# UNA RELACION ENTRE LA TEORIA DE NUMEROS Y EL ALGEBRA

CRISTOBAL MEJIA

El siguiente es el texto de una exposición realizada en el curso de Teoría de números, sobre las relaciones entre la Teoría de números y el algebra.
Se trata de dar solución a tres importantes problemas de la teoría de números, mediante el álgebra: el teorema de Wilson y dos teoremas de Fermat.

A continuación, aclararemos algunos conceptos y la notación utilizada en la demostración de estos teoremas:
Usaremos la notación $(a,b)$ para representar el máximo común divisor de $a$ y $b$. Si $(a,b)=1$ diremos que $a$ y $b$ son primos relativos.
Decimos que $s\neq 0$ divide a $r$ si $r=mb$ para algún $m$, y lo notamos $s|r$.
Sea $n$ = entero fijo, definimos $a\equiv b$ módulo $n$ si $n|(a-b)$.
La relación "congruente módulo n" ($\equiv_n$) define una relación de equivalencia en el conjunto de los enteros. Denotaremos la clase de equivalencia de esta relación (a la que pertenece a) por el símbolo $[a]_n$; y la llamaremos clase de congruencia (mod n) de a.
Si un conjunto G es grupo respecto a una operación "$*$", lo notaremos $\langle G,*\rangle$. Una característica de un grupo G es el número de elementos de que consta; llamaremos a éste "orden de G" y lo notaremos $o(G)$.
Recordemos algunos conceptos de la teoría de grupos:

1. Si $\langle G,\cdot\rangle$ es grupo y $a\in G$, el orden de a es el entero positivo mínimo m tal que $a^m=e$ y lo notaremos $o(a)$.
2. Si $\langle G,\cdot\rangle$ es grupo y $a\in G$, $a^{o(G)}=e$.
   e es el módulo de $\langle G,\cdot\rangle$.

**PRIMER TEOREMA DE FERMAT:**
Si $a\in\mathbb{Z}$, y $p$ es un número primo, entonces $a^p\equiv a$ mód $p$.

Dem:
i) si $(a,p)\neq 1$ entonces $p|a$. Luego $p|a(a^{p-1}-1)$. Por lo tanto $p|a^p-a$ entonces $a^p\equiv a$ mód $p$

ii) Si $(a,p)=1$:
Si $\mathbb{Z}^*_p=\{[1]_p,[2]_p,[3]_p,\dots,[p-1]_p\}$ entonces $\langle \mathbb{Z}^*_p,\cdot\rangle$ forma grupo.
Sea $x\in\mathbb{Z}^*_p$; $x=[a]p$ para algún $a\in\mathbb{Z}$, por tanto:
$([a]_p)^{p-1}=[a]_p^{\,o(\mathbb{Z})}=[1]_p$ entonces $a^{p-1}\equiv 1$ mód $p$, por consiguiente $p|a^{p-1}-1$.
Entonces $p|a(a^{p-1}-1)$ de donde $p|a^p-a$. Luego $a^p\equiv a$ mód $p$.

LEMA 1: Si G es un grupo abeliano finito y $\exists!\, a_k\in G$ tal que $o(a_k)=2$ entonces $a_1\cdot a_2\cdots a_n=a_k$. Donde $G=\{a_1,a_2,\dots,a_n\}$
Como G es abeliano, podemos reordenar el producto $a_1\cdots a_n$ de la siguiente manera: $b_1\cdot b_2\cdot b_{3_2}\cdot b_4\cdot b_{5_4}\cdots b_{n-2}\cdot b_{{n-1}_{n-2}}\cdot b_n$

donde $b_1=e$, $b_n=a_k=a_k^{-1}$ (Puesto que $o(a_k)=2$) y tal que el inverso de cada elemento quede a continuación de éste, es decir, $b_{i_{i-1}} = (b_{i-1})^{-1}$ con $i = 3, \dots n$ y así:

$$a_1 . a_2 \dots a_n = \underbrace{b_1 . b_2}_{e} . \underbrace{b_{3_2} . b_4}_{e} . \underbrace{b_{5_4} \dots b_{n-2}}_{e} . \underbrace{b_{n-1_{n-2}} . b_n}_{e} = e . b_n$$
$$= a_k$$

TEOREMA DE WILSON:

Si $p$ es primo, entonces $(p-1)! \equiv -1$ mód $p$.

Dem:

Sea $\mathbb{Z}_p = \{[1]_p, [2]_p, \dots, [p-1]\}$, $\langle \mathbb{Z}_p^*, \cdot \rangle$ forma grupo abeliano finito.

Es fácil ver que $[p-1]_p^2 = [1]_p$, $[p-1]^2 = [p(p-2)+1]$ y así $o([p-1]_p) = 2$.

Veamos que este es el único elemento de $\mathbb{Z}_p^*$ cuyo orden es 2:

Supongamos que existe $x \in \mathbb{Z}_p^*$, $x \neq [p-1]$ y $x \neq [1]$ y tal que $o(x) = 2$.

Si $x \in \mathbb{Z}_p^*$, entonces $x = [a]_p$ para algún $a \in \mathbb{Z}$ y así $[a]_p^2 = [1]_p$

Por tanto $[a^2-1]_p = [0]_p$. Luego $p \mid (a^2-1)$, entonces $p \mid (a+1)(a-1)$

Si $(a+1, p) = 1$ entonces $p \mid (a-1)$. Por consiguiente $[a-1]_p = [0]_p$. Luego $[a]_p = [1]_p$, que es una contradicción.

Luego $[p-1]_p$ es el único elemento en $\mathbb{Z}_p^*$ tal que $o([p-1]_p) = 2$ y así, aplicando el lema 1 tenemos que:

$[1]_p . [2]_p \dots [p-1]_p = [p-1]_p$ entonces $[1.2.3 \dots (p-1)]_p = [p-1]_p$

pero $[p-1]_p = [-1]_p$ entonces $[(p-1)!]_p = [-1]_p$ luego $(p-1)! \equiv -1$ mód $p$.

LEMA 2: Si $(p,c) = 1$ y $\exists\, x, y \in \mathbb{Z}$ tales que $x^2+y^2 = cp$ entonces $p = a^2+b^2$ para algunos enteros $a, b$.

Omitimos la demostración de este lema (Ver Algebra Moderna, I.N. Herstein. pag 134)

LEMA 3: Si $p$ es un número primo de la forma $4n+1$ entonces puede resolverse la congruencia $x^2 \equiv -1$ mód $p$.

Dem:

Sea $x = 1.2 \dots (p-1)/2$ Como $p = 4n+1$ entonces $p-1 = 4n$ y por tanto, en este producto para la obtención de $x$ hay $2n$ elementos y así, por ser $x$ un número par, $x = (-1)(-2) \dots \left(-\frac{p-1}{2}\right)$

pero $p-k \equiv -k$ mód $p$ y $x^2 = 1.2 \dots \left(\frac{p-1}{2}\right).(-1)(-2) \dots \left(-\frac{p-1}{2}\right)$

entonces $x^2 = 1.2 \dots \left(\frac{p-1}{2}\right)(p-1).(p-2) \dots \left(p - \frac{p-1}{2}\right)$

$= 1.2 \dots \left(\frac{p-1}{2}\right).\left(\frac{p+1}{2}\right) \dots (p-2).(p-1) = 1.2 \dots (p-1)$

entonces $x^2 = (p-1)!$ pero por teorema de Wilson, $(p-1)! \equiv -1$ mod $p$

entonces $x^2 \equiv -1$ mód $p$.

## SEGUNDO TEOREMA DE FERMAT :

Si $p$ es un número primo de la forma $4n+1$; entonces $p=a^2+b^2$ para algunos enteros $a$ y $b$.

Dem:
Como $p=4n+1$ entonces $x^2 \equiv -1$ mód $p$ tiene solución, según el lema 3 demostrado anteriormente entonces $[x]^2=[x][x]=[-1]$, con $0 \leq x \leq p-1 \Rightarrow x^2 \leq (p-1)^2 \Rightarrow x^2 \leq p^2-2p+1$, entonces, $x^2+1 \leq p^2-2p+1 = p^2-2(p-1) \leq p^2$ pues $p-1>0$

Pero $x^2 \equiv -1$ mód $p$ entonces $p \mid x^2+1$. Luego $x^2+1=cp$ para algún $c \in \mathbb{Z}$ entonces $cp \leq p^2$ (ya que $x^2 \leq p^2-1$) $\Rightarrow c \leq p \Rightarrow (c,p)=1$

Y así, aplicando el lema 2, $\exists\, a,b \in \mathbb{Z} \mid p=a^2+b^2$

Bibliografía :

Herstein, I.N. Algebra moderna, editorial Trillas, Mexico 1974.

DEAN, Richard A. Elements of Abstract Algebra. Ed. John Wiley and sons, Inc, New York.

VINOGRADOV, Ivan M. Fundamentos de la teoría de números. ed. Mir, Moscu.