

This homework contains 25 points. You are encouraged to collaborate on the homework, but you must write your own solutions and list your collaborators on your solution sheet (you will not lose any mark by doing this). Please drop your submissions into the dropbox near SHB 924.

Problem 1 (8 pts). Solve the following problems.

- (a) (2 pts.) Define $\gcd(a_1, a_2, \dots, a_n)$ as the GCD of a_1, a_2, \dots, a_n . Show that $\gcd(a_1, a_2, \dots, a_n) = \gcd(\gcd(a_1, a_2, \dots, a_{n-1}), a_n)$.
- (b) (2 pts.) Prove that any positive integer N is divisible by 11 if and only if the difference between the sum of odd digits and the sum of even digits is divisible by 11.
- (c) (2 pts.) Prove that for any integer n , $n^{6k} - 1$ is divisible by 7 if $\gcd(n, 7) = 1$ and k is a positive integer.
- (d) (2 pts.) Given two sticks with length 123 and 567. You can always glue the sticks of the same kind. Find the smallest positive difference by choosing suitable sticks. Also explain how to achieve that value. Show your steps clearly.

Problem 2 (6 pts). Leo is going to buy a flat whose price is \$2,110,000. The bankrate is 1.07. Tom suggests Leo borrow 60% of loan to buy the flat and the repay the loan in 25 years. Assume payments and rates are considered annually, and payments are made at the end of each year.

- (a) (2 pts.) How much should Leo pay annually so as to repay the loan in 25 years?

Jesse shows up and disagrees with Tom's suggestion. He predicts that the value of the flat raise by 12% every two years. So he recommends Leo to rent the flat \$100,000 per year, and save the money (both annual saving and 40% downpayment) through renting the flat, instead of buying it. He also suggests Leo doing investment in stock market using saved money to get 10% annual return.

- (b) (1 pt.) Calculate the value of the flat after 25 years.
- (c) (3 pts.) Hence, help Leo to decide whether the option of Tom or Jesse is better by considering his wealth after 25 years. Assume that the bankrate remains unchanged and Jesse's prediction is correct.

Problem 3 (5 pts). Jesse studied hard in Chinese remainder theorem. He found a nice pattern when he calculated $y \equiv b \pmod{65}$. Refer to the following table.

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	40	15	55	30	5	45	20	60	35	10	50	25
1	26	1	41	16	56	31	6	46	21	61	36	11	51
2	52	27	2	42	17	57	32	7	47	22	62	37	12
3	13	53	28	3	43	18	58	33	8	48	23	63	38
4	39	14	54	29	4	44	19	59	34	9	49	24	64

He wrote 0 at the top left corner of the table, incremented the value by 1 and put the new entries diagonally. By wrapping horizontally and vertically, he can construct the solutions of Chinese remainder theorem, modulo 65. For example, by looking at the third row and fourth column, the entry 42 is the solution of

$$\begin{aligned} b &\equiv 2 \pmod{5} \\ b &\equiv 3 \pmod{13} \end{aligned}$$

Please help Jesse to prove the followings. Let $m = m_1 m_2 \cdots m_k$, for any pair m_i, m_j so that $i \neq j$, we have $\gcd(m_i, m_j) = 1$. Let u be an integer so that $0 \leq u < m$, denote the relations $u_i = u \pmod{m_i}$ where $0 \leq u_i < m_i$ as

$$u \sim (u_1, u_2, \dots, u_k)$$

- (a) (2 pt.) Let u, v be any integers. Show that if $v > 0$ and u divides v , then
- (i) for any integer x , $(x \pmod{v}) \pmod{u} = x \pmod{u}$.
 - (ii) for any integers x and y , $x \equiv y \pmod{v} \implies x \equiv y \pmod{u}$.
- (b) (2 pts.) Suppose we have $u \sim (u_1, u_2, \dots, u_k)$ and $v \sim (v_1, v_2, \dots, v_k)$. Prove the followings:
- (i) $(u + v) \pmod{m} \sim ((u_1 + v_1) \pmod{m_1}, (u_2 + v_2) \pmod{m_2}, \dots, (u_k + v_k) \pmod{m_k})$
 - (ii) $(uv) \pmod{m} \sim (u_1 v_1 \pmod{m_1}, u_2 v_2 \pmod{m_2}, \dots, u_k v_k \pmod{m_k})$
- (c) (1 pt.) Hence, prove that, for all integers y, b ,

$$y \equiv b \pmod{m_i}$$

for $i = 1, 2, \dots, k$ if and only if

$$y \equiv b \pmod{m}$$

Problem 4 (6 pts).

(a) (2 pts.) Let n be an integer satisfying

$$n \equiv a \pmod{3}$$

$$n \equiv b \pmod{5}$$

$$n \equiv c \pmod{p}$$

where p is a prime number. If, by using Chinese remainder theorem, we have $n \equiv 55 \times a + 66 \times b + 45 \times c \pmod{15p}$ while $p, 3$ and 5 are pairwise relatively prime, what is the smallest possible p ?

(b) It is known that even if we do not know how to do factorization efficiently, RSA could still be insecure if we do not implement it carefully. Consider the following scenario.

Suppose Leo, Tom and Hackson wants to speed up encryption, they choose $e = 3$ for their public keys. Let them be $(N_1, 3)$, $(N_2, 3)$ and $(N_3, 3)$ respectively. Then they published the keys on their personal homepage. Now Lap Chi wants to give them his encrypted midterm paper of CSC2110 separately, using their public keys on the web. He verifies that no pairs of the keys are identical. Then he posts these three encrypted messages on his personal homepage. But Jesse discovers that it is insecure. He collects the public keys from the homepage of Leo, Tom and Hackson and their corresponding encrypted midterm papers from Lap Chi's homepage. He shows to Lap Chi how he successfully recovers the original midterm paper in a second and therefore Lap Chi needs to re-propose another set of midterm paper.

(i) (3 pts.) Explain why Jesse can efficiently recover the encrypted midterm paper.

(ii) (1 pt.) Let the original message be M . Assume $M < N_i$ for $i \in \{1, 2, 3\}$. The table below shows what Jesse has on his hand:

Names	Public keys (N_i, e_i)	Encrypted message
Tom	$(187, 3)$	143
Leo	$(355, 3)$	84
Hackson	$(265, 3)$	134

Show that how you can recover the original message using the method you have described in previous part.