Ayudantía 5

1. Introducción a los números p-ádicos

Comencemos estudiando congruencias módulo una potencia de un primo.

Ejercicio 1: Considere la siguiente congruencia

$$x^2 \equiv 2 \mod 7^n, \tag{1.1}$$

encuentre las soluciones para $n = 1, 2, 3$.

Solución. Para $n = 1$ la congruencia posee dos soluciones $x_0 \equiv \pm 3 \mod 7$. Ahora considere $n = 2$

$$x^2 \equiv 2 \mod 7^2, \tag{1.2}$$

esto implica que $x^2 \equiv 2 \mod 7$. Por tanto, cada solución de (1.2) es de la formma $x_0 + 7t_1$, donde x_0 es la solución de (1.1). Así que, las soluciones que buscamos son de la forma $x_1 = 3 + 7t_1$. (Las soluciones de la forma $-3 + 7t_1$ se encuentran de la misma forma.) Substituyendo la expresión para x_1 en (1.2), obtenemos

$$\begin{aligned} (3 + 7t_1)^2 &\equiv 2 \mod 7^2, \\ 9 + 6 \cdot 7t_1 + 7^2 t_1^2 &\equiv 2 \mod 7^2, \\ 1 + 6t_1 &\equiv 0 \mod 7, \\ t_1 &\equiv 1 \mod 7. \end{aligned}$$

Así que, $x_1 \equiv 3 + 7 \cdot 1 \mod 7^2$. Similarmente, cuando $n = 3$ tenemos $x_2 = x_1 + 7^2 t_2$ y desde la congruencia

$$(3 + 7 + 7^2 t_2)^2 \equiv 2 \mod 7^3$$

deducimos que $t_2 \equiv 2 \mod 7$; esto es,

$$x_2 \equiv 3 + 7 \cdot 1 + 7^2 \cdot 2 \mod 7^3.$$

□

Podemos continuar de manera infinita y obtenemos la secuencia

$$x_0, x_1, \ldots, x_n, \ldots \tag{1.3}$$

las cuales satisfacen

$$\begin{aligned} x_0 &\equiv 3 \mod 7, \\ x_n &\equiv x_{n-1} \mod 7^n, \\ x_n^2 &\equiv 2 \mod 7^{n+1}. \end{aligned}$$

La construcción de la secuencia (1.3) recuerda al proceso para encontrar la raíz cuadrada de 2. En efecto, para calcular $\sqrt{2}$, se debe encontrar una secuencia de racionales $r_0, r_1, \ldots$ cuyos cuadrados convergen a 2,

$$|r_n^2 - 2| < \frac{1}{10^n}.$$

En nuestro caso, construimos una secuencia de enteros $x_0, x_1, \ldots$ para los cuales $x_n^2 - 2$ es divisible por 7^{n+1}. Este análogo se vuelve más preciso si decimos que dos enteros son ***cercanos*** (o bien, p-***cercanos***), cuando su diferencia es divisible por una potencia de p suficientemente larga. Con este concepto de cercanía podemos decir que los cuadrados de los números en la secuencia (1.3) se vuelven arbitrarianmente 7-cercanos a 2 cuando n crece.

Definición 1.1: Sea p algún primo. Una secuencia de enteros $\{x_n\} = \{x_0, x_1, \ldots\}$ que satisface $x_n \equiv x_{n-1} \mod p^n$ para cada $n \geq 1$, determina un objeto llamado ***entero p-ádico***

$$x = x_0 + x_1 \cdot p + x_2 \cdot p^2 + \ldots = \sum_{i=0}^{\infty} x_i p^i.$$

El conjunto de todos los enteros p-ádicos se denota $\mathbb{Z}_p$.

Ejemplo 1.2: La 7-ádica solución de $x^2 = 2$ es $3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 + \ldots$

Podemos definir la divisibilidad de los enteros p-ádicos como se hace en cualquier anillo conmutativo; α divide a β si $\beta = \alpha\gamma$. Para saber cuales enteros p-ádicos se tiene inversa, es decir, si son inversibles o unidad, se tiene el siguiente resultado

Teorema 1.3: *Un entero p-ádico, el cual está determinado por $\{x_0, x_1, x_2, \ldots\}$, éste es una unidad syss $x_0 \not\equiv 0 \mod p$.*

Definición 1.4: Una fracción de la forma α/p^k, $\alpha \in \mathbb{Z}_p$, $k \geq 0$, determina un p-ádico fraccionario, o más simple, un ***número p-ádico***. Dos fracciones, α/p^k y β/p^m determinan el mismo número p-ádico syss $\alpha p^m = \beta p^k$ en $\mathbb{Z}_p$.

El conjunto de todos los números p-ádicos se denota como $\mathbb{Q}_p$.

Definición 1.5: Sea $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ una función. Si satisface las siguientes condiciones

1. $\varphi(a) \geq 0$ con igualdad syss $a = 0$,
2. $\varphi(ab) = \varphi(a)\varphi(b)$,
3. $\varphi(a+b) \leq \max(\varphi(a), \varphi(b))$,

diremos que φ es una ***valuación no arquimediana***.

Ejemplo 1.6: Si consideramos algún p primo, podemos escribir de manera única cualquier racional como

$$a = \frac{r}{s}p^n, \qquad s > 0,$$

donde r, y s son enteros coprimos, $p \nmid rs$ y n es un entero el cual puede ser positivo, negativo o cero. Ahora definamos para $a \neq 0$

$$\varphi(a) = p^{-n},$$

y $\varphi(0) = \infty$. Podemos verificar que φ es una valuación no arquimediana, le diremos valuación p-ádica y le escribiremos como $|\cdot|_p$.

A través de este ejemplo podemos definir $v_p(a) = -\log|a|_p$, éste también es una valuación no arquimediana.

2. Congruencias y enteros p-ádicos

Teorema 2.1: *Sea $F(x_1, \ldots, x_n)$ un polinomio con coeficientes enteros racionales. La congruencia*

$$F(x_1, \ldots, x_n) \equiv 0 \mod p^k$$

posee solución para cada $k \geq 1$ syss la ecuación

$$F(x_1, \ldots, x_n) = 0$$

posee solución en $\mathbb{Z}_p$.

Teorema 2.2 (Lema de Hensel): *Si* $f(x) \in \mathbb{Z}_p[x]$ *y* $a \in \mathbb{Z}_p$ *satisfacen* $f(a) \equiv 0 \mod p$ *y* $f'(a) \not\equiv 0 \mod p$ *entonces existe un único* $\alpha \in \mathbb{Z}_p$ *tal que* $f(\alpha) = 0$ *en* $\mathbb{Z}_p$ *y* $\alpha \equiv a \mod p$.

Ejercicio 2: Sea $f(x) = x^2 - 2$ busque las soluciones enteras 7-ádicas.

3. Principio local-global

El principio local-global enuncia, de manera escencial, que un teorema o propiedad se cumple sobre $\mathbb{Q}$ syss se cumple en $\mathbb{R}$ y en $\mathbb{Q}_p$ para cada p. Diremos que $\mathbb{Q}$ es un ***campo global*** y $\mathbb{R}$, $\mathbb{Q}_p$ ***campos locales***.

En clases vieron casos de existencia de soluciones no triviales para polinomios homogéneos de grado 2. Un clásico teorema relacionado es

Teorema 3.1 (Euler): *Un entero positivo* m *puede ser escrito como una suma de dos cuadrados syss cada* p *que divide a* m *con* $p \equiv 3 \mod 4$ *tiene una multiplicidad par como un factor de* m.

Para trabajar éste teorema en términos p-ádicos, primero describiremos de manera equivalente un entero p-ádico.

Ejercicio 3:

1. Para un primo $p \equiv 1 \mod 4$, todo entero p-ádico es una suma de dos enteros cuadrados p-ádicos.

2. Para un primo $p \equiv 3 \mod 4$, un entero no nulo p-ádico t es una suma de dos cuadrados en $\mathbb{Z}_p$ syss $v_p(t)$ es par.

3. Concluya que un entero no nulo es la suma de dos cuadrados en $\mathbb{Z}$ syss es una suma de dos cuadrados en $\mathbb{R}$ y en cada $\mathbb{Z}_p$.

Referencias

1. Borevich, Z. I. y Shafarevich, I. R. *Number Theory* (Academic Press, 1966).
2. Conrad, K. *The local-global principle* https://kconrad.math.uconn.edu/blurbs/.
3. Hua, L. K. y Shiu, P. *Introduction to Number Theory* (Springer-Verlag Berlin Heidelberg, 1982).

Correo electrónico: rseplveda@uc.cl