ for possibly different e, f, then $xy \equiv z$ for possible different z:

$$\begin{aligned} \frac{ac}{bd} &= \frac{e}{f} \\ acf &= bed \\ xbydf &\equiv bzfd \\ xy &\equiv z \end{aligned}$$

□

Exercise 2. *Proof.* Consider the sequence $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \cdots \frac{1}{p-1}$. We can show that no two elements in this series are equivalent mod odd p. FTOC suppose there are two integers a, b such that $\frac{1}{a} \equiv \frac{1}{b}$, let this be equal to x. Then $ax \equiv 1 \equiv bx$. Since p is prime, all integers in $[1, p-1]$ are relatively prime to p. Thus $ax \equiv bx \implies a \equiv b$, which is impossible since $a \neq b$ and $a + pk > p - 1$ for $k \in \mathbb{N}$ as $a \geq 1$. Thus every fraction is uniquely equivalent to an element in $\mathbb{Z}/p$.

Thus the sum of all the elements in this series is just $1+2+3+4+\cdots+p-1$ as every element of $\mathbb{Z}/p$ must be in this series (there are $p-1$ elements in $\mathbb{Z}/p$ and $p-1$ unique elements in the sequence). Thus the sum is just $(p-1)(p)/2 \equiv 0$. □

Exercise 3. *Proof.* By the hypothesis, $x^4+y^4 = x^7y+1 \equiv 0 \pmod{x^4+y^4}$. Thus $y \equiv \frac{-1}{x^7} \implies x^4 + (\frac{-1}{x^7})^4 = \frac{x^{32}+1}{x^{28}} \equiv 0 \implies x^{32}+1 \equiv 0$. ☐

Exercise 4. *Proof.* Let $(a, m) = d$. Thus $a = dk$ for some $k \in \mathbb{Z}$ such that $(k, m) = 1$. Thus we have it that $dkx \equiv b$. Thus $dkx = b + mj$ for some $j \in \mathbb{Z}$. Since $d \mid m$, $d \mid b$. Then we can show that if $d \mid b, \exists x$. We can show that $x \equiv k^{-1}(e + fj)$ where $ed = b$ and $fd = m$ is a solution: $ax \equiv dkk^{-1}(e + fj) \equiv de + dfj \equiv b + mj \equiv b$. Thus $\exists x$ iff $d|b$. ☐

Exercise 5. *Proof.* Let $x = 3a + r_1 = 4b + r_2 = 5c + r_3$ for some $a, b, c \in \mathbb{Z}$. Then $3a+r_1 \equiv r_2 \pmod 4$. Thus $3a \equiv r_2 - r_1 \implies a \equiv 3r_2 - 3r_1 \equiv 3r_2 + r_1$. Therefore $a = 3r_2 + r_1 + 4d$ for some integer d. Substituting into x, we get $x = 9r_2 + 3r_1 + 12d$. We can repeat this with $x = 5c + r_3$ to get the result. ☐

Exercise 6. *Proof.* The verify part is just back-of-the-napkin math, so I'll leave it out of this. Then we do some algebra:

$$\begin{aligned} 10\text{ind } 2 + 60\text{ind } y &\equiv 70\text{ind } 14 \pmod{19} \\ 1 + 6\text{ind } y &\equiv 7 \cdot 7 \\ 6\text{ind } y &\equiv 48 \\ \text{ind } y &\equiv 8 \\ y &\equiv 9 \end{aligned}$$

☐

Exercise 7. *Proof.*

$$\text{ind } y = [t_0, t_1, t_2] \implies \text{ind } y^2 = [2t_0, 2t_1, 2t_2]$$

Thus $y^2 \equiv 2^{2t_2} \equiv 1 \pmod 3$ and $y^2 \equiv (-1)^{2t_0}5^{2t_1} \equiv 1 \pmod 8$. Thus $y^2 \equiv 1$. ☐

Exercise 8. *Proof.* Let $\text{ind } y = [t_0, t_1, t_2, \cdots, t_s]$. Thus $\text{ind } y^4 = [4t_0, \cdots, 4t_s]$. For a non-trivial solution, $4t_i \equiv 0 \pmod{\phi(p_i^{a_i})}$. Since t_i varies, the only way for this to occur is for $\phi(p_i^{a_i})|4 \implies \phi(p_i^{a_i}) = 1, 2, 4$. Testing small p_i and a_i reveals that this is only the case when $p_i = 3, 5, 4, 8, 16$ (trivial to see that it can't be greater). ☐