Práctica 1

1. Teorema de Euler-Fermat

   Sea $n > 0$ y $\{a_1, a_2, ..., a_{\varphi(n)}\}$ un sistema reducido de restos módulo n (o sea, $(a_i, n) = 1$ y son no congruentes módulo n). Si a es coprimo con n pruebe que $\{aa_1, aa_2, ..., aa_{\varphi(n)}\}$ es de nuevo un sistema reducido de restos módulo n.

   Probar que para todo a coprimo con n

   $$a^{\varphi(n)} \equiv 1(n)$$

2. Sea $\{a_1, a_2, ..., a_{\varphi(n)}\}$ un sistema reducido de restos módulo n, $(n > 2)$ y N el número de soluciones de $x^2 \equiv 1(n)$. Probar que

   $$a_1 a_2 ... a_{\varphi(n)} \equiv (-1)^{N/2}(n).$$

3. Probar que la función

   $$f(n) = \sum_{d|n} \varphi(d)$$

   es multiplicativa y calcular $f(p^k)$. Probar que

   $$n = \sum_{d|n} \varphi(d)$$

4. Encontrar el orden de 2 módulo 17 y módulo 19.

5. Sea g una raíz primitiva módulo n. Probar que

   $$g^k \text{ es primitiva } \iff (k, \varphi(n)) = 1.$$

6. Sea $p \neq 2$ primo. Sea g una raíz primitiva módulo p. Probar:

   (a)
   $$g^{\frac{p-1}{2}} \equiv -1(p)$$

   (b) Si g' es otra raíz primitiva, entonces gg' no es primitiva

   (c) Si g' es tal que $gg' \equiv 1(p)$, entonces g' es primitiva.

7. Sea $p > 3$ es primo. Mostrar que el producto de todas las raíces primitivas módulo p es $\equiv 1(p)$.

8. Sea $p > 2$ primo.

   (a) Probar que hay tantas raíces primitivas módulo $2p^k$ como raíces primitivas módulo p^k.

   (b) Sea g primitiva módulo p^k. Probar que g es primitiva módulo $2p^k \iff g$ es impar.

9. (a) Encontrar raíces primitivas módulo 26 y módulo 25.

   (b) Mostrar que 3 es raíz primitiva módulo 7^k y módulo $2 \cdot 7^k, \forall k \geq 1$.

10. (a) Sea $f(x) \in \mathbb{Z}[x]$ y $n = p_1^{a_1} p_2^{a_2} ... p_t^{a_t}$. Entonces, $f(x) \equiv 0(n)$ tiene solución si y solo si $f(x) \equiv 0(p_i^{a_i})$ tiene solución para todo $i = 1, ..., t$.

    (b) Sea N el número se soluciones de $f(x) \equiv 0(n)$ y N_i el número de soluciones de $f(x) \equiv 0(p_i^{a_i})$. Probar que $N = N_1 ... N_t$.

    (c) Sea p un primo impar y sea $n = p^k$, $n = 2p^k$ o $n = 4$. Probar que 1 y -1 son las únicas soluciones de $x^2 \equiv 1(n)$.

    Mostrar que esto es falso si n no es de alguno de los tipos mencionados en c).

    (d) Probar que $x^2 \equiv 1(2^a)$ tiene una solución si $a = 1$, dos si $a = 2$ y cuatro si $a \geq 3$.

    (e) Encuentre el número de soluciones de $x^2 \equiv 1(n)$.

11. Mostrar que 7 y 18 son las únicas soluciones de $x^2 \equiv -1(5^2)$. Encontrar las soluciones de $x^2 \equiv -1(5^3)$.

12. Sea a impar y $n \geq 3$. Mostrar que si $x^2 \equiv a(2^n)$ tiene solución, hay exactamente 4.

    Determinar los valores de a para los cuales las congruencias siguientes son resolubles: $x^2 \equiv a(2^4)$, $x^2 \equiv a(2^5)$, $x^2 \equiv a(2^6)$.

13. (a) Resolver $3x^2 + 9x + 7 \equiv 0(13)$.

    (b) Sea p primo, $p \neq 2$ y $(a, p) = 1$. Mostrar que la ecuación $ax^2 + bx + c \equiv 0(p)$ es resoluble si y solo si $b^2 - 4ac$ es cero o un residuo cuadrático módulo p.

14. Mostrar que $6x^2 + 5x + 1 \equiv 0(p)$ tiene solución $\forall p$ primo, pero no tiene solución entera.

15. (a) Sea a un residuo cuadrático módulo p ($p \neq 2$ primo), entonces $p - a$ es residuo cuadrático módulo p si y solo si $p \equiv 1(4)$.

    (b) Si $p \equiv 3(4)$, las soluciones de $x^2 \equiv a(p)$ son $x = \pm a^{\frac{p+1}{4}}(p)$.

16. (a) Si ab es residuo cuadrático módulo p, entonces a y b son ambos residuos o ambos no residuos cuadráticos.

(b) Si a y b son ambos residuos o ambos no residuos cuadráticos, la ecuación $ax^2 \equiv b(p)$ tiene solución.

17. Sea $p \neq 2$ primo. Los residuos cuadráticos módulo p son $\equiv 1, 2^2, 3^2, ..., (\frac{p-1}{2})^2$.

18. Calcular $(\frac{-23}{59})$, $(\frac{461}{773})$.

19. Probar que el número de soluciones de $x^2 \equiv a(p)$ está dado por $1 + \left(\frac{a}{p}\right)$.

    Si $p \nmid a$ el número de soluciones de $ax^2 + bx + c \equiv 0(p)$ es $1 + \left(\frac{b^2-4ac}{p}\right)$.

20. Determinar cuáles congruencias son resolubles:

    $x^2 \equiv 219(419)$

    $2x^2 + 5x - 9 \equiv 0(101)$

21. $\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) = 0$

    $\sum_{x=1}^{p-1} \left(\frac{ax+b}{p}\right) = 0$ si $p \nmid a$.

22. Sea p primo. Mostrar que
$$\sum_{x=1}^{p-2} \left(\frac{x(x+1)}{p}\right) = -1.$$

23. Sean $a, b \in \mathbb{Z}$ con $b > 0$ y $b = p_1 \dots p_r$, con p_i primos no necesariamente distintos. Se define el símbolo de Jacobi como
$$\left(\frac{a}{b}\right) \underset{def}{=} \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_r}\right).$$

    Probar que el símbolo de Jacobi satisface:

    (a) Si $a \equiv a'(b)$ entonces $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$.

    (b) $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$.

    (c) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.

    (d) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.

    (e) LRC: Si b, b' son impares coprimos,
$$\left(\frac{b}{b'}\right)\left(\frac{b'}{b}\right) = (-1)^{\frac{b-1}{2}\frac{b'-1}{2}}.$$

24. Evaluar el símbolo de Legendre $\left(\frac{1801}{8191}\right)$.

    (a) Sólo usando la ley de reciprocidad para el símbolo de Legendre.

(b) Usando la ley de reciprocidad para el símbolo de Jacobi.

25. Sea $p \in \mathbb{Z}$ primo. Probar que $p \equiv 1(4) \iff p$ es suma de cuadrados en $\mathbb{Z} \iff -1$ es un cuadrado módulo p.

26. Escribir 113 como suma de dos cuadrados.

27. Sea $p \neq 2$ primo, a y k coprimos con p. Mostrar que si la ecuación $x^2 - ay^2 = kp$ tiene solución, entonces $\left(\frac{a}{p}\right) = 1$. Considere $x^2 + 5y^2 = 7$ y muestre que la recíproca no es cierta.

    Muestre que $\forall p \equiv \pm 3(8)$ la ecuación $x^2 - 2y^2 = p$ no tiene solución.

28. Probar que todo primo $p \equiv 1, 3(8)$ se puede escribir en la forma $p = a^2 + 2b^2$.

29. Verificar que

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & p \equiv 1, 3(8) \\ -1 & p \equiv 5, 7(8) \end{cases}$$

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1(6) \\ -1 & p \equiv 5(6) \end{cases}$$

    Encontrar p primo tal que $p = x^2 + y^2 = u^2 + 2v^2 = r^2 + 3s^2$.