ANEXO

Fragmento del capítulo "CICLOS" de la novela de Neal Stephenson "1. El código Enigma" que forma parte de la trilogía "CRIPTONOMICON". Publicado por NOVA en 2005 de la edición original de 1999[1].

(…)
—Perdóname. —Alan frena de pronto y baja de la bicicleta. Levanta la rueda trasera del pavimento, la hace girar con la mano libre, luego se agacha y tira de la cadena. Contempla el mecanismo con toda atención, interrumpida por algunos estornudos.

La cadena de la bicicleta de Turing tiene un eslabón débil. La rueda trasera tiene un radio doblado. Cuando el eslabón y el radio entren en contacto, la cadena se romperá y caerá sobre la carretera. No sucede a cada vuelta; en caso contrario la bicicleta sería completamente inútil. Sólo sucede cuando el eslabón y la rueda se encuentran en cierta posición relativa.

Basándose en suposiciones razonables respecto a la velocidad que el doctor Turing puede mantener, un ciclista enérgico (digamos 25 km/h) y el radio de la rueda trasera de la bicicleta (un tercio de metro), si el eslabón débil golpease contra el radio doblado a cada vuelta, la cadena se caería cada tercio de segundo.

De hecho, la cadena no cae a menos que el radio doblado y el eslabón débil coincidan. Ahora, supongamos que describimos la posición de la rueda trasera usando la θ habitual. Por simplificar, digamos que cuando la rueda empieza en la posición donde el radio doblado es capaz de golpear el eslabón débil (aunque sólo si el eslabón débil está ahí para ser golpeado) entonces $\theta = 0$. Si usas grados como unidades, durante una revolución completa de la rueda θ llegará hasta los 359 grados antes de volver a 0, en cuyo punto el radio doblado volverá a estar en posición de golpear la cadena. Y ahora supongamos que describes la posición de la cadena con la variable C de la siguiente forma muy simple: asignas un número a cada eslabón de la cadena. El eslabón débil tiene el número 0, el siguiente el 1, y a continuación, hasta l=1 donde l es el número total de eslabones de la cadena. Una vez más, para simplificar, digamos que cuando la cadena se encuentra en la posición donde el eslabón débil es capaz de golpear el radio doblado (aunque sólo si el radio doblado está ahí para ser golpeado) entonces C=0.

Entonces, para intentar descubrir cuándo caerá la cadena de la bicicleta del doctor Turing, todo lo que precisamos saber sobre la bicicleta está contenido en los valores de θ y C. Ese par de números define el estado de la bicicleta. La bicicleta tiene muchos estados posibles y puede haber muchos valores diferentes de (θ, C) pero sólo uno de esos estados, el (0, 0), es el que hará que la bicicleta caiga.

Supongamos que empezamos en ese estado, es decir, con ($\theta = 0$, C = 0), pero la cadena no ha caído porque el doctor Turing (conociendo muy bien el estado de su bicicleta en un momento dado) se ha detenido en medio de la carretera (casi provocando una colisión con su amigo y colega Lawrence Pritchard Waterhouse, porque la máscara antigás le bloquea la visión periférica). El doctor Turing ha tirado de la cadena hacia un lado mientras la adelanta ligeramente, evitando así que golpee el radio doblado. Ahora vuelve a subirse a la bicicleta y sigue pedaleando. La circunferencia de la rueda trasera es de unos dos metros, así que cuando se ha trasladado unos dos metros sobre la carretera, la rueda ha dado una vuelta completa y ha alcanzado de nuevo la

[1] Las notas de pie de página en este anexo, así como en el resto del volumen, son notas del autor de este texto. La nota con asterisco (*) casi al final del anexo, es original de la novela.

posición $\theta = 0$, siendo ésa la posición, recuerden, en la que el radio doblado está en posición para golpear el eslabón débil.

¿Qué hay de la cadena? Su posición, definida por C, comienza en 0 y llega a 1 cuando el siguiente eslabón se traslada a la posición fatal, luego 2 y así sucesivamente. La cadena debe moverse en sincronía con los dientes del engranaje en el centro de la rueda trasera, y ese engranaje tiene *n* dientes, por lo que después de una revolución completa de la rueda trasera, de nuevo $\theta = 0$, C=n. Después de una segunda vuelta completa de la rueda trasera, de nuevo $\theta = 0$ pero ahora C=2n. En la siguiente C=3n y así sucesivamente. Pero hay que recordar que la cadena no es infinita sino un bucle con sólo *l* posiciones; en C=*l* vuelve a C=0 y repite el ciclo. Por lo que al calcular el valor de C es necesario realizar aritmética modular, es decir, si la cadena tiene un centenar de eslabones (*l*=100) y el número total de eslabones que han sido desplazados es 135, entonces el valor de C no es 135 sino 35. Cuando tienes un número superior o igual a *l*, restas repetidamente *l* hasta que obtienes un número menor que *l*. Los matemáticos escriben esa operación como mod *l*. Por tanto, los valores sucesivos de C, cada vez que la rueda trasera da una vuelta hasta $\theta = 0$, son:

C¡=n mod *l*, 2n mod *l*, 3n mod *l*,..., in mod *l*

donde i = (1, 2, 3,... ∞)

más o menos, dependiendo de cuánto tiempo quiera Turing seguir pedaleando en su bicicleta. Después de un rato, a Waterhouse ya le parece infinitamente largo.

La cadena de la bicicleta de Turing se caerá cuando la bicicleta alcance el estado { $\theta = 0$, C=0) y visto lo escrito anteriormente, eso sucederá cuando i (que no es más que un contador que indica cuantas vueltas ha dado la rueda trasera) alcanza algún valor hipotético tal que in mod /=0, o, para explicarlo claramente, sucederá si hay algún múltiplo de n (como, oh[2], 2n, 3n, 395n o 109.948.368.443n) que resulte también ser un múltiplo de *l*. En realidad, puede haber muchos de esos llamados múltiplos comunes, pero desde un punto de vista práctico el único que importa es el primero —el mínimo común múltiplo, o MCM— porque ése será el que se alcance primero y el que hará caer la cadena.

Si, digamos, el engranaje tiene veinte dientes (n=20) y la cadena tiene cien eslabones (*1*=100), entonces después de un giro de la rueda tenemos C=20, después de dos C=40, luego 60, luego 80 y finalmente 100.

Pero como tomamos el módulo aritmético, ese valor debe cambiarse por 0. Por tanto, después de cinco vueltas de la rueda trasera, hemos llegado al estado ($\theta = 0$, C=0) y la cadena de Turing caerá. Cinco revoluciones de la rueda trasera sólo le harán avanzar diez metros, y por tanto, con esos valores de *l* y n la bicicleta es prácticamente inútil. Claro está, todo eso es cierto si Turing es tan estúpido como para empezar a pedalear con la bicicleta en el estado-que-hace-caer-la-cadena. Si, en el momento de empezar a pedalear, se encuentra en su lugar en el estado ($\theta = 0$, C=l), entonces los valores subsiguientes serán C=21, 41, 61, 81, 1, 21... y así sucesivamente; la cadena nunca se caerá. Pero se trata de un caso degenerado, donde «degenerado» tiene el significado matemático de «enojosamente aburrido». En teoría, siempre que Turing ponga su bicicleta en el estado correcto antes de aparcarla fuera del edificio, nadie podrá robársela; la cadena se caerá apenas después de haber avanzado diez metros.

Pero si la cadena de Turing tiene ciento y un eslabones (*l*=101) y después de cinco revoluciones tenemos C=100, y después de seis tenemos C=19, luego

C= 39, 59, 79, 99,18, 38, 58, 78, 98,17, 37, 57, *77*, 97,16, 36, 56, 76,
96,15, 35, 55, 75, 95,14, 34, 54, 74, 94,13, 33, 53, 73, 93,12, 32, 52,

[2] El autor de Optimiza buscó dos ediciones en español del libro y en ambas encontró la expresión “oh”. No sabemos qué significa.

72, 92,11, 31, 51, 71, 91,10, 30, 50, 70, 90, 9,29, 49, 69, 89, 8,28,48,
68, 88, 7,27,47, 67, 87, 6, 26, 46, 66, 86, 5,25, 45, 65, 85,4,24,44, 64,
84, 3,23, 43, 63, 83,2,22,42, 62, 82,1, 21,41, 61, 81, 0

Así que no será hasta la revolución 101 de la rueda trasera que la bicicleta vuelva al estado *(8=0,* C=0) cuando cae la cadena. Durante ese centenar más uno de vueltas, la bicicleta de Turing ha recorrido un quinto de kilómetro, que no está mal. Así que la bicicleta se puede usar.

Sin embargo, al contrario que en el caso degenerado, no es posible situar la bicicleta en un estado tal que la cadena nunca caiga. Tal cosa puede demostrarse repasando la lista anterior de valores de C y comprobando que todo posible valor de C, todo posible valor entre 0 y 100, está en la lista. Eso significa que no importa en qué valor esté C cuando Turing empieza a pedalear, tarde o temprano llegará al C=0 fatal y la cadena caerá. Por tanto, Turing puede dejar la bicicleta en cualquier sitio con la confianza de que, si la roban, no recorrerá más de un quinto de kilómetro sin que la cadena se caiga.

La diferencia entre el caso degenerado y el caso no degenerado está relacionada con las propiedades de los números implicados. La combinación de (n=20, *l*=100) tiene propiedades radicalmente diferentes con respecto a (n=20, *l*=101). La diferencia principal es que 20 y 101 son «primos relativos», lo que significa que no tienen factores comunes.

Eso significa que su MCM es un número grande —de hecho, es igual a *1* x n = 20 x 1001 = 2020. Mientras que el MCM de 20 y 100 es sólo 100. La bicicleta *1*=101 tiene un periodo largo —pasa por muchos estados diferentes antes de volver al principio—, mientras que la bicicleta *l*=100 tiene un periodo de unos pocos estados.

Supongamos que la bicicleta de Turing fuese una máquina de cifrado que actuase por sustitución alfabética, lo que es lo mismo que decir que reemplazaría cada una de las 26 letras del alfabeto por alguna otra letra. Una A en el texto original se podría convertir en una T en el texto cifrado, B podría transformarse en F, C podría convertirse en M, y así hasta llegar a la Z. Por sí mismo, sería un código absurdamente fácil de romper; cosa de niños. Pero supongamos que el esquema de sustitución cambiase de una letra a la siguiente. Es decir, supongamos que la primera letra del texto original fuese cifrada usando cierto alfabeto de sustitución, la segunda letra del texto original fuese cifrada usando un alfabeto de sustitución completamente diferente, y la tercera con otro diferente, y así sucesivamente. Eso se conoce como un cifrado polialfabético.

Supongamos que la bicicleta de Turing fuese capaz de generar un alfabeto diferente para cada uno de sus diferentes estados. Por tanto, el estado *(θ =0,* C=0) correspondería, digamos, a este alfabeto de sustitución:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Q G U W B I Y T F K V N D O H E P X L Z R C A S J M

pero el estado (θ =180, C=15) correspondería a este otro, diferente:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B O R I X V G Y P F J M T C Q N H A Z U K L D S E W

Dos letras no serían cifradas usando el mismo alfabeto de sustitución, es decir, hasta que la bicicleta no llegase de nuevo al estado inicial *(θ =0,* C=0) y empezase a repetir el ciclo. Eso significa que se trata de un sistema polialfabético periódico. Ahora bien, si la máquina tuviese un periodo corto, se repetiría con frecuencia, y por tanto sería útil, como sistema de cifrado, sólo contra los niños. Cuanto más largo sea el periodo (cuanto mayor sea su primitividad relativa) con menos frecuencia vuelve al mismo alfabeto de sustitución, y más seguro es.

La Enigma de tres rotores es ese tipo de sistema (es decir, polialfabético periódico). Sus rotores, como el sistema de la bicicleta de Turing, contienen ciclos dentro de ciclos. Su periodo es 17.576, lo que significa que el alfabeto de sustitución que cifra la primera letra del mensaje no volverá a

emplearse hasta que se llegue a la letra 17.577. Pero con Tiburón[3], los alemanes han añadido un cuarto rotor, elevando el periodo hasta 456.976. Los rotores se sitúan en una posición inicial diferente elegida al azar al comienzo de cada mensaje. Como los mensajes alemanes nunca llegan a los 450.000 caracteres, la Enigma nunca usa dos veces el mismo alfabeto de sustitución en un mismo mensaje, razón por la que los alemanes la consideran un buen sistema.

Un grupo de aviones de transporte pasan por encima de sus cabezas, muy probablemente en dirección al aeródromo de Bedford. Los aviones producen un zumbido diatónico curiosamente musical, como una gaita tocando dos tonos simultáneamente. Eso recuerda a Lawrence otro fenómeno más relacionado con la rueda de la bicicleta y la máquina Enigma.

—¿Sabes por qué los aviones suenan así? —pregunta.
—No, ahora que lo pienso. —Turing vuelve a quitarse la máscara antigás. Tiene la boca algo abierta y mueve los ojos de un lado a otro. Lawrence lo ha pillado por sorpresa.
—Me di cuenta en Pearl. Los motores de los aviones son rotatorios[4] —dice Lawrence—. Por tanto, deben tener un número impar de cilindros.
—¿Por tanto?
—Si tuviesen un número par, los cilindros estarían directamente en oposición, a ciento ochenta grados, y no funcionarían mecánicamente.
—¿Porqué no?
—Lo he olvidado. Pero no funcionaría.

Alan arquea las cejas. Claramente no está convencido.
—Es algo relativo a los cigüeñales —aventura Waterhouse, poniéndose algo a la defensiva.
—No estoy seguro de estar de acuerdo —dice Alan.
—Vamos a estipularlo... considéralo una condición de contorno —dice Waterhouse. Pero sospecha que Alan ya está concentrado, diseñando mentalmente un motor rotatorio de avión con un número par de cilindros.
—En todo caso, si los miras, todos tienen un número impar de cilindros —sigue diciendo Lawrence—. Por lo que el sonido de la expulsión se combina con el sonido de la hélice para producir ese sonido de dos tonos.

Alan vuelve a subir a la bicicleta y pedalea por el bosque sin hablar.

En realidad, no han estado hablando sino más bien mencionando ciertas ideas y dejando que el otro desarrolle las implicaciones. Es una forma extremadamente eficaz de comunicarse; elimina los elementos redundantes de los que se quejaba Alan en el caso de FDR[5] y Churchill.

Waterhouse está pensando en ciclos dentro de ciclos. Ya ha decidido que la sociedad humana es uno de esos supuestos de ciclos dentro de ciclos* y ahora intenta decidir si es como la bicicleta de Turing (funciona bien durante un rato, y de pronto la cadena se cae; de ahí la ocasional guerra mundial) o como la máquina Enigma (se mueve incomprensiblemente durante un tiempo, y luego de pronto los rotores se alinean como en un tragaperras y todo queda claro en una especie de epifanía global o, si se prefiere, Apocalipsis) o como un motor rotatorio de avión (gira, gira y gira; no sucede nada especial, simplemente produce mucho ruido).

* No tiene datos reales para sostenerlo, pero le parece una idea genial.

[3] Nombre dado por la Marina de Alemania durante la Segunda Guerra Mundial a su modificación de la máquina “Enigma” (N del autor de Optimiza)
[4] En la época en que se ambientó esta parte de la novela, ya no quedaban muchos aviones con motor rotativo.
[5] FDR son las iniciales usuales en esa época para referirse a Franklin Delano Roosevelt, presidente de EE.UU. durante la mayor parte de la Segunda Guerra Mundial (N del autor de Optimiza)