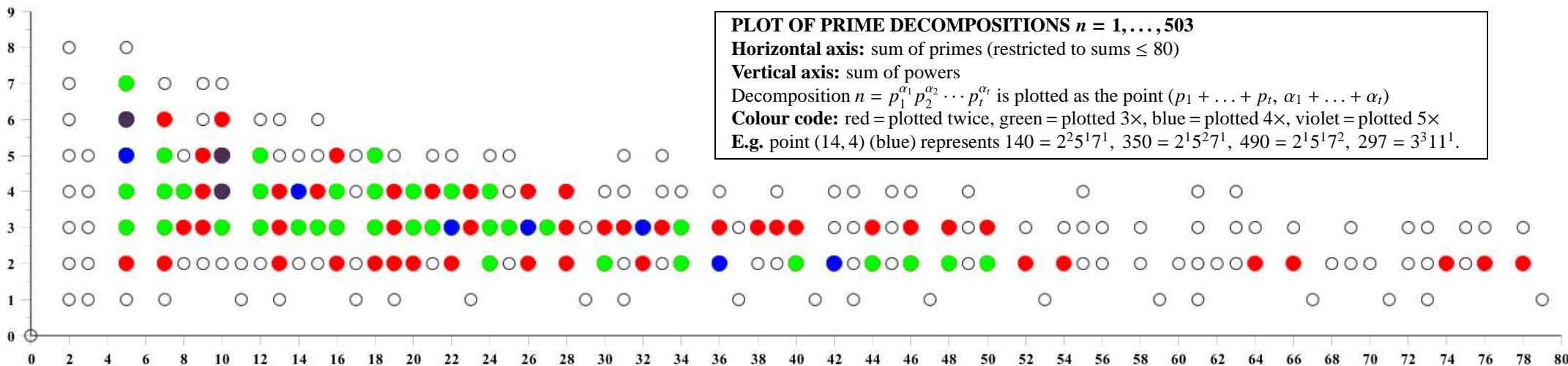# THEOREM OF THE DAY

The Fundamental Theorem of Arithmetic *Every integer greater than one can be expressed uniquely (up to order) as a product of powers of primes.*

PLOT OF PRIME DECOMPOSITIONS $n = 1, \ldots, 503$
Horizontal axis: sum of primes (restricted to sums ≤ 80)
Vertical axis: sum of powers
Decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ is plotted as the point $(p_1 + \ldots + p_t, \alpha_1 + \ldots + \alpha_t)$
Colour code: red = plotted twice, green = plotted 3×, blue = plotted 4×, violet = plotted 5×
E.g. point (14, 4) (blue) represents $140 = 2^2 5^1 7^1$, $350 = 2^1 5^2 7^1$, $490 = 2^1 5^1 7^2$, $297 = 3^3 11^1$.

In the above visualisation a positive integer determines a walk in the positive quadrant of the plane, starting at the origin: for each prime power, in order, we walk the prime horizontally followed by its power vertically. The fundamental theorem says that this walk exists and is unique.

Existence may be proved by contradiction, assuming a smallest counterexample N, necessarily composite since primes automatically factorise. Then $N = a \times b$, where a and b, being smaller than N have prime factorisations. But the product of two prime factorisations is again a prime factorisation, so our counterexample fails.

Uniqueness follows from Euclid, *Elements*, **Book 7, Proposition 30**: *if a prime divides the product of two numbers then it must divide one or both of these numbers.* Again, assume a smallest counterexample having two different factorisations, $F_1 = F_2$, say. Take a prime p from F_1: it divides F_2 whence, by repeated application of Euclid, it divides a prime in F_2 which it must therefore equal. Dividing both sides of the equality by p gives a smaller counterexample which is a contradiction.

Other than visualising factorisations the plot suggests various elementary observations around the **Goldbach Conjecture**: *every even integer greater than 2 is a sum of two primes.* Thus, we observe that Goldbach will follow if there is a factorisation walk to every point of the form $(2k, 2)$, for $k > 3$. For example, the point $(50, 2)$ is green—there are three walks to this point. They correspond to the factorisations $141 = 3^1 47^1$, $301 = 7^1 43^1$ and $481 = 13^1 37^1$, whence $50 = 3 + 47 = 7 + 43 = 13 + 37$. Eventually $(50, 2)$ will plot blue because there is a final factorisation, $589 = 19^1 31^1$, which is beyond the range of our data, which stops at $n = 503$. The point $(80, 2)$, which has no walk in our plot, will eventually also plot blue. The smallest factorisation plotting this point is $n = 511 = 7^1 73^1$. The truth of Goldbach would not, conversely, guarantee walks to all points $(2k, 2)$: specifically, this fails for p prime such that the only Goldbach sum for $2p$ is $2p = p + p$, corresponding to the factorisation p^2, which plots at $(p, 2)$. It is believed that this only occurs for $p = 2$ and $p = 3$. In 1959, Waclaw Sierpiński proved that a stronger version of Goldbach, that every even number greater than 6 is a sum of two distinct primes, is equivalent to asserting that every integer greater than 17 is a sum of three distinct primes. This says that every point $(2k, 2)$, $k > 3$, is plotted if and only if every point $(m, 3)$, $m > 17$, is plotted.

Although Euclid provided the key ingredient for uniqueness, the more subtle aspect of the Fundamental Theorem, the theorem itself then had to wait more than two thousand years before it was finally established as the bedrock of modern number theory by Gauss, in 1798, in his *Disquisitiones Arithmeticae*.