UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE CIENCIAS
Escuela Profesional de Matemáticas CICLO 2019-I

Primera Práctica Dirigida de
Introducción a las Estructuras Algebraicas (CM-361)

1. Si $p \geq 2$ es un número primo, pruebe que $\sqrt{p}$ no es un número racional.

2. Sean $a, b, c \in \mathbb{Z}$ con $a > 0$. Demuestre que $MCD(ab, ac) = aMCD(b, c)$.

3. Si p es un número primo y $k \in \mathbb{Z}$ tal que $1 \leq k < p$, demuestre que p divide a $\binom{p}{k}$.

4. **Algoritmo de Euclides.** Sean $a, b \in \mathbb{Z}^+$ tal que $b \not| a$. Si $r_0 = a$, $r_1 = b$; aplicando sucesivamente el algoritmo de la división obtenemos $r_2, r_3, \ldots, r_n, r_{n+1}$ definidos por las relaciones:

$$\begin{array}{rcll} r_0 & = & r_1 q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 & = & r_2 q_2 + r_3, & 0 < r_3 < r_2 \\ & \vdots & & \vdots \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_n q_n + r_{n+1}, & r_{n+1} = 0. \end{array}$$

En este caso pruebe que r_n el último resto no nulo, es el $MCD(a, b)$.

5. Usando el principio del buen orden pruebe que todo entero positivo $m > 1$ es divisible por algún número primo.

6. Si $n \geq 5$ es un entero no divisible por ningún primo $p \leq \sqrt{n}$, pruebe que n es un número primo.

7. Un conjunto A es **finito** si existe $n \in \mathbb{N}$ tal que $\#A = n$. En caso contrario diremos que A es infinito. ¿ El conjunto de los números primos es finito o infinito ? Justifique su respuesta.

8. Si $a|x$, $b|x$ y $MCD(a, b) = 1$, pruebe que $ab|x$.

9. Si $MCD(a, b) = 1$, pruebe que $MCD(a + b, a^2 - ab + b^2)$ es 1 ó es 3.

10. Probar que $MCD(a, b) = MCD(a + b, MCM(a, b))$.

11. Si $n \geq 2$, pruebe que la suma $\displaystyle\sum_{k=1}^{n} \frac{1}{k}$ no es un entero.

12. Sea p un número primo y $n \in \mathbb{Z}^+$. Hallar una fórmula para la mayor potencia de p que divide a $n!$.

13. Dados $a, m, n \in \mathbb{Z}^+$, pruebe que

$$MCD(a^m - 1\ ,\ a^n - 1) = a^{MCD(m,n)} - 1.$$

14. Sean $a, b \in \mathbb{Z} \setminus \{0\}$, $N \in \mathbb{Z}$ y $d = MCD(a, b)$. Si x_0, y_0 es solución particular de $ax + by = N$; pruebe que para todo $t \in \mathbb{Z}$: $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$ son todas las soluciones de esta ecuación.

15. Demuestre que existen infinitos primos de la forma $4n + 3$.

16. Asumiendo la validez del 1^{er} principio de inducción matemática, demuestre el principio del buen orden.

17. Si $MCD(a, b) = 1$, pruebe que el $MCD(a^3 + b^3, a^2 + b^2)$ es 1 ó es 2.

18. Pruebe que, si $2^n + 1$ es un número primo entonces es un primo de Fermat.

19. Demostrar que, si $m > n \geq 0$, entonces $2^{2^n} + 1$ divide a $2^{2^m} - 1$ y por consiguiente $MCD(2^{2^n} + 1, 2^{2^m} - 1) \neq 1$.

20. Suponga que $a^2 + b^2 = c^2$ con $a, b, c \in \mathbb{Z}$ primos entre si 2 a 2. Pruebe que existen enteros u y v tales que $c - b = 2u^2$, $c + b = 2v^2$ y $MCD(u, v) = 1$ consecuentemente $a = 2uv$, $b = v^2 - u^2$ y $c = u^2 + v^2$. Recíprocamente muestre que si u y v son dados, entonces los tres números a, b y c dados por estas fórmulas satisfacen $a^2 + b^2 = c^2$.

21. Dado cualquier entero positivo n, muestre que existen n enteros compuestos consecutivos.

22. Probar que si $m > n$ entonces $a^{2^n} + 1$ es un divisor de $a^{2^m} - 1$: además si a, m y n son enteros positivos con $m \neq n$, entonces el $MCD(a^{2^n} + 1, a^{2^m} + 1)$ es 1 si a es par y es 2 si a es impar.

23. Sea $\overline{a} \in \mathbb{Z}_n \setminus \{\overline{0}\}$. Pruebe que existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{ab} = 1$, si y sólo sí, $MCD(a, n) = 1$.

24. Pruebe que para todo $a, b \in \mathbb{Z}$, $a^2 + b^2$ no tiene resto igual a 3 cuando se divide por 4.

25. Sean $m, n \in \mathbb{Z}$ primos entre si. Si definimos $f : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$ por $f(x) = (\ \overline{x}, \overline{\overline{x}}\ )$ para todo $x \in \mathbb{Z}$, pruebe que f es sobreyectiva. Este resultado es conocido como el *Teorema Chino del Resto.*

26. Si $x^2 + y^2 = z^2$ (en $\mathbb{Z}$) demostrar que:

    (a) Al menos uno de los valores x, y, z es divisible por 3.

    (b) Al menos uno de los valores x, y, z es divisible por 5.

    (c) xyz es múltiplo de 4.

    (d) $xyz \equiv_{60} 0$.

27. Si $a \in \mathbb{Z}^+$ es tal que $MCD(a, 561) = 1$, pruebe que $a^2 \equiv_3 1$, $a^{10} \equiv_{11} 1$ y $a^{16} \equiv_{17} 1$: luego usando estos resultados pruebe que $a^{560} \equiv_{561} 1$. Este ejercicio muestra que el recíproco del Pequeño Teorema de Fermat no es válido.

28. Pruebe que no existe un entero a tal que $a^2 \equiv_{100} 35$.

29. Si $MCD(a, m) = 1$, pruebe que existe $x \in \mathbb{Z}$ tal que $ax \equiv_m b$. Más aun si x_0 es una solución particular entonces $x_0 + km$, $k \in \mathbb{Z}$ son todas las soluciones de esta ecuación.

30. Probar que $5n^3 + 7n^5 \equiv_{12} 0$ para todo entero n.

31. *Teorema de Wilson.* Siendo $p \in \mathbb{Z}^+$ un número primo, pruebe que $(p-1)! \equiv_p -1$ ¿El recíproco se cumple?
Sugerencia. Trabajar con $\mathbb{Z}_p \setminus \{\overline{0}\}$.

32. Si p es un primo impar, sea $q = \frac{p-1}{2}$. Pruebe que

$$(q!)^2 + (-1)^q \equiv_p 0$$

Esto nos proporciona a $q!$ como solución explícita de la congruencia $x^2 + 1 \equiv_p 0$ cuando $p \equiv_4 1$ y demuestra que $q! \equiv_p \pm 1$, si $p \equiv_4 3$.

33. Para un primo impar p muestre que el numerador de $1 + \dfrac{1}{2} + \dfrac{1}{3} + \ldots + \dfrac{1}{p-1}$ es divisible por p.

34. Sean p y q distintos primos impares tales que $p - 1$ divide a $q - 1$. Si $MCD(n, pq) = 1$ muestre que $n^{q-1} \equiv_{pq} 1$.

35. Resuelva la ecuación $x^2 - 1 = 0$ en $\mathbb{Z}_{15}$ (note que existen más de dos soluciones). Este ejercicio muestra que existen polinomios cuyo número de raíces es mayor que su grado. ¿Esto es una contradicción?. ¿Porqué?.

Uni, 19 de Marzo del 2018 **Mg. Manuel Toribio / Dr. Joe Palacios**