Universidad de Concepción
Facultad de Ciencias Físicas y Matemáticas
Departamento de Matemática

Listado 06: Símbolo de Legendre y reciprocidad cuadrática
Teoría de Números (527288)

1. Determinar los siguientes valores del símbolo de Legendre.

   (a) $\left(\dfrac{36}{97}\right)$ (b) $\left(\dfrac{650}{4591}\right)$ (c) $\left(\dfrac{-78}{3373}\right)$ (d) $\left(\dfrac{5!}{101}\right)$

2. Determinar la cantidad de soluciones de cada una de las siguientes ecuaciones.

   (a) $x^2 + 2x + 5 \equiv 0 \pmod{71}$
   (b) $x^2 + 2x - 8 \equiv 0 \pmod{10}$
   (c) $x^2 + x + 76 \equiv 0 \pmod{101}$
   (d) $x^2 + x + 82 \equiv 0 \pmod{3 \cdot 7 \cdot 11}$

3. Utilizando ambos suplementos del cálculo del símbolo de Lagrange, determinar todos los valores de p que satisfacen $\left(\dfrac{-2}{p}\right) = 1$.

4. Determinar todos los valores de p que satisfacen cada una de las siguientes condiciones.

   (a) $\left(\dfrac{3}{p}\right) = 1$ (b) $\left(\dfrac{5}{p}\right) = 1$ (c) $\left(\dfrac{-5}{p}\right) = 1$

5. Con las notaciones del apunte Reciprocidad cuadrática - notaciones y previos, escribir las expresiones para G_1, G_2, G_3 y G_4 con $p = 5$ (no calcular ζ) y verificar las igualdades $G_a = \left(\dfrac{a}{p}\right) G_1$ para estos casos.

Mini-proyecto: Otra forma de estudiar el segundo suplemento

A continuación se presenta una demostración geométrica del método para determinar el valor de $\left(\dfrac{2}{p}\right)$ para p primo impar.
Esta demostración no utiliza métodos algebraicos con raíces complejas de 1. El objetivo es contar la cantidad de puntos del siguiente conjunto S:

$$S = \left\{ (a, b) \in U_p \times U_p \,:\, \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1 \,\wedge\, a + b \equiv 1 \pmod{p} \right\}$$

Para esta cuenta habrá que utilizar el primer suplemento, el valor de $\left(\dfrac{-1}{p}\right)$.

6. Mostrar: el conjunto solución de la ecuación $x^2 + y^2 \equiv 1 \pmod{p}$ en $(\mathbb{Z}/p\mathbb{Z})^2$ es

$$\{(-1, 0)\} \cup \left\{ \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right) \,:\, t \in \mathbb{Z}/p\mathbb{Z} \,\wedge\, t^2 + 1 \not\equiv 0 \pmod{p} \right\}$$

*(Indicaciones: (a) Una de las inclusiones se puede verificar sustituyendo en la ecuación. (b) Para la otra, si (x, y) es solución, considerar la recta $y = t(x + 1)$ que pasa por dicha solución y por $(-1, 0)$, y despejar x, y de este sistema. (c) Para resolver el sistema quedará una ecuación cuadrática, pero **ya sabemos una de sus soluciones**. Se puede despejar la otra solución.)*

7. A partir del problema anterior y el primer suplemento: mostrar que la ecuación $x^2 + y^2 \equiv 1 \pmod{p}$ en $(\mathbb{Z}/p\mathbb{Z})^2$ tiene $p - 1$ soluciones si $p \equiv 1 \pmod{4}$ y tiene $p + 1$ soluciones si $p \equiv 3 \pmod{4}$. *(Indicación: al contar el número de elementos del conjunto solución, ¿cuántos valores puede tomar t?)*

8. A partir del problema anterior: mostrar que la ecuación $x^2 + y^2 \equiv 1 \pmod{p}$ en $(U_p)^2$ tiene $p - 5$ soluciones si $p \equiv 1 \pmod{4}$ y tiene $p - 3$ soluciones si $p \equiv 3 \pmod{4}$. *(Indicación: se achicó el conjunto. ¿Cuáles soluciones desaparecieron?)*

9. A partir del problema anterior, mostrar que la cardinalidad del conjunto S es $(p - 5)/4$ si $p \equiv 1 \pmod{4}$ y es $(p - 3)/4$ si $p \equiv 3 \pmod{4}$. *(Indicación: la diferencia entre el problema anterior y éste es que antes importaban los valores x, y de los números que se elevan al cuadrado; ahora sólo importan a, b, los cuadrados mismos. Muchos elementos del conjunto anterior ahora se consideran repetidos.)*

10. A partir de las expresiones del problema anterior, mostrar que $|S|$ es impar si y sólo si $p \equiv \pm 1 \pmod{8}$. *(Indicación: considerar caso a caso los valores $p \equiv 1, 3, 5, 7 \pmod{8}$.)*

11. Mostrar que la función $\sigma : S \to S$ dada por $\sigma(a, b) = (b, a)$ es su propia inversa. Concluir: la paridad de $|S|$ es igual a la paridad del conjunto de puntos $(a, b) \in S$ con $a = b$. *(Indicación: la función σ empareja cada punto de S con otro punto de S... o consigo mismo.)*

12. Mostrar: si $(a, a) \in S$, entonces $2a \equiv 1 \pmod{p}$ y $\left(\frac{2}{p}\right) = 1$. *(Indicación: reemplazar en la definición de S, y recordar las reglas de multiplicación de símbolos de Legendre.)*

13. De los dos ejercicios anteriores: mostrar que $|S|$ es impar si y sólo si $\left(\frac{2}{p}\right) = 1$. *(Indicación: recordar que p es impar, así que la cantidad de soluciones de $2a \equiv 1 \pmod{p}$ no varía con p.)*

14. Demostrar el segundo suplemento. *(Indicación: usar las dos equivalencias encontradas para que $|S|$ sea impar.)*