Automorfimos y la Función de Euler

Fernando Soto Agreda

1. LA FUNCION DE EULER

1.1 La función de Euler $\varphi : \mathbf{N} \to \mathbf{N}$ aplica a cada número natural n en el número de primos relativos con él no mayores que $n-1$.

Esta función posee un comportamiento extraño. Si p es un número primo $\varphi(p) = p-1$, si n es compuesto y $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ es su descomposición en factores primos se halla que $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$.

Por ejemplo: $\varphi(6) = 2$, $\varphi(8) = 4$, $\varphi(10) = 4$, $\varphi(12) = 4$,
$\varphi(20) = 8$, $\varphi(23) = 22$, $\varphi(26) = 12$, $\varphi(28) = 12$,
$\varphi(31) = 30$, $\varphi(33) = 20$, $\varphi(63) = 36$, $\varphi(65) = 48$.

1.2 Las imágenes de cada n bajo la función de Euler se consiguen usando este hermoso algoritmo y resultan impredecibles. He encontrado que infinitos números naturales $\varphi(n)$ poseen menor grado de impredecibilidad ya que se puede prefijar para ellos un divisor.

En efecto: si $s \in \mathbf{N}$ y $m \in \mathbf{N}$ ocurre que

$$s \mid \varphi(m^s - 1) \quad \text{y} \quad 2s \mid \varphi(m^s + 1)$$

Por ejemplo: $3 \mid \varphi(3^3-1)$, $6 \mid \varphi(3^3+1)$, $5 \mid \varphi(2^5-1)$, $10 \mid \varphi(2^5+1)$

El camino para comprobar este resultado de la teoría de números atraviesa la teoria de grupos.

1.3 La función de Euler posee carácter multiplicativo ya que $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

La función de Euler pertenece a las funciones de N en N que preservan la estructura de semigrupo $(N, \cdot)$, sinembargo debe restringirse el dominio a $N - \{1\}$ ya que $\varphi(1) = 0$ y se ha tomado $N = \{1, 2, 3, \ldots\}$. φ es un endomorfismo de la estructura $(N, \cdot)$.

1.4 ENDOMORFISMOS. Una función $f:(G, *) \to (\overline{G}, \cdot)$ se llama *homomorfismo* entre los monoides $(G, *)$ y $(G, \cdot)$ si para cada $a \in G$, $b \in G$, $f(a * b) = f(a) \cdot f(b)$.

Cuando las dos estructuras son semigrupos con identidad e y $\overline{e}$ respectivamente y siendo $f(G) = \left\{f(g) \mid g \in G\right\}$ y $f^{-1}(\overline{g}) = \left\{x \in G \mid f(x) = \overline{g}\right\}$ es fácil demostrar como $\left(f^{-1}(\overline{e}), *\right)$ es subsemigrupo de $(G, *)$.

Para un semigrupo con identidad $(G, *, e)$ el conjunto $\mathcal{U}(G)$ conformado por todos los elementos inversibles de la estructura construyen el grupo $(\mathcal{U}(G), *)$.

Cuando $(G, *) = (\overline{G}, \cdot)$ cada homomorfismo se llama endomorfismo. $\mathrm{End}(G, *) = \left\{f : G \to G \mid f \text{ es homomorfismo}\right\}$. La estructura $(\mathrm{End}(g, *), \circ)$ es un semigrupo con identidad y por lo expuesto anteriormente sus elementos inversibles. $\mathcal{U}(\mathrm{End}(G, *))$ conforma el grupo de los automorfismos de $(G, *)$ $(\mathrm{Aut}(G, *), \circ)$.

1.4.1 Por ejemplo, la estructura $(N, +)$ posee carácter cíclico y su generador es 1. Sus endomorfismos se construyen con solo señalar la imagen de 1.

En efecto, si $f(1) = a$ con $a \in N$, $f(2) = f(1 + 1) = f(1) + f(1) = 2f(1) = 2a$, $f(3) = f(2) + f(1) = 2f(1) + f(1) = 2a + a = 3a$ y en general $f(n) = na$. Se observa como $f(n + m) = (n + m)a = na + ma = f(n) + f(m)$.

Esto demuestra como los únicos endomorfismo posibles en $(N, +)$ son de la

forma $f_n(1) = n$, es decir $f_n(a) = na$ para todo $a \in \mathbb{N}$ y cada natural n define un endomorfismo. Al tomar f_n y f_m en $\mathrm{End}(\mathbb{N}, +)$ vemos como

$$(f_n \circ f_m)(a) = f_{nm}(a) \text{ para todo } a \in \mathbb{N}.$$

Los dos últimos resultados demuestran como la aplicación

$$g : (\mathbb{N}, \cdot) \to \left(\mathrm{End}(\mathbb{N}, +), \circ\right) \text{ tal que } g(n) = f_n$$

es un homomorfismo de semigrupos sobreyectivo y como $g(n) = g(m)$ implica que $n = m$, g es biyección. g se llama isomorfimo entre las estructuras; se dice que ellas son isomorfas y se escribe $(\mathbb{N}, \cdot) \approx (\mathrm{End}(\mathbb{N}, +), \circ)$. En general $(G, *) \approx (\overline{G}, \cdot)$ si existe un homomorfismo biyectivo entre ellas.

Dos estructuras isomorfas son indistinguibles entre sí, salvo por el nombre de sus elementos. Por ejemplo, el isomorfismo entre $(\mathbb{N}, \cdot)$ y $(\mathrm{End}(\mathbb{N}, +), \circ)$ asegura como el único elemento inversible en $(\mathrm{End}(\mathbb{N}, +), \circ)$ es $g(1) = f_1$ que no es otra que la función idéntica.

2. ENDOMORFISMOS DE GRUPOS CICLICOS

Generalizamos aquí el ejemplo del parágrafo 1.4.1. Los grupos cíclicos $(G, *)$, $G = \left\{a^r \mid a \in G, r \in \mathbb{Z}\right\}$, facilitan la construcción de endomorfismos; para el caso cada uno de ellos se obtiene con solo definir la imagen de un generador a de G:

$$\mathrm{End}(G, *) = \left\{f_m : G \to G \mid f_m(a^r) = a^{rm}, m \in \mathbb{Z}\right\}$$

Es fácil demostrar que los f_m, $m \in \mathbb{Z}$ son los únicos endomorfismos posibles en un grupo cíclico $(G, *)$.

Son conocidos los siguientes hechos: todo grupo cíclico infinito es isomorfo a $(\mathbb{Z}, +)$, todo grupo cíclico finito de orden n es isomorfo a $(\mathbb{Z}_n, +)$, todo subgrupo de $(\mathbb{Z}, +)$ es de la forma $(n\mathbb{Z}, +)$ con $n \in \mathbb{N}$, así que:

2.1 $f_m \circ f_n = f_{nm}$

2.2 Si G es infinito $f_m = f_n$ si y solo si $m = n$

2.3 Si G es finito de orden u; $f_m = f_n$ siempre que $m = nu$.

Igual que en el ejemplo 1.4.1 encontramos que

$$\Big(\mathrm{End}(\mathbf{Z}, +), \circ\Big) \approx (\mathbf{Z}, \cdot) \text{ y } \Big(\mathrm{Aut}(\mathbf{Z}, +), \circ\Big) \approx (\{-1, 1\}, \cdot)$$

$$\text{y } \Big(\mathrm{End}(\mathbf{Z}_n, +), \circ\Big) \approx (\mathbf{Z}_n, \cdot) \text{ y } \Big(\mathrm{Aut}(\mathbf{Z}_n, +), \circ\Big) \approx (\mathcal{U}(\mathbf{Z}_n), \cdot)$$

Recordemos que $\mathcal{U}(\mathbf{Z}_n)$ es el conjunto de todos los primos relativos con n menores que él y por lo tanto el número u orden de los automorfismos de $(\mathbf{Z}_n, +)$ está dado por $\varphi(n)$. Es válido que $a \in \mathcal{U}(\mathbf{Z}_n)$ ssi $a \equiv 1(\mathrm{Mód}\, n)$.

3. EL TEOREMA DE LAGRANGE

Simplemente mencionamos este fabuloso resultado de la teoría de grupos. Si $(G, *)$ es un grupo finito de orden n y $(H, *)$ es subgrupo de G de orden m, entonces m es un divisor de n.

4. EL RESULTADO

4.1 Resulta obvio como $m^s \equiv 1(\mathrm{Mód}(m^s - 1))$, como m^s y $m^s - 1$ son primos entre sí y por ende m y $m^s - 1$ también. De modo que $m \in \mathcal{U}(\mathbf{Z}_{m^s-1})$ y por ende la función $f_m(a) = ma$ para cada $a \in \mathbf{Z}_{m^s-1}$ define sobre $(\mathbf{Z}_{m^s-1}, +)$ un automorfismo.

f_m es un automorfismo de orden s. Así, el subgrupo generado por f_m, $(\langle f_m \rangle, \circ)$ de $\Big(\mathrm{Aut}(\mathbf{Z}_{m^s-1}, +), \circ\Big)$ tiene exactamente s elementos.

En efecto $f_m^s(a) = m^s a = a$ para cada $a \in \mathbf{Z}_{m^s-1}$ ya que $m^s \equiv 1(\mathrm{Mód}\mathbf{Z}_{m^s-1})$ siendo s el menor entero positivo que logra esta congruencia.

Como el orden de $\mathrm{Aut}(\mathbb{Z}_{m^s-1}, +)$ está dado por el valor $\varphi(m^s-1)$ y utilizando el teorema de Lagrange vemos como

$$s \mid \varphi(m^s-1)$$

4.2 Nuevamente $m^s \equiv -1 (\mathrm{Mód}(m^s+1))$ y m y m^s+1 son primos entre sí. $(\langle f_m \rangle, \circ)$ es subgrupo de $\left(\mathrm{Aut}(\mathbb{Z}_{m^s+1}, +), \circ\right)$ de orden $2s$ de donde se concluye que

$$2s \mid \varphi(m^s+1)$$

Si antes teníamos temor de asegurar como, por ejemplo el 17 divide a x o y número, ahora podemos decir que 17 divide a $\varphi(2^{17}-1)$, a $\varphi(3^{17}-1)$, a $\varphi(3^{34}-1)$, etc., con la incertidumbre de no conocer de antemano estos valores de Euler.

5. EPILOGO

Es conocido que un natural p es primo si y solo si $\varphi(p) = p-1$. Si suponemos que m^s-1 es primo encontramos que $\varphi(m^s-1) = m^s-2$ y de acuerdo con el resultado desarrollado en este artículo vemos que $s \mid m^s-2$ necesariamente.

Esto demuestra como, si $s \nmid m^s-2$ entonces m^s-1 es un no primo, resultado que se constituye en examen para primos. Del mismo modo se comprueba que si $2s \nmid m^s$ entonces m^s+1 no es primo.

Por ejemplo: $4 \nmid 2^4-2$ lo que indica como $2^4-1 = 15$ no es primo;

$6 \nmid 4^3$ luego 65 no es primo;

$14 \nmid 6^7$, así $6^7+1 = 27937$ no es primo;

$34 \nmid 2^{17}$ y por ende $2^{17}+1 = 131073$ tampoco es primo.

Por el contrario, si $s \mid_{m^s - 2}$ o $2s \mid_{m^s}$ no puede asegurarse que $m^s - 1$ o $m^s + 1$ sean primos, pero es más probable que así sea.

Por ejemplo: $3 \mid_{8^3 - 2}$ pero $8^3 - 1 = 511$ no es primo;

$8 \mid_{2^4}$ pero $2^4 + 1 = 65$ no es primo;

$16 \mid_{2^8}$ y $2^8 + 1$ es primo;

$8 \mid_{6^4}$ y $6^4 + 1 = 1297$ también es primo.

BIBLIOGRAFIA

[1] A.A. KARATSUBA. Fundamentos de la Teoría Analítica de los Números. Moscú. Editorial Mir. 1979.

[2] I. VINOGRADOV. Fundamentos de la Teoría de los Números. Moscú. Editorial Mir. 1977.

[3] MUTAFIAN. Generalidades y Grupos. París. 1979.

DEPTO. DE MATEMATICAS Y ESTADISTICA
UNIVERSIDAD DE NARIÑO
PASTO (N).