- Assignment One JA 2025
  ICS 2310 Discrete Structures II

- SCT211-0535/2022
  AKECH DAU ATEM

Question 1(20 Marks). Prove or disprove, for integers a, b, c and d:

(a) If a □ b and a □ c, then a □ (b + c).
Proof:

- Since **a □ b**, there exists an integer **k** such that **b = a □ k**.
- Since **a □ c**, there exists an integer m such that **c= a□ m**.
- Then, **b + c = a □ k + a □ m = a □ (k + m)**
- Since **k + m** is an integer, **a □ (b + c).**

We concluded that the statement is **true**.

(b) If a □ bc and gcd(a , b) =1, then a □ c.

Proof:

- Since **gcd(a, b)=1**, by **Bézout's identity**, there exist integers **x** and **y** such that ***ax*+ *by* = 1.**
- Multiply both sides by **c**: **axc+byc = c**.
- Since **a □ bc**, there exists an integer **k** such that **bc=a□k**.
- Substitute into the equation: **axc+aky=c**, which simplifies to **a(xc+ky)=c**.
- Thus, a | c.

We concluded that the statement is **true**.

(c) If *a* and *b* are perfect squares and *a* | *b*, then *a* | *b* .

Proof:

- Let **a=k^2** and **b = m^2** where **k** and **m** are integers.
- Since **a □ b**, there exists an integer **n** such that **b = a□n**, so **m^2=k^2□n.**
- This implies **n** = **( )^2. Since** **n** is an integer**,** must be rational, but **m** and **k** are integers, so **k □ m.**
- Thus, = **k** divides = **m**.

Conclusion: The statement is **true**.

(d) If ab □ cd, then a □ c or a □ d.

Disproof:

- Counterexample: Let **a=6, b=5, c=10, d=3**.
- Then **ab**=30 and **cd** = 30, so **ab □ cd**.
- However, **6□10** and **6□3**.
- Thus, the statement is **false.**

Conclusion: The statement is **false**.

Question 2 On Euclids algorithm:

(a) Euclid's Algorithm in (Pseudo-code)

Input: Two integers a and b (where a≥b≥0)
Output: gcd(a,b)

function gcd(a, b):

```
while b ≠ 0:
remainder = a mod b // Compute remainder of a divided by b
a = b                        // Replace a with b
b = remainder           // Replace b with remainder
return a                    // When b = 0, a is the GCD
```

b) Proof that Euclid's Algorithm Correctly Finds GCD

Proof:

1. **Invariant:** At each step, **gcd(a, b)=gcd(b, a mod b).**
Let **d = gcd(a, b).** Then **d □ a** and **d □ b**, so **d □ (a−qb)** where **q = □a/b□. Thus, d □ (a mod b).**

Conversely,
if **d′=gcd(b, a mod b),** then **d′ □ b** and **d′□(a−qb)**, so **d′ □a**.

Thus, **d′ □ gcd (a,b).**

Therefore, **gcd(a,b) = gcd(b, a mod b).**

2. **Termination:** The algorithm terminates because **a mod b < b,** so the second argument strictly decreases and must eventually reach 0.

3. **Correctness:** When **b = 0, gcd(a,0) = a**, which is the correct GCD.

Conclusion: Euclid's algorithm terminates and correctly computes nullgcd(a,b)

(c) Compute gcd(1247,899,5014,998)

First, compute gcd pairwise:

Step 1: Compute gcd(1247,899):

1247 = 899(1) + 348

899 = 348(2) + 203

348 = 203(1) + 145

203 = 145(1) + 58

145 = 58(2) + 29

58 = 29(2) + 0

So, gcd(1247,899) = 29.

Step 2: Compute gcd(29,5014)

5014 = 29(172) + 26

29 = 26(1) + 3

26 = 3(8) + 2

3 = 2(1) + 1

2 = 1(2) + 0

So, gcd (29,5014) = 1.

Step 3: Computenullgcd(1,998)

998 = 1(998) + 0

So, gcd(1,998) = 1.

Answer: gcd(1247,899,5014,998) = 1.

(d) Inverse of 144 mod 233

We need to find **x** such that **144x ≡ 1(mod 233).**

Using the **Extended Euclidean Algorithm**:

233 = 144(1) + 89

144 = 89(1) + 55

89 = 55(1) + 34

55 = 34(1) +21

34 = 21(1) + 13

21 = 13(1) + 8

13 = 8(1) + 5

8 = 5(1) + 3

5 = 3(1) + 2

3 = 2(1) + 1

2 = 1(2) + 0

Now back-substitute to express 1 as a combination of 144 and 233:

1. 1 = 3−2(1)

2. 1 = 3 – 1 (5 – 3 (1)) = 3 – 5 + 3(1) = (2)3 – 5

3. 1 = 2(8 – 5) – 5 = 8(2) – 5(2) - 5 = 8(2) – 5(3)

4. 1 = 8(2)-3(13 - 8(1)) = 8(2) – 13(3) + 8(3) = 8(5) – 13(3)

5. 1 = 5(21 - 13(1)) -13(3) = 21(5) – 13(5) – 13(3) = 21(5) – 13 (8)

6. 1 = 21(5) – 8(34 – 21(1)) = 21(5) – 34 (8) + 21 (8) = 21(13) – 34(8)

7. 1 = 13(55-34(1)) – 34(8) = 55(13) – 34(13) - 34(8) = 55(13) – 34(21)

8. $1 = 55(13) - 21(89 - 55(1)) = 55(13) - 89(21) + 55(21) = 55(34) - 89(21)$

9. $1 = 34(144 - 89(1)) - 89(21) = 144(34) - 89(34) - 89(21) = 144(34) - 89(55)$

10. $1 = 144(34) - 55(233 - 144\ (1)) = 144(34) - 233(55) + 144(55) = 144(89) - 233(55)$

Thus, $1 = 144(89) - 233(55)$,

$144(89) + \cancel{233(-55)} = 1 \bmod 233$

Answer: The inverse of **144 mod 233** is **89**.

(e) Compute $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ mod 7.

First, simplify each term modulo 7:

1. **2^{20} mod 7**:
$\phi(7) = 6$, so $2^6 \equiv 1 (\text{mod} 7)$.
$20 = 6\times3+2$,
so $2^{20} \equiv (2^6)^3 \cdot 2^2 \equiv 1\cdot4 \equiv 4(\text{mod} 7)$.

2. 3^{30} mod 7:
$3^6 \equiv 1(\text{mod} 7)$.
$30 = 6\times5$, so $3^{30} \equiv (3^6)^5 \equiv 1(\text{mod} 7)$.

3. 4^{40} mod 7:
$4 \equiv 4\ (\text{mod} 7)$, $4^2 \equiv 2(\text{mod} 7)$, $4^3 \equiv 1(\text{mod} 7)$.
$40 = 3\times13+1$, so $4^{40} \equiv (4^3)^{13} \cdot 4^1 \equiv 1\cdot4 \equiv 4(\text{mod} 7)$.

4. 5^{50} mod 7:
$5 \equiv 5(\text{mod} 7)$, $5^2 \equiv 4(\text{mod} 7)$, $5^3 \equiv 6(\text{mod} 7)$, $5^4 \equiv 2(\text{mod} 7)$, $5^5 \equiv 3(\text{mod} 7)$, $5^6 \equiv 1(\text{mod} 7)$.
$50 = 6\times8 + 2$, so $5^{50} \equiv (5^6)^8 \cdot 5^2 \equiv 1\cdot4 \equiv 4(\text{mod} 7)$.

5. 6^{60} mod 7:
$6 \equiv -1\ (\text{mod} 7)$,
so $6^{60} \equiv (-1)^{60} \equiv 1(\text{mod} 7)$.

Now sum them up:
$4 + 1 + 4 + 4 + 1 \equiv 14 \equiv 0\ (\text{mod} 7)$.
Answer: The sum is congruent to **0 mod 7.**