NUMEROS. 22 - 1992
S.C.P.M. "ISAAC NEWTON"

NUMEROS CIRCULARES:
Estudio algebraico y algorítmico

VICTOR ARENZANA HERNÁNDEZ
VICENTE TRIGO ARANDA

Los números circulares tienen una antigua tradición en el campo de la aritmética. El matemático español Juan Pérez de Moya (fl. 1554-1573) los recogió en su *Arithmética* como unos números que tenían la notable propiedad de quedar reproducidos en las últimas cifras de sus sucesivas potencias. Dada la difusión que tuvo la obra, hasta 1875 llegó a alcanzar treinta ediciones, los números circulares eran conocidos por buena parte de los estudiosos de las matemáticas en España. Sin embargo, debido a la laboriosidad que conllevaban los cálculos su análisis detallado fue dejado de lado.

Como ocurre con muchas cuestiones de la teoría de números, a las que en principio no se les llega a ver una utilidad práctica fuera del campo de la matemática especulativa, el tema de los números circulares quedó relegado al campo de las curiosidades numéricas. Así, Martin Gardner en su libro *Los mágicos números del Doctor Matrix* recoge el tema de los números circulares y expone algunas propiedades de los mismos, asignándoles el nombre de números automórficos.

Nos ha parecido interesante estudiar detenidamente la generación de números circulares y una serie de propiedades de forma sistemática en base 10, ampliando el estudio a otros sistemas de numeración.

1.- EXISTENCIA Y PRIMERAS PROPIEDADES

Definición: Un número natural α, no nulo y distinto de la unidad, de n cifras se dice **circular** cuando las n últimas cifras de todas sus potencias conforman el número α.

Proposición 1ª: Un número α de n cifras es circular si y sólo si se cumple cualquiera de las tres condiciones siguientes, equivalentes entre sí:

a) las n últimas cifras de α^2 forman el número α.
b) el cociente $(\alpha^2-\alpha)/10^n$ es un número natural.
c) $\alpha(\alpha-1)$ es múltiplo de 10^n

Demostración: Evidentemente si α es circular se cumple la condición a). Veamos el recíproco:

Si se cumple que α^2 termina en α, podemos escribir que:

$$\alpha^2 = x\cdot 10^n + \alpha$$

y, por consiguiente, se cumple:

$$\alpha^3 = \alpha\cdot x\cdot 10^n + \alpha^2$$

y, como α^2 termina en α y el primer sumando de la igualdad anterior no influye en las cifras finales, se cumple:

$$\alpha^3 = y\cdot 10^n + \alpha$$

luego α^3 finaliza en α. Reiterando el proceso se prueba para cualquier potencia natural de α.

Las condiciones b) y c) son trivialmente equivalentes a a).

Ejemplos: Los números que se muestran en la columna de la izquierda son todos ellos circulares, ya que su cuadrado finaliza en ellos mismos.

Número	Cuadrado
25	625
76	5776
625	390625
376	141376
0625	390625
9376	87909376

Obsérvese en la tabla anterior (número 0625) que la primera cifra de un número circular puede ser cero.

Proposición 2ª: La cifra de las unidades de un número circular ha de ser necesariamente 5 o 6.

Demostración: Los únicos dígitos que elevados al cuadrado finalizan en ellos mismos son 0, 1, 5 y 6. Veamos que las dos primeras opciones (finalizar en 0 o 1) no son válidas.

a) Imposibilidad de que un número circular termine en cero:

Si un número α de n cifras termina en m ceros su cuadrado terminará en 2m ceros; por consiguiente, las n últimas cifras de α^2 no coincidirán nunca con α. Por tanto, α no será circular.

b) Imposibilidad de que un número circular termine en uno:

Si un número α terminara en las cifras $\sigma 1$ su cuadrado tendría por cifra de las decenas (2σ mod 10) y por cifra de las unidades 1. Y como (2σ mod 10) nunca puede ser σ, α^2 no tendría la misma terminación que α y, por tanto, α no será circular.

Como en los ejemplos ya se ha comprobado que existen números circulares acabados en cinco y en seis queda probada la proposición.

Proposición 3ª: Si α es un número circular de n cifras, también es circular el número $\beta = 10^n - \alpha + 1$.

Demostración: De acuerdo con la Proposición 1ª, basta probar que $(\beta^2 - \beta)/10^n$ es un número natural.

$$(\beta^2 - \beta)/10^n = [(1 + 10^n - \alpha)^2 - (1 + 10^n - \alpha)]/10^n =$$
$$= [10^{2n} + 10^n + \alpha^2 - \alpha - 2\alpha \cdot 10^n]/10^n = [\alpha^2 - \alpha]/10^n + 10^n + 1 - 2\alpha$$

Como $[\alpha^2 - \alpha]/10^n$ es un número natural y $10^n + 1 - 2\alpha$ es, con toda seguridad un número entero, se sigue que $[\beta^2 - \beta]/10^n$ será también un número entero, pero como es positivo, ya que lo son su numerador y su denominador, será un número natural. Por consiguiente β será un número circular.

Consecuencia:

Según la proposición anterior se ha probado que los números circulares van siempre por parejas y, (por la proposición 2ª) uno finaliza en 5 y el otro en 6. Así, para encontrar la pareja de un número circular finalizado en 5 (6) bastará con cambiar la última cifra por 6 (5) y colocar en cada posición 9 menos la cifra del mismo lugar del número dado.

De este forma, sabiendo que el número 8.212.890.625 es circular se deduce que también es circular el número 1.787.109.376

Proposición 4ª: Sean α y β dos números circulares de n cifras finalizados en 5 y 6, respectivamente. Se tiene:

a) α divisible por 5^n
b) α-1 divisible por 2^n
c) β divisible por 2^n
d) β-1 divisible por 5^n
e) $\alpha \cdot \beta$ termina en n ceros.

Demostración: Como $\alpha \cdot (\alpha-1) = x \cdot 10^n$ y α acaba en cinco, es evidente que α-1 acabará en cuatro, por consiguiente α-1 aportará los factores pares, y, por ende, las potencias de dos, que serán, por lo menos, 2^n del producto. Del mismo modo, las potencias de cinco solamente pueden ser aportadas al producto por α y serán, al menos, 5^n. Lo que prueba a) y b).

Los apartados c) y d) son análogos; e) se deduce de a) y c).

2.- RESULTADOS RELATIVOS A SU UNICIDAD

Proposición 5ª: Si α es un número circular, al suprimir su primera cifra de la izquierda resulta un número también circular.

Demostración:

Si $\alpha = a_n a_{n-1} a_{n-2} \ldots\ldots a_0$, también se puede escribir en la forma

$$\alpha = a_n \cdot 10^n + a_{n-1} a_{n-2} \ldots\ldots a_0 = a_n \cdot 10^n + \delta$$

Vamos a probar que $\delta = a_{n-1} a_{n-2} \ldots\ldots a_0$ es un circular.

Como α es circular α^2 debe acabar en $a_n a_{n-1} a_{n-2} \ldots\ldots a_0$, es decir:

$$\alpha^2 = a^2_n \cdot 10^{2n} + 2 \cdot a_n \cdot \delta \cdot 10^n + \delta^2$$

finaliza en $a_n a_{n-1} a_{n-2} \ldots\ldots a_0$

Como la suma $a^2_n \cdot 10^{2n} + 2 \cdot a_n \cdot \delta \cdot 10^n$ no afecta a las n cifras de la derecha (ya que acaba en n ceros como mínimo), es evidente que δ^2 acabará en $a_{n-1} a_{n-2} \ldots\ldots a_0$, que es precisamente δ. Por tanto δ es un número circular.

Proposición 6ª: Sea un número circular de n cifras terminado en 6

$$\alpha = a_{n-1} a_{n-2} \ldots\ldots a_0$$

Existe una única cifra, σ , que hace que $N = \sigma a_{n-1} a_{n-2} \ldots\ldots a_0$ sea un número circular.

Demostración: Podemos escribir abreviadamente

$$N = \sigma \cdot 10^n + \alpha$$

Para que N sea circular ha de cumplir que $[N^2 - N]/10^{n+1}$ sea un número natural.

$$[N^2 - N]/10^{n+1} = [\sigma^2 \cdot 10^{2n} + \alpha^2 + 2 \cdot \alpha \cdot \sigma \cdot 10^n - \sigma \cdot 10^n - \alpha]/10^{n+1} =$$
$$= \sigma^2 \cdot 10^{n-1} + [2 \cdot \alpha \cdot \sigma - \sigma]/10 + [\alpha^2 - \alpha]/10^{n+1}$$

Para que esta expresión sea un número natural es preciso que lo sea

$$[2 \cdot \alpha \cdot \sigma - \sigma]/10 + [\alpha^2 - \alpha]/10^{n+1}$$

y para ello que

$$\sigma \cdot (2\alpha - 1) \pmod{10} + [\alpha^2 - \alpha]/10^n \pmod{10} = 10$$

Si α acaba en seis la igualdad anterior se transforma, teniendo en cuenta que $2\alpha - 1$ acaba en 1 y que σ es una cifra y, por tanto, menor que 10, en:

$$\sigma + [\alpha^2 - \alpha]/10^n \pmod{10} = 10$$

Equivalentemente:

$$\sigma = 10 - [\alpha^2 - \alpha]/10^n \pmod{10}$$

Lo que prueba que la cifra σ existe y es única.

Del mismo modo puede probarse la existencia de una sola cifra que añadida a la izquierda de un número circular acabado en cinco resulte otro número circular. Dado el principio de complementariedad probado en la proposición 3ª, se deduce inmediatamente que la cifra σ que se debe añadir cuando el número circular acaba en 5 será:

$$\sigma = [\alpha^2 - \alpha]/10^n \pmod{10}$$

Consecuencia:

Hasta ahora se ha probado que los números circulares van siempre por parejas y que no existen dos números circulares de n cifras que finalicen en el mismo dígito. De esta forma, dado un número circular de n cifras se conocen trivialmente todos los circulares inferiores a él. Así, sabiendo que 8.212.890.625 es circular, puede afirmarse que los únicos números circulares de menos de 10 cifras finalizados en 5 son: 212.890.625, 12.890.625, 2.890.625, 890.625, 90.625, 0.625, 625, 25 y 5.

3.- ALGORITMO PARA OBTENER NUMEROS CIRCULARES

Las proposiciones vistas anteriormente hacen referencia a la unicidad de los números circulares de n cifras, dada su cifra de las unidades. Las proposiciones siguientes ofrecen el algoritmo que permite encontrar la nueva cifra que debe colocarse al principio de un número circular para obtener uno superior.

Proposición 7ª: Si α es un número circular de n cifras acabado en cinco, las n+1 últimas cifras de α^2 conforman un número también circular.

Demostración: Basta observar que para conseguir a partir de un número circular de n cifras acabado en cinco su correspondiente número circular de n+1 cifras hay que añadir la cifra:

$$\sigma = [\alpha^2 - \alpha]/10^n \pmod{10}$$

Es evidente que σ es la cifra n+1, por la derecha, de $\alpha^2 - \alpha$ y, por ser α circular, será también la n+1 cifra de α^2. Por tanto, las n+1 últimas cifras de α^2 constituyen un número circular.

Proposición 8ª: Si α es un número circular de n cifras acabado en seis, se consideran las n+1 cifras finales de su cuadrado. Sustituyendo la primera de ellas, σ, por $(10 - \sigma)$ se obtiene un número también circular.

Demostración: Es evidente a partir del principio de complementariedad demostrado en la proposición tercera, ya que $[\alpha^2 - \alpha]/10^n \pmod{10}$ es la cifra que ocupa el lugar n+1 en α^2. De aquí y de la proposición sexta que establece para el caso de terminar en seis que

$$\sigma = 10 - [\alpha^2 - \alpha]/10^n \pmod{10}$$

se sigue la tesis.

Codificando estos algoritmos en Turbo Pascal, se encuentran prontamente los dos números circulares de 250 cifras:

```
  9 219 341 881 909 581 659 524 477 861 846 140
912 878 298 438 431 703 248 173 428 886 572 737
663 146 519 104 988 029 447 960 814 673 760 503
957 196 893 714 671 801 375 619 055 462 996 814
764 263 903 953 007 319 108 169 802 938 509 890
062 166 509 580 863 811 000 557 423 423 230 896
109 004 106 619 977 392 256 259 918 212 890 625
```

0 780 658 118 090 418 340 475 522 138 153 859
087 121 701 561 568 296 751 826 571 113 427 262
336 853 480 895 011 970 552 039 185 326 239 496
042 803 106 285 328 198 624 380 944 537 003 185
235 736 096 046 992 680 891 830 197 061 490 109
937 833 490 419 136 188 999 442 576 576 769 103
890 995 893 380 022 607 743 740 081 787 109 376

Por tanto, con estos dos números se tienen, realmente, todos los números circulares que posean 250 o menos cifras.

4.- AMPLIACION DEL ESTUDIO A OTRAS BASES DE NUMERACION

Un número α se considerará circular en una base b cuando su cuadrado, en esa base, finalice en α. Evidentemente las proposiciones 1ª, 3ª y 5ª mantienen su validez sin más que sustituir la base 10 del sistema decimal por la nueva base b.

Seguidamente se estudiarán las condiciones precisas para que existan números circulares en una base cualquiera b.

Proposición 9ª: Una condición necesaria para que existan números circulares en una base dada b es que el anillo **Z/b** tenga dos divisores de cero consecutivos; es decir, que posea un elemento idempotente.

Demostración: Para que un número sea circular es necesario que su última cifra, σ, cumpla que:

$$\sigma^2 - \sigma = x \cdot b \quad \text{con } x \in \mathbf{N}$$

Evidentemente σ pertenece al anillo **Z/b**. La ecuación anterior se puede escribir en este anillo como $\sigma \cdot (\sigma - 1) = 0$, lo que prueba la proposición.

Proposición 10ª: i) Si la base b del sistema de numeración es un número primo no existen en esa base números circulares.

ii) Si $b = p^n$, donde p es un número primo, no existen números circulares.

Demostración:

i) En el caso de ser b primo **Z/b** es un cuerpo y no tendrá divisores de cero de ningún tipo.

ii) Si hubiera números circulares en **Z/b** se cumpliría:

$$\alpha \cdot (\alpha - 1) = 0$$

donde α (ó $\alpha - 1$) serán de la forma p^m con $m<n$ y $\alpha - 1$ (ó α) no tendrá ningún factor p. Lo cual es absurdo.

Proposición 11ª: Si una base b verifica $b = p^k \cdot q^l$, donde p y q son números primos, el anillo **Z/b** tiene elementos idempotentes.

Demostración: Para que tenga divisores de cero consecutivos se ha de cumplir la condición $\alpha \cdot (\alpha - 1) = 0$, siendo α múltiplo de p y α-1 múltiplo de q, lo que implica que se debe cumplir que la diferencia entre un múltiplo de p y otro de q sea 1. Pero esta condición se cumple, puesto que como p y q son primos entre sí (ya que son primos) su máximo común divisor es 1. Aplicando la identidad de Bezout se tiene que existen m y n tal que:

$$m \cdot p + n \cdot q = 1$$

que es lo que deseábamos probar.

Esta proposición puede generalizarse sin dificultad para el caso que la base se pueda descomponer en potencias de más de dos factores primos distintos.

Hasta ahora se ha demostrado que sólo pueden existir números circulares, que irán siempre por parejas, en bases que no son números primos ni potencias de un único primo.

Sin embargo, al contrario que sucedía en base 10, las parejas de números circulares de n cifras ya no tienen por que ser únicas. Así, por ejemplo, en base 30 existen tres parejas de números circulares de dos cifras:

3 10 y 26 21   7 15 y 22 16   10 25 y 19 6

Por otro lado, es evidente que los elementos idempotentes son números circulares de una cifra. Seguidamente se demostrará que existe una correspondencia entre números idempotentes y circulares de cualquier número de cifras. Esto es, si en **Z/b** hay m elementos idempotentes también hay m números circulares de cualquier número de cifras.

Lema 1º: Si en un anillo α es idempotente, $2\cdot\alpha - 1$ es unidad

Demostración: El inverso de $2\alpha - 1$ es él mismo, ya que:

$$(2\alpha - 1)\cdot(2\alpha - 1) = (\alpha + \alpha - 1)^2 = \alpha^2 + \alpha^2 + 1 + 2\alpha^2 - 2\alpha - 2\alpha$$

y, como por ser α idempotente $\alpha^2=\alpha$, se tiene:

$$(2\alpha - 1)\cdot(2\alpha - 1) = \alpha + \alpha + 1 + 2\alpha - 2\alpha - 2\alpha = 1 \quad \text{c.q.d.}$$

Lema 2º: Sea σ un elemento unidad de **Z/b**. Los productos $\sigma\cdot x$, donde $x \in$ **Z/b**, son todos ellos distintos.

Demostración: Si existieran dos elementos distintos $x,y \in$ **Z/b** tales que $\sigma\cdot x = \sigma\cdot y$ se tendría:

$$\sigma\cdot x - \sigma\cdot y = \sigma\cdot(x - y)$$

con los elementos σ, $x-y$ distintos de cero. Este hecho contradice la hipótesis de que σ es unidad en **Z/b**.

Proposición 12ª: La existencia de elementos idempotentes en **Z/b** implica la existencia de números circulares de cualquier número de cifras en la base b.

Demostración: Para demostrar la existencia aplicamos el método de inducción sobre el número de cifras n.

Como **Z/b** tiene elementos idempotentes, es evidente que existen números circulares de una cifra: los propios elementos idempotentes.

Supongamos ahora que existe un número circular α de n cifras:

$$\alpha = a_{n-1}a_{n-2}.......a_0$$

basta probar que existe una única cifra σ de forma que el número

$$\beta = \sigma \cdot b^n + \alpha$$

sea circular. Es decir, que sea un número natural el cociente:

$$[\beta^2 - \beta]/b^{n+1}$$

y, como:

$$[\beta^2 - \beta]/b^{n+1} = [\sigma^2 \cdot b^{2n} + \alpha^2 + 2 \cdot \alpha \cdot \sigma \cdot b^n - \sigma \cdot b^n - \alpha]/b^{n+1} =$$

$$= \sigma^2 \cdot b^{n-1} + [2 \cdot \alpha \cdot \sigma - \sigma]/b + [\alpha^2 - \alpha]/b^{n+1}$$

debe ser natural la suma:

$$[2 \cdot \alpha \cdot \sigma - \sigma]/b + [\alpha^2 - \alpha]/b^{n+1}$$

es decir, se ha de verificar:

$$\sigma \cdot (2\alpha - 1) \pmod b + [\alpha^2 - \alpha]/b^n \pmod b = b$$

Haciendo el cálculo en las clases residuales **Z/b**, se debe cumplir:

$$\sigma \cdot (2\alpha - 1) + [\alpha^2 - \alpha]/b^n \equiv 0$$

Por consiguiente, se busca un σ que cumpla:

$$\sigma \cdot (2\alpha - 1) \equiv - [\alpha^2 - \alpha]/b^n$$

Por el lema 1º, al ser α idempotente, $2\alpha - 1$ es unidad. Aplicando el lema 2º se deduce que existe un único valor σ que cumple la ecuación. c.q.d.

Corolario:

De la expresión anterior, se deduce que el algoritmo de la proposición 7ª para obtener el siguiente número circular (las n+1 últimas cifras de α^2) sólo es válido cuando la cifra σ de las unidades del número verifica:

$$2\sigma - 1 \equiv -1 \ \ (b) \quad \Longrightarrow \quad 2\sigma \equiv 0 \ \ (b)$$

lo que exige que b sea par, puesto que $\sigma = b/2$.

Además, por ser el número circular, σ también lo es; luego:

$$\sigma \cdot (\sigma - 1) = \text{múltiplo de b} \quad \Longrightarrow \quad b \cdot (b-2)/4 = \text{múltiplo de b}$$

y esto exige que la base b sea un múltiplo de 4 mas 2.

Así pues, el algoritmo citado anteriormente es válido para 3 en base 6, para 5 en base 10, para 9 en base 18, etc. A título ilustrativo, presentamos las parejas de números circulares de 250 cifras en base 6 y base 18.

Base 6

```
  4 540 022 031 320 041 433 102 104 311 203 135
010 153 123 521 453 414 143 451 415 124 035 000
342 304 200 324 004 030 242 454 030 504 331 054
320 225 324 551 522 014 003 204 313 053 302 300
223 202 232 243 042 010 534 051 031 024 011 045
451 323 455 255 430 332 042 521 020 413 310 422
403 341 355 525 055 521 314 155 152 221 350 213
```

```
  1 015 533 524 235 514 122 453 451 244 352 420
545 402 432 034 102 141 412 104 140 431 520 555
213 251 355 231 551 525 313 101 525 051 224 501
235 330 231 004 033 541 552 351 242 502 253 255
332 353 323 312 513 545 021 504 524 531 544 510
104 232 100 300 125 223 513 034 535 142 245 133
152 214 200 030 500 034 241 400 403 334 205 344
```

Base 18

```
  c 862 e2d b5h ad6 1d2 4bh bb9 gf8 0d7 01e ghe
agc 912 427 7c7 765 af6 0bf c59 503 7d3 2fe 75f
e7f 98b gc5 ghg e22 04e 196 3a2 c02 161 a4h dh8
312 h4c g0f g4d bh2 cc5 491 hd0 6b3 b81 c85 60f
125 069 f04 5gg d9g c9b 054 61a 40d g82 477 aed
8a8 264 bec a48 4f1 5ec ga3 hg0 986 1g8 d4e ehf
h00 6h9 37h hgg 7ge gae a80 1g4 c96 8da 4e1 249
```

```
  5 9bf 3f4 6c0 74b g4f d60 668 129 h4a hg3 103
715 8gf dfa a5a abc 72b h62 5c8 che a4e f23 ac2
3a2 896 15c 101 3ff hd3 g8b e7f 5hf gbg 7d0 409
egf 0d5 1h2 1d4 60f 55c d8g 04h b6e 69g 59c bh2
gfc hb8 2hd c11 481 586 hcd bg7 dh4 19f daa 734
979 fbd 635 7d9 d2g c35 17e 01h 89b g19 4d3 302
0hh b08 ea0 011 a13 173 79h g1d 58b 947 d3g fda
```