Suplemento

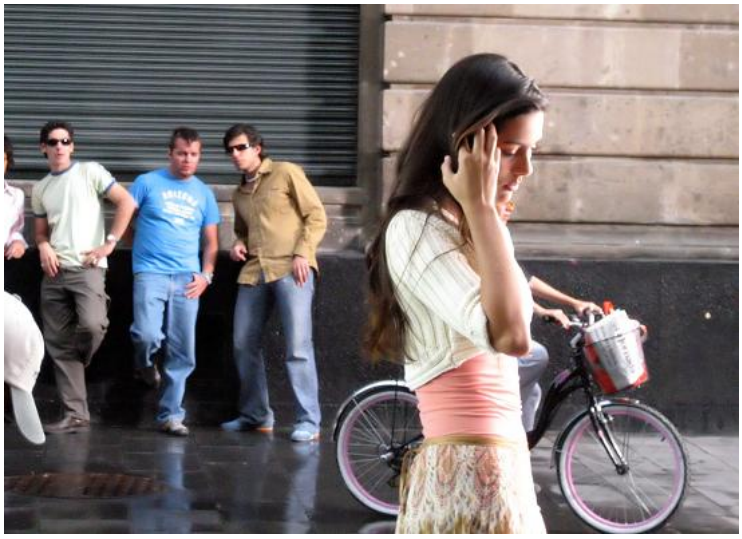
La hoja volante

Número 9

- Conseguir pareja
- Otra paradoja
- Más infinitos
- Observación PARTNeR
- Torres de potencias

Conseguir pareja

Si yo os digo lo siguiente: *"Hay 50 estudiantes (25 mujeres y 25 hombres) en un grupo de último año de bachillerato. Si cada chica de la clase resulta atractiva para exactamente cinco chicos y sabe que ella les gusta a esos cinco chicos y cada chico es compañía agradable para exactamente cinco chicas de la clase y sabe que a ellas cinco les gusta él, entonces es posible formar parejas para que cada chico vaya a la fiesta de fin de curso con una chica que le guste y cada chica asista con uno que le guste".*



Aunque en el fondo tampoco es tan sorprendente, es probable que no os lo creáis (quizá más de uno por experiencia). Pues si os digo que esto es una aplicación directa de un teorema matemático quizá os empiecen a gustar (más) las matemáticas, ¿no?

Veámoslo, el teorema se llama "Teorema de Hall" y es como sigue: Sea G = (V, A) un grafo bipartito con V descompuesto como X ∪ Y. Existe un pareamiento completo de X en Y si y sólo si para todo subconjunto D de X, el número de elementos de D es menor o igual que el número de elementos del subconjunto de Y formado por aquellos vértices adyacentes a los de D.

¿Un poco técnico? A ver, empecemos por la primera frase. Piden un grafo, es decir, un conjunto de puntos (vértices) unidos por líneas (o aristas). Por eso definen el grafo (G de grafo) a partir de V y de A (V de vértices, A de aristas). Además, piden que el grafo sea bipartito. Eso quiere decir que podemos dividir nuestro conjunto V en dos (X e Y) de modo que todas las aristas tengan el origen en X y el destino en Y (o al revés, eso da igual, porque el grafo no lo queremos orientado: si una arista va de un punto c a un punto d, entonces también sirve para ir del punto d al c). Un emparejamiento completo de X en Y, E, es un subconjunto de A (las aristas del grafo G) tal que ningún vértice de V es incidente con más de una arista de E y cada vértice de X es incidente con alguna arista de E (más fácil: de ningún puntito salen 2 rayitas y de todos los puntitos de X sale una rayita). Después de esta explicación, sólo queda por aclarar el concepto de adyacencia. Este concepto es sencillo, simplemente,

dos vértices son adyacentes si hay una arista que los une (así, la última frase se refiere al conjunto de los vértices de Y a los que se puede llegar desde los vértices que forman D).

En vez de usar el teorema en esta forma, emplearemos el siguiente corolario: Sea G = (V, A) un grafo bipartito con V descompuesto como X ∪ Y. Existe un pareamiento completo de X en Y si para algún k natural el grado de x es mayor o igual que k y el grado de y es menor o igual que k, para todos los vértices x de X e y de Y.

El grado de un vértice es el número de aristas que inciden en él (el número de rayitas que le salen). La demostración del corolario a partir del teorema es así:

Para un subconjunto D de X de, digamos, m elementos, como los vértices de X tienen grado mayor o igual que k entonces saldrán de todos los vértices de X al menos km aristas. Además, como los vértices de Y tienen grado menor o igual que k, las km aristas en el peor de los casos (repitiéndose todas el máximo de veces posible) llegan a km / k = m vértices de Y. Por el teorema de Hall se concluye que existe el pareamiento completo.

Este corolario nos explica por qué es cierta nuestra primera afirmación del baile (todos los grados son 5, y se cumplen las hipótesis del corolario con k = 5).

Otras cosas que se pueden hacer con este tipo de teoremas es realizar horarios compatibles o políticas de contratación según las necesidades de una empresa y también se pueden utilizar para resolver problemas del estilo de los del tablero de ajedrez y las fichas del dominó más complicados (donde los argumentos de paridad no son suficientes), pero eso lo dejaremos para otra ocasión.

Otra paradoja
La paradoja del hiperjuego

Os voy a describir un juego curioso, se llama "hiperjuego".

Un juego se considera normal cuando termina en un número finito de movimientos. Un ejemplo obvio de juego normal es el mus. El ajedrez también es un juego normal, si tenemos en cuenta las reglas de torneo.

El primer paso en el hiperjuego es decidir qué juego normal se va a jugar. Por ejemplo, si tú y yo jugáramos al hiperjuego y yo tuviera que empezar, podría decir: "Vamos a jugar al ajedrez". Entonces tú haces la primera jugada de ajedrez, y seguimos jugando al ajedrez hasta que el juego se termina. Otra posibilidad es que en mi primera jugada del hiperjuego dijera: "Vamos a jugar al mus" o cualquier juego normal que me apeteciera. Pero el juego que eligiera debería ser normal; no se permite elegir un juego que no sea normal.

Con estas condiciones, se nos plantea el siguiente problema: ¿el hiperjuego es normal o no?

Supongamos que es normal. Dado que en la primera jugada del hiperjuego puedo elegir cualquier juego normal, puedo decir: "Vamos a jugar al hiperjuego". En ese momento estamos dentro del hiperjuego y te toca a ti. Puedes contestar: "Vamos a jugar al hiperjuego" y el proceso puede seguir indefinidamente, en contra de la presunción de que el hiperjuego es normal. Así pues, el hiperjuego no es un juego normal. Pero, puesto que el hiperjuego no es normal, en mi primera jugada no puedo elegir el hiperjuego, debo elegir un juego normal. Habiendo elegido un juego normal, el juego debe terminar finalmente, en contra del hecho demostrado de que el hiperjuego no es normal. ¿No es asombroso?

Esta paradoja la inventó el matemático William Zwicker.

Más infinitos

Aunque seguro que muchos ya lo conocéis, daremos, como prometimos, un ejemplo de un conjunto infinito con un cardinal más grande que el de los números naturales. El conjunto va a ser "el conjunto de todos los conjuntos que se pueden formar con los naturales". Es decir los elementos de este conjunto son a su vez conjuntos, los subconjuntos de los naturales. Por ejemplo: el conjunto vacío, el $\{1\}$, el $\{1, 2\}$, el $\{19, 6, 1982\}$ (mi cumple, jejeje, ¡ojo, que el orden no importa, este conjunto es el mismo que $\{1982, 19, 6\}$, por ejemplo).

Podemos observar que cada uno de los subconjuntos de los naturales se puede representar con una cadena infinita de unos y ceros (ponemos un 1 si el natural que corresponde con esa posición está en el subconjunto y un 0 si no). Es decir, los 4 conjuntos que hemos puesto como ejemplos se representarían así:

```
1   2   3   4   5   6   7   ...   18   19   20   ...   1981   1982   1983   ...
-------------------------------------------------------------------------------
0   0   0   0   0   0   0   ...    0    0    0   ...      0      0      0   ...
1   0   0   0   0   0   0   ...    0    0    0   ...      0      0      0   ...
1   1   0   0   0   0   0   ...    0    0    0   ...      0      0      0   ...
0   0   0   0   0   1   0   ...    0    1    0   ...      0      1      0   ...
```

Supongamos ahora que el conjunto de todos los subconjuntos de los naturales (partes de los naturales o conjunto potencia de los naturales, se suele llamar) tuviera el mismo cardinal que éstos, es decir, que sus elementos se pudieran escribir en una lista uno detrás de otro. Llegaremos a una contradicción que demostrará que el cardinal del conjunto de partes de los naturales es mayor.

Para ello basta suponer que tenemos la lista con todas las cadenas que representan a los subconjuntos de los naturales (una lista de cadenas infinitas de ceros y unos, cada una en una línea). Vamos a construir una nueva cadena de ceros y unos que no está en la lista, lo que nos dará un nuevo subconjunto que no aparece en la misma. Es tan sencillo como mirar a la primera posición de la primera fila, si es un 0 escribimos un 1 en nuestra nueva cadena y si es un 1 escribimos un 0. Ahora miramos a la segunda posición de la segunda fila de la lista y escribimos también lo contrario de lo que ponga en la segunda posición de nuestra nueva cadena. Como se puede uno imaginar, la tercera posición de la nueva cadena tendrá un 1 si en la tercera fila la posición tercera era un 0 y un 0 si era un 1. Como me canso de escribir y vosotros de leer, supongamos que seguimos haciendo esto con todas las posiciones. Obviamente, nuestra nueva cadena no coincide con ninguna de las que había en la lista (difiere del elemento j de la lista al menos en la posición j). Esto constituye una contradicción con el hecho de que en la lista tuviéramos escritas todas las cadenas (que representaban a todos los subconjuntos de los naturales). Luego ya tenemos un conjunto infinito de cardinal mayor que los naturales ¡el conjunto de todos sus subconjuntos!

Observación PARTNeR

Al final se realizó la observación casi como estaba previsto. ¿Por qué casi? Para saberlo tendréis que leer la estupenda crónica que nos ha mandado Celso Frade. Muchas gracias, Celso.

Resultados de la observación (5 de Abril de 2006).

Bueno, pues ya pasamos la prueba de fuego. Espero que siguierais la observación desde la red pero como no me fío, os la voy a resumir.

Tras enviar el plan de observación y darnos el visto bueno, allí estábamos, los 18 alumnos seleccionados de la asignatura de Tecnología de 4º de la E.S.O. organizados en grupos de 2, mi compañero el profesor Julián Elvira prestándome su inestimable ayuda y yo mismo. Tras establecer comunicación a la hora prevista y sin problemas, hubo un pequeño problema técnico en la estación de Robledo que retrasó el inicio de la observación casi 20 minutos. Pero bueno, si aún no os he dicho lo que íbamos a observar... Pues la fuente problema era el **MICROCUÁSAR LSI +61 303**.

Muy bien, pero os diréis, ¿y eso qué es lo que es?

Ya que insistís..., en primer lugar es un objeto que se encuentra a unos 6.520 años-luz de la Tierra, es decir, **¡¡unas 14.000.000 veces la distancia que nos separa de Plutón aproximadamente!!**. Aunque construyéramos una nave espacial tan veloz que fuera capaz de llegar a la Luna **¡¡en sólo 1 segundo!!**, tardaríamos casi 5.300 años en llegar. Creo que os he convencido de que tendremos que conformarnos con observarlo desde aquí.

Bien, pues este objeto, además de otras peculiaridades que lo sitúan como objetivo prioritario de múltiples proyectos científicos, es un emisor de ondas de radio y es por ello por lo que lo podemos observar. Además, presenta pequeños estallidos en radio de forma periódica cada 26.496 días. Estos estallidos nos dan información de lo que sucede en este sistema, del origen de este misterioso objeto. Resumiendo mucho para no aburrir a nadie, un microcuásar es un sistema binario en el que uno de los dos componentes es una estrella "normal", en este caso una estrella B0 V ó III de rápida rotación y el otro componente es un agujero negro o una estrella de neutrones. Este objeto compacto está "robando" material de la estrella compañera, el cual, al acercarse al objeto compacto y por el principio de conservación del momento angular, empieza a rotar y caer en espiral formando un disco de acreción. Como este disco se encuentra a una temperatura muy elevada, emite rayos X, ondas de radio, partículas subatómicas relativistas, etc...

Vaya, me está quedando una explicación un poco complicada. Seguro que agradecéis este esquemita.

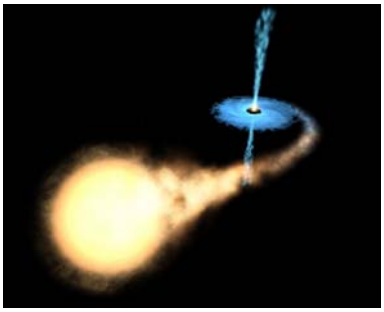
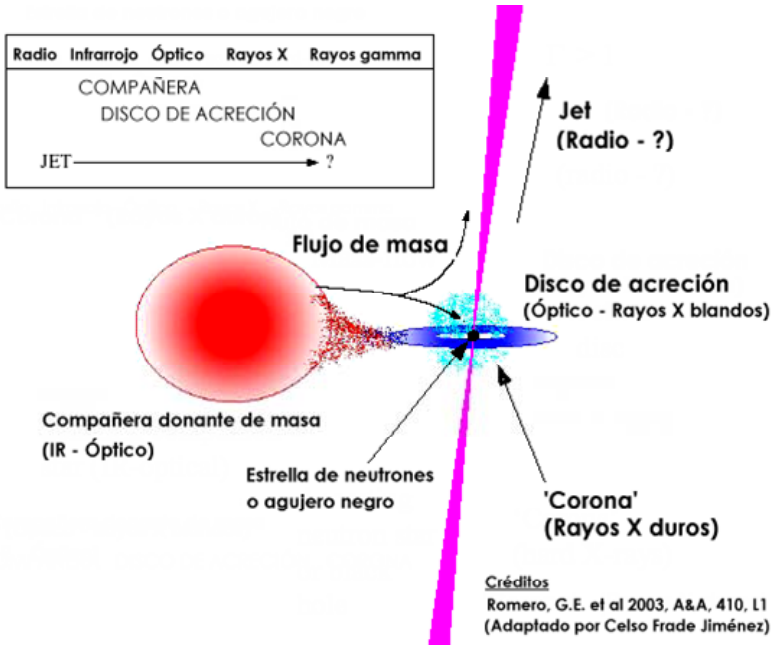


Ilustración del microcuásar LSI +61 303



Pues el caso es que esto es lo que observaron este grupo de chicos y chicas y fueron ellos mismos los que estuvieron dirigiendo la antena de 34 metros de diámetro (34 metros equivale a un edificio de unas 9 plantas). Obviamente, todas las observaciones son registradas por el centro de control de la antena pero nosotros, también tomamos algunas medidas para poder reproducir alguno de los resultados. Aquí tenéis alguna de las fotos obtenidas durante la observación.

Bueno, espero haberos enseñado alguna cosita interesante. Por cierto, durante las dos últimas medidas sobre el microcuásar detectamos unos picos de intensidad inesperados a los que no nos supieron dar información desde Robledo por lo que habrá que esperar al análisis de los datos para descartar cualquier causa accidental.

Pero, ¿y si no fue un pico inusual?...

CELSO FRADE

Torres infinitas de potencias

Santiago Egido Arteaga
La Hoja Volante

18 abril 2006

¿Cuánto vale $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}}$? Es decir, nos preguntamos por el valor de una torre de potencias en la que el número de exponentes es infinito. Empecemos recordando que 3^{3^3} significa $3^{(3^3)} = 7.625.597.484.987$ en vez de $(3^3)^3 = 19.683$.

Está claro que, de tener esto algún sentido, es infinito. Muchas personas estarían encantadas de dar por zanjado el tema al haber llegado aquí, pero si usted está leyendo esto es porque posiblemente le gusta marear la perdiz, así que le agradará saber que a este tipo de cosas se les puede definir un valor en aritmética modular. Veamos cómo.

Imaginemos que queremos calcular $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \pmod{21}$. Como es un potencia, podemos usar el teorema de Euler-Fermat; $\phi(21) = \phi(3) \times \phi(7) = 2 \times 6 = 12$, de forma que $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \equiv 3^{\left(3^{3^{3^{\cdot^{\cdot^{\cdot}}}}} \pmod{12}\right)} \pmod{21}$.

Estupendo, ahora ya no tenemos que calcular $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \pmod{21}$, sino que nos basta con conocer $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \pmod{12}$, que es obviamente mucho más fácil. Como es otra potencia, volveremos a usar el mismo truco; $\phi(12) = 4$, así que nos hará falta conocer $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \pmod{4}$, y como $\phi(4) = 2$, para ello necesitaremos $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \pmod{2}$, y dado que $\phi(2) = 1$, esto lo podremos averiguar a partir de $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \pmod{1}$. Pero claro, esto último ya lo conocemos, porque en el mundo de los enteros módulo 1 hay una gran demanda de resultados que no sean 0. De forma que podemos decir que $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \equiv 0 (\mathrm{mod}\ 1)$, de donde $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \equiv 3^0 \equiv 1 (\mathrm{mod}\ 2)$, de donde $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \equiv 3^1 \equiv 3 (\mathrm{mod}\ 4)$, de donde $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \equiv 3^3 \equiv 3 (\mathrm{mod}\ 12)$, de donde $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \equiv 3^3 \equiv 6 (\mathrm{mod}\ 21)$. Hecho.

Antes de seguir tenemos que hablar de una complicación técnica. En el cálculo anterior podríamos habernos parado al llegar a $3^{3^{3^{3^{\cdot^{\cdot^{\cdot}}}}}} \pmod{2}$. Eso

tiene que valer 1 porque todas las potencias de 3 son impares, ¿no? Y de hecho, los dos argumentos dan el mismo resultado. Pero las cosas se tuercen si consideramos $2^{2^{2^{\cdot^{\cdot}}}} \pmod 2$; esto debería ser 0 porque todas las potencias de 2 son pares, y sin embargo el argumento del párrafo anterior nos dice que vale 1 (porque el exponente módulo 1 vale 0). Empezaremos a marearnos si observamos que al calcular $4^{4^{4^{\cdot^{\cdot}}}} \pmod{21}$ podemos "plantarnos" al llegar al módulo 12, porque $4^i \equiv 4 (\text{mod } 12) \ \ \forall i > 0$. Y claro, como $13 = 12 + 1$, también podríamos plantarnos al llegar al módulo 12 si estuviésemos interesados en calcular $13^{13^{13^{13^{\cdot^{\cdot}}}}} \pmod{21}$.

A los supersticiosos les dará un pasmo el contemplar una torre de potencias con infinitos treces, pero nuestro problema es que hay varias formas diferentes de definir el valor de una torre infinita, y, aunque casi todas proporcionan los mismos resultados, algunas no. Es una suerte que las torres infinitas de potencias no sirvan para nada; si se usasen para construir aviones, yo no me atrevería a subirme a un jumbo.

Curiosamente, esta ambigüedad no importa mucho; el lector interesado podrá comprobar fácilmente que todas las operaciones que vamos a hacer funcionan perfectamente con cualquiera de las posibles definiciones, a condición de usar consistentemente una única definición para cada torre infinita. Como puede ser un poco lioso recordar cómo hemos definido cada cosa, a partir de ahora nos plantaremos siempre en el módulo 1, y ya está.

Por supuesto, no es necesario que todos los números en la torre sean iguales; todo funciona exactamente igual de bien con torres como $2^{3^{4^{5^{\cdot^{\cdot}}}}}$, lo que ocurre es que tener todos los números iguales ayuda visualmente en las fórmulas donde hayan dos torres. Porque, ahora que sabemos cómo definir el valor de las torres, podemos meterlas en las fórmulas de toda la vida. Por ejemplo, todos recordamos aquello de $(a^b)^c = a^{b \times c}$, así que ahora podremos escribir cosas tan horribles como

$$\left(2^{2^{2^{\cdot^{\cdot}}}}\right)^{\left(3^{3^{3^{\cdot^{\cdot}}}}\right)} \equiv \left(2^{\left(2^{2^{\cdot^{\cdot}}}\right)}\right)^{\left(3^{3^{3^{\cdot^{\cdot}}}}\right)} \equiv 2^{\left(\left(2^{2^{2^{\cdot^{\cdot}}}}\right) \times \left(3^{3^{3^{\cdot^{\cdot}}}}\right)\right)} (\text{mod } N)$$

para todo N. Por ejemplo, para $N = 21$; $2^{2^{2^{\cdot^{\cdot}}}} \equiv 16 (\text{mod } 21)$, $2^{2^{2^{\cdot^{\cdot}}}} \equiv 4 (\text{mod } 12)$, $3^{3^{3^{\cdot^{\cdot}}}} \equiv 6 (\text{mod } 21)$, y $3^{3^{3^{\cdot^{\cdot}}}} \equiv 3 (\text{mod } 12)$, y efectivamente, $16^3 \equiv (2^4)^3 \equiv 2^{4 \times 3} (\text{mod } 21)$. Obsérvese que hemos sustituido la torre infinita $2^{2^{2^{\cdot^{\cdot}}}}$ por 16 o por 4, según esté en la base o en el exponente: no es que $2^{2^{2^{\cdot^{\cdot}}}}$ tenga

un "valor absoluto" que funcione siempre, sino que está definido modularmente, y el módulo con el que se debe operar en la base es diferente al del exponente. ¡Esto no es ninguna trampa! También decimos que

$$25^{25} \equiv 4^{25} \equiv 4^1 (\text{mod } 21)$$

y no tenemos ningún problema en operar módulo 21 en la base y módulo 12 en el exponente.

Aquí tenemos una congruencia más monstruosa todavía, con tres niveles, que usa la vieja fórmula de $a^b \times a^c = a^{b+c}$:

$$\left(3^2\right)^{\left(2^{2^{2^{\cdot^{\cdot}}}}\right)} \equiv 3^{\left(2 \times 2^{2^{2^{\cdot^{\cdot}}}}\right)} \equiv 3^{2^{\left(1+2^{2^{2^{\cdot^{\cdot}}}}\right)}} (\text{mod } N)$$

y de nuevo podemos comprobarlo para $N = 21$; ahora el exponente del exponente hay que calcularlo módulo 4, y como $2^{2^{2^{\cdot^{\cdot}}}} \equiv 2 (\text{mod } 4)$, tenemos que efectivamente $9^4 \equiv 3^{(2\times 4)} \equiv 3^{2^{1+2}} (\text{mod } 21)$.

El lector encontrará fácil construir más monstruos que usen $(a \times b)^c = a^c \times b^c$. Recuérdese, sin embargo, que en general,

$$\left(2^{2^{2^{\cdot^{\cdot}}}}\right)^{2^{2^{2^{\cdot^{\cdot}}}}} \not\equiv 2^{2^{2^{\cdot^{\cdot}}}} (\text{mod } N),$$

si bien precisamente $N = 21$ es un caprichoso caso particular donde se produce la congruencia.

En cierto sentido, es sorprendente que se pueda definir el valor de las torres infinitas de potencias, porque en aritmética modular hay pocas cosas que funcionen. Por ejemplo, como los polinomios existen en el mundo modular, podríamos intentar definir la función seno modularmente tomando el límite de los polinomios de Taylor del seno. El problema es que no hay límites modulares...

También podemos rizar el rizo y manipular torres infinitas de potencias que continúen más allá de la parte infinita; cosas como $2^{2^{2^{\cdot^{\cdot^{\cdot}}}}3}$ (mod N), es decir, infinitos doses culminados por un tres cimero. Pero, decepcionantemente, eso vale lo mismo que $2^{2^{2^{\cdot^{\cdot}}}}$ (mod N), porque, al evaluar la torre, lo que hacemos en realidad es quedarnos con un trozo finito por abajo. Pero nos queda la gloria la gloria de haber ido más allá del infinito y haber vuelto, y ya ves, como si tal cosa.

Todo esto parece una gran chorrada, así que para dar la impresión de que las torres infinitas de potencias son algo serio, las compararemos con un problema famoso y reconocidamente importante.

Teorema. El problema de calcular el valor modular de las torres infinitas de potencias es tan difícil como el problema de factorizar números enteros.

En otras palabras, si pudiésemos calcular el valor de las torres infinitas de potencias en un tiempo polinómico, entonces también podríamos factorizar números enteros N en un tiempo polinómico de $\log(N)$, y viceversa. Uf, de repente parece que estábamos haciendo algo muy trascendente, ¿verdad?

Bueno, no daremos una demostración formal, porque al fin y al cabo todo esto es una chorrada, pero bosquejaremos una demostración.

La parte fácil es calcular el valor de las torres suponiendo que podemos factorizar. Como hemos visto, los pasos del cálculo corresponden a $\phi(N)$, $\phi(\phi(N))$, $\phi(\phi(\phi(N))) = \phi^3(N)$, etc., que calcularemos de la forma obvia, factorizando el ϕ anterior. El lector podrá demostrar solito que $\phi^i(N) \leq \max(1, N \times 2^{1-i})$, de forma que necesitaremos como mucho $\log_2(N)$ pasos, y todas las operaciones involucradas se pueden hacer en tiempo logarítmico.

La parte bonita es factorizar N en tiempo polinómico suponiendo que podemos calcular el valor de las torres en tiempo polinómico. Observemos que las torres finitas de potencias son un caso particular de las infinitas; por ejemplo, $2^3 = 2^{3^{1^{1^{\cdot^{\cdot}}}}}$ (esto es una igualdad, no sólo una congruencia). Bien, del párrafo anterior sabemos que $\phi^{\log_2(N)+1}(N) = 1$ (porque no puede ser menor que uno). Si conocemos $\phi^i(N)$ podemos averiguar cuánto vale $\phi^{i-1}(N)$ construyendo torres de potencias de i alturas y "jugando" con el último exponente. Por ejemplo, si $\phi^3(N) = 12$, entonces $\phi^2(N)$ sólo puede valer 13, 21, 26 ó 42, y sabemos factorizar estos números por la forma en que llegamos a ellos. Sustituyendo "unos cuantos" valores de x en $2^{2^x} \pmod N$ podremos averiguar cuál de esos cuatro candidatos es el período. Vale, es un poco complicado, pero se hace en tiempo logarítmico. Bien, pues procedemos inductivamente; empezamos con $\phi^{\log_2(N)+1}(N) = 1$ y llegamos a conocer $\phi(N)$, y de aquí obtenemos rápidamente una factorización de N, porque para todo x primo relativo con N tenemos $(x^{\phi(N)/2} + 1) \times (x^{\phi(N)/2} - 1) \equiv 0 (\text{mod } N)$.