La aritmética del reloj

José Ángel Cid

Diario Jaén, 07 de Noviembre de 2013

EL RINCON MATEMATICO

La aritmética del reloj

José Ángel Cid
Departamento de Matemáticas de la Universidad de Vigo

Todo el mundo sabe que en la aritmética de la escuela 6+7=13, pero no es tan conocido que hay otros tipos de aritmética en los que el resultado puede ser diferente. Sin in ir más lejos, si usted tiene un reloj de pulsera de agujas entonces su reloj marcará la una cuando hayan pasado siete horas desde las seis. En símbolos matemáticos indicamos esta igualdad como 6+7=1 (mod. 12), léase, 6 más 7 es igual a 1 módulo 12. Podríamos generalizar esta aritmética a un reloj arbitrario de k horas y entonces escribiríamos a=b (mod. k) para indicar que b-a es múltiplo de k. Este tipo de aritmética puede parecer una simple curiosidad, sin embargo su uso es esencial por ejemplo en el criptosistema RSA en el que se basan las transacciones por internet. A continuación vamos a explicar una inesperada relación entre la aritmética modular y las barajas de cartas.

Algunos magos y judadores profesionales son capaces de realizar mezclas perfectas (también conocidas como mezclas faro). Para realizar una mezcla perfecta con una baraja de 2n cartas hay que dividir la baraja en dos mazos idénticos (es decir, con n cartas cada uno) e intercalar exactamente una carta de cada mazo, dejando como carta superior de la baraja la misma carta que ocupaba esa posición inicialmente. Podría parecer que después de realizar varias mezclas perfectas la baraja está totalmente desordenada y que es imposible saber en que posición se encuentra cada carta, pero nada más lejos de la realidad. Por ejemplo una baraja española de 40 cartas se recicla (es decir vuelve a su orden original) después de 12 mezclas perfectas y una baraja de póker de 52 cartas se recicla, curiosamente, después de solo 8 mezclas. Saber como se distribuyen las cartas en una mezcla perfecta es una información muy interesante, tanto para realizar trucos de magia como para desplumar a pardillos. Pues bien, la posición que ocupa la carta i (empezando a contar desde 0 por la parte superior) después de una mezcla perfecta viene dada por una igualdad en un reloj de 2n-1 horas. En particular una baraja de 2n cartas se recicla después de k mezclas perfectas si y solo si 2^k=1 (mod. 2n-1). El menor valor de k que resuelve la ecuación anterior se llama el orden de 2 módulo 2n-1 y es un número misterioso del que se sabe muy poco. Sorprendentemente una simple cuestión sobre mezclas de cartas nos lleva más allá de la frontera de las matemáticas conocidas hasta territorios inexplorados.

Para colaborar en esta sección, contactar con el Departamento de Matemáticas, en la dirección jquesada@ujaen.es

Todo el mundo sabe que en la aritmética de la escuela $6 + 7 = 13$, pero no es tan conocido que hay otros tipos de aritmética en los que el resultado puede ser diferente. Sin in ir más lejos, si usted tiene un reloj de pulsera de agujas entonces su reloj marcará la una cuando hayan pasado siete horas desde las seis. En símbolos matemáticos indicamos esta igualdad como $6 + 7 = 1\,(mod.\,12)$, léase, 6 más 7 es igual a 1 módulo 12. Podríamos generalizar esta aritmética a un reloj arbitrario de k horas y entonces escribiríamos $a = b\,(mod.\,k)$ para indicar que b-a es múltiplo de k. Este tipo de aritmética puede parecer una simple curiosidad, sin embargo su uso es esencial por ejemplo en el criptosistema RSA en el que se basan las transacciones por internet. A continuación vamos a explicar una inesperada relación entre la aritmética modular y las barajas de cartas.

Algunos magos y judadores profesionales son capaces de realizar mezclas perfectas (también conocidas como mezclas faro). Para realizar una mezcla perfecta con una baraja de $2n$ cartas hay que dividir la baraja en dos mazos idénticos (es decir, con n cartas cada uno) e intercalar exactamente una

carta de cada mazo, dejando como carta superior de la baraja la misma carta que ocupaba esa posición inicialmente. Podría parecer que después de realizar varias mezclas perfectas la baraja está totalmente desordenada y que es imposible saber en que posición se encuentra cada carta, pero nada más lejos de la realidad. Por ejemplo una baraja española de 40 cartas se recicla (es decir vuelve a su orden original) después de 12 mezclas perfectas y una baraja de póker de 52 cartas se recicla, curiosamente, después de solo 8 mezclas. Saber como se distribuyen las cartas en una mezcla perfecta es una información muy interesante, tanto para realizar trucos de magia como para desplumar a pardillos. Pues bien, la posición que ocupa la carta i (empezando a contar desde 0 por la parte superior) después de una mezcla perfecta viene dada por una igualdad en un reloj de $2n-1$ horas. En particular una baraja de $2n$ cartas se recicla después de k mezclas perfectas si y solo si $2^k = 1\,(mod.\, 2n-1)$. El menor valor de k que resuelve la ecuación anterior se llama el orden de 2 módulo $2n-1$ y es un número misterioso del que se sabe muy poco. Sorprendentemente una simple cuestión sobre mezclas de cartas nos lleva más allá de la frontera de las matemáticas conocidas hasta territorios inexplorados.

Para saber más:

- Marcus du Sautoy, Los misterios de los números, El Acantilado, 2012.

- Persi Diaconis and Ron Graham, The solutions to Elmsley's problem, *Math Horizons*, Feb. 2007, pg. 22 - 27. Disponible en `http://www-stat.stanford.edu/~cgates/PERSI/papers/pre-elmsley.pdf`