**🎓 Gauss's Sum Formula**Gauss's method is designed to **quickly and efficiently calculate the sum of a sequence of consecutive numbers**, especially from **1 to n**, **without having to add each number one by one**.

**🔷 Problem:**  
Find the sum of all whole numbers from 1 to **n**.

**✅ Formula:**  
Sum = n(n + 1) ÷ 2

**🔷 Example:**  
Find the sum from 1 to 300:

Sum = 300 × (300 + 1) ÷ 2  
Sum = 300 × 301 ÷ 2  
Sum = 45,150

**📝 Why it works (in plain language):**

* Pair numbers from opposite ends: (1 + n), (2 + n−1), (3 + n−2), etc.
* Each pair adds to the same total.
* There are n ÷ 2 such pairs (if n is even).

**🧩 Tips to Remember:**

* "n(n + 1) ÷ 2" is your shortcut.
* Works for any sequence starting at 1.
* To sum numbers from **a to b**, use:  
  Sum = [b(b + 1) ÷ 2] − [(a − 1)a ÷ 2]

**Set Formulas**

1. **Union of Two Sets:**  
   n(A ∪ B) = n(A) + n(B) − n(A ∩ B)
2. **Union of Disjoint Sets:**  
   If A ∩ B = ∅, then  
   n(A ∪ B) = n(A) + n(B)
3. **Union of Three Sets (Inclusion-Exclusion Principle):**  
   n(A ∪ B ∪ C) = n(A) + n(B) + n(C) − n(A ∩ B) − n(B ∩ C) − n(A ∩ C) + n(A ∩ B ∩ C)
4. **Intersection of Two Sets (using union):**  
   n(A ∩ B) = n(A) + n(B) − n(A ∪ B)
5. **Union in terms of set differences:**  
   n(A ∪ B) = n(A − B) + n(B − A) + n(A ∩ B)

**The number of subsets of a set with nelements is 2n.**

For any set A, the empty set (∅) is one of its subsets.  
So, when counting the number of subsets, always include the empty set.

**Example:**  
If A = {w, y}, its subsets are:

* ∅
* {w}
* {y}
* {w, y}

That makes a total of 4 subsets, including the empty set.

**How to Find All Natural Number Factors of 63**

1. **Start with 1 and the number itself:**  
   1 and 63 are always factors of 63.
2. **Test each whole number from 2 up to the square root of 63:**
   * The square root of 63 is about 7.94, so test up to 7.
3. **For each number, check if it divides 63 evenly:**
   * If 63 divided by the number gives a whole number (no remainder), both the number and the result are factors.
4. **List all factor pairs:**
   * 1 × 63 = 63
   * 3 × 21 = 63
   * 7 × 9 = 63
5. **Write all unique factors in ascending order:**  
   1, 3, 7, 9, 21, 63

**Divisibility Rules**

**2**  
A number is divisible by 2 if its last digit is even (0, 2, 4, 6, or 8).

**3**  
A number is divisible by 3 if the sum of its digits is divisible by 3.

**4**  
A number is divisible by 4 if the number formed by its last two digits is divisible by 4.

**5**  
A number is divisible by 5 if its last digit is 0 or 5.

**6**  
A number is divisible by 6 if it is divisible by both 2 and 3.

**8**  
A number is divisible by 8 if the number formed by its last three digits is divisible by 8.

**9**  
A number is divisible by 9 if the sum of its digits is divisible by 9.

**10**  
A number is divisible by 10 if its last digit is 0.

**No, it is not divisible by 10 because it ends in 9.**

**12**  
A number is divisible by 12 if it is divisible by both 3 and 4.

What are the two primes that are consecutive natural​ numbers?

2,3

Can there be any other primes that are consecutive natural​ numbers?

No, because every pair of consecutive natural numbers will include at least one even number, and the only even prime is 2.

LCM

Get prime factorization of both numbers

Then get all unique primes and use the higher powers of each

So,

96 and 60

= 2^5 \* 3 and 2^2\*3\*5

LCM = 2^5 \* 3 \* 5

= 480

GCF

Get prime factorization of both numbers

Then get only the common prime factors, lowest powers

So,

260 and 156

2^2\*5\*13 and 2^2\*3\*13

GCF = 2^2\*13 = 52  
  
  
### Diffie-Hellman-Merkle key exchange scheme

Alice - Sender

Bob - Receiver

Find Alice and​ Bob's common key K with the given values of​ M, n,​ a, and b.

| M | n | a | b |

| --- | --- | --- | --- |

| 77 | 99 | 55 | 66 |

A = M^a(mod n)

B = M^b (mod n)

A = M^a mod n = 77^55 mod 99

B = M^b mod n = 77^66 mod 99

To find K = B^a (mod n)

To find K = A^b (mod n)

K = B^a mod n = (77^66 mod 99)^55 mod 99

K = A^b mod n = (77^55 mod 99)^66 mod 99

C is Ciphertext (hidden message), so instead of k for exponent, you use e

\*\*Ciiphertext should be lower than mod.\*\*

C = M^k (mod n) -> C=M^e (mod n)

C = 22^7 (mod 119)

C = 78

Apply RSA algorithm to find decryption exponent d

and the plaintext message M

q = 17, q = 5, e = 19, C= 65

Find n

n = p x q

n = 17 x 5

n = 85

Find l

l = (p-1) (q-1)

l = 16 x 4

l = 64

Find d

d = (lx + 1) / e

d = (64x + 1) / 19 trial and error, x = 1

d = (64(1) + 1)/ 19

d = 65/19, doesn't work, need whole number

... x = 2, 3, 4, 5, 6, 7, ...

d = (64x + 1) / 19

d = (64(8) + 1)/ 19

d = 27

So, decipher exponent is 27

M = C^d mod n

M = 65^27 (mod 85)

Since 65^27 is too big, have to split up the exponent

First, get binary of exponent.

11011 (16 + 8 + 2 + 1) = 27

Since the '4' column has a zero, don't use

\*\*Calculate\*\*

65^1 = 65 mod 85

65² ≡ 60 mod 85

65⁸ ≡ 50 mod 85

65¹⁶ ≡ 35 mod 85

\*\*Combine together\*\*

#### \*\*Step 1:\*\*

35×50

=175035×50

=1750

1750 mod  85

=501750 mod85

=50

50 is used in step 2 with the next number to reduce

#### \*\*Step 2:\*\*

50×60

=300050×60

=3000

3000 mod  85

=253000 mod85

=25

25 is used in step 3 with the next number to reduce

#### \*\*Step 3:\*\*

25×65

=162525×65

=1625

1625 mod  85

=101625 mod85

=10

No more numbers. So, M = 10

---

#### \*\*Why This Order?\*\*

- \*\*You can multiply in any order\*\*, but it's easiest to go left to right.

- At each step, you multiply two numbers, then immediately reduce modulo 85.

- This keeps the numbers small and avoids overflow or calculation errors.