1 Short Question

Q 1. Find $GCD(564, 978)$.

Q 2. Find $GCD(72, 184, 300)$.

Q 3. Find $SPC(364, 516)$ and values of $s, t$ in $364s + 516t$ that achieve the $SPC$.

Q 4. Show how to get 75 gallons of water by using 327 and 564 gallon jugs. Please reduce number of rounds of transferring water.

Q 5. It is now 16 : 24 on Monday. Find the time and the day of the week after 98714 minutes.

Q 6. Use: (i) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$ (ii) $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$ to prove:

$$a \equiv b \pmod{n} \text{ and } c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}.$$ 

Q 7. Calculate $9865^{67} \pmod{38}$ by repeated squaring.

Q 8. Calculate multiplicative inverse of 47981 (mod 95963) (hint: $GCD(47981, 95963) = 1$).

Q 9. Express $3 + 3 \cdot 3^3 + 5 \cdot 3^5 + 7 \cdot 3^7 + ... + (2n - 1) \cdot 3^{2n-1}$ in closed form.

Q 10. Express $(2n + 2) \cdot 10^{-n-1} + (2n + 4) \cdot 10^{-n-2} + (2n + 6) \cdot 10^{-n-3} + (2n + 8) \cdot 10^{-n-4} + ...$ in closed form and calculate it for $n = 5$.

Q 11. Use Integral Method to find upper and lower bounds of $\sum_{i=1}^{n} i^3$.

2 Long Question

Q 12. (a) Calculate $x^i \pmod{n}$ for $i = 1 \text{ to } 7, \ n = 7, \ x = 978$

(b) Calculate $x^i \pmod{n}$ for $i = 1 \text{ to } 7, \ n = 7, \ x = 675$

(c) State Fermat’s Little Theorem. Do results of (a) and (b) obey the theorem?

Q 13. Under Turing’s Code (Version 1.0), given key $k = 29$:

(a) Encrypt the message $m_1 = 439$

(b) Encrypt the message $m_2 = 881$

(c) A guy gets the encrypted message $km_1, km_2$ in previous parts, can he get the correct key? (show the calculation)

Q 14. Under Turing’s Code (Version 2.0), given prime $p = 79$ and key $k = 32$:

(a) Encrypt the message $m = 65$

(b) Compute multiplicative inverse of $m \pmod{p}$

(c) Show how to perform plain-text attack if $mk, m$ and $p$ are known.

Q 15. Under RSA, given $p = 13, q = 37$:

(a) Calculate $n = pq, T = (p - 1)(q - 1)$

(b) Given $e = 35$, calculate $d = e^{-1} \pmod{T}$

(c) Encrypt the message $m = 37$ into $m'$

(d) Decrypt the message $m'$ in (c)

Q 16. Explain why a number written in decimal is divisible by 11 if and only if the sum of its odd digits minus the sum of its even digits is a multiple of 11 (Hint $10 \equiv -1 \pmod{11}$).

Q 17. Refer to Problem 9.10.7 in lecture notes of MIT.
Q 18. Given the price of a flat is $2,000,000, interest rate is 12%, loan period is 20 years, inflation rate is 6%, payment and rates are considered annually, suppose John wants to borrow 70% of loan to buy the flat:

(a) What is the annual payment?

(b) What’s the value of flat after 20 years?

(c) Suppose John can rent the flat for $180,000 annually, and there are always investment opportunites in the stock market that gives 12% annual return. How much properties will John have if he rent the flat and invet the money saved in the stock market?

Q 19. Suppose you deposit $20000 into bank account, $19000 next year from now, $18000 in two years from now and so on. Given annual interest rate is 5%:

(a) Write down the summation formula for total amount after nth deposit.

(b) Express the formula of (a) in closed form. (Hint: \( \sum_{i=1}^{n} ix^i = (x - (n + 1)x^{n+1} + nx^{n+2})/(1 - x)^2 \))

(c) How much money will you get after 10 years?