

Problem 1 (8 pts).

- (a) Let $g = \gcd(a_1, a_2, \dots, a_n)$, $h = \gcd(\gcd(a_1, a_2, \dots, a_{n-1}), a_n)$.
As $g|a_i$ for $1 \leq i \leq n$. It implies that $g|\gcd(a_1, a_2, \dots, a_{n-1})$ and $g|a_n$. We have
 $g|\gcd(\gcd(a_1, a_2, \dots, a_{n-1}), a_n)$ and therefore $g \leq h$.

As $h|\gcd(a_1, a_2, \dots, a_{n-1})$ and $h|a_n$, we can conclude $h|a_i$ for $1 \leq i \leq n$. Therefore we
can conclude $h|\gcd(a_1, a_2, \dots, a_n)$ and thus $h \leq g$.

Combining, we have $g = h$.

- (b) First, note that $10 \equiv -1 \pmod{11}$, and $100 \equiv 1 \pmod{11}$. We observe that $10^{2k+1} \equiv -1 \pmod{11}$
and $10^{2k} \equiv 1 \pmod{11}$. Let $N = \sum_{i=0}^k 10^i d_i$ so that k is the largest integer
satisfying $10^k \leq N$. So $N \equiv \sum_{i=0}^k 10^i d_i \pmod{11}$. We set $d_{k+1} = 0$ if k is even. It follows
that we can rewrite the previous modulo equation as

$$N \equiv \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} (d_{2i} - d_{2i+1}) \pmod{11}$$

the right hand side shows the difference of sum of odd digits and even digits and the proof
completes.

- (c) Since $\gcd(n, 7) = 1$ and 7 is a prime number, by Fermat's little theorem, $n^6 \equiv 1 \pmod{7}$.
Hence we know that $n^{12} \equiv 1 \pmod{7}$ using multiplication rule. By repeating the process we
can say $n^{6k} \equiv 1 \pmod{7}$ and therefore $n^{6k} - 1 \equiv 0 \pmod{7}$.
- (d) It simply asks about $\text{spc}(123, 567)$. Since $\gcd(123, 567) = \text{spc}(123, 567)$,

$$\begin{aligned} 567 &= 4 \times 123 + 75 \\ 123 &= 1 \times 75 + 48 \\ 75 &= 1 \times 48 + 27 \\ 48 &= 1 \times 27 + 21 \\ 27 &= 1 \times 21 + 6 \\ 21 &= 3 \times 6 + 3 \\ 6 &= 3 \times 2 + 0 \end{aligned}$$

and we have the shortest positive difference equal to 3. To realize how we can achieve such

difference, we use extended Euclid's algorithm from what we obtained above. Thus we have

$$\begin{aligned} 75 &= 567 - 4 \times 123 \\ 48 &= 123 - 1 \times 75 = 5 \times 123 - 567 \\ 27 &= 75 - 1 \times 48 = 2 \times 567 - 9 \times 123 \\ 21 &= 48 - 1 \times 27 = 14 \times 123 - 3 \times 567 \\ 6 &= 27 - 1 \times 21 = 5 \times 567 - 23 \times 123 \\ 3 &= 21 - 3 \times 6 = 83 \times 123 - 18 \times 567 \end{aligned}$$

By gluing 83 sticks with length 123 and 18 sticks with length 567, we can achieve the required value. (*We accept any valid solution if you use extended Euclid's algorithm and yield such valid solution.*)

Problem 2 (6 pts). *We accept any assumption that help you in solving the subproblems if it does not contradict to the original problem statement.*

- (a) The required answer is the total current value of the payments. Let V be the loan, x be the annual payment and b be the bankrate. Denote $r = \frac{1}{b}$. We have $V = \sum_{i=1}^{25} x \times \frac{1}{b^i} = \sum_{i=1}^{25} x \times r^i = xr \times \frac{1 - r^{25}}{1 - r}$. We get x by calculating $\frac{V}{r} \times \frac{1 - r}{1 - r^{25}}$. As $V = 2,110,000 \times 60\% = 1,266,000$ and $r = \frac{1}{1.07}$, we have $x \approx \$108,636$.
- (b) It asks the future value of the flat after 25 years. Please note that this time $b = \sqrt{1.12} \approx 1.0583$. So the required answer is $2,110,000 \times 1.0583^{25} \approx \$8,699,769$.
- (c) For the 40% downpayment, it contributes to $2,110,000 \times 40\% \times 1.1^{25} \approx \$9,144,492$. By renting he can actually save $108636 - 100000 = \$8,636$. So if he also puts this saving into stock market annually, he can get $\sum_{i=0}^{24} 8636 \times 1.1^i = 8636 \times \frac{1 - 1.1^{25}}{1 - 1.1} \approx \$849,325$.
- If Leo accepts Tom's suggestion, his wealth will be $\$8,699,769$ after 25 years.
 If Leo accepts Jesse's suggestion, his wealth will be $9144492 + 849325 = \$9,993,817$ after 25 years.
 It turns out that renting the flat gives Leo more wealth after 25 years. Jesse's option is better.

Problem 3 (5 pts).

- (a) (i) We have $v = cu$ for some positive integer c . By quotient-remainder theorem, $x = (cu)d + r$ for some non-negative integer d and r . It follows that $x \bmod v = r$. For $x \bmod u$, we have $r \bmod u$ because $u \mid (cu)d$. So it follows that $(x \bmod v) \bmod u = r \bmod u = x \bmod u$ and the proof completes.
- (ii) If $x \equiv y \pmod{v}$, we can say $x = vp + r$ and $y = vq + r$ for some non-negative integers p, q, r . Again we can express x and y as $x = (cu)p + r$ and $y = (cu)q + r$. And then we can conclude $x \equiv r \pmod{u}$ and $y \equiv r \pmod{u}$. It follows that $x \equiv y \pmod{u}$.
- (b) By (a)(i), we know that $x \bmod m_i = (x \bmod m) \bmod m_i$ for any integer x . So:
- (i) $(u + v) \bmod m_i = ((u + v) \bmod m) \bmod m_i$ for $1 \leq i \leq k$. Since $(u + v) \bmod m_i = (u_i + v_i) \bmod m_i$, we have $(u_i + v_i) \bmod m_i = ((u + v) \bmod m) \bmod m_i$ for $1 \leq i \leq k$. By the definition of relation \sim , we can immediately conclude $(u + v) \bmod m \sim ((u_1 + v_1) \bmod m_1, (u_2 + v_2) \bmod m_2, \dots, (u_k + v_k) \bmod m_k)$.
- (ii) By putting $x = uv$ and since $uv \bmod m_i = (u \bmod m_i)(v \bmod m_i) \bmod m_i = u_i v_i \bmod m_i$, it is similar to (b)(i) and the result follows.
- (c) It is trivial that $0 \sim (0, 0, \dots, 0)$ and $1 \sim (1, 1, \dots, 1)$. Note that $b \sim (b \bmod m_1, b \bmod m_2, \dots, b \bmod m_k)$ actually implies $y \equiv b \pmod{m_i} \iff y \equiv b \pmod{m}$. The problem remains is to show whether $b \sim (b \bmod m_1, b \bmod m_2, \dots, b \bmod m_k)$ always exists for any integer b . We can use (b)(i) to show that $(1 + 1) \bmod m \sim ((1 + 1) \bmod m_1, (1 + 1) \bmod m_2, \dots, (1 + 1) \bmod m_k) \iff 2 \bmod m \sim (2 \bmod m_1, 2 \bmod m_2, \dots, 2 \bmod m_k)$. Then we use this with $1 \sim (1, 1, \dots, 1)$ to conclude $3 \bmod m \sim (3 \bmod m_1, 3 \bmod m_2, \dots, 3 \bmod m_k)$ by using (b)(i) again. By repeatedly using (b)(i) or using induction, $b \sim (b \bmod m_1, b \bmod m_2, \dots, b \bmod m_k)$ always exists and hence the proof completes.

Problem 4 (6 pts).

- (a) Notice $n \equiv c \pmod{p}$ and $n \equiv 55 \times a + 66 \times b + 45 \times c \pmod{15p}$. By reduction on the result of Chinese remainder theorem, we have $n \equiv 55 \times a + 66 \times b + 45 \times c \pmod{p}$. Using modular arithmetic property, we can conclude $55 \times a + 66 \times b + 44 \times c \equiv 0 \pmod{p}$. The smallest p is therefore 11.

Alternative

$N_1 N_1^{-1} = 55 = 5 \times 11$, $N_2 N_2^{-1} = 66 = 3 \times 2 \times 11$. Candidate p can be 2 or 11. Suppose p is 2, $N_1 = 10$, but N_1^{-1} is not an integer. Suppose p is 11, $N_1 = 55$, hence $N_1^{-1} = 1$ and $N_1 N_1^{-1} \equiv 1 \pmod{3}$. $N_2 = 33$, hence $N_2^{-1} = 2$ and $N_2 N_2^{-1} \equiv 1 \pmod{5}$. Therefore $p = 11$ is the smallest valid solution.

- (b) (i) Since $M < N_i$ for $1 \leq i \leq 3$, $M^3 < N_1 N_2 N_3$. By setting up the following modulo equations

$$M^3 \equiv C_1 \pmod{N_1}$$

$$M^3 \equiv C_2 \pmod{N_2}$$

$$M^3 \equiv C_3 \pmod{N_3}$$

where C_1, C_2, C_3 are the three encrypted midterm papers, we can use Chinese remainder theorem to solve for M^3 . And since $M^3 < N_1 N_2 N_3$, we don't need to adjust M^3 . By directly taking the cube root of M^3 , the original midterm paper is recovered.

- (ii) Substituting the variables, we have

$$M^3 \equiv 143 \pmod{187}$$

$$M^3 \equiv 84 \pmod{355}$$

$$M^3 \equiv 134 \pmod{265}$$

In this case, $\gcd(355, 265) = 5$ and we have to reduce the modulo equations into

$$M^3 \equiv 143 \pmod{187}$$

$$M^3 \equiv 13 \pmod{71}$$

$$M^3 \equiv 28 \pmod{53}$$

$$M^3 \equiv 4 \pmod{5}$$

Step 1: $N = 187 \times 71 \times 53 \times 5 = 3518405$

Step 2: $N_1 = 18815$, $N_2 = 49555$, $N_3 = 66385$, $N_4 = 703681$

Step 3: $1308 \times 187 - 13 \times 18815 = 1 \implies N_1^{-1} = 187 - 13 = 174$

$16751 \times 71 - 24 \times 49555 = 1 \implies N_2^{-1} = 71 - 24 = 47$

$11 \times 66385 - 13778 \times 53 = 1 \implies N_3^{-1} = 11$

$703681 - 140736 \times 5 = 1 \implies N_4^{-1} = 1$

Step 4: $M^3 = (143 \times 18815 \times 174 + 13 \times 49555 \times 47 + 28 \times 66385 \times 11 + 4 \times 703681 \times 1) \pmod{3518405} = 970299$

Therefore, $M = \sqrt[3]{M^3} = 99$