Problema 1. Determinar los siguientes órdenes:
(a) $\text{ord}_{13}2$. (b) $\text{odr}_7 2$, (c) $\text{ord}_{241}2$, (d) $\text{ord}_{17}2$, (e) $\text{ord}_{21}10$, (f)$\text{odr}_{25}9$

Problema 2. Sea b el inverso de a módulo n, demostrar que el $ord_n(b) = ord_n(a)$.

Problema 3. Demostrar que no existe ningún entero r tal que $ord_n r = \varphi(n)$ para los siguientes valores de n:
(a) $n = 12$, (b) $n = 20$, (c) $n = 16$, (d) $n = 28$.

Problema 4. Hallar el cociente y el resto de dividir en $\mathbb{Z}_{13}[x]$ los siguientes pares de polinomios:
(a) $x^6 + 3x^5 + 6x^4 + 4x^3 + 6x^2+8x + 10$ y $x^3 + 3x^2 + 5x + 1$
(b) $x^4 + 3x^3 + x + 3$ y $x^2 + 2x + 1$
(c) $2x^5 + 6x^4 + 3x^3 + 3x^2+4x + 5$ y $x^4 + 3x^2 +3x + 6$
(d) $x^5 + 6x^4 + 3x^3 + 3x^2+4x + 5$ y $3x^4 + 3x^2 +3x + 6$

Problema 5. Encontrar el máximo común divisor de los siguientes pares de polinomios $\mathbb{Q}[x]$
(a) $x^4 + 3x^3 + x + 3$ y $x^2 + 2x + 1$
(b) $x^6 + 3x^5 + 6x^4 + 4x^3 + 6x^2+8x + 10$ y $x^3 + 3x^2 + 5x + 1$
(c) $x^4 + 3x^2 +3x + 6$ y $x^5 + 6x^4 + 3x^3 + 3x^2+4x + 5$

Problema 6. Encontrar el máximo común divisor de los siguientes pares de polinomios $\mathbb{Z}_7[x]$
(a) $x^4 + 3x^3 + x + 3$ y $x^2 + 2x + 1$
(b) $x^6 + 3x^5 + 6x^4 + 4x^3 + 6x^2+8x + 10$ y $x^3 + 3x^2 + 5x + 1$
(c) $x^4 + 3x^2 +3x + 6$ y $x^5 + 6x^4 + 3x^3 + 3x^2+4x + 5$
Resolver en cada caso las correspondientes identidades de Bézout.

Problema 7. Encontrar el máximo común divisor de los siguientes pares de polinomios $\mathbb{Z}_{11}[x]$
(a) $x^5 + 6x^4 + 8x^3 + 6x^2 + x + 10$ y $x^4 + x^3 + 8x^2 + 7x + 7$
(b) $x^5 + 6x^4 + 8x^3 + 6x^2 + x + 10$ y $x^4 + x^3 + 6x^2 + 2x + 8$
(c) $x^8 + 6x^7 + 7x^6 +6x^5 + 4x^4 +3x^3 +7x + 10$ y $2x^2 + 4x + 2$
(d) $3x^8 + 7x^7 + 10x^6 + 4x^5 + 5x^4 +9x^3 +10x + 4$ y $x^2 + 2x + 1$
Resolver en cada caso las correspondientes identidades de Bézout.

Problema 8. Resolver las congruencias:
(a) $x^2 \equiv 31(\text{mod}75)$, (b) $x^2 \equiv 46(\text{mod}231)$, (c) $x^2 \equiv 46(\text{mod}21)$, (d) $x^2 \equiv 1156(\text{mod}3^2 5^3 7^5 11^6)$

Problema 9. (*Residuos cuadráticos*) Un entero a se dice residuo cuadrático módulo n si mcd(a, n) = 1 y la ecuación

$$x^2 \equiv a \ (\text{mod } n)$$

posee solución. Por ejemplo, en $\mathbb{Z}_{11}$, los residuos cuadráticos son 1, 3, 4, 5 y 9.
Sea $n = 4$, p^k, $2p^k$ (p primo impar). Demostrar que a es residuo cuadrático si, y sólo si, $a^{\frac{\varphi(n)}{2}} \equiv 1(\text{mod n})$

Problema 10. Demuestra que si a es resto cuadrático módulo un primo p, entonces las soluciones de $x^2 \equiv a$ (mod p) son:
(a) $x \equiv \pm a^{n+1}$ (mod p), si $p = 4n + 3$

Problema 11. Demostrar que si p es primo y k es entero positivo, entonces las únicas soluciones de $x^2 = x$ (mod p^k) son todos los enteros tales que $x \equiv 0$ ó 1 (mod p^k)

Problema 12. Resolver cada una de las ecuaciones de congruencias:
(a)$x^2 + 4x + 2 \equiv 0$ (mod 7),(b) $x^2 + 4x + 2 \equiv 0$ (mod 49), (c) $x^2 + 4x + 2 \equiv 0$ (mod 343),

Problema 13. Resolver cada una de las ecuaciones de congruencias:
(a)$x^2 + 102x+2 \equiv 0$(mod 7), (b) $x^2 + 102x+2 \equiv 0$(mod 49), (c) $x^2 + 102x+2 \equiv 0$(mod 343),

Problema 14. Resolver cada una de las ecuaciones de congruencias:
(a)$x^4+2x^2+3x+2\equiv 0$(mod 7), (b) $x^4+2x^2+3x+2\equiv 0$(mod 49), (c)$x^4+2x^2+3x+2\equiv$ (mod 343),
Problema 15. Resolver la ecuación polinómica de congruencias:
(a) $x^2 + 6x - 31 \equiv 0$ (mod 72), (b) $x^2 + 18x - 823 \equiv 0$ (mod 1800),
(c) $3x^2 + 6x - 31 \equiv 0$ (mod 72), (d) $3x^2 + 18x - 823 \equiv 0$ (mod 1800),
Problema 16. Resolver la ecuación polinómica de congruencias:
$13x^7 - 42x - 649 \equiv 0$ (mod 1800),
Problema 17. Resolver la ecuación polinómica de congruencias:
(a) $x^8 - x^4 + 1001 \equiv 0$ (mod 539), (b) $x^8 - x^4 + 462 \equiv 0$ (mod 539),
Problema 18. Encontrar todas las raíces de $x^4 + x^3 + 3x^2 + 2x + 2 \equiv 0$ (mod 7),
Problema 19. En el cuerpo $\mathbb{Z}_{11}$ todas las raíces de los polinomios que se indican:
(a) $x^2 + 2$, (b) $x^2 + 10$, (c) $x^3 + x^2 + 2x + 2$
En todos los casos factorizar los polinomios como producto de polinomios irreducibles.
Problema 20. Demostrar que si p es un número primo verificando $p \equiv 1(mod\ 4)$, entonces existe un entero x tal que $x^2 \equiv -1\ (mod\ p)$
Problema 21. Sea p un número primo. Demostrar que cada coeficiente del polinomio $f(x) = (x-1)(x-2)\ldots.(x-p+1) - x^{p-1} + 1$ es divisible por p.
Problema 22. Considerar la congruencia caudrática $ax^2 + bx + c \equiv 0$(mod p), donde p es primo y a, b, y c son enteros con p no divisor de a.
(a) Sea $p = 2$. Determinar que congruencias cuadráticas tienen solución.
(b) Sea p primo impar y sea $d = b^2 - 4ac$. Demostrar que la congruencia $ax^2+bx+c\equiv 0$(mod$p$), es equivalente a la congruencia $y^2 = d$ (mod p), donde $y=2ax+b$. Concluir que si $d \equiv 0$ (mod p), entonces existe exactamente una solución x módulo p; si d es residuo cuadrático de p, entonces existen dos soluciones incongruentes módulo p; y si d no es resto cuadrático de p, entonces no hay soluciones.
Problema 23. Resolver las siguientes ecuaciones:
(a) $x^2 + 13x + 17 \equiv 0$ (mod 23), (b)$x^2 + 5x + 1 \equiv 0$ (mod 23), (c) $x^2+13x+2\equiv 0$ (mod 23),
Problema 24. Resolver las siguientes ecuaciones:
(a)$x^2 + 13x + 17 \equiv 0$ (mod 529), (b)$x^2 + 5x + 1 \equiv 0$ (mod 529), (c) $x^2+13x+2\equiv 0$ (mod 529),