Del reparto en la tribu al candado digital: breve reseña histórica de la divisibilidad

El matemático Carl Friedrich Gauss afirmó en el siglo XIX: *«La matemática es la reina de las ciencias, y la teoría de los números es la reina de las matemáticas»*. Durante mucho tiempo, en las aulas, la divisibilidad se ha enseñado como un mero conjunto de reglas mecánicas (las famosas «reglas de divisibilidad» o la búsqueda del mínimo común múltiplo). Sin embargo, la historia nos revela que la divisibilidad no es un simple trámite escolar. Es la búsqueda de los «átomos» que componen la realidad numérica, un viaje que comenzó con el reparto de alimentos en la antigüedad y que hoy protege cada mensaje secreto que enviamos por internet.

1. El banquete de la tribu: Pares, impares y la obsesión pitagórica

Antes de que existieran los algoritmos, la divisibilidad nació de una necesidad física y social: **compartir**. Repartir 12 piezas de fruta entre 3 personas era posible sin que sobrara nada; repartir 13 piezas dejaba un «resto». De esta experiencia cotidiana surgió la primera y más profunda clasificación de los números: **pares e impares**.

Para los **pitagóricos** (siglo VI a.C.), esta división no era solo aritmética, sino filosófica y moral. El número par, al ser divisible por 2, representaba lo justo, lo simétrico y lo limitado. El número impar, al resistirse a una división exacta y dejar siempre un residuo, era considerado caótico, imperfecto y misterioso. Fue en esta época donde la mente humana dejó de ver los números solo como «cantidades de cosas» para empezar a verlos como **entidades con propiedades internas**. Nació la curiosidad por saber *cómo* se comportaban los números entre sí, dando lugar a conceptos como los «números amigos» o los «números perfectos» (aquellos que son iguales a la suma de sus divisores propios, como el 6, ya que 1+2+3 = 6).

El estudio sistemático de los divisores y sus propiedades fascinaba a los pitagóricos, pero fue el matemático y filósofo neopitagórico **Nicomaco de Gerasa** quien, en su obra *Introducción a la Aritmética* (*Introductio Arithmetica*, c. 100 d.C.), clasificó exhaustivamente los números en función de sus divisores propios. Nicomaco definió los números perfectos, abundantes y deficientes según la suma de sus divisores, un estudio que, como señala el historiador Florian Cajori en su *A History of Mathematics* (1893), sentó las bases de la teoría de la divisibilidad que hoy usamos para resolver problemas de empaquetado y reparto. Por otro lado, la búsqueda de múltiplos comunes, esencial para resolver problemas de periodicidad y dimensiones, hunde sus raíces en la geometría práctica y la agrimensura de la antigüedad, donde hallar medidas comunes era vital para la construcción y el comercio.

2. Los átomos de la matemática: Euclides y el algoritmo (Siglo III a.C.)

El gran salto de la especulación filosófica a la demostración lógica llegó con **Euclides de Alejandría** y su obra maestra, *Los Elementos* (específicamente en los libros VII, VIII y IX). Euclides fue el primero en estudiar la divisibilidad con rigor científico. Dos de sus aportaciones siguen siendo el núcleo de lo que estudiamos hoy:

- **El algoritmo de Euclides:** para encontrar el Máximo Común Divisor (MCD) de dos números, Euclides no inventó una fórmula mágica, sino un *procedimiento* (un algoritmo) basado en restas sucesivas. Es considerado el algoritmo más antiguo de la historia que aún se utiliza hoy en día.
- **El teorema fundamental de la aritmética:** Euclides demostró que todo número entero mayor que 1 es, o bien un número primo, o bien puede descomponerse en un producto de números primos de una única manera. Con este hallazgo, los **números primos** (aquellos que solo son divisibles por 1 y por sí mismos) dejaron de ser simples curiosidades para convertirse en los «ladrillos» o «átomos» indestructibles con los que se construye todo el universo de los números naturales.

3. La aritmética del reloj: Gauss y los restos (Siglo XIX)

Durante siglos, matemáticos como Pierre de Fermat o Leonhard Euler se obsesionaron con encontrar patrones en los números primos, tratando de predecir dónde aparecerían. Pero fue **Carl Friedrich Gauss** quien, en 1801, cambió las reglas del juego con su obra *Disquisitiones Arithmeticae*.

Gauss se dio cuenta de que, en la divisibilidad, lo que importaba no era el resultado exacto de una división, sino **el resto**. Inventó la **aritmética modular** (o «la matemática del reloj»). Si son las 10:00 y pasan 5 horas, generalmente no decimos que son las 15:00, sino las 3:00. Gauss formalizó esta idea (congruencias) para estudiar la divisibilidad. Demostró que los números primos, aunque parezcan aparecer al azar en la recta numérica, en realidad obedecen a leyes profundas y ocultas si se observan a través de los «restos» que dejan al dividirlos. Esta rama de las matemáticas, la Teoría Analítica de Números, permitió empezar a predecir la distribución de los primos.

4. Epílogo: la ironía de la matemática «inútil» y el candado digital

A principios del siglo XX, el matemático G.H. Hardy se jactaba de que la teoría de los números (el estudio de la divisibilidad y los primos) era la rama más «pura» e «inútil» de las matemáticas, precisamente porque no tenía ninguna aplicación en el mundo real. Se equivocaba de manera espectacular.

En 1977, tres científicos (Rivest, Shamir y Adleman) crearon el **algoritmo RSA**, la base de la criptografía moderna. ¿Cómo funciona? Se basa en una asimetría de la divisibilidad: es muy fácil multiplicar dos números primos gigantes (de cientos de dígitos), pero es **computacionalmente imposible** hacer el proceso inverso (encontrar los divisores primos del número resultante) usando los ordenadores actuales. Hoy, cada vez que introduces tu contraseña en el banco, envías un mensaje cifrado por WhatsApp o compras por Internet, tu dispositivo está multiplicando números primos gigantes para crear un «candado» digital.

Lo que comenzó como la necesidad de una tribu antigua para repartir su comida de forma justa, y que los griegos elevaron a la categoría de filosofía pura, se ha convertido en el guardián invisible de la era de la información. La divisibilidad no es solo una regla para hacer fracciones; es el lenguaje con el que la humanidad aprendió a proteger sus secretos.

Bibliografía:

- **Euclides. (c. 300 a.C.).** *Los Elementos* (Libros VII-IX).
- **Cajori, F. (1893)**. *A history of mathematics*. Macmillan and Co.
- **Gauss, C. F. (1801).** *Disquisitiones Arithmeticae*. (Edición moderna de Yale University Press, 1965).
- **Singh, S. (1999).** *Los códigos secretos: La historia de los códigos y su desciframiento*. Editorial Debate.
- **Dunham, W. (2011).** *El viaje de las matemáticas: A través de los grandes teoremas*. Editorial Pirámide.