Matemáticas a tu alrededor

Fernando Chamizo

Universidad Autónoma de Madrid

Colegio Mayor Universitario Loyola

23 de marzo de 2022

Una cita perezosa

"[. . .] es una ironía que la ciencia más poética, más cerca del arte por el arte, sostenga una parte de la ingeniería y las aplicaciones. Las matemáticas están ahí, entre ruedas dentadas, entre chips de silicio, viajando por fibra óptica, y no son un lujo prescindible; no son solo verdades, sino también puños que empujan maquinarias inmensas".

"La Matemática y la ciencia oculta"

Antes de comenzar... las matemáticas de los matemáticos

Los poliedros convexos cumplen

$$\textbf{V}\text{értices} + \textbf{C}\text{aras} = \textbf{A}\text{ristas} + 2.$$

Con ello se puede demostrar que solo existen los cinco poliedros regulares mencionados por Platón en “El Timeo”.

4, 4, 6   8, 6, 12   6, 8, 12   20, 12, 30   12, 20, 30

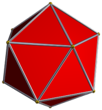
Antes de comenzar. . . las matemáticas de los matemáticos

Los poliedros convexos cumplen

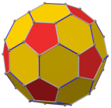
$$\textbf{V}\text{értices} + \textbf{C}\text{aras} = \textbf{A}\text{ristas} + 2.$$

Con ello se puede demostrar que solo existen los cinco poliedros regulares mencionados por Platón en “El Timeo”.

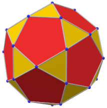
. . . y ayudar a diseñar balones de fútbol.



12, 20, 30



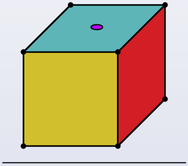
60, 32, 90 (clásico)



30, 32, 60 (Champ. 17/18)

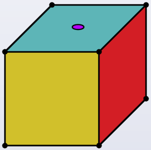
¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

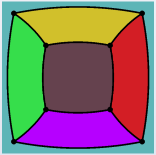
Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.



¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.

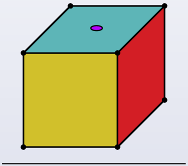


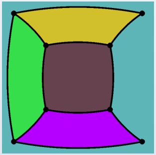


Regiones $\to$	C-1
Fronteras $\to$	A
Vértices $\to$	V

¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.

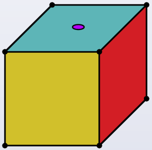


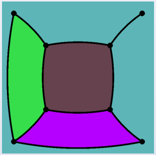


Regiones $\rightarrow$	C-1
Fronteras $\rightarrow$	A
Vértices $\rightarrow$	V

¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.

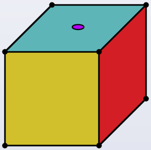


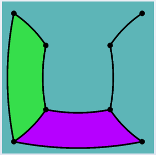


Regiones $\rightarrow$	C-1
Fronteras $\rightarrow$	A
Vértices $\rightarrow$	V

¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.

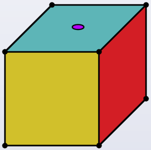


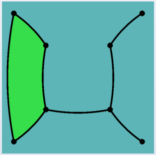


Regiones $\rightarrow$	C-1
Fronteras $\rightarrow$	A
Vértices $\rightarrow$	V

¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.

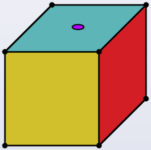


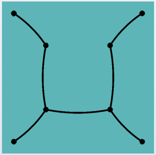


Regiones $\to$	C-1
Fronteras $\to$	A
Vértices $\to$	V

¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.

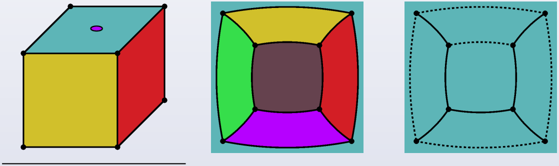




Regiones $\rightarrow$	C-1
Fronteras $\rightarrow$	A
Vértices $\rightarrow$	V

¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

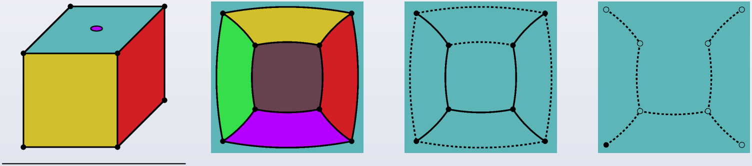
Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.



Regiones →	C-1	0
Fronteras →	A	A-(C-1)
Vértices →	V	V

¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

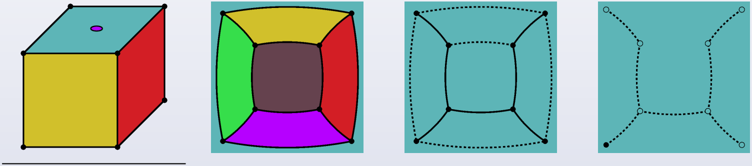
Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.



Regiones $\rightarrow$	C-1	0	0
Fronteras $\rightarrow$	A	A-(C-1)	0
Vértices $\rightarrow$	V	V	V-(A-C+1)

¿Cómo demostrar $V + C = A + 2$? (solo para fanáticos)

Hacemos un agujero, soplamos por él hasta que el poliedro sea el mapa de una isla rodeada de mar. Inundamos cada región y después quitamos cada frontera restante.



Regiones $\rightarrow$	C-1	0	0
Fronteras $\rightarrow$	A	A-(C-1)	0
Vértices $\rightarrow$	V	V	V-(A-C+1)

Como solo queda un vértice, $V - (A - C + 1) = 1$ y esto es lo mismo que $V + C = A + 2$.

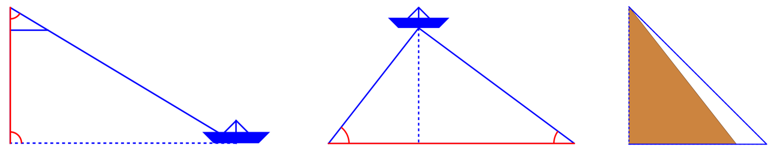
Medir: de la Tierra a las estrellas

Se considera a Tales de Mileto (s. VI AC) el primer matemático. Fuentes antiguas aseguran que midió la altura de las pirámides de Egipto y que podía calcular la distancia de los barcos a la costa.

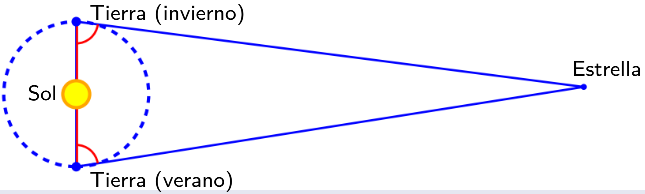
Medir: de la Tierra a las estrellas

Se considera a Tales de Mileto (s. VI AC) el primer matemático. Fuentes antiguas aseguran que midió la altura de las pirámides de Egipto y que podía calcular la distancia de los barcos a la costa.

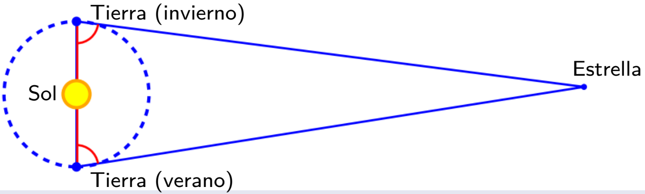
Idea: Un triángulo siempre se puede resolver con tres datos que no sean todos ángulos.



Desde el siglo XIX se usa el paralaje estelar, un método análogo para calcular la distancia a las estrellas cercanas. Requiere medir con precisión ángulos de menos de $1/5000$ grados.



Desde el siglo XIX se usa el paralaje estelar, un método análogo para calcular la distancia a las estrellas cercanas. Requiere medir con precisión ángulos de menos de $1/5000$ grados.



El paralaje estelar es un primer peldaño de la *escalera de distancias cósmicas*, una serie de métodos para realizar medidas astronómicas cada vez más grandes.

En el mundo cotidiano, la trigonometría es fundamental desde las obras públicas al posicionamiento por GPS.

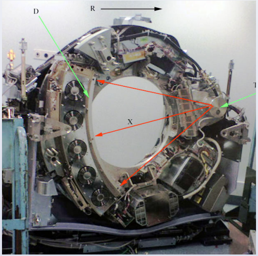
La mirada interior (TAC y resonancias)

Las TAC y resonancias son técnicas no invasivas que han revolucionado la práctica médica moderna. ¿Cómo funcionan?

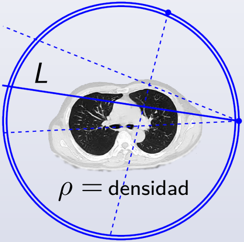
La mirada interior (TAC y resonancias)

Las TAC y resonancias son técnicas no invasivas que han revolucionado la práctica médica moderna. ¿Cómo funcionan?

TAC (basada en rayos X)



Realidad

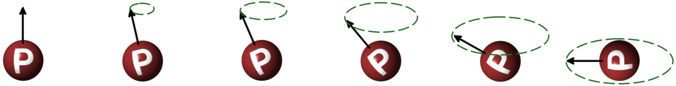


Modelo

Los rayos X que llegan a los detectores por L, están atenuados una cantidad que depende de la integral $\int_L \rho$.

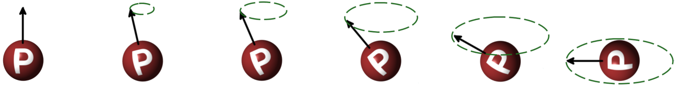
Resonancia (basada en el espín de protones)

Los protones de los átomos de hidrógeno (sobre todo del agua) en nuestro cuerpo se comportan como imanes diminutos que se pueden alinear con un campo magnético y hacer oscilar con radiofrecuencia.



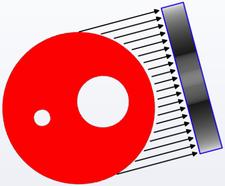
Resonancia (basada en el espín de protones)

Los protones de los átomos de hidrógeno (sobre todo del agua) en nuestro cuerpo se comportan como imanes diminutos que se pueden alinear con un campo magnético y hacer oscilar con radiofrecuencia.



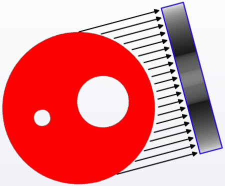
Es posible "contar protones" en una línea recta combinando

- Física $\rightarrow$ Principios del XX (física del espín)
- Matemáticas $\rightarrow$ Principios del XIX (análisis de Fourier)
- Tecnología $\rightarrow$ Finales de la década de 1970



En cualquiera de los casos la información obtenida es la “sombra traslúcida” de la muestra en un montón de direcciones.

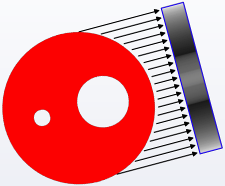
En 1917 J. Radon introdujo una fórmula para recuperar objetos a partir de todas sus “sombras traslúcidas”.



En cualquiera de los casos la información obtenida es la "sombra traslúcida" de la muestra en un montón de direcciones.

En 1917 J. Radon introdujo una fórmula para recuperar objetos a partir de todas sus "sombras traslúcidas".

$$\rho(x, y) = \int_0^{2\pi} \int_0^{\infty} r\widehat{P}_\alpha(r) e^{2\pi i r(x \cos\alpha + y \operatorname{sen}\alpha)}\, dr\, d\alpha.$$

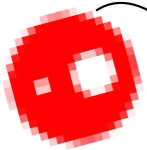


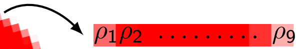
En cualquiera de los casos la información obtenida es la “sombra traslúcida” de la muestra en un montón de direcciones.

En 1917 J. Radon introdujo una fórmula para recuperar objetos a partir de todas sus “sombras traslúcidas”.

¿Por qué es esto posible? Una idea:

Recta $\to$ ecuación para las densidades “pixeladas” de la cual se puede despejar y sustituir en otras ecuaciones.





$$\rho_1 + \rho_2 + \cdots + \rho_9 = k$$
$$\rho_1 = k - \rho_2 - \cdots - \rho_9$$

Hablando en privado a voces

La especificación Bluetooth establece una conexión cercana ($\approx 10\,m$) entre un par de dispositivos mediante ondas de radio. La capacidad máxima es de decenas de pares de dispositivos próximos.

Hablando en privado a voces

La especificación Bluetooth establece una conexión cercana ($\approx 10\,m$) entre un par de dispositivos mediante ondas de radio. La capacidad máxima es de decenas de pares de dispositivos próximos.

¿Cómo funciona?

Tres puntos fundamentales:

1. Se establecen 79 canales permitiendo el **salto de frecuencia** 1600 veces/s.
2. Se divide la información en **paquetes cortos** (< 1K).
3. Se aplican métodos de reducción de ruido y **detección de errores**.

Hablando en privado a voces

La especificación Bluetooth establece una conexión cercana ($\approx 10\,m$) entre un par de dispositivos mediante ondas de radio. La capacidad máxima es de decenas de pares de dispositivos próximos.

¿Cómo funciona?

Tres puntos fundamentales:

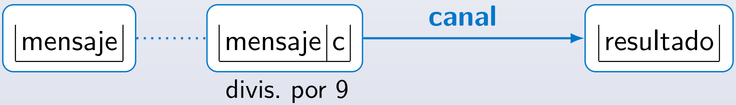
1. Se establecen 79 canales permitiendo el **salto de frecuencia** 1600 veces/s.
2. Se divide la información en **paquetes cortos** (< 1K).
3. Se aplican métodos de reducción de ruido y **detección de errores**.

La detección de errores en muchas aplicaciones es una generalización de la prueba del nueve.

$$9 \text{ divide a } n \quad \Leftrightarrow \quad \text{Suma de cifras de la suma de cifras\dots}$$
$$\text{\dots de la suma de cifras de } n = 9.$$

$$37978746379252364673742336977392482601061 \quad \to \quad 189 \quad \to \quad 18 \quad \to \quad 9$$

Esquema:



c es un dígito de control para forzar la divisibilidad por 9. Si el resultado no es múltiplo de nueve, ha habido un error.

Métodos muy sofisticados usados en los Blu-ray permiten, no solo detectar errores, sino también corregirlos en tiempo real.

Los protocolos usados en Bluetooth se suelen asociar a divisibilidad por polinomios:

$$
\begin{array}{lcl}
\text{CRC-8} & \rightarrow & x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\text{CRC-16-CCITT} & \rightarrow & x^{16} + x^{12} + x^5 + 1
\end{array}
$$

Los protocolos usados en Bluetooth se suelen asociar a divisibilidad por polinomios:

$$\begin{array}{lcl} \text{CRC-8} & \to & x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1 \\ \text{CRC-16-CCITT} & \to & x^{16}+x^{12}+x^5+1 \end{array}$$

La detección de errores por divisibilidad se usa en muchas aplicaciones cotidianas: Códigos de barras, **IBAN**.

ES 06 2038 0603 2860 0103 6580

rotación

2038 0603 2860 0103 6580 ES 06

letras→num. $\mathtt{E}=14$, $\mathtt{S}=28$

2038 0603 2860 0103 6580 1428 06

El resultado menos 1 debe ser divisible por 97:

$2038060328600103658014280 5 = 21010931222681481010456 5 \times 97$.

En España además hay una seguridad extra basada en la divisibilidad por 11.

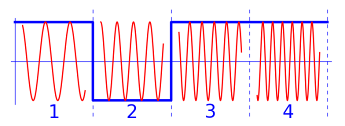
Hablando en privado a voces (II)

El paso de 3G a 4G fue un hito en la historia de la telefonía móvil ligado al desarrollo de los *smartphones*, que cobraron sentido gracias a que la velocidad de transmisión de datos se multiplicó.

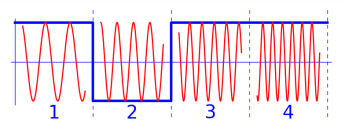
Parte del avance se debió al uso de OFDM (*orthogonal frequency division multiplexing*) para un mejor aprovechamiento del ancho de banda.

"ortogonal" es la forma matemática de decir "perpendicular".

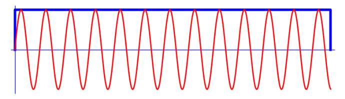
Sin OFDM (4 usuarios):



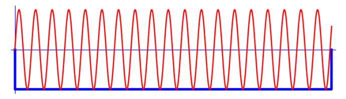
Sin OFDM (4 usuarios):

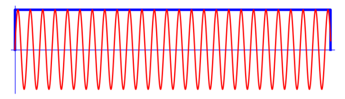


Con OFDM: suma de

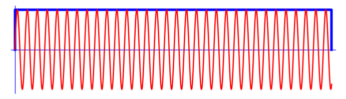


,



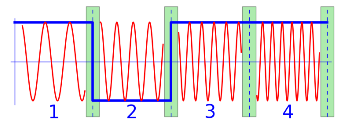


,

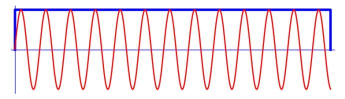


Se puede recuperar el dato de cada usuario usando ondas digitalizadas “perpendiculares”.

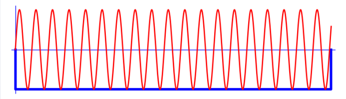
Sin OFDM (4 usuarios):

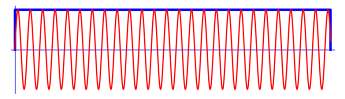


Con OFDM: suma de

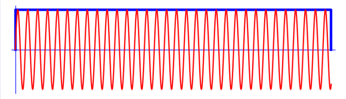


,



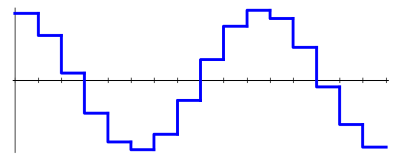


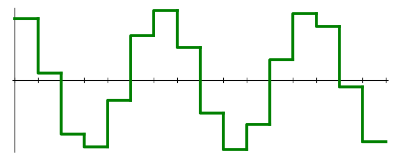
,



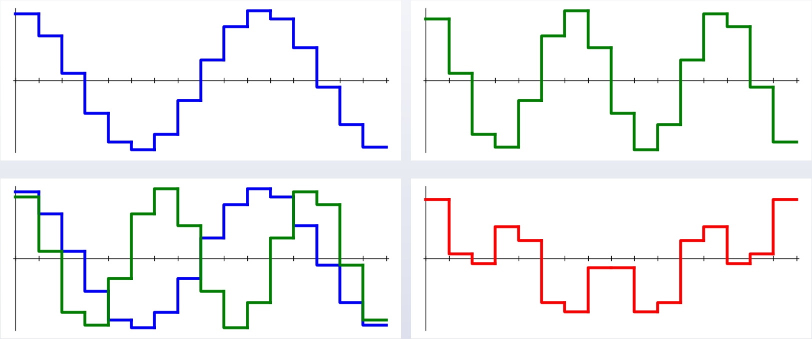
Se puede recuperar el dato de cada usuario usando ondas digitalizadas “perpendiculares”.

La perpendicularidad significa que el promedio del producto de las ondas es cero.





La perpendicularidad significa que el promedio del producto de las ondas es cero.



La perpendicularidad y el tratamiento de estas ondas digitalizadas es la base de muchas aplicaciones.

Datos "crudos": $1924 \times 453 \times 3 \approx 2{,}6\,\mathrm{M}$

Compresión sin pérdidas (png): $1{,}8\,\mathrm{M}$, **jpg:** $382\,\mathrm{K}$

Datos "crudos": $1924 \times 453 \times 3 \approx 2{,}6\,\mathrm{M}$
Compresión sin pérdidas (png): $1{,}8\,\mathrm{M}$, **jpg:** $382\,\mathrm{K}$

Filtrado de frecuencias (jpg): $73\,\mathrm{K}$,

Datos "crudos": $1924 \times 453 \times 3 \approx 2{,}6\,\mathrm{M}$
Compresión sin pérdidas (png): 1,8 M, **jpg:** 382 K

Filtrado severo de frecuencias (jpg): 30 K,

Top secret

Es muy conveniente que un terminal reconozca la contraseña de muchos usuarios, pero no es muy seguro que se almacenen todas las contraseñas en cierta parte de la memoria.

¿Se pueden reconocer datos sin almacenarlos?

Funciones de un solo sentido $f : \text{dato} \longrightarrow \text{resultado}$

Es fácil hallar $f(\text{dato})$ pero en la práctica es imposible recuperar el dato del resultado.

Top secret

Es muy conveniente que un terminal reconozca la contraseña de muchos usuarios, pero no es muy seguro que se almacenen todas las contraseñas en cierta parte de la memoria.

¿Se pueden reconocer datos sin almacenarlos?

Funciones de un solo sentido $f : \text{dato} \longrightarrow \text{resultado}$

Es fácil hallar $f(\text{dato})$ pero en la práctica es imposible recuperar el dato del resultado.

$p =$ número primo de cientos de cifras
$b =$ número entero fijado $d =$ dato (menor que p).

$$\boxed{f = \text{resto al dividir } b^d \text{ por } p}$$

Calcular $f(\textit{dato}) \rightarrow$ del orden de cientos de operaciones.

Actualmente, recuperar el dato requiere hasta del orden de $\sqrt{p}$ operaciones.

$$\begin{array}{l|l} 38^{54} & 103 \\ \hline (?) & \dots \end{array}$$

El número 38^{54} tiene 86 cifras.
¿Se puede calcular su resto al dividir por 103 con lápiz y papel?

$$\begin{array}{r|l} 38^{54} & 103 \\ \hline (?) & \dots \end{array}$$

El número 38^{54} tiene 86 cifras.
¿Se puede calcular su resto al dividir por 103 con lápiz y papel?

$$\begin{array}{ccccccccccc} 38^{54} = 38^{2+4+16+32} = & 38^2 & \times & 38^4 & \times & & \times & 38^{16} & \times & 38^{52} \\ \rightarrow & 38^2 & \times & r_2^2 & \times & r_4^2 & \times & r_8^2 & \times & r_{16}^2 \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ & r_2 & & r_4 & & r_8 & & r_{16} & & r_{32} \end{array}$$

El resto buscado es el mismo que el de $2 \times 4 \times 50 \times 28 \rightarrow 76$.

$$\begin{array}{r|l} 38^{54} & 103 \\ \cline{2-2} (?) & \ldots \end{array}$$

El número 38^{54} tiene 86 cifras.
¿Se puede calcular su resto al dividir por 103 con lápiz y papel?

$$\begin{array}{lccccccccccc}
38^{54} = 38^{2+4+16+32} = & 38^2 & \times & 38^4 & \times & & \times & 38^{16} & \times & 38^{52} \\
\rightarrow & 38^2 & \times & r_2^2 & \times & r_4^2 & \times & r_8^2 & \times & r_{16}^2 \\
 & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 & r_2 & & r_4 & & r_8 & & r_{16} & & r_{32} \\
38\times 38=1444 & \shortparallel & & \shortparallel & & \shortparallel & & \shortparallel & & \shortparallel \\
14\times 103=1442 & 2 & & 4 & & 16 & & 50 & & 28
\end{array}$$

El resto buscado es el mismo que el de $2 \times 4 \times 50 \times 28 \rightarrow 76$.

Colgaré esta presentación en:

https://www.uam.es/fernando.chamizo

Gracias por la atención