Miscelánea Matemática **22**, *37–49 (1995)*

Geometría de iteraciones numéricas

Alfinio Flores Peñafiel
Arizona State University
Tempe, Arizona

Resúmen

Simples iteraciones numéricas dan lugar a interesantes patrones geométricos, en los que los alumnnos descubren intrigantes relaciones numéricas. La aritmética del reloj nos sirve para entender estas relaciones. Además, sorprendentemente, al iterar funciones distintas tales como $x \to x^2 \pmod{p}$, y $x \to 2x \pmod{p-1}$, se obtienen esencialmente las mismas figuras si p es primo. Un isomorfismo entre grupos cíclicos sirve para explicar por qué los diagramas tienen las misma forma.

Introducción

El resultado de iterar funciones numéricas tales como $x \to x^2 \pmod{n}$ puede ser representado mediante patrones geométricos. Muchas veces estos diagramas tiene formas bellas, por ejemplo, Dewdney (1988) presenta diagramas de iteraciones de la función $x \to x^2 \pmod{n}$ para $n = 100$. Las cadenas de números se pueden obtener utilizando una calculadora o, si los números son grandes, mediante un programa de cómputo. Para ciertos valores de n, los alumnos pueden descubrir semejanzas sorprendentes en los diagramas de

funciones distintas. Aquí se exploran los diagramas correspondientes a las iteraciones de dos funciones, $x \to x^2 \pmod p$, y $x \to 2x \pmod{p-1}$.

1 La iteración de $x \to x^2 \pmod p$.

Sea p un número primo. Se itera la función $x \to x^2 \pmod p$. Es decir, se toma un número menor que p, se eleva al cuadrado, se divide entre p y nos quedamos con el residuo, o sea lo reducimos módulo p, y el resultado se vuelve a someter al mismo proceso. Continuamos iterando hasta que obtengamos un número que ya haya aparecido. Empezamos con un nuevo número y repetimos el proceso, y así hasta agotar las posibilidades.

Ejemplo 1.1. Sea $p = 17$. Las cadenas de números son

$0 \to 0$ $1 \to 1$ $2 \to 4 \to 16 \to 1$ $3 \to 9 \to 13 \to 16$
$5 \to 8 \to 13$ $6 \to 2$ $7 \to 15 \to 4$ $10 \to 15$
$11 \to 2$ $12 \to 8$ $14 \to 9$

Podemos ahora asociar a este proceso una gráfica en donde el 1 es un gran atractor y el 0 forma un ciclo por sí mismo. Nótese que la suma de dos números que confluyen al mismo punto, por ejemplo los extremos de ramas adyacentes, es 17.

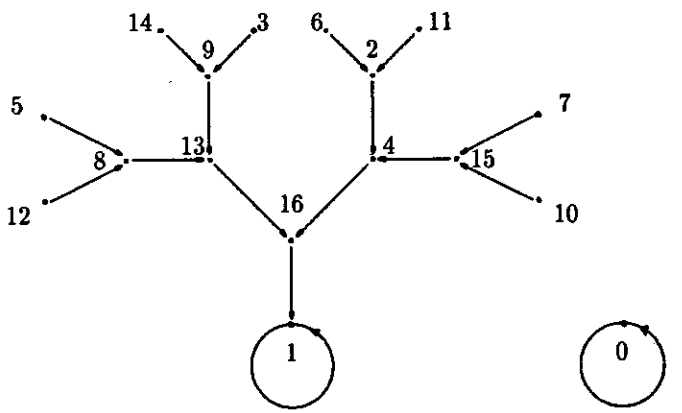

Figura 1. Iteración de $x \to x^2 \pmod{17}$

Ejemplo 1.2. Sea $p = 13$. Procediendo igual que antes, esta vez el diagrama obtenido está compuesto de tres partes. Hay tres atractores, donde uno de ellos forma un ciclo de dos elementos ($3 \leftrightarrow 9$). Aquí la suma de dos números que confluyen al mismo punto es 13.

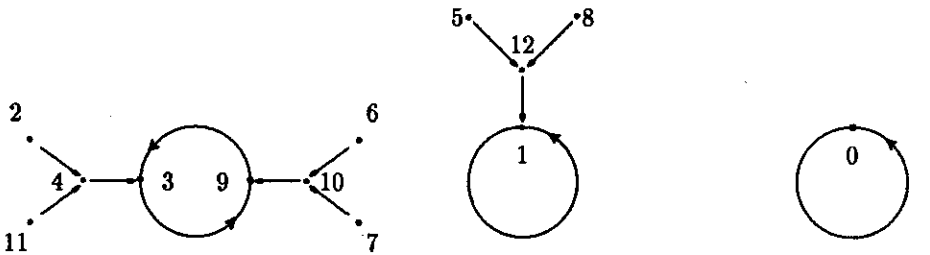

Figura 2. Iteración de $x \to x^2 \pmod{13}$

1.3 Explicando un descubrimiento. En la figura 1, dos números que confluyen al mismo punto suman 17 (el módulo), y en la figura 2 los números suman 13 (el módulo). Podemos ver por qué esto tiene que ser así usando la aritmética del reloj (aritmética modular). Al conservar el residuo al dividir entre 17, tenemos esencialmente la misma situación que en un reloj, pero con 17 *horas*..

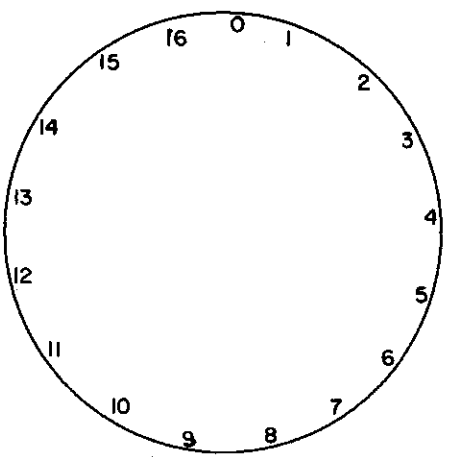

Figura 3. Un reloj con 17 horas

Podemos sumar los números en el *reloj*, por ejmplo, $3+5=8$, $9+14=6$, $11+6=0$. Los números que suman 17, en esta aritmética son inversos aditivos, por ejemplo $4+13=0$, de modo que $13=-4$. Al escribir 13 como -4 se ve claro por qué 4 y 13 tienen el mismo cuadrado, por lo que el en el diagrama confluyen al mismo número.

2 La iteración de $x \to 2x \pmod{p-1}$.

Sea p un número primo. Se itera la función $x \to 2x \pmod{p-1}$. Es decir, se toma un número menor que $p-1$, se multiplica por 2, se divide entre $(p-1)$ y nos quedamos con el residuo, o sea lo reducimos $\pmod{p-1}$, y el resultado se vuelve a someter al mismo proceso. Continuamos iterando hasta que aparezca un número que ya haya salido. Empezamos con un nuevo número y repetimos el proceso, y así hasta agotar los números menores que $p-1$.

Ejemplo 2.1. Sea $p=17$. La cadena de números es:

$0 \to 0$	$14 \to 12 \to 8 \to 0$	$1 \to 2 \to 4 \to 8$	
$5 \to 10 \to 4$	$15 \to 14$	$11 \to 6 \to 12$	$3 \to 6$
$7 \to 14$	$13 \to 10$	$9 \to 12$	

Podemos ahora asociar a este proceso una gráfica, en donde el 0 es un gran atractor.

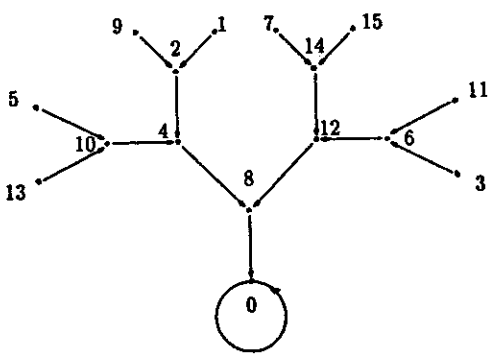

Figura 4. Iteración de $x \to 2x \pmod{16}$

Observa que todos los números impares están en los extremos de las ramas, en el siguiente nivel los números de la forma $2m$, donde m es un impar, luego los de la forma 2^2m, etc. Nota que la diferencia entre los números que confluyen al mismo punto, por ejemplo en ramas adyacentes, es siempre 8, la mitad del módulo.

Ejemplo 2.2. Sea $p = 13$. Itera la función $x \to 2x \pmod{12}$. La gráfica en este caso es

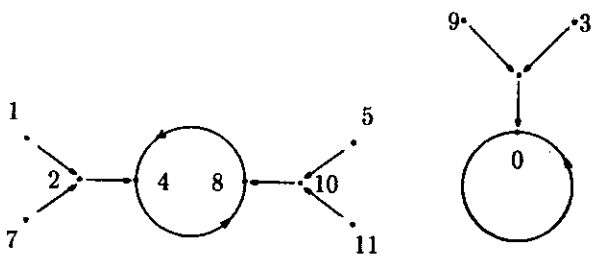

Figura 5. Iteración de $x \to 2x \pmod{12}$

En este caso, la diferencia entre dos números que confluyen al mismo punto es 6, la mitad del módulo.

2.3 Explicando otro descubrimiento. Vimos en las figuras 4 y 5 que la diferencia entre números en los extremos de ramas adyacentes es la mitad del módulo. Considera un *reloj* con 16 horas. Los números que difieren en 8, estan separados exactamente por media circunferencia. Al multiplicarlos por 2, la diferencia será una circunferencia completa, es decir, los resultados coincidirán.

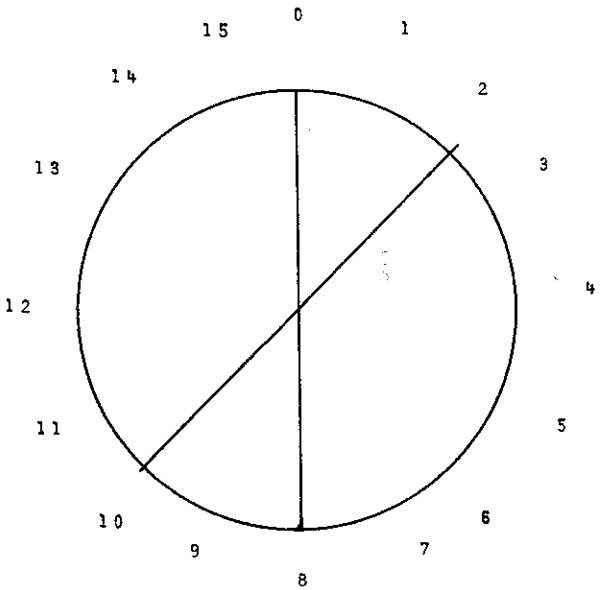

Figura 6. Multiplicando por 2 (mod 16)

3 Una semejanza sorprendente de diagramas.

Compara la gráfica de 1.1 con la de 2.1, y la de 1.2 con la de 2.2. Las gráficas son idénticas para las iteraciones de $x \to x^2 \pmod{p}$ y para las iteraciones de $x \to 2x \pmod{p-1}$, excepto por el atractor extra (0) en $\pmod{p}$. La explicación de por qué los diagramas son esencialmente iguales la podemos obtener analizando la estructura de $\{1, 2, 3, \ldots, p-1\}$, con la multiplicación $\pmod{p}$, y la de $\{0, 1, 2, \ldots, p-2\}$, con la suma $\pmod{p-1}$.

3.4.1 Isomorfismo de grupos. El conjunto $\{1, 2, 3, \ldots, 16\}$ con la multiplicación $\pmod{17}$ es un grupo, ya que la multiplicación $\pmod{17}$

satisface las siguientes condiciones: la operación es asociativa, el resultado de operar dos elementos está en el mismo conjunto, existe un elemento idéntico (el 1), cada uno de los elementos tiene un inverso multiplicativo (ésta es la razón por la que en esta discusión dejamos fuera el 0). Se trata además de un grupo cíclico, es decir, un grupo generado por uno de sus elementos: 3 es un generador en $\{1, 2, 3, \ldots, 16\}$ con la multiplicación (mod 17), ya que las potencias sucesivas de 3, reducidas módulo 17, nos dan $1, 3, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6$.

Por otro lado, el conjunto $\{0, 1, 2, \ldots, 15\}$ con la adición (mod 16) es también un grupo cíclico: sumando 1 (mod 16) ,sucesivamente obtenemos todos los elementos de $\{0, 1, 2, \ldots, 15\}$, es decir, 1 es un generador. Dos grupos cíclicos con el mismo número de elementos son isomorfos. Un isomorfismo puede ser dado mediante un generador de cada grupo. La correspondencia entre los grupos está dada explícitamente por

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Dicho sea de paso, esta correspondencia fue utilizada por el joven Gauss para demostrar que el polígono regular de 17 lados se puede construir con regla y compás (Gindikin, 1988). Nota que los números en la fila de arriba se comportan como los *logaritmos* de los números en la fila de abajo. Para multiplicar dos números en la fila de abajo, basta sumar los números correspondientes en la de arriba, y leer el resultado debajo de la suma. Por ejemplo, para multiplicar 15×16, podemos sumar sus imágenes $6 + 8$, el resultado de la multiplicación, 2 está debajo de 14. Esto se puede hacer con cualesquiera dos números, lo cual es evidente si se expresan los números de abajo como potencias de 3. Que la correspondencia sea un isomorfismo de grupos, quiere decir que se preservan las operaciones, $f(a \times b) = f(a) + f(b)$, el elemento idéntico multiplicativo corresponde al idéntico aditivo, $f(1) = 0$, y los inversos de los números también se corresponden, $f(a^{-1}) = -f(a)$.

En particular, si n corresponde a m, el número correspondiente a $n \times n$ es $m + m$, es decir, el número correspondiente a m^2 es $2n$.

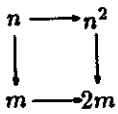

Figura 7. Elementos y funciones correspondientes

Esto explica por qué los diagramas para las iteraciones de la función $x \to x^2 \pmod p$ y de la función $x \to 2x \pmod{p-1}$ son idénticos. Nota que los elementos correspondientes mediante el isomorfismo tiene el mismo papel en los dos diagramas.

Ejercicio. Muestra explícitamente un isomorfismo entre los grupos $\{0, 1, 2, \ldots, 11\}$, con la suma $\pmod{12}$ y $\{1, 2, 3, \ldots, 12\}$ con la multiplicación $\pmod{13}$. Observa como elementos correspondientes tienen papeles equivalentes en los diagramas.

Ejercicio. Demuestra que dos números que sumen 17 tienen el mismo cuadrado $\pmod{17}$. Por ejemplo, $13 \times 13 = 4 \times 4 \pmod{17}$, ya que $13 = 16 \times 4 \pmod{17}$, $16 \times 16 = 1 \pmod{17}$.

Ejercicio. Muestra que el descubrimiento de la sección 2.3 es *equivalente* al descubrimiento de la sección 1.3. Sugerencia: $4 = 8 * 12 \pmod{16}$, $8 + 8 = 0 \pmod{16}$.

¿Qué pasa si n no es primo? ¿Qué sucede con los diagramas correspondientes a $x \to x^2 \pmod n$ y a $x \to 2x \pmod{n-1}$ si n no es primo? Si n no es primo, entonces el conjunto $\{1, 2, 3, \ldots, n-1\}$, con la multiplicación $\pmod n$ no es un grupo (¿por qué?). Sin embargo $\{0, 1, 2, \ldots, n-2\}$, con la suma $\pmod{n-1}$ sí es un grupo cíclico. Los diagramas para las iteraciones

pueden ser muy distintos, ya que no hay la misma estructura subyacente.

Ejemplo 3.3. Si $n = 9$, el diagrama para $x \to 2x \pmod 8$ es un árbol,

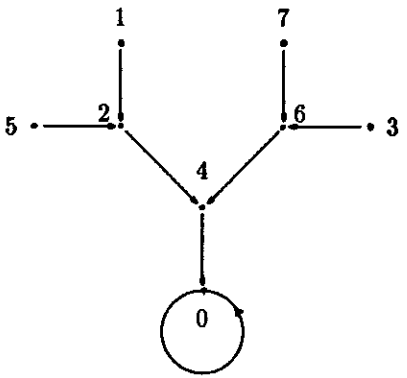

Figura 8. Iteración de $x \to x^2 \pmod 8$

en cambio, la forma del diagrma para $x \to x^2 \pmod 9$ es muy distinta.

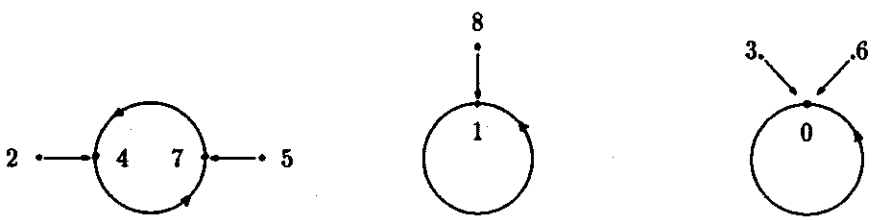

Figura 9. Iteración de $x \to x^2 \pmod 9$

4 Extensiones.

Si p es primo, los diagramas obtenidos de iterar $x \to x^3 \pmod p$ y $x \to 3x \pmod{p-1}$ serán idénticos (excepto por el atractor 0 en el primer caso). Esto queda muy claro si observamos que si n corresponde a m, entonces $n \times n \times n$

(mod p) corresponde a $m+m+m \pmod{p-1}$. En general, si p es primo, los diagramas correspondientes a las iteraciones de $x \to x^k \pmod{p}$, y de $x \to kx \pmod{p-1}$ son idénticos, por la correspondencia de $n \times n \times \cdots \times n$ (k veces) con $m+m+\cdots+m$ (k veces).

Ejemplo 4.1. Itera la función $x \to x^3 \pmod{7}$. El diagrama consta de 3 partes. Los atractores son $1, 6, 0$.

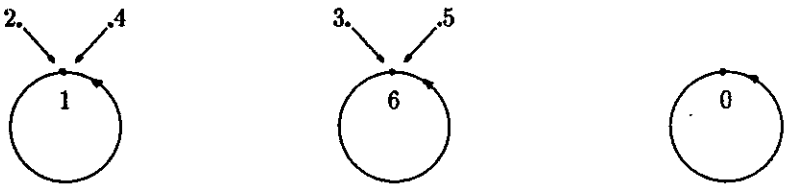

Figura 10. Iteración de $x \to x^3 \pmod{7}$

Ejemplo 4.2. Itera la función $x \to 3x \pmod{6}$. El diagrama consta de dos partes, y los atractores son 0 y 3.

Figura 11. Iteración de $x \to 3x \pmod{6}$

Un isomorfismo entre los grupos, se puede dar asociando el generador 1 de $\{0,1,2,3,4,5\}$, con la suma (mod 6) con el generador 5 de $\{1,2,3,4,5,6\}$, con la multiplicación (mod 7).

$$\begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 1 & 5 & 4 & 6 & 2 & 3 \end{array}$$

Ejercicio. Al multiplicar el número 142857 por cada uno de los números $1, 5, 4, 6, 2, 3$ obtenemos los mismos dígitos que al principio sólo que desplazados cíclicamente hacia la derecha $0, 1, 2, 3, 4, 5$, lugares. Relaciona esto con el isomorfismo.

Ejemplo 4.3. ¿Cuál es la forma del diagrama para la función $x \to x^2 \pmod{p}$, si p es un primo de Fermat? El diagrama para $x \to x^2 \pmod{257}$ será idéntico al de la función $x \to 2x \pmod{256}$, ya que 257 es un primo de Fermat, es decir de la forma

$$p = 2^{2^k} + 1 .$$

En este caso, como 256 es una potencia de 2, el diagrama que se obtiene también tiene la forma de un árbol binario. Se muestran aquí el gran atractor 0, algunos de los principales nodos intermedios, y algunos valores en los extremos de las ramas. Todos los números impares están en los extremos de las ramas. En cada nivel sucesivo, los nodos son múltiplos impares de potencias crecientes de 2.

En general, si $p - 1$ es una potencia de 2, el diagrama para $x \to 2x \pmod{p-1}$ es un árbol binario. De modo que el diagrama para $x \to x^2 \pmod{p}$, si p es un primo de Fermat, también es un árbol binario.

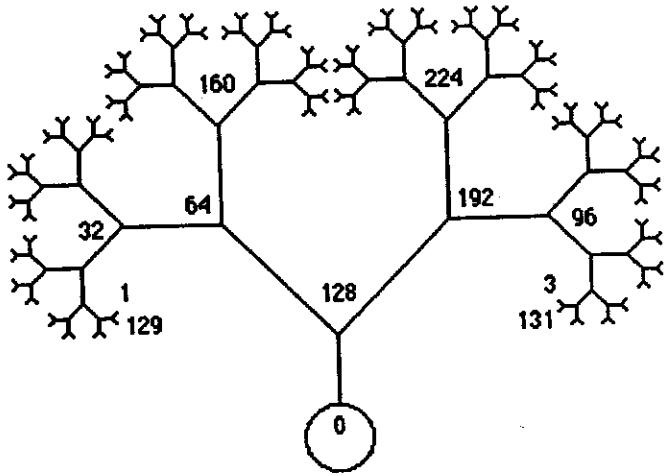

Figura 12. Iteración de $x \to 2x \pmod{256}$

Conclusión.

Representar la iteración de una función numérica, mediante una figura geométrica es una herramienta poderosa en matemáticas, y resulta atractivo para los alumnos. Los alumnos se sorprenden al encontrar los mismos diagramas al iterar dos funciones distintas, x^2 y $2x$. La idea de grupos con la misma estructura sirve para explicar el parecido entre los diagramas. Los alumnos tienen así, la oportunidad de conectar ideas de tres grandes campos de las matemáticas, relacionando la iteración de funciones numéricas, con figuras geométricas y con ideas básicas de álgebra.

Bibliografía

[1] Dewdney, A.K. *The armchair universe.* Freeman, 1988.

[2] Gindikin, S. G. *Tales of mathematicians and physicists.* Boston. Birkhauser, 1988.