Math Test 1 Notes

🎓 Gauss's Sum Formula

Sum from 1 to n:
Formula:

$$Sum = n(n+1)2\text{Sum} = \frac{n(n+1)}{2}$$

Example:

$$1 + 2 + ... + 300 = 300 \times 3012 = 45,150 1 + 2 + ... + 300 = \frac{300 \times 301}{2} = 45,150$$

To sum from a to b:

$$b(b+1)2 - (a-1)a2 \frac{b(b+1)}{2} - \frac{(a-1)a}{2}$$

✨ Set Formulas

1. **Union:**

$$n(A \cup B) = n(A) + n(B) - n(A \cap B) n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

2. **Disjoint Sets:**

$$A \cap B = \emptyset \Rightarrow n(A \cup B) = n(A) + n(B) A \cap B = \emptyset \Rightarrow n(A \cup B) = n(A) + n(B)$$

3. **Three Sets (Inclusion-Exclusion):**

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C) n(A \cup B$$

4. **Intersection via Union:**

$$n(A \cap B) = n(A) + n(B) - n(A \cup B) n(A \cap B) = n(A) + n(B) - n(A \cup B)$$

5. **Union via Differences:**

$$n(A \cup B) = n(A - B) + n(B - A) + n(A \cap B) n(A \cup B) = n(A - B) + n(B - A) + n(A \cap B)$$

Subsets:

- A set with n elements has 2n2^n subsets (including ∅\emptyset).
- Example:

$$A = w, y \Rightarrow \emptyset, w, y, w, yA = \{w, y\} \Rightarrow \emptyset, \{w\}, \{y\}, \{w, y\}$$

🤔 Finding Factors

Example: 63

1. Start with 1 and 63.
2. Test integers up to

$$63 \approx 7.9\sqrt{63} \approx 7.9$$

3. Factor pairs: (1,63), (3,21), (7,9)
   All factors: 1, 3, 7, 9, 21, 63

✔️ Divisibility Rules

Number	Rule
2	Last digit is even
3	Sum of digits divisible by 3
4	Last two digits form number divisible by 4
5	Ends in 0 or 5
6	Divisible by 2 **and** 3
8	Last 3 digits form number divisible by 8
9	Sum of digits divisible by 9
10	Ends in 0
12	Divisible by 3 **and** 4

Consecutive Primes: Only 2 and 3 are consecutive.

🔢 LCM and GCF

LCM (Least Common Multiple):

1. Prime factor both numbers
2. Use **highest powers** of all primes

**Example:

$$96 = 2^5 \times 3 \qquad 60 = 2^2 \times 3 \times 5$$

$$LCM = 2^5 \times 3 \times 5 \qquad = 480$$

GCF (Greatest Common Factor):

1. Prime factor both numbers
2. Use **lowest powers** of common primes

**Example:

$$260 = 2^2 \times 5 \times 13 \qquad 156 = 2^2 \times 3 \times 13$$

$$GCF = 2^2 \times 13 = 52$$

🛡️ Diffie-Hellman-Merkle Key Exchange

Given: M = 77, n = 99, a = 55, b = 66

$$A = M^a mod n = 77^{55} mod 99$$

$$B = M^b mod n = 77^{66} mod 99$$

$$Key K = B^a mod n = A^b mod n$$

🔐 RSA Encryption & Decryption

$$C = M^e (mod\, n)$$

To compute the ciphertext `C` use:

$$C = M^e (mod\, n)$$

Given:

$$M = 89$$

$$n = 91 \quad (modulus)$$
$$e = 11$$

Step-by-step calculation:

$$Rewrite \quad 89^{1}1 \quad as \quad 89^{1}0 \times 89$$
$$Compute \quad 89 \equiv -2 (mod\, 91) \qquad = (-2)^{10} \qquad = 1024$$
$$Multiply \quad 1024 \times 89 (mod\, 91)$$
$$Compute \quad 1024 (mod\, 91) \equiv 2$$
$$2 \times 89 = 178 (mod\, 91) \qquad \equiv 45$$
$$result: \quad C = 45$$

The encrypted message is **45**.

Given: p = 17, q = 5, e = 19, C = 65 find the smallest natural number for the decryption exponent and the message M

$$M = C^{d} (mod\, n)$$

To get the decryption exponent

Calculate the Modulus

$$n = pq = 85$$
$$l = (p-1)(q-1) \qquad = 16 \times 4 = 64$$

Find d:

$$d = \frac{lx+1}{e}$$
$$d = \frac{64x+1}{119}$$

Try many numbers, start from 1 and go up until whole number:

$$x = 8: \qquad d = \frac{64(8)+1}{119} \qquad = 27$$

The smallest natural number for the decryption exponent **d** is: 27

Decrypt: for M

$$M = C^{d} mod\ n \qquad = 65^{27} mod\ 85$$

Use exponentiation by squaring:

Binary of 27: 11011 → 1 + 2 + 8 + 16

$$65^1 mod\ 85 \quad \equiv 65\ mod\ 85 \quad which\ is\ just \quad \equiv 65$$

$$65^2\ mod\ 85 \quad \equiv 8565\ mod\ 85 \quad \equiv 60\ mod\ 85$$

$$65^8\ mod\ 85 \quad \equiv 8565\ mod\ 85 \quad \equiv 50\ mod\ 85$$

$$65^{16} mod\ 85 \quad \equiv \ 8565\ mod\ 85 \quad \equiv 35\ mod\ 85$$

Summary:

$$(65 \times 60 \times 50 \times 35)\ mod\ 85$$

Final:

Reduce mod each time.

$$35{\times}50\ mod\ 85 \quad = 1750\ mod\ \ 85 \quad = 50$$

So the result, 50, goes to multiply the next number

$$50{\times}60 = 3000 mod\ 85 = 2550 \times 60 = 3000 \quad \mathrm{mod}\ \ 85 = 25$$

The result 25 goes to multiply the next number

$$25{\times}65 = 1625 mod\ 85 = 1025 \times 65 = 1625 \quad \mathrm{mod}\ \ 85 = 10$$

Plaintext Message M = 10