ADVANCED MATHEMATICS

Integer numbers

1. For each of the following pairs of integer numbers, find the *greatest common divisor* (GCD), the *least common multiple* (LCM) and a *Bézout identity*:
   a) 10672, 4147; b) 12075, 4655; c) 2597, 1369; d)1312, 800; e) 322, 406.

2. For a and b two positive integers prove that, if d is the GCD of a and b, then d divides $na + mb$ for every pair of integers n and m.

3. Prove that $\gcd(n, n+1) = 1$, $\forall n \in \mathbb{Z}$. What are the possible values of $\gcd(n, n+2)$ and $\gcd(n, n+6)$?

4. Given a, b, $c \in \mathbb{Z}$ such that $\gcd(a, b)$ =$\gcd(a, c) = 1$, decide if the following statements are true or false:
   a) $\gcd(ab, a) = 1$; b) $\gcd(b, c) = 1$; c) $\gcd(bc, a) = 1$; d) $\gcd(ab, c) = 1$.

5. If $a \equiv b \bmod(n)$ and $a \equiv b \bmod(m)$, prove that $a \equiv b \bmod(\mathrm{lcm}(m, n))$.

6. Given $[n] \in \mathbb{Z}_m$. Prove that the existence of $[n]^{-1}$ (ie. the inverse of $[n]$ in class mod(m)) is equivalent to $\gcd(n, m) = 1$.

7. Find the inverses of the following numbers in the corresponding integer classes **a)** 6 in $\mathbb{Z}_{17}$; **b)** 3 in $\mathbb{Z}_{10}$; **c)** 7 in $\mathbb{Z}_{16}$.

8. Find the elements of $\mathbb{Z}_9$, $\mathbb{Z}_{15}$ and $\mathbb{Z}_{24}$ that have an inverse with respect to the product.

9. Find the solutions of the following equations:
   a) $12x = 2$ in $\mathbb{Z}_{19}$; b) $7x = 2$ in $\mathbb{Z}_{24}$; c) $31x = 1$ in $\mathbb{Z}_{50}$; d) $25x = 10$ in $\mathbb{Z}_{65}$.

10. Solve the following congruences:
    a) $5x \equiv 17 \bmod(19)$; b) $5x \equiv 17 \bmod(15)$; c) $34x \equiv 60 \bmod(98)$;
    d) $35x \equiv 119 \bmod(139)$; e) $125x \equiv 27 \bmod(256)$; f) $211x \equiv 658 \bmod(900)$.

11. Check the compatibility of the following systems of congruences, and solve them if it is possible:

$$\text{a)}\ \left.\begin{array}{c} x \equiv 2 \bmod(4) \\ x \equiv 4 \bmod(5) \end{array}\right\} \quad \text{b)}\ \left.\begin{array}{c} x \equiv 2 \bmod(3) \\ x \equiv 3 \bmod(4) \\ x \equiv 4 \bmod(5) \end{array}\right\} \quad \text{c)}\ \left.\begin{array}{c} x \equiv 18 \bmod(7) \\ x \equiv 3 \bmod(12) \\ x \equiv 7 \bmod(5) \\ x \equiv 11 \bmod(28) \end{array}\right\}$$

$$\text{d)}\ \left.\begin{array}{c} x \equiv 3 \bmod(17) \\ x \equiv 4 \bmod(18) \\ x \equiv 5 \bmod(19) \end{array}\right\} \quad \text{e)}\ \left.\begin{array}{c} x \equiv 2 \bmod(5) \\ 2x \equiv 1 \bmod(7) \\ 3x \equiv 4 \bmod(11) \end{array}\right\} \quad \text{f)}\ \left.\begin{array}{c} 2x \equiv 3 \bmod(7) \\ 5x \equiv 4 \bmod(9) \\ 3x \equiv 1 \bmod(10) \end{array}\right\}$$

12. Find the positive solutions of the following linear *diophantine equations*:
    a) $18x + 5y = 48$; b) $54x + 21y = 906$ c) $1588x - 5y = 7$.

13. Find the integers $10 < c < 20$ such that $84x + 990y = c$ has a solution, and solve in the compatible cases.

14. While in USA, Mr. Smith run out of cash and went to the bank to exchange a traveler check. The cashier mistakenly gave him the number of dollars as cents, and the number of cents as dollars. Without realising this Mr. Smith spent 68 cents in stamps, and then he was surprised when he realised that the amount of remaining cash was exactly twice of the value of the traveler check he previously exchanged. Find the minimum value of that check.

15. A seller of informatic equipment placed an order for some quantity in between 100 to 1500 units to a firm. They were sent in full containers, with a capacity of 68 units each. The seller distributed them to different selling points by means of small vans with a capacity for 20 units each and he left 32 units stored in the warehouse. Find how many units were asked to the firm in the placing order.

16. Find **(i)** $(a+b)^2$ in $\mathbb{Z}_2$. **(ii)** $(a+b)^3$ in $\mathbb{Z}_3$. **(iii)** Prove that if p is prime and $1 \leq k \leq p-1$ then the binomial coefficient $\binom{p}{k}$ is divisible by p. Deduce, by using Newton's binomial, a formula for $(a+b)^p$ in $\mathbb{Z}_p$, for p a prime number.

17. Find the multiples of 28 with their last two digits equal to 16.

18. Prove that for every integer n, the numbers $n^3 - 7n + 7$ and $n-1$ are coprimes.

19. a) **Quick sum** Let the mapping $f : \mathbb{Z}_{140} \to \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ defined as $f([n]_{140}) = ([n]_4, [n]_5, [n]_7)$. Prove that f is a *bijection* and compute $f^{-1}(f(35) + f(56))$.
b) **Quick product** Let the mapping $g : \mathbb{Z}_{2052} \to \mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_{19}$ defined as $g([n]_{2052}) = ([n]_4, [n]_{27}, [n]_{19})$. Prove that g is a bijection and compute $g^{-1}(g(35)g(56))$.

20. a) Let φ be the *Euler function*. Prove that $\varphi(m)$ is equal to the cardinal of the set $\mathbb{Z}_m^*$, that is, the set of the intertible elements of $\mathbb{Z}_m$.
b) Compute $\varphi(11), \varphi(16), \varphi(17), \varphi(25)$, and $\varphi(100)$. (Use that $\varphi(nm) = \varphi(n)\varphi(m)$ if $\gcd(n,m) = 1$ why?).

21. a) Find the last digit of the numbers 2^{333} and 3^{1313}.
b) Compute the remainder when dividing $(2^{37})^{73}$ by 37.
c) Find the last two digits of the numbers 2^{4927} and $4^{4^{4^4}}$.

22. Find the zeros in $\mathbb{Z}_5$ of each of the polinomials $f(x) = x^5 + 3x^3 + x^2 + 2x$ and $g(x) = 2x^{219} + 2x^{57} + 3x^{44}$ of $\mathbb{Z}_5[x]$.

23. A number from 0 to 26 is assigned to the 27 letters of the alphabet {A,B,...,Ñ,....} so that is identified with 0, B with 1 and so on. Thus, the modular equation $C(x) = (x+k) \bmod(27)$, where x runs over the letters of the message that we want to send, allows the coding of a message with "key" $k = 0, 1, 2, \dots, 26$. (This is *Caesar* cypher coding).
a) We receive the message: "GQQEUASKKJÑYQUBK". Knowing that the key is 6, what is the meaning of this message?
b) What is the formula used to decypher the message
c) Use Caesar code with key $k = 3$, to cypher the message: "PACIENCIA".