Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Héctor Pastén **Ayudante:** José Cuevas Barrientos
Curso: Teoría de Números **Sigla:** MAT2225
Fecha: 29 de septiembre de 2023

Principio local-global

1. Reciprocidad cuadrática

Comenzaremos por presentar unos ejercicios básicos de reciprocidad cuadrática para poder sacarle mayor provecho a los resultados del principio local-global.

Definición 1.1: Sea $n > 0$ un entero. Una ***raíz primitiva módulo*** n es un número g coprimo a n, tal que para todo número coprimo a a n existe algún $m > 0$ tal que $g^m \equiv a \pmod{n}$.

Otra manera de verlo es que el conjunto $U_n := (\mathbb{Z}/n\mathbb{Z})^\times$ unidades módulo n está formado precisamente por las clases de congruencia coprimas con n y que es un grupo con el producto. Una raíz primitiva es, entonces, un generador de U_n.

1. Demuestre las siguientes afirmaciones:
   a) Para todo primo p existe una raíz primitiva módulo p.
   Pista: Emplee el pequeño teorema de Fermat. □
   b) Si g es una raíz primitiva módulo p, entonces g o $g + p$ es una raíz primitiva módulo p^2.
   c) No obstante, no todos los enteros admiten una raíz primitiva módulo n; de un ejemplo.

Definición 1.2: Sea g una raíz primitiva módulo n. Dado a coprimo con n defina[1] $\text{índ}_g(a) := m$ como el mínimo natural (incluyendo $m = 0$) tal que $g^a \equiv 1 \pmod{n}$.

2. Demuestre que si g_1, g_2 son dos raíces primitivas módulo $n > 2$, entonces para todo h coprimo con n, se cumple que $\text{índ}_{g_1}(h), \text{índ}_{g_2}(h)$ tienen igual paridad.

Definición 1.3: Sea p un número primo y sea g una raíz primitiva módulo p. Se define el ***símbolo de Legendre*** como:

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & p \mid a, \\ (-1)^{\text{índ}_g(a)}, & p \nmid a. \end{cases}$$

El ejercicio anterior prueba que el símbolo de Legendre está bien definido.

3. Sea p un número primo. Demuestre las siguientes:
   a) Para un número a coprimo a n tenemos que $(a/p) = 1$ syss existe un número h tal que $h^2 \equiv a \pmod{p}$. En este caso, decimos que a es un ***residuo cuadrático módulo*** p.
   b) Para a, b coprimos a n se tiene que $(ab/p) = (a/p)(b/p)$.
   c) Demuestre que si $p \equiv 1 \pmod{4}$, entonces -1 es un residuo cuadrático módulo p.

2. Principio local-global

Definición 2.1: Una ***H-solución módulo*** p de $f(x) = 0$ es un entero a tal que $f(a) \equiv 0 \pmod{p}$, pero $f'(a) \not\equiv 0 \pmod{p}$; donde $f'(x)$ es la derivada (formal) de $f(x)$.

[1] A veces se denota $\log_g$ y se llama *logaritmo discreto*.

Un ***principio local-global*** es un criterio bajo el cual una determinada ecuación diofántica $f(x_1, \ldots, x_n) = 0$, donde $f(\boldsymbol{x})$ tiene coeficientes en $\mathbb{Z}$, tiene soluciones enteras si tiene soluciones en $\mathbb{R}$ y tiene H-soluciones módulo p para todo p. Recuérdese:

Teorema 2.2 (Hasse-Minkowski): Las formas cuadráticas satisfacen un principio local-global.

4. *a*) Empleando el principio local-global demuestre que todo primo $p \equiv 1 \pmod 4$ es suma de dos cuadrados. (Aquí puede asumir que la existencia de una solución racional implica la existencia de una solución entera.)
   b) Empleando la identidad
   $$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2, \tag{1}$$
   concluya una mejor clase de números que se pueden escribir como suma de dos cuadrados.
5. Demuestre que el principio local-global falla en la ecuación
   $$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0,$$
   es decir, que admite soluciones reales y H-soluciones para todo p, pero no admite soluciones racionales.
6. Demuestre que el principio local-global falla en la ecuación $x^2 + 11y^2 = 3$.

3. Comentarios adicionales

La expresión «H-solución» es de mi autoría y está allí para referenciar un uso escondido del *lema de Hensel*. Una versión más precisa del principio local-global es que relaciona la existencia de soluciones en los enteros p-ádicos $\mathbb{Z}_p$ con soluciones enteras. Una buena introducción, a mi juicio, yace en el libro Cassels [**1**].

El ejemplo de una *forma* (i.e., polinomio homogéneo) aguda que contradice el principio local-global es el ***ejemplo de Selmer***:
$$3x^3 + 4y^3 + 5z^3 = 0,$$
pero la demostración es más larga e involucra un mejor manejo del lema de Hensel (cfr. Conrad [**2**]).

El paso de «existe solución racional» a «existe solución entera» puede formalizarse mejor con el siguiente resultado:

Lema 3.1 (Davenport-Cassels): Sea $a \in \mathbb{Z}$ tal que la ecuación $a = x_1^2 + \cdots + x_n^2$ tiene soluciones en $\mathbb{Q}$. Entonces la misma ecuación tiene soluciones en $\mathbb{Z}$.

No obstante, se suele escribir este resultado para $n = 3$ ya que para $n = 4$ es un teorema de Legendre que la ecuación siempre admite solución; para $n = 1$ es trivial y para $n = 2$ es conocida la clasificación de los enteros que son sumas de dos cuadrados. La demostración se puede ver en Rajwade [**3**].

Finalmente, la identidad (1) pierde cierto misterio si pensamos $a^2 + b^2 = |a + \mathrm{i}b|^2$, donde $\mathrm{i} = \sqrt{-1}$. Si hacemos el mismo juego en los cuaterniones y en los octoniones, obtendremos identidades parecidas para sumas de 4 y de 8 cuadrados resp.; la busqueda de estas identidades es un problema interesante conocido como el *problema de Hurwitz*, ya resuelto y expuesto de manera elemental en [**3**].

Referencias y lecturas adicionales

1. Cassels, J. W. S. *Local Fields* (Cambridge University Press, 1986).
2. Conrad, K. *The local-global principle* `https://kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf`.
3. Rajwade, A. R. *Squares* (Cambridge University Press, 1993).

Correo electrónico: `josecuevasbtos@uc.cl`