De paseo por el cosmos

elescritoriodeenrique.com

Enrique Ferres

Bienvenidos al Escritorio de Enrique. ¿Os sorprende el título? ¿Por qué esos primos llevan mi apellido? En este artículo voy a hablaros de estos números que he descubierto recientemente[1]. También veremos qué es un número escrito en otra base distinta de la decimal, aprenderemos a contar cuántos candidatos a este tipo de números hay para un número de cifras concreto y sabremos para qué son importantes los números primos en la vida real. ¡Seguid leyendo, que este tema está recién sacado del horno!

Sistemas de numeración

Las personas solemos contar de 10 en 10. Los primeros números naturales son el 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9. Todos ellos tienen una sola cifra. El siguiente número al 9 es el 10, que tiene dos cifras, y seguimos contando: 10, 11, 12, 13, 14, 15, 16, 17, 18 y 19. En todo sistema necesitamos unas unidades con las que representar lo que contamos. Los números del 0 al 9 tienen una sola cifra porque son lo que llamamos "unidades". A partir del 10 hasta el 99 lo llamamos decenas. En estos números, que podemos representar como XY, tenemos que la X representa cuántas decenas llevamos contadas, y la Y cuántas unidades en esa última decena. El número 12 significa 1 decena y 2 unidades, y el número 23 significa 2 decenas y 3 unidades. Después del 99 viene el 100. Este número de tres cifras quiere decir que ya hemos contado 10 decenas, y a esas 10 decenas la llamamos centena. Entonces, los números de tres cifras, que podemos representarlos como XYZ, significan X centenas, Y decenas y Z unidades. Para llegar a un millar, 1000, necesitamos contar 100 decenas, y así sucesivamente. Es una progresión que crece de forma exponencial. Cada vez que añadimos 1 cifra al número, hay que añadir un 0. Para tener una decena necesitamos $10^0 = 1$ decenas (obvio). Para tener una centena necesitamos $10^1 = 10$ decenas. Para tener un millar necesitamos $10^2 = 100$ decenas. El exponente del 10 indica cuántos ceros se añaden al 1.

El sistema decimal es bastante reciente en el tiempo, y se supone que proviene de contar

[1] Quien simplemente tenga interés en estos números puede ir directamente a la página 4.

con los dedos de las manos (lo siento si tienes más de diez o menos de diez dedos, te habrá costado más aprender a contar). Sin embargo, no es el único sistema de numeración que ha habido en el tiempo. Aún seguimos comprando los huevos por docenas y midiendo los minutos y segundos de 60 en 60. Otro sistema de numeración bastante más reciente es el hexadecimal, es decir, contando de 16 en 16. Los números en este sistema son 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F (del 10 al 15 se representan con las letras de la A a la F). Es un sistema un poco raro, pero en informática es tremendamente útil.

Sistema binario

Hablando de sistemas de numeración e informática, el sistema por antonomasia es el binario (base 2). Todo el mundo sabe que es un sistema formado solo por 0's y 1's, pero suele ser bastante desconocido.

Lo primero que hay que destacar es que todo número decimal puede expresarse en sistema binario de manera única (no hay un decimal que pueda escribirse de varias maneras diferentes en binario). Y lo segundo es que todo número binario puede expresarse en sistema decimal de manera única . Juntando las dos frases esto significa que las dos formas de escribir números son equivalentes, y que lo mismo me da expresar un número n en decimal que en binario.

¿Cómo se traduce un número binario a decimal? La idea que subyace detrás de esto es que todo número decimal se puede escribir como suma de potencias de 2. En el sistema decimal tenemos que cualquier número, como por ejemplo el 329, se puede escribir como suma de potencias de 10, en este caso

$$329 = 3 \cdot 10^2 + 2 \cdot 10^1 + 9 \cdot 10^0$$

(los coeficientes que acompañan a las potencias de 10 son las unidades del sistema decimal, del 0 al 9). En el sistema binario lo que tenemos es que los números decimales se pueden escribir como suma de potencias de 2, y los coeficientes serán las unidades del sistema binario (0 y 1). Veamos un ejemplo.

En sistema decimal, la posición de las cifras importa mucho. El 329 tiene un 9 multiplicado por 10^0 (diremos que la posición es 0). Tiene un 2 multiplicado por 10^1 (la posición es 1). Y tiene un 3 multiplicado por 10^2 (la posición es 2). Así, empezamos a contar por el 0 de derecha a izquierda y sumamos todo. Para encontrar la representación decimal de un número binario vamos a hacer lo mismo. Queremos saber qué número es el 1110 (binario) en sistema decimal. Así que contamos las posiciones: hay un 0 en la posición 0 y tres 1's en las posiciones 1, 2 y 3. Cuando hay un 0, lo multiplicamos por 2^{posicion}, y cuando hay un 1, lo mismo. Así, el 1110 es

$$1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 8 + 4 + 2 + 0 = 14.$$

Por tanto, el número 1110 es el 14 escrito en binario.

Por otra parte, la traducción de decimal a binario se basa en el mismo principio, pero ahora lo que tenemos que hacer es dividir entre 2. Se ve mejor con un ejemplo. Cojamos

el 14 y olvidémonos de que ya sabemos cual es su representación binaria. Dividimos 14 entre 2 y nos queda cociente 7 y resto 0. Lo escribimos mejor con la fórmula VIP del blog,

$$\text{dividendo} = \text{divisor} \cdot \text{cociente} + \text{resto}.$$

Así, $14 = 7 \cdot 2 + 0$. Ahora hacemos lo mismo con 7 entre 2. Sucesivamente vamos dividiendo el cociente que nos va saliendo entre 2 hasta que el cociente sea 0.

$$\begin{aligned} 14 &= 7 \cdot 2 + 0 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 2 + 1 \\ 1 &= 0 \cdot 2 + 1 \end{aligned}$$

Ahora, como ya hemos llegado a tener cociente 0, cogemos los restos que nos han aparecido y los "pegamos" desde el final hasta el principio: 1110. Ahí tenemos el 14 escrito en binario. Por cierto, todo número par, en binario tiene un 0 como última cifra, y todo impar un 1.

Para terminar de entender mejor todo esto, muchas veces se utiliza un subíndice para saber en qué sistema estamos leyendo el número, así que este es un buen momento para introducirlo. El número 14 está en el sistema decimal, así que lo escribimos como 14_{10}. El 1110 está en sistema binario, así que lo escribimos como 1110_2.

Esto es especialmente útil cuando hay números decimales, como el 10, que solo tienen 1's y 0's y se puede confundir si se están leyendo en decimal o en binario. 10 en decimal es 10_{10}, mientras que 10 en binario es 10_2. Además, $10_2 = 2^1 + 0 \cdot 2^0 = 2_{10}$.

Números primos

Los números primos son, por así decirlo, los átomos de los números (naturales de aquí en adelante). El Teorema Fundamental de la Aritmética dice que todo número se descompone como producto de números primos de manera única. Como todos sabréis, un número primo es un número que solo es divisible por él mismo y por 1, y que un número sea divisible por otro quiere decir que al dividirlos, el resto es 0. El primer número primo es el 2 (no, ni el 0 ni el 1 son primos), y es el único número primo par, pues el resto de números pares son divisibles entre 2. La lista sigue así: 2, 3, 5, 7, 11, 13, 17, 19, ... En el artículo Una sencilla construcción con regla y compás tenéis una demostración de la infinitud del conjunto de números primos.

Los números primos desempeñan una labor fundamental en el sistema de encriptación de claves de seguridad. Básicamente, de manera muy general, estos sistemas consisten en tratar de averiguar, a partir de un número gigantesco, cuales son los primos que lo dividen. El número gigantesco lo puede ver todo el mundo, pero es imposible que nadie pueda encontrar sus divisores utilizando los algoritmos tradicionales. La única forma de encontrarlos es conociéndolos (contraseña). A esto se le llama sistema clave pública/privada y es tremendamente interesante.

Precisamente por esa necesidad de encriptar la información es tan importante encontrar números primos cada vez más grandes. Sin embargo, es una tarea complicadísima, pues

existen limitaciones tecnológicas y los algoritmos que hay para saber si un número es o no primo son muy ineficientes. A pesar de eso, el número más grande que se ha encontrado hasta la fecha es el $2^{82589933} - 1$, con 24862048 cifras. Una pasada. A los primos de la forma $2^n - 1$ se les llama primos de Mersenne, en honor al Padre Mersenne (s. XVII), del cual espero hablar más adelante en el blog. No todo número primo es de esta forma, pero sí que, si es primo, entonces n es primo. Existe un proyecto colaborativo llamado GIMPS (Great Internet Mersenne Prime Search) cuyo objetivo es encontrar nuevos primos de Mersenne.

Hay un tipo de algoritmos para ver si un número es primo o no que son probabilísticos. ¡Sí, la probabilidad también se puede aplicar al hecho de ser o no primo! Uno de ellos es el Test de Miller-Rabin. Este algoritmo toma un número y te puede decir que no es primo (cuando te dice que no es primo no se equivoca nunca) o te puede decir que sí es primo. En este último caso, lo bueno que tiene el algoritmo es que puedes calcular la probabilidad de que efectivamente sea un número primo (magia de la probabilidad) como $\frac{1}{4^{num.iteraciones}}$ (además, al hacer el algoritmo un mínimo de una iteración, te garantizas de que la probabilidad de que sea primo sea siempre mayor o igual que 0.75, o 75 %). Otro punto a favor de los algoritmos probabilísticos es que son mucho más rápidos que los deterministas (los fiables). Pero claro, el gran punto en contra es que si te dicen que un número es primo pueden fallar. Para la práctica, se utilizan para lo que he comentado anteriormente de los sistemas clave pública/privada, pero los matemáticos solo podemos afirmar algo cuando estamos seguros del todo, así que en ese sentido los algoritmos probabilísticos sirven para indicar qué números "grandes" sí son candidatos serios a ser números primos.

Otra utilidad de los números primos es tecnológica. Como acabamos de comentar, los algoritmos de búsqueda de números primos son muy ineficientes, tardan mucho en decidir si un número es primo o no, entonces, cuando se desarrollan nuevos ordenadores, procesadores, etc., una de las formas de ver cuánta capacidad de cómputo tienen es utilizando estos algoritmos y viendo cuánto tiempo tardan con respecto a lo que ya había anteriormente. Qué buena gente son estos primos, ¿verdad?

Números primos de Ferres

Por fin llegamos. Hace unos meses publiqué en Twitter (donde, por cierto, todas las semanas escribo mínimo un hilo divulgativo, así que seguidme en @enrique_ferres si no queréis perderos nada) una propiedad muy curiosa que descubrí en el número 101, pero no sabía si habría más números con esa propiedad. Dejé pasar el tiempo esperando encontrar un hueco en el que buscar algo relacionado con este número y con los que cumplieran la propiedad. La semana pasada por fin pude ponerme y, cual fue mi sorpresa, no encontré ABSOLUTAMENTE NADA. Así que he decidido, mientras nadie me diga que estos números tienen otro nombre y que los descubrió otra persona, llamarlos números primos de Ferres. Vamos a ver su definición.

Se dice que un número es primo de Ferres (lo vamos a denotar por PF) si es un número primo formado por 0's y/o 1's de forma que, al escribirlo en binario, el número resultante es primo como número decimal. De manera más matemática, un número n_{10} es un PF si

es un primo formado por 0's y/o 1's de forma que, si $m_2 = n_{10}$, entonces m_{10} es primo.

Parece un trabalenguas, pero ya veréis que no es tan complicado, la clave es que, cuando pasamos el número a binario tenemos que leer ese número binario como si fuese decimal. Veamos algunos ejemplos.

El número 11 ($n_{10} = 11_{10}$) es un número primo formado solo por 1's. Si lo pasamos a binario es el 1011 ($m_2 = 1011_2 = 11_{10} = n_{10}$). Este nuevo número leído como número decimal ($m_{10} = 1011_{10}$) no es un número primo, porque es divisible entre 3.

El número 101 ($n_{10} = 101_{10}$) es un número primo formado por 1's y 0's. Si lo pasamos a binario es el 1100101 ($m_2 = 1100101_2 = 101_{10} = n_{10}$), que leído como número decimal ($m_{10} = 1100101_{10}$) es un número primo. Además, resulta que el 101 es el primer PF.

Con un algoritmo determinista probé a buscar PF's, pero solo llegué hasta números de 7 cifras, porque a partir de 8, este algoritmo y mi ordenador ya no daban para más. Además, me encontré con que el único PF de 7 cifras o menos es el 101. "¿Será el único?" pensé. Entonces probé a utilizar el algoritmo probabilístico de Miller-Rabin y, llegados hasta las 17 cifras, ¡me aparecieron 114 candidatos! Aquí os dejo una lista con todos ellos.

101, 11110111, 1001000111, 10110100001, 10111000001, 10001001001, 11001101011, 11100011101, 101010000001, 100010001001, 100010111101, 110111010101, 110100110101, 1001100101011, 1011101100101, 1110011010001, 1111100010011, 1100011001101, 1110011001101,1110001101101, 10101101000101, 10100000011001, 10011110100011, 10101001011011,10010111111111, 11101100010101, 11010010100101, 11001010110011, 11000011101011,11011110111011, 101000010001001, 101101010010001, 100011110010001, 100111001011001,100010001010111, 100010000011111, 101011101011111, 101100011111111,111010011000011,110111101010011, 110010101111011, 110001111111011, 110110000110101, 110011011111101,110000101001111, 110010111110111, 1000001011110001, 1001011110000101,1010100001010101, 1010010101100101, 1000100110100101, 1001010111110101, 1000001101001101, 1000010110001101, 1000010100110111, 1000001100101111, 1110010011010001, 1111101101101001, 1100110101011101,1101010111011101, 1110000000100111, 1111111110001111, 1100101001111111, 1101100010111111, 10101110110000001, 10111001100100001, 10010000111100001, 10100001111001001, 10001001100110001, 10111011100110001, 10111110110110001, 10010101000111001, 10001001000111001, 10101001010000011, 10001000100101011, 10000001101110011, 10100000101011011, 10101100010000101, 10001011100000101, 10111001110100101, 10101110101010101, 10001000110011101, 10111111000000111, 10100011010000111, 10001110100000111, 10011011100100111, 10111101101000111, 10011010000001111, 10111001001010111, 10011101011010111, 10010001111010111, 10000110110111111, 10010101001111111, 11000011000101001, 11001110111001001, 11101001111101001, 11010101110011001, 11011001010111001, 11101111001011001, 11101110101011001, 11101010011111001, 11100111001101011, 11110010000010011, 11101000000101101, 11111000011001101, 11110100101001101, 11101001101010101, 11111001010011101, 11110111011011101, 11000001100000111, 11100111101000111, 11111110011100111, 11111110001101111, 11010000111101111.

El mayor problema que tienen los algoritmos deterministas no es comprobar si los números de esa lista son primos, sino si sus binarios lo son, porque al pasar un número a binario sus cifras aumentan considerablemente. El número 101 tiene 3 cifras y su binario, el 1100101, tiene 7. Pero es que el siguiente número a probar es el 11110111, de 8 cifras, y su binario es el 101010011000011011011111, ¡que tiene 24 cifras!

Pensé que ya sería mala suerte que de todos esos números que me ha devuelto el algoritmo probabilístico solo el 101 sea PF. Entonces, para salir de dudas de que solo hay un PF comprobé con el algoritmo determinista si 11110111 es PF y, tras 11 horas de ejecución, el algoritmo indicó que, efectivamente, es un PF. ¡El segundo! ¡Hay más de uno! Hasta el momento en el que estoy escribiendo esto, son los dos únicos PF's que he encontrado, a la espera de que se comprueben los otros 112 candidatos. Sin embargo, mis limitaciones tecnológicas me impiden seguir verificando PF's.

Buscando primos de Ferres

Para buscar candidatos a PF no es necesario buscar entre todos los números, sino solamente entre aquellos que están formados por 1's y/o 0's. Así que, si buscamos PF's de dos cifras, los únicos candidatos son 10 y 11. Si buscamos PF's de tres cifras, los únicos candidatos son 100, 101, 110 y 111. La pregunta es: ¿Cuántos candidatos de k cifras hay?

- Si $k = 2$, entonces solo hay 2 candidatos (dejo por aquí 2^1).
- Si $k = 3$, entonces hay 4 candidatos (dejo por aquí 2^2). Una forma de ver los candidatos de 3 cifras es separar los números de la siguiente manera: todos empiezan por 10 u 11 y van seguidos de 1 o 0. Es decir, tenemos números de la forma 10* (en ese espacio va un 1 o un 0, dos posibilidades), y números de la forma 11* (en ese espacio va un 1 o un 0, dos posibilidades). Así que, contando las posibilidades nos salen 4.
- Si $k = 4$, entonces hay 8 candidatos (dejo por aquí 2^3): 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111. Ahora tenemos números de la forma 10** (en los huecos van 00, 01, 10, 11; cuatro posibilidades) y de la forma 11** (en los huecos van 00, 01, 10, 11; cuatro posibilidades). Contando las posibilidades nos salen 8.
- La clave para contar las posibilidades es la siguiente: supongamos que queremos contar los candidatos de k cifras, con $k > 2$. Primero vemos si el número es par o impar. Si es par, lo fragmentamos en parejas de cifras (por ejemplo, para 6 cifras habría 3 parejas), y contamos las posibilidades que hay, teniendo en cuenta que la primera pareja solo puede ser 10 u 11 y el resto pueden ser 00, 01, 10, 11. Si k es impar, fragmentamos por parejas empezando desde la izquierda y la última cifra de la derecha la dejamos desparejada (por ejemplo, para números de 5 cifras habría 2 parejas y una cifra suelta). Hay que tener en cuenta que la primera pareja solo puede ser 10 u 11, la última cifra solo puede ser 0 o 1 y el resto pueden ser 00, 01, 10, 11.

Lo que vamos a obtener es que hay 2^{k-1} candidatos de k cifras para $k \geq 2$. Una demostración rigurosa requeriría de utilizar el principio de inducción. Podéis intentarlo para practicar. En el artículo Algunos tipos de demostraciones encontraréis en qué consiste este principio.

Superprimos de Ferres

Ya para terminar quiero hablar de otro tipo de números que he descubierto y que he decidido llamar superprimos de Ferres. Veamos en qué consisten.

Se dice que un número es superprimo de Ferres (SPF) si es un primo de Ferres que, leído como número binario, es la expresión binaria de un número primo.

Matemáticamente lo expresaríamos de la siguiente manera. Se dice que n_{10} es SPF si es PF y si existe un número primo, p, tal que $p_{10} = n_2$.

No os asustéis que ahora vienen ejemplos. Lo primero es hacer notar que para que un número sea SPF, tiene que ser PF, entonces los candidatos van a estar entre los PF. El primero con el que tenemos que probar es 101. Para ello habría que ver si 101 es la expresión binaria de un número primo. Entonces pasamos 101_2 a decimal:

$$101_2 = 2^2 + 2^0 = 4 + 1 = 5_{10}.$$

Y como 5 es un número primo, concluimos que 101 es SPF. ¡Qué casualidad! El 101 es un número interesantísimo.

Ahora vamos a ver si el otro PF que hemos encontrado es SPF.

$$11110111_2 = 2^7 + 2^6 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0 = 128 + 64 + 32 + 16 + 4 + 2 + 1 = 247_{10}.$$

247 no es un número primo porque es el producto de 13 por 19, así que 11110111 no es SPF.

He comprobado que, si los candidatos a PF de la lista de 114 que he escrito antes fueran, efectivamente, PF, habría 34 SPF. Aquí dejo una lista con todos ellos. Los escribo por parejas en las que aparece el número que es SPF y de qué número primo es expresión binaria.

(101, 5), (10001001001, 1097), (101010000001, 2689), (100010111101, 2237), (110111010101, 3541), (11010010100101, 13477), (11001010110011, 12979), (101011101011111, 22367), (101100011111111, 22783), (110111101010011, 28499), (110110000110101, 27701), (1000001011110001, 33521), (1010100001010101, 43093), (1000001101001101, 33613), (1110000000100111, 57383), (1111111110001111, 65423), (1100101001111111, 51839), (1101100010111111, 55487), (10111001100100001, 95009), (10010000111100001, 74209), (10100001111001001, 82889), (10001001000111001, 70201), (10001000100101011, 69931), (10100000101011011, 82267), (10001011100000101, 71429), (10100011010000111, 83591), (10011101011010111, 80599), (11000011000101001, 99881), (11001110111001001, 105929), (11101110101011001, 122201), (11110010000010011, 123923), (11110100101001101, 125261), (11000001100000111, 99079), (11111110011100111, 130279).

Conclusiones

Los números primos han sido, desde la prehistoria matemática (antes de los griegos), objeto de fascinación y estudio. Hasta ahora no se ha descubierto ningún patrón con el que se distribuyan, pero si se demostrase la Hipótesis de Riemann, que merece su propio

artículo, la cosa cambiaría. De momento, nos conformamos, por la parte práctica, con encontrar números primos grandes. En este sentido, los primos de Ferres podrían tener cierta relevancia. En efecto, la definción de primo de Ferres involucra que el binario del número en cuestión sea, a su vez, un primo (leído como decimal). Pero este binario tiene muchas más cifras que el primo del que proviene. Así que, si alguien demostrase que existen infinitos primos de Ferres (de momento solo sabemos que existen 2 con seguridad) y encontrase una propiedad para comprobar que un número es primo de Ferres que no involucre comprobar que su binario es primo, tendría automáticamente que su binario, de muchas más cifras, es primo. Dos por el precio de uno.

Este ha sido mi primer aporte al mundo de las matemáticas, espero que os haya gustado. Si alguien quiere estudiar este tipo de números, me gustaría que me hiciera partícipe o conocedor de sus avances. Podéis poneros en contacto conmigo a través del blog o enviándome un MD por Twitter. Y ya sabéis, comentad vuestras opiniones y compartid con familiares, amigos y vecinos del barrio. ¡Hasta la próxima!