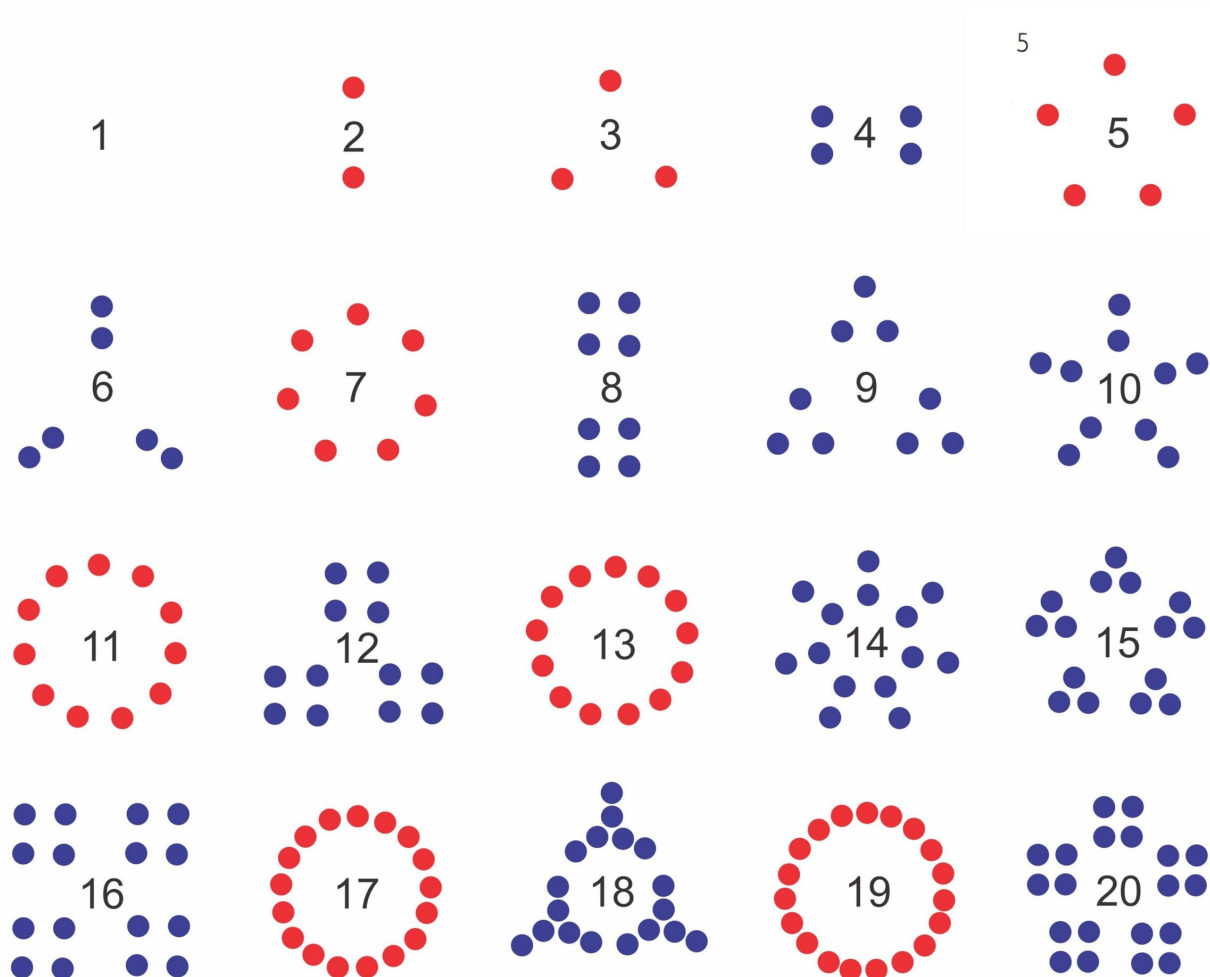


# Prime Numbers: Mysterious Building Blocks

A prime number is one that can only be divided by 1 and itself. Prime numbers are the building blocks for all the natural numbers, each of which can be expressed as a unique product of primes. Although their primacy can be proven by demonstrating that they are not divisible by any other number, where the prime numbers occur among the natural numbers cannot be predicted. Prime numbers are as mysterious as they are essential. The illustration shows the 25 primes (yellow) that occur in the first 100 numbers.

## Some Fundamentals

A “prime number”  $p$  is a natural number (a positive integer) greater than 1 that is divisible only by 1 and itself. A “composite number” is any natural number greater than 1 that is not a prime. In positive terms, a composite number  $n$  is divisible without remainder by two numbers between 1 and  $n$ :  $n=ab$ . The two kinds of numbers can be illustrated graphically. Composite numbers of objects (blue) can be organized into repeating groups (factors), whereas prime numbers of objects (red) cannot:



This idea is also illustrated in a delightful animation of the “Factor Conga” by Stephen Von Worley.

The number 1 was sometimes considered prime, but nowadays 1 is viewed as a special number – “unit” or “unity” – because of two properties (Lamb, 2019). First is the “multiplicative identity” characteristic: any number multiplied by 1 remains the same number. Second is the “multiplicative inverse” characteristic. The multiplicative inverse of a number multiplied by the original number gives 1. The multiplicative inverse of any number greater than 1 is a fraction, e.g., the multiplicative inverse of 2 is  $1/2$ . The multiplicative inverse of 1 is the integer 1.

## Factorization

The determination of the numbers that when multiplied together give a composite number is called "factorization." The simplest algorithm involves "trial division:" one divides each of the primes into the number to see which leaves no remainder, and repeats this with the quotient: The prime factors of 1540 are 2, 5, 7 and 11:

	1540	
divide by 2:	②	770
divide quotient by 2:	②	385
divide quotient by 2:		
divide quotient by 3:		
divide quotient by 5:		⑤      77
divide quotient by 5:		
divide quotient by 7:		⑦      ⑪

Pierre de Fermat (1601-1665) was a French mathematician and magistrate. He is probably most famous for his "last theorem" – that no three positive integers  $a$ ,  $b$ , and  $c$  satisfy the equation  $a^n + b^n = c^n$  for any integer value of  $n$  greater than 2 – for which he claimed to have a "marvelous proof." A proof of the theorem was finally published by Andrew Wiles in 1994.

However, Fermat also proposed a method for factorization based on the equation

$$a^2 - b^2 = (a + b)(a - b)$$

This method works best if the number  $n$  is the product of two nearby integers.

Select  $a$  as the next integer greater than  $\sqrt{n}$ .

Calculate  $b^2 = a^2 - n$ . Increment  $a$  until  $\sqrt{b^2}$  is an integer.

Return values  $a + \sqrt{b^2}$  and  $a - \sqrt{b^2}$

For the number 5959, the following are the steps

$a$	78	79	
80			
$b^2 = a^2 - n$	125	282	441
$\sqrt{b^2}$	11.2	16.8	21

giving  $80+21$  (101) and  $80-21$  (59) as factors of 5959.

Factorization leads to the "Fundamental Theorem of Arithmetic" (also called the "Prime Factorization Theorem") generally attributed to Euclid, a Greek mathematician who worked around 300 BCE in Alexandria:



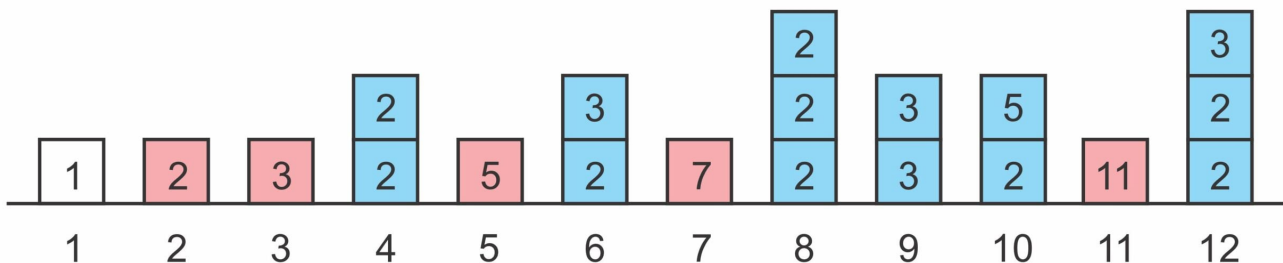
(for the last example, 59 and 101 are the 17<sup>th</sup> and 26<sup>th</sup> primes).

Euclid also proved that the number of primes is infinite. The proof posits a number  $p_n$  that is the largest of all primes. We can then form a number  $N$  by multiplying all the primes up to an including  $p_n$  and adding 1.

$$N = p_1 p_2 p_3 \dots p_n + 1$$

Since every prime less than  $N$  divides once into  $N$  giving a quotient equal to the product of the other prime numbers and leaving a remainder of 1,  $N$  is prime. To postulate a number  $p_n$  as the largest of all primes is impossible. Therefore, the number of primes is infinite.

The natural numbers can be viewed as buildings with the primes having only one storey and the composite numbers having multiple storeys:



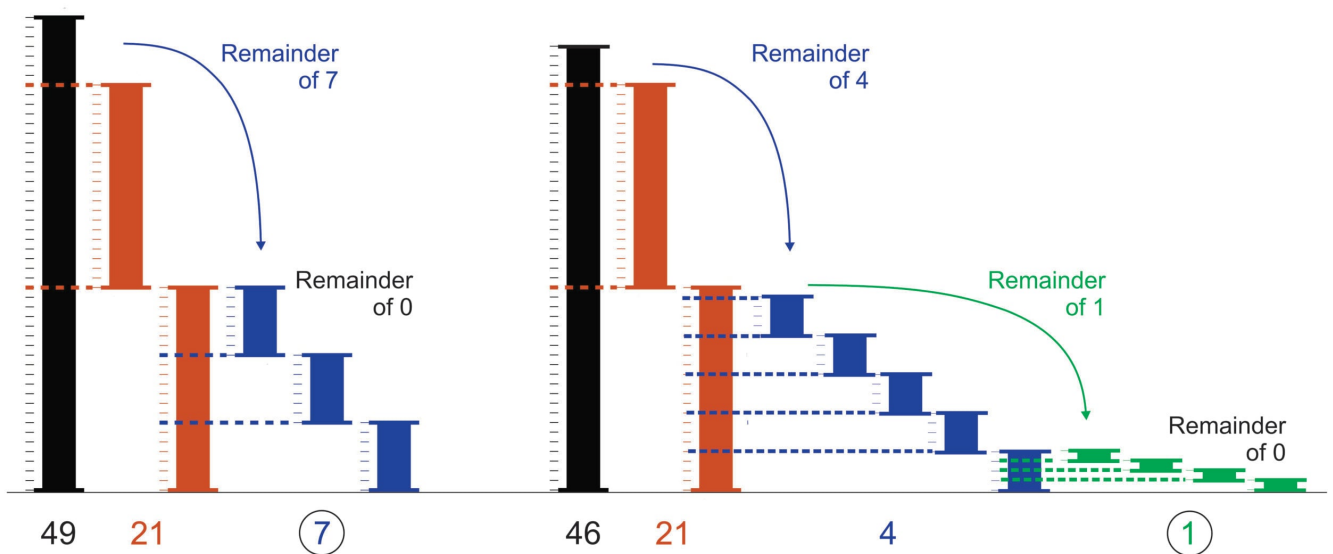
As well as the prime factors one can also determine the greatest common divisor (GCD) of two numbers. Instead of calculating all the prime factors one can use Euclid's algorithm to determine the GCD of two numbers  $a > b$ . One iterates the following commands

Divide  $b$  into  $a$  to give a quotient and remainder.

Replace  $a$  with  $b$  and  $b$  with the remainder.

until the remainder equals zero, in which case the current value of  $b$  is the GCD. The following illustration (modified from Wikipedia) shows the algorithm graphically for 49 and 21

(GCD of 7) and for 46 and 21 (GCD 1):



Two numbers are considered “relatively prime” or “coprime” if their GCD is 1, e.g. 46 and 21.

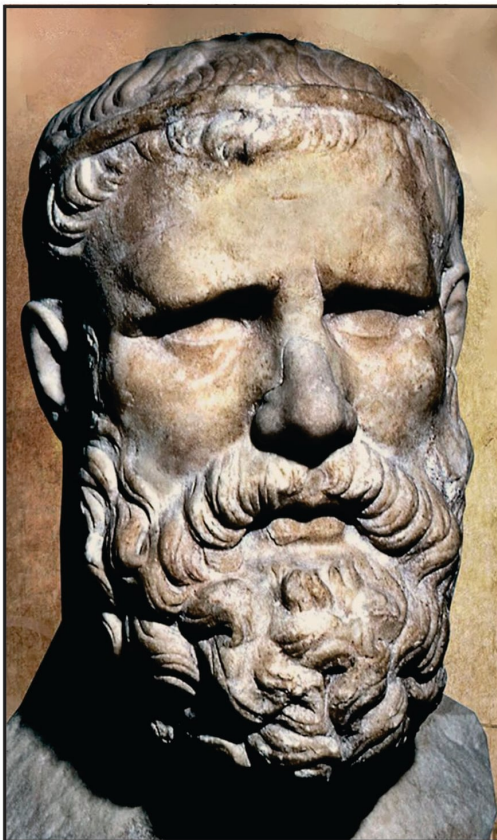
In 1742, the Prussian mathematician Christian Goldbach (1690-1764) conjectured that every even number greater than 2 can be represented as the sum of two prime numbers. This also meant that every odd number is the sum of two primes +1. Goldbach’s conjecture is true for all natural numbers that have been examined, but has not yet been proven.

The prime numbers therefore are the building blocks of arithmetic. Every number can be represented as the product of primes and every even number as the sum of two primes. Du Sautoy (2003, p 5) has called the primes the “very atoms of arithmetic,” and likened the list of primes to the periodic table of the elements.

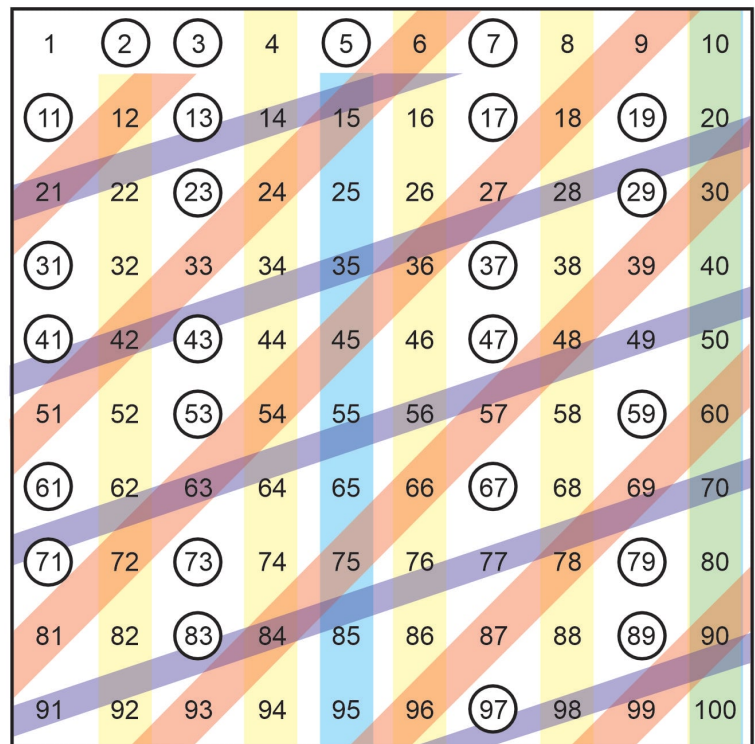
## Finding Primes

Various techniques have been proposed to identify which numbers are prime in a set of numbers. Erastosthenes, the

chief librarian of the Library of Alexandria in the 3<sup>rd</sup> Century BCE, became famous for his remarkably accurate estimate of the circumference of the world (Nicastro, 2008). He also proposed an algorithm for identifying primes that is known as the "Sieve of Erastosthenes." The algorithm iteratively rejects as composite those numbers that are multiples of the prime numbers less than the square root of the maximum number to be evaluated. Thus, to examine the numbers between 1 and 100, one marks the multiples of 2, 3, 5, and 7. When the numbers are arrayed 10 by 10, the multiples of 2 and 5 form vertical lines (yellow and blue, with an overlap as green), and the multiples of 3 and 7 form sloping lines (red and dark blue). The unrejected numbers (circled) are primes.



### The Sieve of Erastosthenes



As the range of numbers to be examined gets large such approaches to identifying primes become very time-consuming even for very fast computers. It would be wonderful if there were a simple equation to identify all the prime numbers.

Unfortunately, there is no such formula (Mackinnon, 1987). Some formulae can identify some prime numbers.

Fermat proposed that numbers of the form

$$2^{2^n} + 1$$

are prime. However, the formula only works for  $n$  between 0 and 4. Leonhard Euler (1707-1783) came up with an intriguing formula

$$n^2 + n + 41$$

but this only works for  $n$  between -1 and 39.

Marin Mersenne (1588-1648) proposed that numbers of the form

$$2^p - 1$$

are prime when  $p$  is prime. However, this only works for some primes: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89 ... Nevertheless, this formula serves to identify numbers as possible primes. The largest known prime number was found in this way.

Recently a formula involving 26 variables has been created that will provide positive and negative numbers when different combinations of integer variables are used for the variables. The positive numbers are primes (Jones et al, 1976). The calculations are laborious and there appears to be no clear logic behind the formula:

THEOREM 1. *The set of prime numbers is identical with the set of positive values taken on by the polynomial*

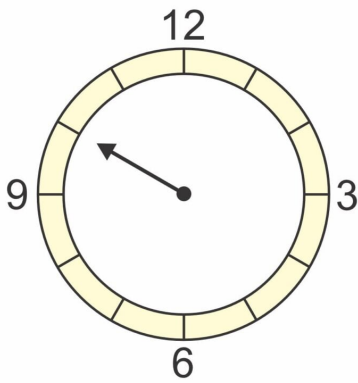
$$\begin{aligned}
 (1) \quad & (k+2)\{1 - [wz + h + j - q]^2 - [(gk + 2g + k + 1) \cdot (h + j) + h - z]^2 - [2n + p + q + z - e]^2 \\
 & - [16(k+1)^3 \cdot (k+2) \cdot (n+1)^2 + 1 - f^2]^2 - [e^3 \cdot (e+2)(a+1)^2 + 1 - o^2]^2 - [(a^2-1)y^2 + 1 - x^2]^2 \\
 & - [16r^2y^4(a^2-1) + 1 - u^2]^2 - [(a + u^2(u^2 - a))^2 - 1] \cdot (n + 4dy)^2 + 1 - (x + cu)^2\}^2 - [n + l + v - y]^2 \\
 & - [(a^2-1)l^2 + 1 - m^2]^2 - [ai + k + 1 - l - i]^2 - [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 \\
 & - [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 - [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2\}
 \end{aligned}$$

*as the variables range over the nonnegative integers.*

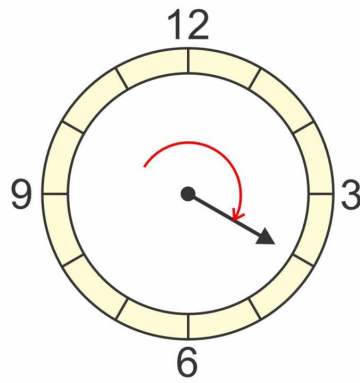
Finding out whether a particular number is prime or composite is a time-consuming process. Basically, one needs to determine the factors of the number. Various algorithms have been proposed to speed up the process. Some combine various approaches such as the sieve of Eratosthenes and Fermat's method based on the difference in squares. However, the process remains slow for very large numbers even on the fastest of computers.

## Modular Arithmetic

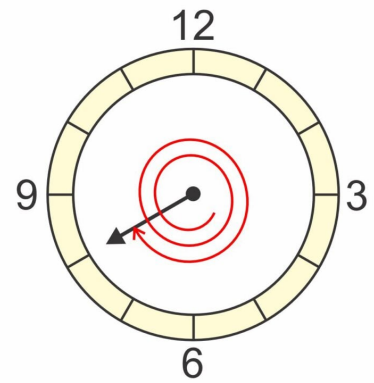
Important to any understanding of primes is an assessment of how clock numbers work. If a simple clock displays 1 to 12 hours on its face, amounts of time are considered to work in increments of 12. Therefore 6 hours later than 10 o'clock shows as 4 o'clock rather than 16, and a further 28 hours later shows as 8 o'clock rather than 32 (or 44 if counting from the initial position):



10



$10 + 6 \equiv 4 \pmod{12}$



$4 + 28 \equiv 8 \pmod{12}$

Carl Friedrich Gauss (1777-1855) first described this type of arithmetic in 1801. The idea is that numbers “wrap around” whenever a value called the “modulus” is reached. The notation

$$a \equiv b \pmod{m}$$

means that  $a$  and  $b$  are “congruent modulo  $m$ ” or

$$a = km + b$$

where  $k$  is a positive integer.

The expression is related to but not the same as the operator “mod” (expressed without brackets) or “%” which gives the remainder when one number is divided by another, e.g.  $7 \text{ mod } 3 = 1$ .

One intriguing aspect of modular systems is that if a number added to by a number that is multiple of the modulus, the result is the original number. In a clock any number of complete rotations will not change the displayed time.

Given these concepts, we can consider Fermat’s “Little Theorem,” so called to distinguish it from his “Last Theorem.” For any integer  $a$  where  $p$  is a prime and  $a$  and  $p$  are relatively prime to each other (have a GCD of 1) then, in

modern notation

$$a^p \equiv a \pmod{p}$$

This expression means that any number raised to a power of a prime yields itself when considered in a system that is modular at the value of the prime. In general, we make  $p > a$ . If  $p < a$ , the procedure yields  $a \bmod p$  rather than  $a$ . We can try this theorem out on small numbers such as  $a = 3$  and  $p = 5$ :  $a^p = 243$  which divided by 5 leaves a remainder of 3.

Fermat proposed the theorem in 1640 but offered no proof. The theorem was proven by Gottfried Leibniz (1646-1716) in 1683 (see details in Wilson, 2020, pp 97-100).

The theorem can also be expressed

$$a^{p-1} \equiv 1 \pmod{p}$$

In this format Fermat's Little Theorem serves as the basis for the "Fermat Primality Test." Any number  $n$  that does not fulfil the criterion

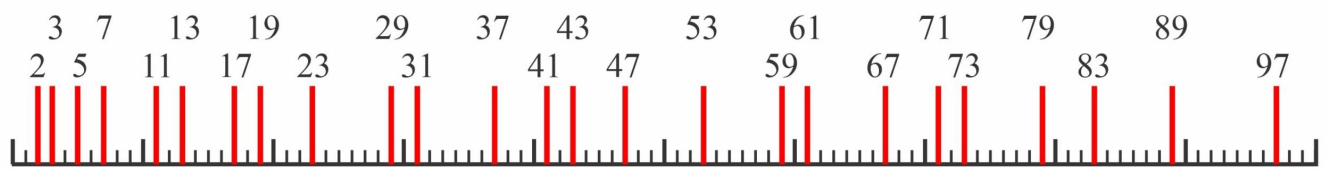
$$a^{n-1} \equiv 1 \pmod{n}$$

where  $a$  is any integer greater than 1 and less than  $n-1$ , is not prime. If it does fulfil the criterion, it is probably prime (a Fermat pseudoprime) and the test should be repeated with a different  $a$ . To be absolutely sure one would have to test all values of  $a$  less than  $\sqrt{n}$ . The test efficiently determines whether a number is composite, but it can be computationally expensive when determining that it is indeed prime.

## **Distribution of Primes**

The prime numbers occur among the more common composite

numbers with no regular pattern:

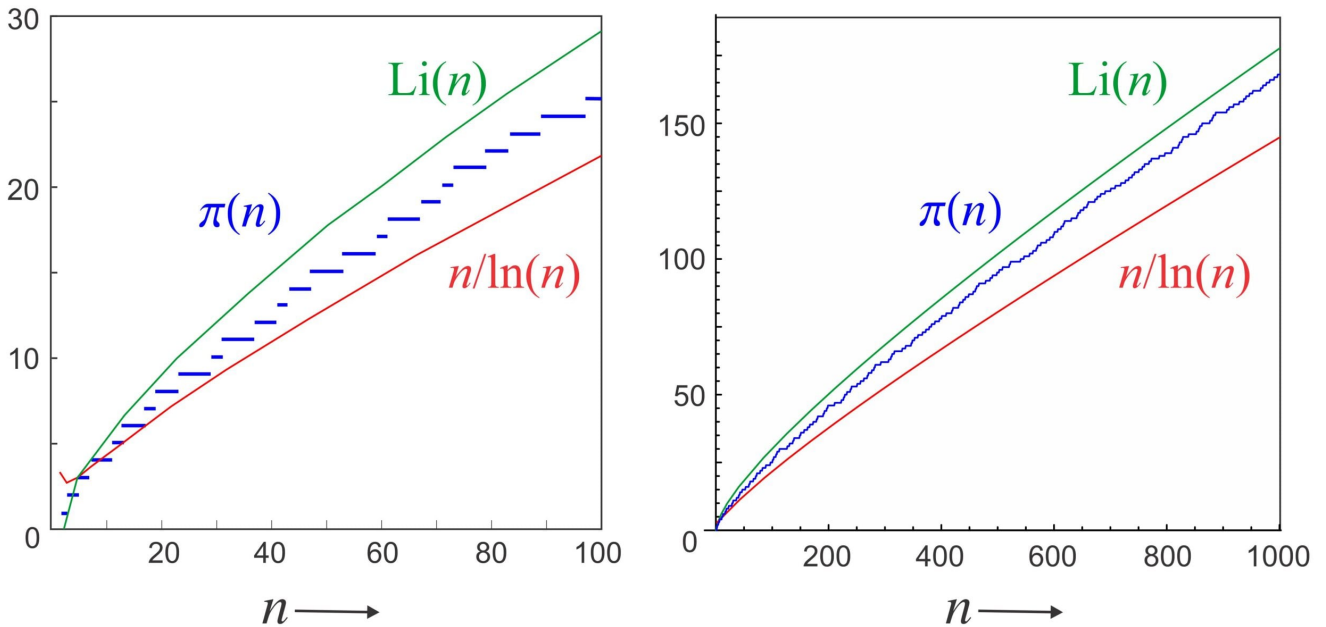


The shortest gap – between 2 and 3 – occurs only once. Primes separated by 2 – twin primes – occur 8 times in the first 100 numbers. In 1849 Alphonse de Polignac (1826-1863) conjectured that for any number  $n$  there are an infinite number of consecutive primes separated by  $n$ . When  $n$  is 2, this is the “twin prime conjecture” (Neale, 2017). Neither the twin prime conjecture nor the more generalized de Polignac conjecture has been proven.

The number of primes less than  $n$  – the “prime number counting function,” customarily denoted as  $\pi(n)$  – increases with increasing  $n$  but the rate of increase decreases as  $n$  increases. In 1792, at the age of 15, Gauss conjectured that the number was approximated by  $n/\ln(n)$ , where “ln” denotes the “natural logarithm” (using the base of  $e$  equal to 2.71828...). This underestimates  $\pi(n)$ , but the relative error decreases as  $x$  increases.

Although it was not published until after his death, Gauss later refined his conjecture, suggesting that  $\pi(n)$  is better approximated by the logarithmic integral of  $n$ :

This estimate is the basis for the “prime number theorem:” as  $n$  increases,  $\pi(n)$  asymptotically approaches  $\text{Li}(n)$ . The following illustration shows the prime number counting function with the two different estimates for  $n$  between 1-100 and 1-1000. There are 25 primes below 100 and 168 below 1000. The actual function is a staircase, with steps occurring at each prime. The estimates are smooth functions.



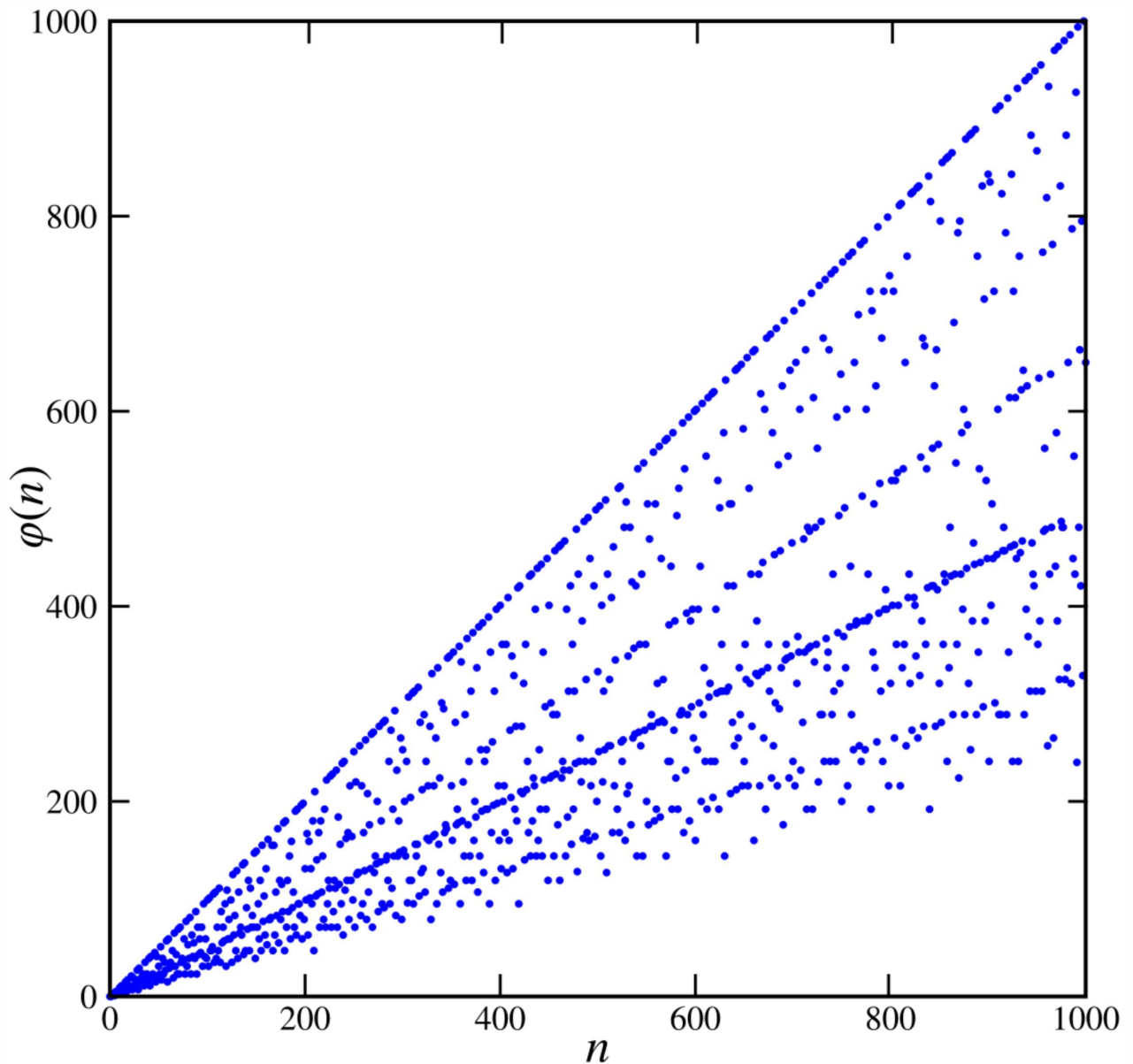
The prime gap is the difference between two consecutive prime numbers

$$g_n = p_{n+1} - p_n$$

The minimum value of  $g_n$  is 2 for  $n > 2$ . The average gap between primes increases as the natural logarithm of these primes, and therefore the ratio of the prime gap to the primes decreases (and is asymptotically zero). The ratio  $g_n / \ln(p_n)$  is called the “merit” of a particular gap. There is no known maximal gap. The maximum recorded gap of 8350 occurred for an 87-digit prime and has a merit value of 41.9. The maximum gap  $g_n$  would have to be less than the prime counting function  $\pi(\pi_n)$  (Lu & Deng, 2020)

In 1763 Euler introduced what has come to be known as “Euler’s Totient Function.” This function, nowadays denoted as  $\varphi(n)$ , counts the number of positive integers less than a given integer  $n$  that are relatively prime to  $n$ . When  $n$  is 12  $\varphi(n)$  is 4 (the numbers 1, 5, 7, 11) and when  $n$  is 13  $\varphi(n)$  is 12 (all numbers less than 13). The word “totient” comes from the Latin

*tot* meaning "that many." The illustration shows the function up to  $n$  of 1000. The upper boundary shows the value when  $n$  is a prime and  $\varphi(n)$  is  $n-1$ .



This function has some intriguing characteristics. Most importantly, for two integers  $a$  and  $b$

$$\varphi(ab) = \varphi(a) \varphi(b)$$

Some sense of this characteristic can be obtained by considering  $a$  as 6 and  $b$  as 7:  $\varphi(6)$  is 2 (the numbers 1 and 5) and  $\varphi(7)$  is 6 because 7 is prime. Therefore  $\varphi(42)$  is 12 (the numbers 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41).

“Euler’s Theorem,” an extension of Fermat’s Little Theorem (and sometimes called the “Fermat-Euler Theorem”), states

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

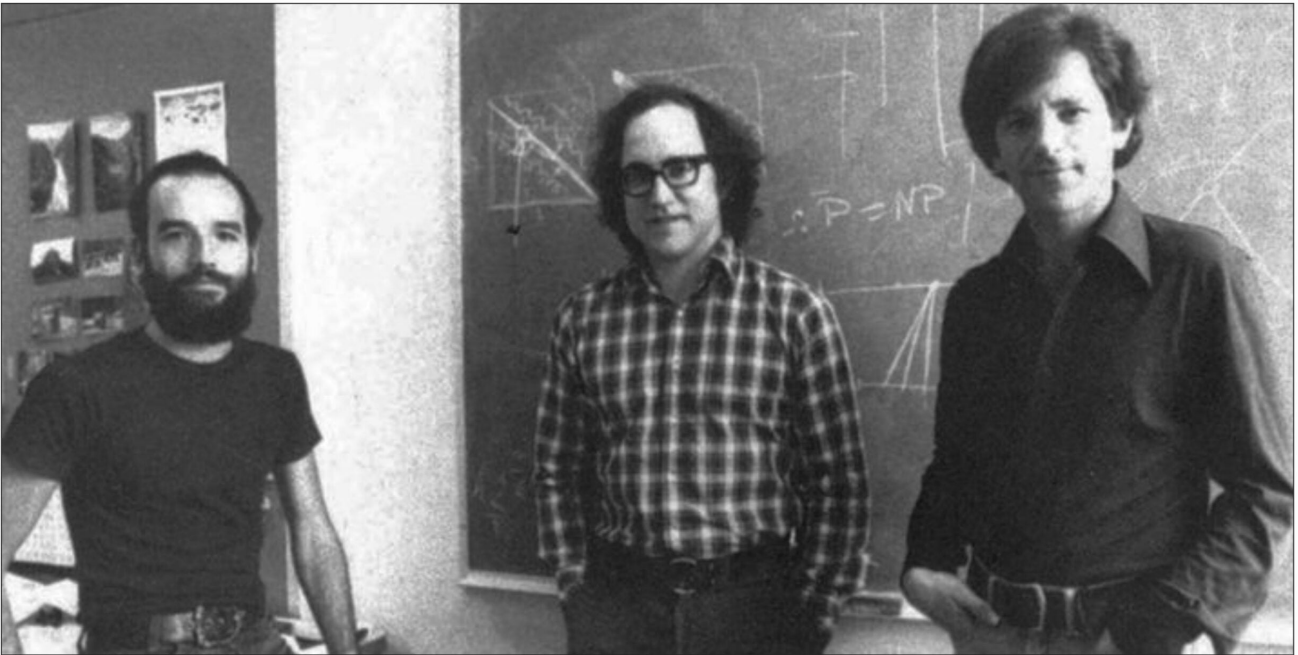
The proof of this generalization of Fermat’s theorem is detailed in Wilson (2020, pp 103-108)

## **Cryptography**

For many years the study of primes was considered “pure” mathematics, in that the truths that it proved had no applications in the real world. The famous number theorist G. H. Hardy (1877-1947) claimed

I have never done anything ‘useful’. No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world. (Hardy, 1940, p 90)

Over the past half century, the idea of pure mathematics has changed. Prime numbers have become an essential part of real-world cryptography. All the information that is transmitted between buyer and seller when something is bought on the internet is kept safe from prying eyes by means of algorithms that use prime numbers. The most common algorithm was initially proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977, and has come to be known as the “RSA cryptosystem.” The following illustration shows Rivest, Shamir and Adleman at the Massachusetts Institute of Technology:



The following are the basic procedures of the RSA algorithm (Rivest et al, 1977; Crandall & Pomerance, 2005, pp 389-391; Watkins, 2014, pp 369-374; Wilson, 2020, 110-111):

(i) *generation of public keys:*

Two different large prime numbers  $p$  and  $q$  are chosen. Nowadays these primes are approximately equal and each about 200 digits in length. A number  $N$  is calculated as the product of these two primes, and Euler's totient ( $T$ ) is calculated for  $N$ . This equals the product of  $p - 1$  and  $q - 1$ . Finally, a number  $E$  ("encryption key") is chosen that is greater than 2, less than  $N-1$  and coprime to  $T$ . The last characteristic can be ensured by using Euler's algorithm to show the  $T$  and  $E$  have 1 as their greatest common divisor (GCD). The number  $E$  is typically chosen as a prime number greater than either  $p$  or  $q$ .

$$N = pq$$

$$T = \varphi(pq) = (p - 1)(q - 1)$$

$$\text{Choose } E \in [3, N - 2] \text{ and } \text{GCD}(E, T) = 1$$

The public keys are  $N$  and  $E$ ;  $p$  and  $q$  (and  $T$ ) are kept secret.

(ii) *encryption of the message*

The message (or part of a message) is coded into a large number  $M$  using a simple substitution cipher. For example, each letter could be represented as a two-digit numbers from 01 to 26.  $M$  is then encrypted to give the number  $C$  ("ciphertext") using public keys  $N$  and  $E$  according to the formula

$$C \equiv M^E \pmod{N}$$

The number  $M$  has increased dramatically, and the clock (modulus  $N$ ) has revolved many times so that the clock face shows a number  $C$  completely different from  $M$ .  $E$  must be coprime to  $T$  to make sure that  $C$  does not return as the same number as  $M$ .

(iii) *decryption of the message*

To decrypt the message, we must calculate a number  $D$  ("decryption key") that is the modular multiplicative inverse of  $E$

$$DE \equiv 1 \pmod{T} \text{ or } D = E^{-1} \pmod{T}$$

Finding the multiplicative inverse is a simple trial and error process. Iteratively increment  $k$  and then calculate  $(k \cdot E) \pmod{T}$  until it equals 1, at which time  $D$  is made equal to  $k$ . In an example using small numbers,  $E$  of 7 and  $T$  of 72 (the totient for 7 and 13)

$$k=1, 7 \pmod{72} \text{ is } 7$$

$$k=2, 14 \pmod{72} \text{ is } 14$$

...

$$k=30, 210 \pmod{72} \text{ is } 66$$

$$k=31, 217 \pmod{72} \text{ is } 1, \text{ therefore } D \text{ is } 31.$$

Having obtained  $D$ , we can decrypt the coded message to obtain the original message according to the formula

$$M \equiv C^D \pmod{N}$$

The number has again increased but after many revolutions the clock face now shows the same number as it was before the original encryption. Because  $D$  is the modular multiplicative inverse of  $E$ , when the clock wraps around because of  $E$  and then because of  $D$  it is the same as it the clock face had just stayed the same.

(iv) *example*

The following is an example using small numbers

Let  $p=3$  and  $q=11$ ;  $N=pq=33$

$T = (p-1)*(q-1) = 2*10 = 20$

Let  $E = 7$ , check  $\text{GCD}(7,20)=1$

Find  $D$  to ensure  $(D*E)\text{mod}20=1$

Determine  $D$  to be 3 because  $3*7\text{mod}20=1$

Let  $M = 31$

Encrypt message as  $C=M^E\text{mod}N = 31^7\text{mod}33 =4$

Decrypt message as  $C^D\text{mod}N = 4^3\text{mod}33=31$

(v) *breaking the code.*

In order to break the RSA code an outside observer would have to find  $D$ . This would require finding the two primes  $p$  and  $q$  that when multiplied together gave the public number. From  $p$  and  $q$  one would know  $T$ . Then one could derive  $D$ . Finding  $p$  and  $q$  would require factoring  $N$ , a computationally demanding task when  $N$  is very large. The RSA system remains safe provided

that it takes longer to compute the factors of N than the length of time that the system uses any particular numbers p and q.

## Zeta Function

In his studies of infinite series published in 1737, Euler proved a remarkable identity:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

The left side of the equation shows the sum of the reciprocals of all natural numbers raised to the power s. This has become known as  $\zeta(s)$  or the "zeta function"

$$\zeta(s) = 1/1^s + 1/2^s + 1/3^s + 1/4^s \dots + 1/n^s$$

The right side of the equation is a product of multiple terms each involving one of the prime numbers:

$$\zeta(s) = 1/(1-2^{-s}) * 1/(1-3^{-s}) * 1/(1-5^{-s}) * 1/(1-7^{-s}) \dots * 1/(1-p^{-s})$$

When s is 2, the function is the sum of the reciprocals of all the natural numbers squared:

$$\zeta(2) = 1/1^2 + 1/2^2 + 1/3^2 + 1/4^2 \dots + 1/n^2$$

Euler demonstrated that  $\zeta(2) = \pi^2/6$ . This was intriguing since the zeta equation now linked the natural numbers to the irrational number  $\pi$ . Euler also proved that  $\zeta(4)$  is  $\pi^4/90$  and  $\zeta(6)$  is  $\pi^6/945$ . Values of the function for odd values of s have

no clear formulation.

To prove his product function, Euler used a sieving approach as illustrated below:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

Divide the infinite series by  $2^s$

$$\frac{1}{2^s} \zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \dots$$

Subtract this from the original zeta function to remove all elements that have a factor of 2:

$$\left(1 - \frac{1}{2^s}\right) \zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \frac{1}{13^s} + \dots$$

Repeat the process by dividing by the  $3^s$  where 3 is the next prime:

$$\frac{1}{3^s} \left(1 - \frac{1}{2^s}\right) \zeta(s) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \frac{1}{33^s} + \dots$$

Subtracting again, we get:

$$\left(1 - \frac{1}{3^s}\right) \left(1 - \frac{1}{2^s}\right) \zeta(s) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \frac{1}{17^s} + \dots,$$

Repeating the process infinitely for all primes, we get:

$$\dots \left(1 - \frac{1}{11^s}\right) \left(1 - \frac{1}{7^s}\right) \left(1 - \frac{1}{5^s}\right) \left(1 - \frac{1}{3^s}\right) \left(1 - \frac{1}{2^s}\right) \zeta(s) = 1$$

Dividing both sides by everything but the  $\zeta(s)$  we obtain:

$$\zeta(s) = \frac{1}{\left(1 - \frac{1}{2^s}\right) \left(1 - \frac{1}{3^s}\right) \left(1 - \frac{1}{5^s}\right) \left(1 - \frac{1}{7^s}\right) \left(1 - \frac{1}{11^s}\right) \dots}$$

This can be written as an infinite product over all primes  $p$ :

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

In 1859 Bernhard Riemann considered Euler's zeta function using complex variables. He made  $s = \sigma + it$ , where  $\sigma$  and  $t$  are real numbers and  $i$  is the square root of  $-1$ . Using values derived from this function he was able to adjust Euler's prime number theorem – as  $n$  increases,  $\pi(n)$  asymptotically approaches  $\text{Li}(n)$  – so that it accurately represented the actual staircase function that is  $\pi(n)$ .

The Riemann Zeta Function is as complex as its variable, and I am afraid I find it impossible to understand. Both Derbyshire (2003) and Du Sautoy (2003) have written books about the function. In his original paper Riemann also proposed a hypothesis about the nontrivial zero-values of the function that appear on a line where the real value of the variable equals  $\frac{1}{2}$ . His hypothesis holds for all values of the function so far examined. However, the hypothesis is not yet proven. The Clay institute has offered a prize of 1 million dollars for the proof. I shall not be collecting this prize, but I shall enthusiastically applaud its winner.

The following video was made for Quanta Magazine by Alex Kontorovich about the Riemann Zeta Function and the Riemann Hypothesis.

<https://creatureandcreator.ca/wp-content/uploads/2025/12/riemann-video.mp4>

## **Epilogue**

We can conclude with a quotation from Du Sautoy (2003, p 6) about the primes:

Prime numbers present mathematicians with one of the strangest tensions in their subject. On the one hand a number is either prime or it isn't. No flip of a coin will suddenly make a number divisible by some smaller number. Yet there is no denying that the list of primes looks like a randomly chosen sequence of numbers. Physicists have grown used to the idea that a quantum die decides the fate of the universe, randomly choosing at each throw where scientists will find matter. But it is something of an embarrassment to have to admit that these fundamental numbers on which mathematics is based appear to have been laid out by Nature flipping a coin, deciding at each toss the fate of each number. Randomness and chaos are anathema

to the mathematician. Despite their randomness, prime numbers – more than any other part of our mathematical heritage – have a timeless, universal character. Prime numbers would be there regardless of whether we had evolved sufficiently to recognise them.

In Paolo Gordan's 2010 novel *The Solitude of the Primes*, the character Mattia muses

Prime numbers are divisible only by one and by themselves. They stand in their place in the infinite series of natural numbers, squashed in between two others, like all other numbers, but a step further on than the rest. They are suspicious and solitary, which is why Mattia thought they were wonderful. Sometimes he thought that they had ended up in that sequence by mistake, that they'd been trapped like pearls on a necklace. At other times he suspected that they too would rather have been like all the others, just ordinary numbers, but for some reason they weren't capable of it. (p 111)

And we cannot leave the topic without some praise for the mathematicians that discovered so much about them. The following are portraits of some of these marvelous thinkers. They all contributed extensively to our knowledge beyond their work with the primes. Fermat worked with Pascal on the mathematics of probability; Gauss was the first to measure the earth's magnetic field; Euler proposed his "identity:"

$$e^{i\pi} + 1 = 0$$

which united the logarithms, pi and imaginary numbers just like his product formula united the natural numbers, primes and pi; and Riemann worked on the non-Euclidean geometry that Einstein would use in his Theory of relativity.



Pierre de Fermat (1601-1665)



Leonhard Euler (1707-1783)



Carl Friedrich Gauss (1777-1855)



Bernhard Riemann (1826-1866)

## References

- Crandall, R. E., & Pomerance, C. (2005). *Prime numbers: a computational perspective* (Second Edition). Springer.
- Derbyshire, J. (2003). *Prime obsession: Bernhard Riemann and the greatest unsolved problem in mathematics*. Joseph Henry Press
- Du Sautoy, M. (2003). *The music of the primes: searching to solve the greatest mystery in mathematics*. HarperCollins.
- Giordano, P. (2010). *The solitude of prime numbers*. Penguin
- Hardy, G. H. (1940). *A mathematician's apology*. Cambridge University Press.
- Jones, J. P., Sato, D., Wada, H., & Wiens, D., (1976). Diophantine representation of the set of prime numbers. *The American Mathematical Monthly*, 83, 449-464.
- Lamb, E. (2019). Why isn't 1 a prime number? And how long has it been a number? Scientific American Blog.
- Lu, Y.-P. & Deng, S.-F. (2020). An upper bound for the prime gap. arXiv:2007.15282
- Mackinnon, N. (1987). Prime number formulae. *The Mathematical Gazette*, 71(456), 113–114.
- Neale, V. (2017). *Closing the gap: the quest to understand prime numbers*. Oxford University Press.
- Nicastro, N. (2008). *Circumference: Eratosthenes and the ancient quest to measure the globe*. St. Martin's Press.
- Riemann, G. F. B. (1859). Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsber. Königl. Preuss. Akad. Wiss. Berlin*, 671-680. English translation by D. R. Wilkins
- Rivest, R.L., Shamir, A., & Adleman, L. (1977). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*(Technical report). MIT Laboratory for Computer

Science.

Watkins, J. J. (2014). *Number theory: a historical approach*. Princeton University Press.

Wilson, R. J. (2020). *Number theory: a very short introduction*. Oxford University Press.

---

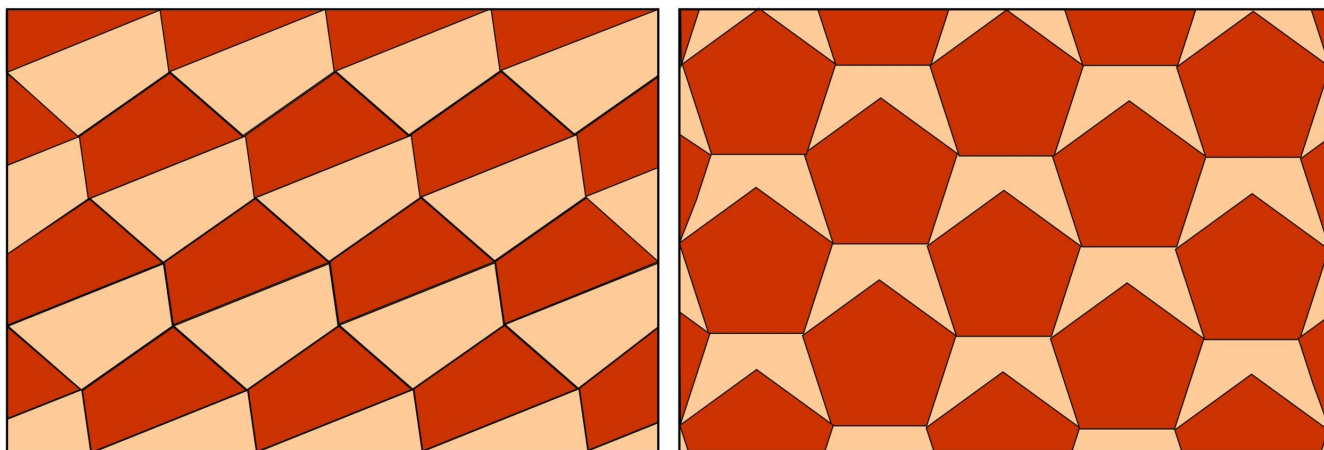
# Tessellations

Tessellation is “a collection of shapes [tiles] that fit together without gaps or overlap to cover the infinite mathematical plane” (Fathauer, 2021). Most tilings are “periodic,” in the sense that the pattern repeats itself when “translated” (shifted without rotation). In the 1970s Roger Penrose described several sets of tiles that could cover the plane aperiodically. The search then began for the “einstein” (one stone) – a single tile that could cover the plane aperiodically. In March of 2023, Smith, Myers, Kaplan & Goodman-Strauss described a tile, commonly known as the “hat” that covered the plane aperiodically. However, to do so, this tile had to be occasionally turned over (to make its mirror image). Subsequently in May of 2023, the same authors reported another tile that could cover the plane aperiodically without any need for mirror images. This tile was called the “spectre.” This posting briefly reviews these recent developments in a style more visual than verbal.

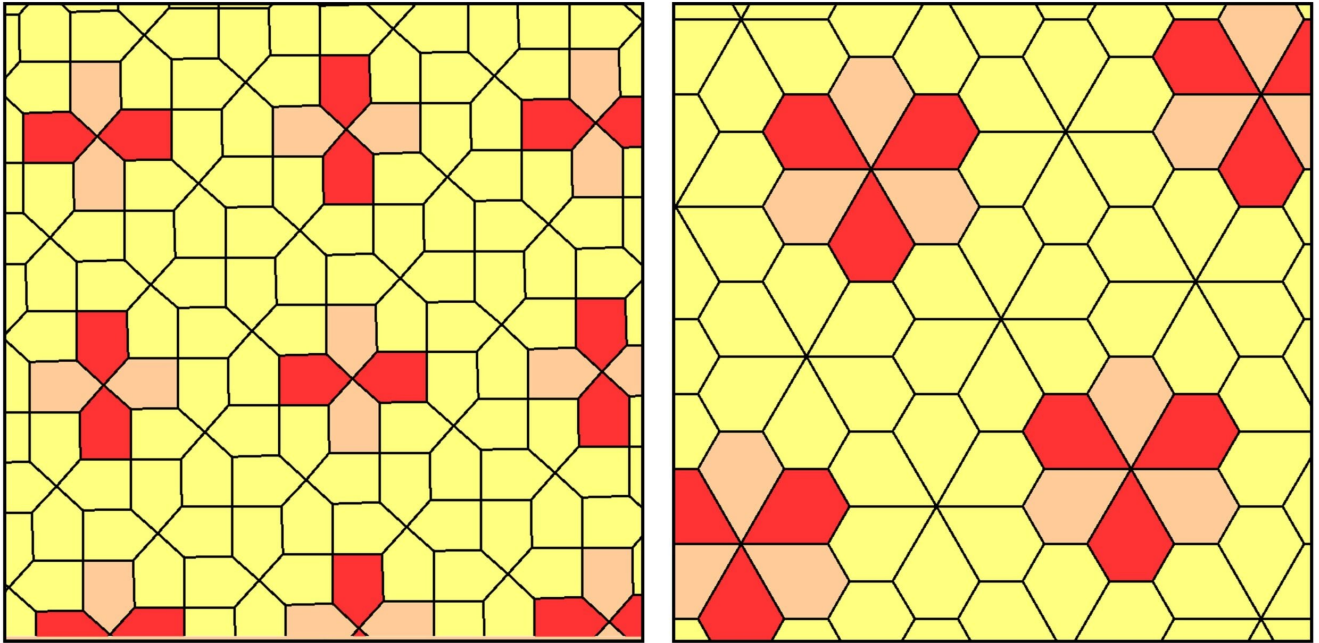
## Tiling a Surface

Many different patterns can tile a surface (Grünbaum &

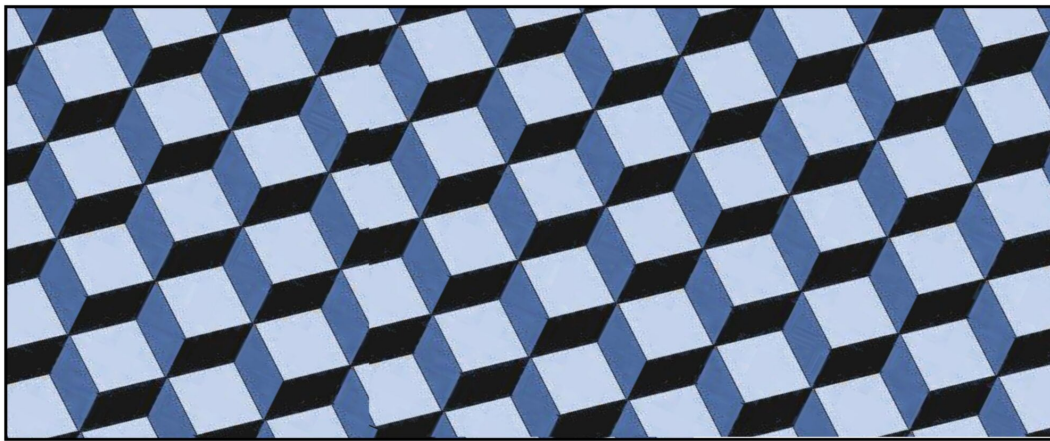
Shephard, 1987; Fathauer, 2021) Any triangle can completely cover a surface provide one allows the tiles to be rotated  $180^\circ$ . Regular quadrilaterals and regular hexagons can cover the surface without the need for rotation. Irregular quadrilaterals can cover the surface if rotation is allowed (below left). Regular pentagons cannot cover the surface unless they are combined with tiles of a different shape (below right). Both illustrated tilings are periodic in the horizontal directions. The left pattern is also periodic along an axis at rotated a little clockwise from the vertical. The right pattern is also periodic in the vertical direction. This illustration (and all subsequent illustrations) can be viewed separately and in greater resolution by clicking on it.



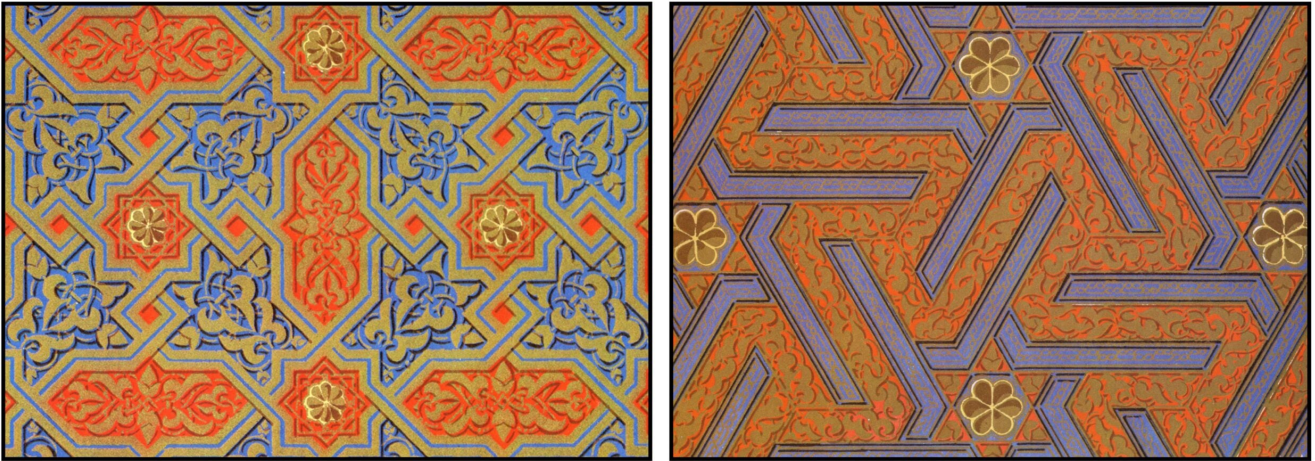
Although regular pentagons cannot, some irregular pentagons can cover the surface. The following shows two pentagonal tilings – “Cairo” and “Floret.” In the latter, the pentagons are placed together in a hexagonal rosette.



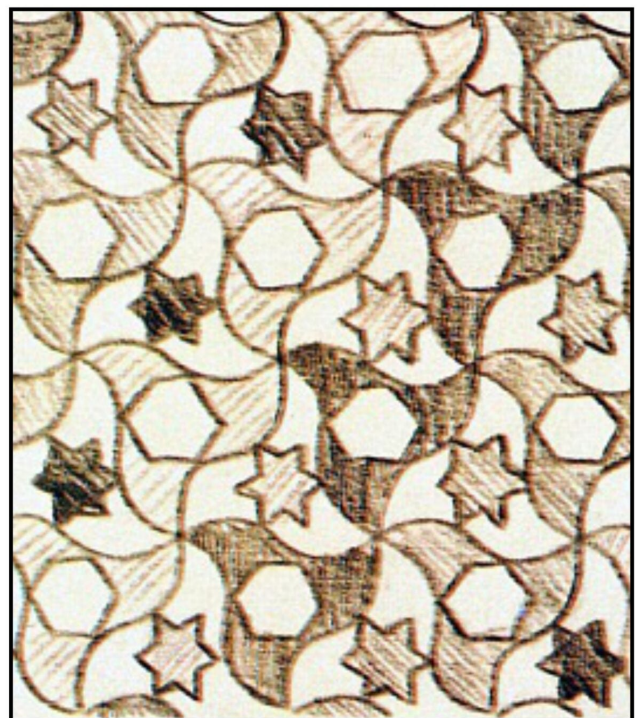
Tiles of different shapes can be combined to form beautiful patterns. The following illustration shows a floor pattern from Pompeii with a striking *trompe l'oeil* effect.



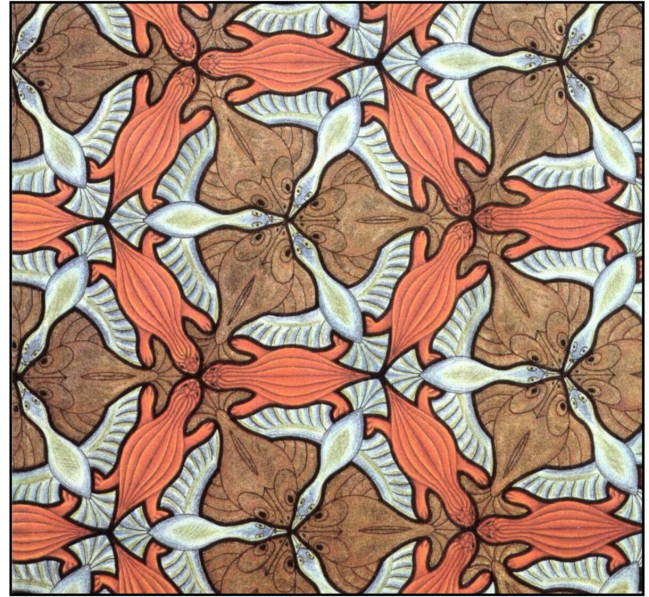
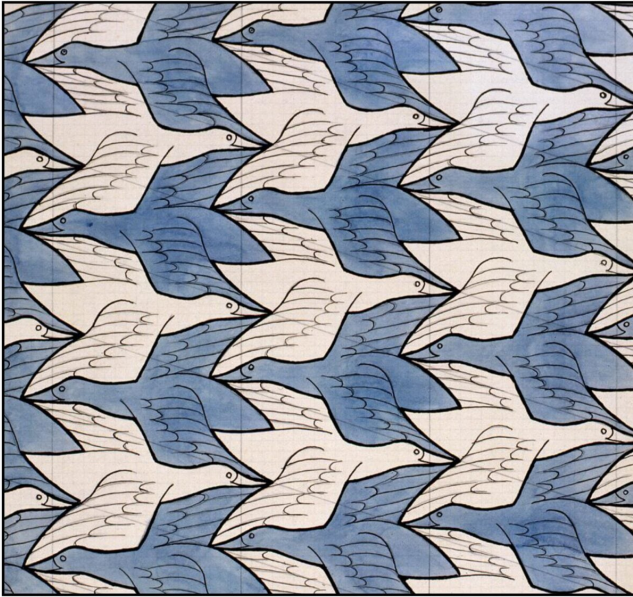
Islamic culture avoids any representation of living forms since only the Divinity can create life. Islamic artists have therefore developed many different types of geometric ornamentation (Bonner, 2017). These patterns are tiled onto floors and ceilings, woven into rugs, carved through screens of wood or stone, and bound around beautiful books, The following are two intricate designs from the Alhambra taken from *The Grammar of Ornament* (1868) by Owen Carter Jones.



The Dutch artist Maurits Cornelis Escher (1898-1972) became fascinated by the Islamic designs that he saw in the Alhambra (Escher, 2008; Gelgi, 2010; Behrends, 2022). The following shows some tiling from the Alhambra together with a 1938 sketch by Escher (adapted from Wikipedia):

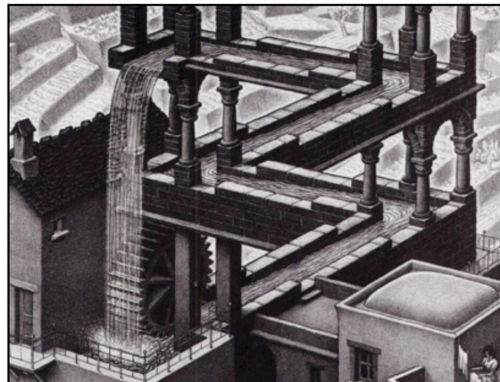


Escher evolved his own style of tessellation using representations of living things instead of geometric shapes. The following shows two representations of his work: a simple two-bird design from 1938 and a more complicated bird-fish-reptile design with three-fold symmetry from 1948.



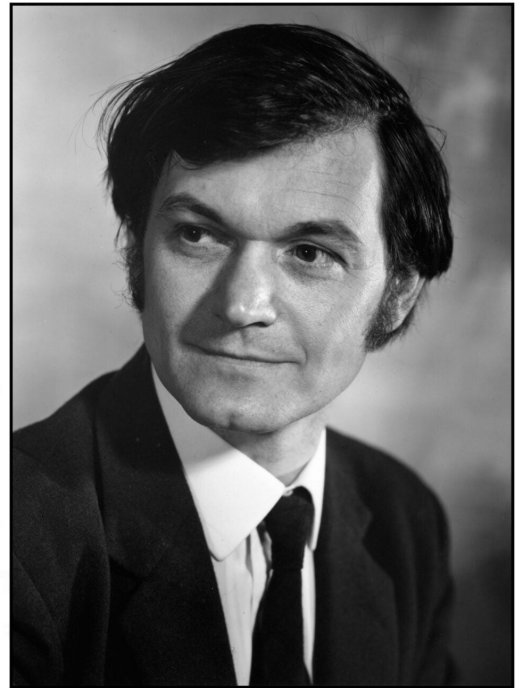
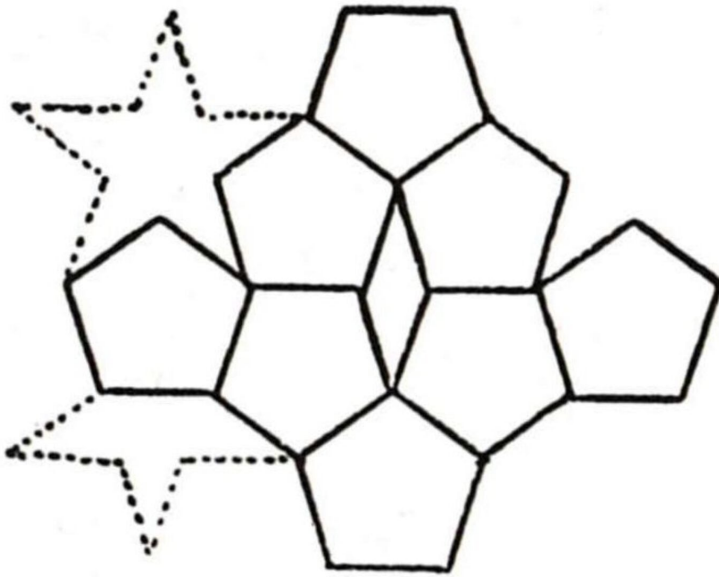
## Penrose Tilings

Later in his life Escher studied the problems of representing reality in two dimensions, and produced many illustrations of “impossible objects” such as *The Waterfall* (1961) in the illustration below. In the late 1950s, Roger Penrose, a mathematician whose work on black holes was to win him the Nobel Prize in 2020, and his father devised the “Penrose Triangle” which epitomizes the perceptual impossibilities portrayed Escher’s work

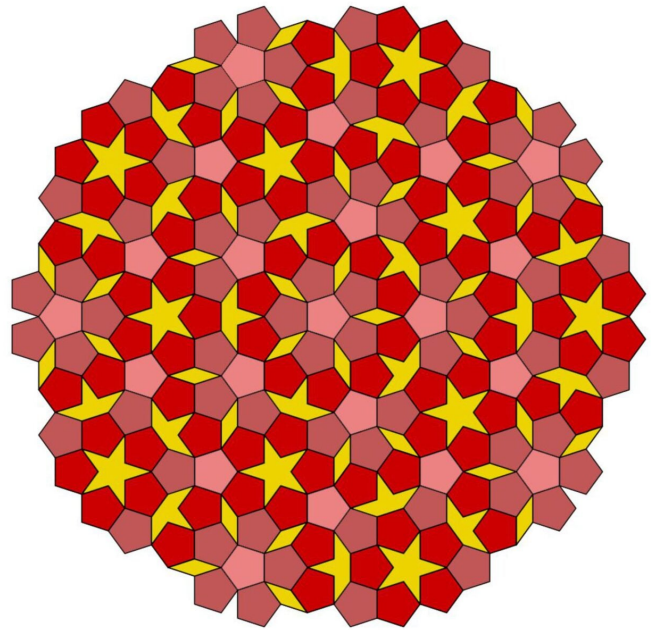
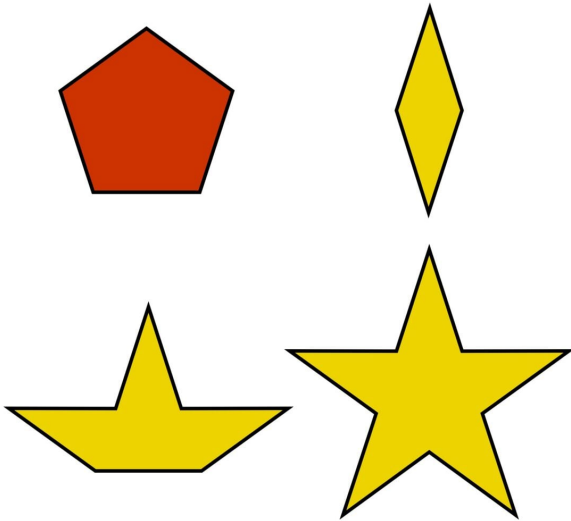


In the 1970s, Penrose became interested in the possibility of tiling the plane aperiodically (Penrose, 1974, Gardner, 1997). The following illustration shows some of his early ideas about tiling with pentagons (Penrose, 1978) together with a

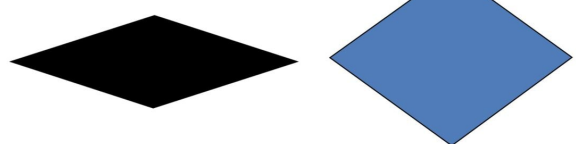
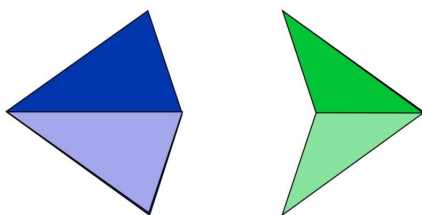
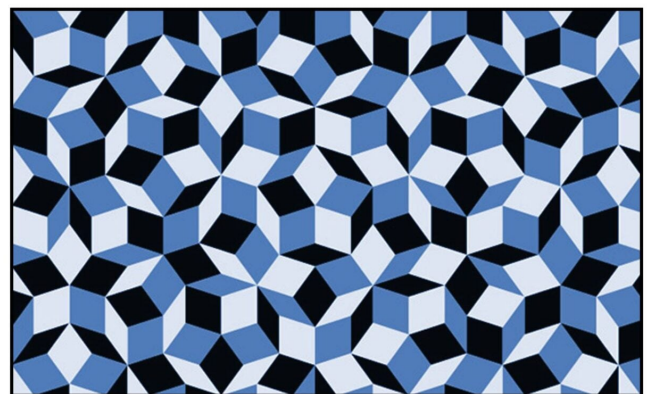
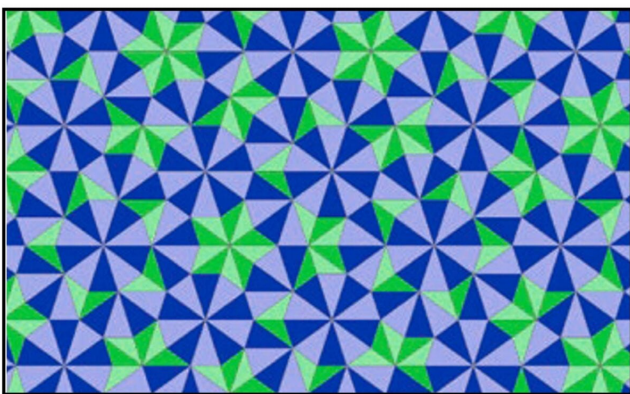
photographic portrait from about that time.



From these ideas he designed a set of tiles – a pentagon, a boat, a diamond and a pentagram – that could cover the plane aperiodically. However, in order for the tiling to succeed there had to be “matching rules” for what could adjoin the edges of the pentagon. These rules could be embodied by making the edges of the shapes notched or curved. In effect, this led to three kinds of pentagon. The following diagram, adapted from Wikipedia, shows the aperiodic pattern, with the three pentagons colored in different shades of red.



Penrose derived other patterns that tiled the plane aperiodically with only two shapes. Illustrated below is a tiling based on kites and dart shapes with the matching rules shown by the shading, and a tiling based on two rhombuses, with the matching rules shown in the colors. The tilings are aesthetically pleasing: like life, the shapes are the same but the pattern always changing.

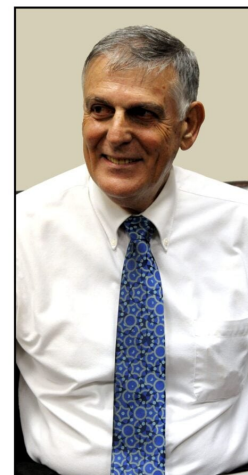
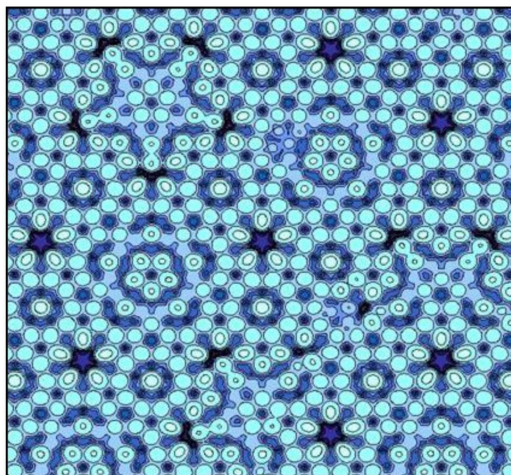
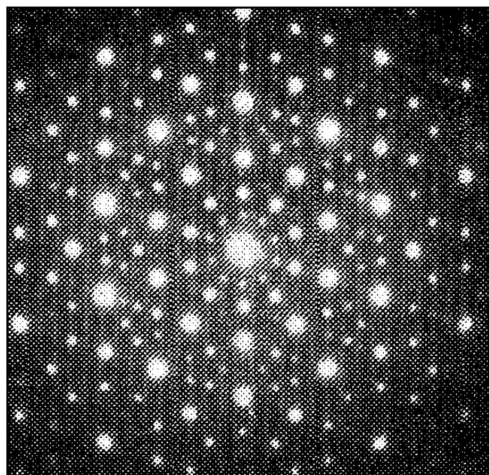


## Quasicrystals

Tilings explain how planes are covered; crystallography explains how spaces are filled. Only certain shapes can combine together to fill the space. According to classical physics, the crystalline structure of matter can show only 2-, 3-, 4- and 6-fold rotational symmetries on diffraction using x-ray or other radiation beams.

In 1984, Dan Shechtman and his colleagues reported a diffraction pattern of a metal alloy with ten-fold symmetry. From this initial finding came the study of quasicrystals (de Boissieu, 2012). Instead of tetrahedrons, cubes and octahedrons which can fit together to fill the space, decahedrons (ten-sided solids) and icosahedrons (twenty-sided solids) cannot fit together without other intercalating solids to fill the gaps. In effect these structures are the three-dimensional equivalents of Penrose's pentagonal tilings.

Quasicrystalline structures have smooth hard surfaces. They are useful in non-stick cookware, non-corroding instruments, and broadband reflectors. Schechtman won the Nobel prize for his work in 2011. The illustration below shows one of the original diffractograms, the surface pattern of a quasicrystal, and a portrait of Schechtman wearing a tie showing the structure of another quasicrystal.

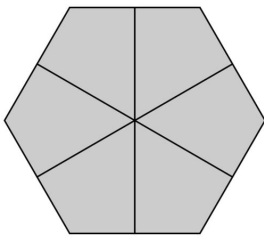


## The Einstein Tile

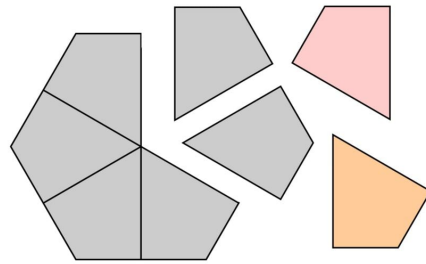
Once Penrose had shown that sets of shapes could cover the plane aperiodically, the question arose as to whether there a single tile – the *ein Stein* or “one stone” – could do so. In early 2023, David Smith, a retired print technician and amateur mathematician living in Yorkshire, discovered a shape – the “hat” – that apparently tiles the plane aperiodically. The structure of the hat is described in the following illustration:

### Making the Hat

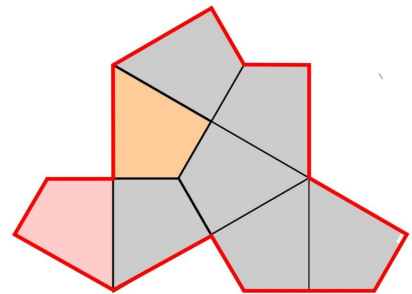
Regular hexagon divided  
into 6 kites



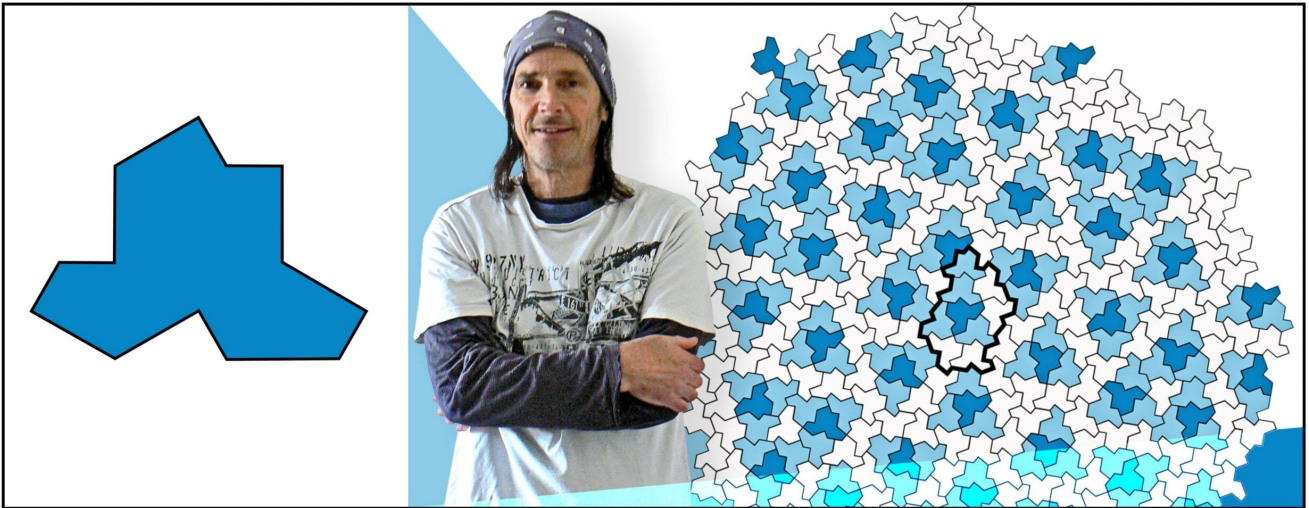
Take out 2 kites and  
double these



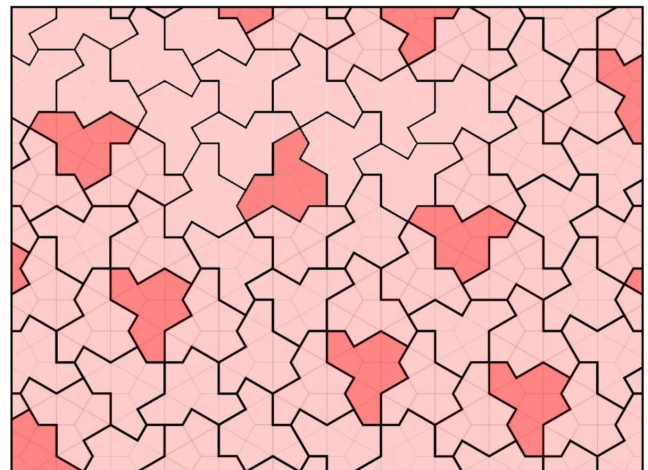
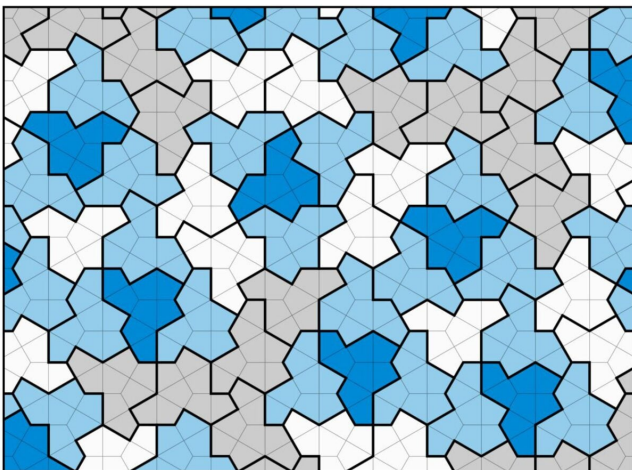
Add removed and doubled  
kites to remaining shape



Smith contacted colleagues at the University of Waterloo in Canada, and they proved that this was indeed true (Smith et al, 2023a; Bischoff, 2023). The illustration below (derived from Whipple article in *The Times*) shows Smith together with his aperiodic tiling:



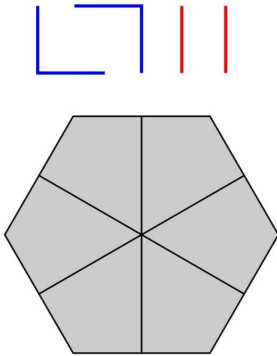
When the hat tiles the plane aperiodically, the pattern contains recognizable “metatiles.” These are shown in the illustration below left as the blue, white and grey combinations of hats. In order to tile the plane some of the hats have to mirror-inverted (equivalent to turning the hat over). This is shown in the illustration below right. In the real world where ceramic tiles are only finished on one side, this would require the manufacture of two separate tiles.



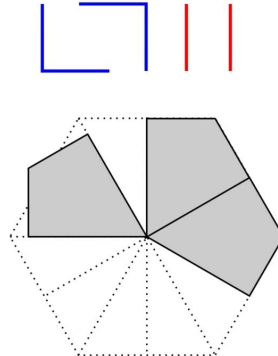
Soon after their initial report of an aperiodic monotile was published, Smith discovered another tile – the “spectre” – that could tile the plane aperiodically without any mirror-inversions (Smith et al, 2023b). The structure of the spectre tile is illustrated below:

## Designing the Spectre

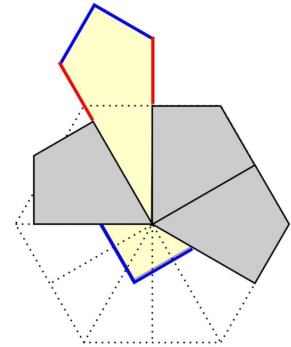
Regular hexagon divided into 6 kites; 2 Right Angles and 2 lines, all one half the length of the hexagon side



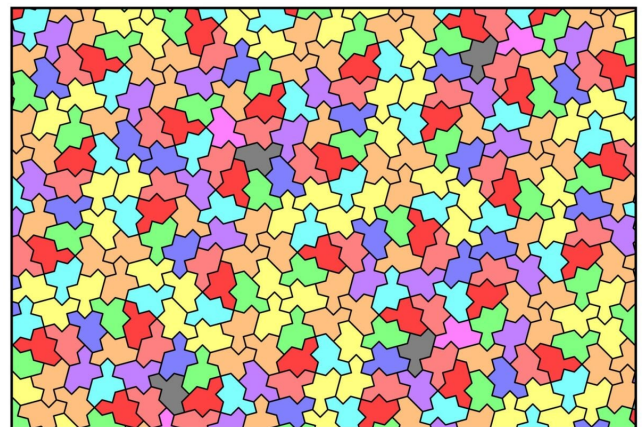
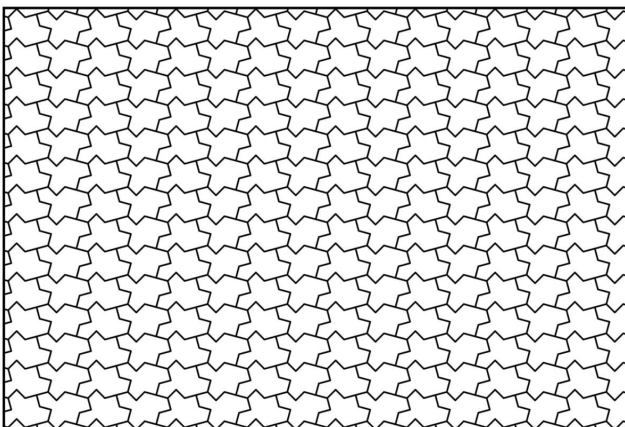
Keep two adjacent kites and one opposing kite; rotate that kite 30 degrees closer to the adjacent kites



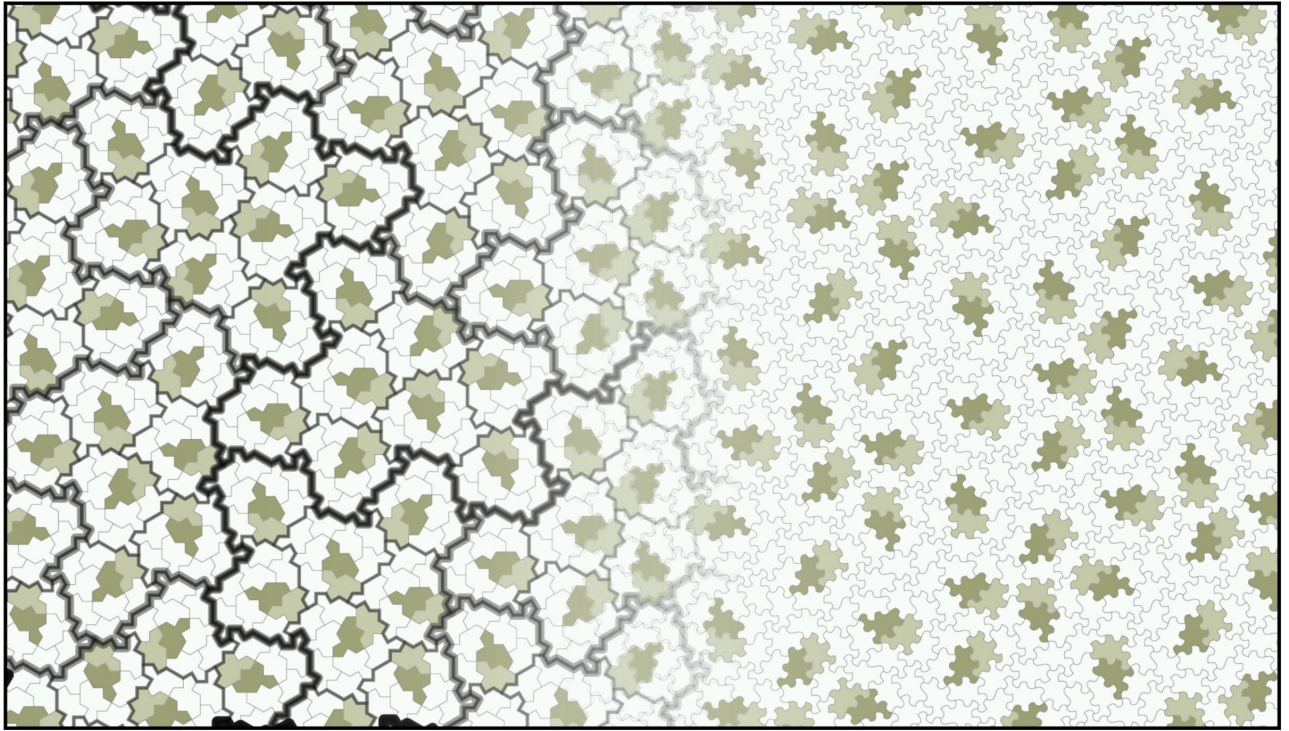
Create head from two lines and one right angle; create tail with remaining right angle

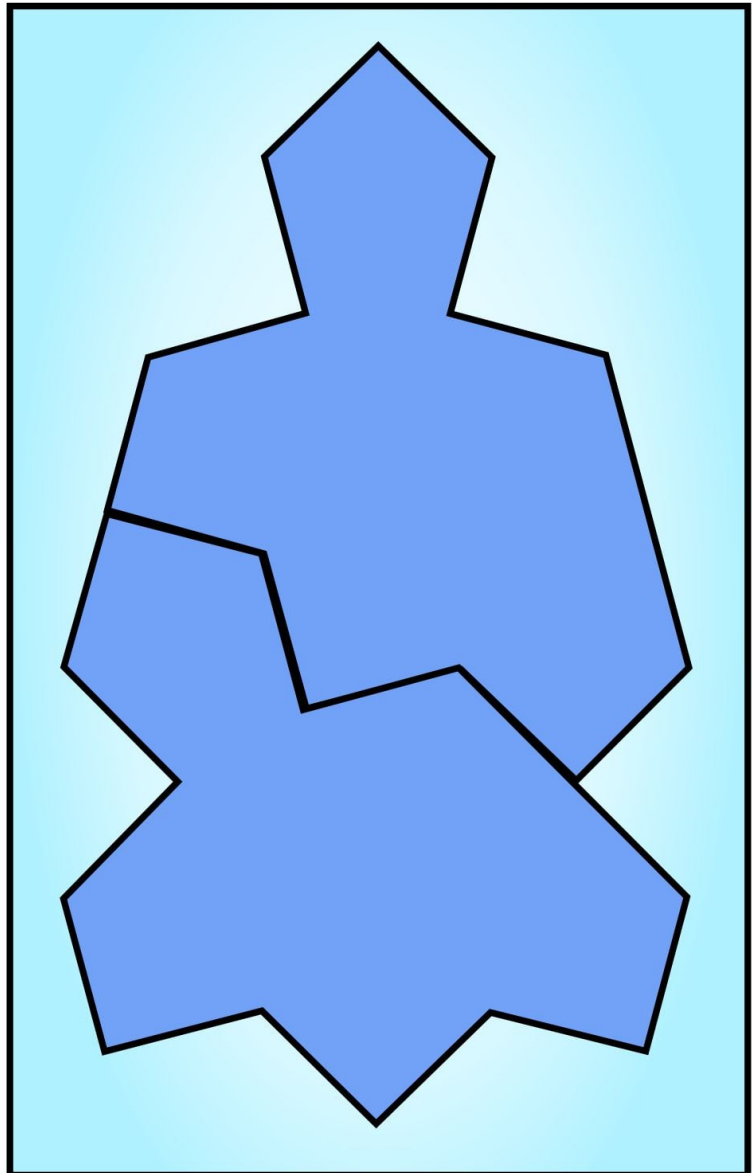


If mirror-inversions are allowed the spectre can tile the plane periodically (lower left); it is only if mirror inversions are forbidden and particular matching rules are in place, that aperiodic tiling is possible (lower right). Both illustrations are the work of Simon Tatham.



The following illustration is taken from the report by Smith and his colleagues. On the left the tiling shows the metatile structure of the tiling pattern and on the right the tiles have curved edges to enforce the matching rules.





One of the repeating combinations that occurs in the spectre tiling is the “buddha” shape illustrated on the right. This combination is shaded in the illustration above, and by the red green combination in the illustration before that.

### **Envoi**

Aperiodic patterns based on simple elements and uncomplicated rules are beautiful. They can represent a peaceful universe of myriad things.

### **References**

Behrends, E. (2022). *Tilings of the Plane: From Escher Via*

*Möbius to Penrose*. Springer.

Bischoff, M. (2023) Newfound mathematical Einstein shape creates a never repeating-pattern. *Scientific American*, April 10, 2023.

Bonner, Jay. (2017). *Islamic Geometric Patterns: Their Historical Development and Traditional Methods of Construction*. Springer New York.

de Boissieu, M. (2012). Atomic structure of quasicrystals. *Structural Chemistry*, 23(4), 965–976.

Escher, M. C. (2008). *The graphic work*. Taschen.

Fathauer, R. W. (2021). *Tessellations: mathematics, art, and recreation*. CRC Press/Taylor & Francis Group.

Gardner, M. (1997). *Penrose tiles to trapdoor ciphers: – and the return of Dr. Matrix*. Mathematical Association of America.

Gelgi, F. (2010). The influence of Islamic art on M. C. Escher. *Fountain Magazine* (July, 2010).

Grünbaum, B., & Shephard, G. C. (1987). *Tilings and patterns*. W.H. Freeman.

Penrose, R. (1974) The role of aesthetics in pure and applied mathematical research. *Bulletin of the Institute of Mathematics and Its Applications*, 10, 266-271.

Penrose, R. (1978). Pentaplexity. *Eureka*, 39, 16–22.

Shechtman, D.; Blech, I.; Gratias, D.; Cahn, J. (1984). Metallic Phase with Long-Range Orientational Order and No Translational Symmetry. *Physical Review Letters*, 53(20), 1951–1953.

Smith, D., Myers, J. S., Kaplan, C. S.; Goodman-Strauss, C. (2023a, March). An aperiodic monotile. arXiv:2303.10798

Smith, D., Myers, J. S., Kaplan, C. S.; Goodman-Strauss, C. (2023b, May). A chiral aperiodic monotile. arXiv:2305.17743

Whipple, T. (2023). Retired Yorkshireman solves elusive "Einstein tile" maths problem. *The Times*, April 3, 2023