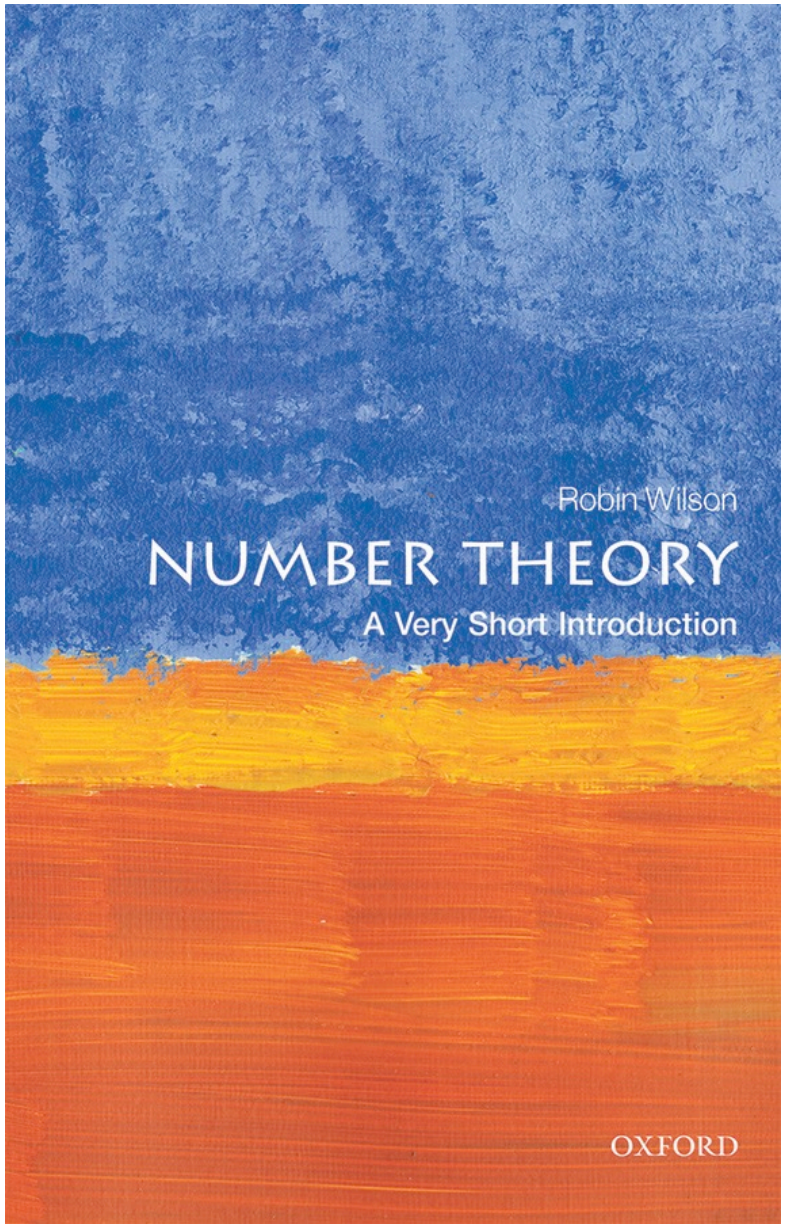


Number Theory : The Queen of Mathematics

Robin Wilson

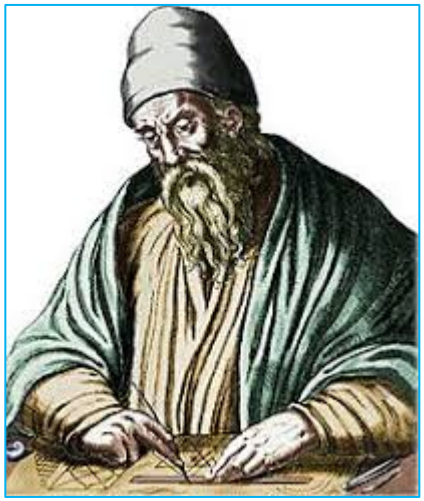
Open University and Oxford, and Gresham College, London

Some prime figures

Euclid

Fermat

Euler Gauss



Gauss: ***Mathematics is the queen of the sciences and number theory is the queen of mathematics***

What is number theory?

Number theory **is the branch of mathematics that's primarily concerned with our *counting numbers*, 1, 2, 3, ...**

Particularly important are *prime numbers*, the 'building blocks' of our number system, whose only factors are themselves and 1:

prime: 11, 13, 17, 19

non-prime: $15 = 3 \times 5$, $18 = 2 \times 9 = 2 \times 3 \times 3$,

$91 = 7 \times 13$, $323 = 17 \times 19$

2047? 30,031? 4,294,967,297 ?

Some questions

- Is 4,294,967,297 prime?
- Are any of the numbers 11, 111, 1111, 11111, . . . perfect squares?
- In which years does February have five Sundays?
- How many right-angled triangles with whole-number sides have a side of length 29?
- Can one construct a regular polygon with 100 sides if measuring is forbidden?
- How many shuffles are needed to restore the order of the cards in a pack with two Jokers?
- How do prime numbers help to keep our credit cards secure?

Four topics

Prime numbers

Euclid's theorem; Dirichlet's theorem; Mersenne primes; Fermat primes; a problem in geometry

Perfect squares

results on squares; right-angled triangles; two results of Fermat

Clock arithmetic

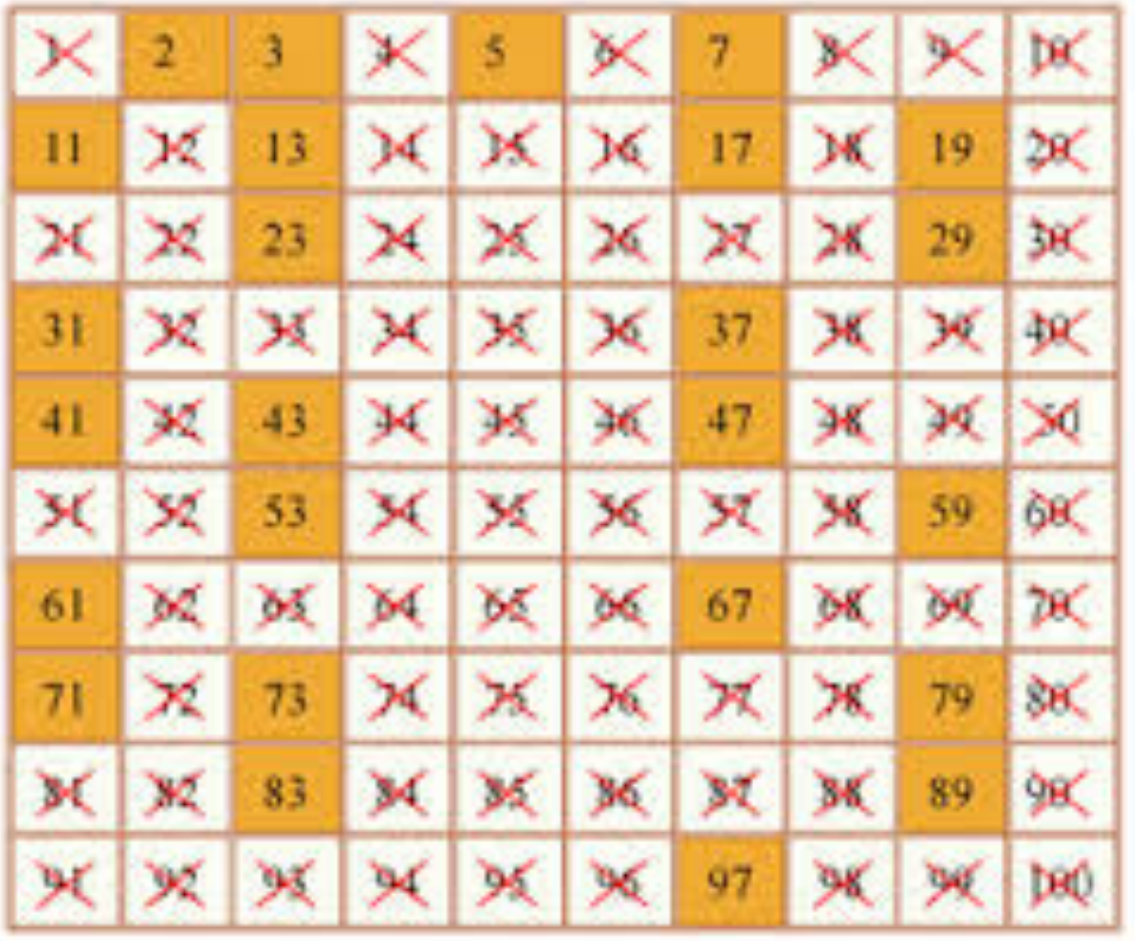
modular arithmetic; calendar problems

Fermat & Euler's theorems

counting necklaces, shuffling cards; protecting your credit cards

Prime numbers

Every number can be written in only one way as a product of primes.



~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

$60 = 2 \times 2 \times 3 \times 5$ (or $2 \times 5 \times 3 \times 2$, etc.)

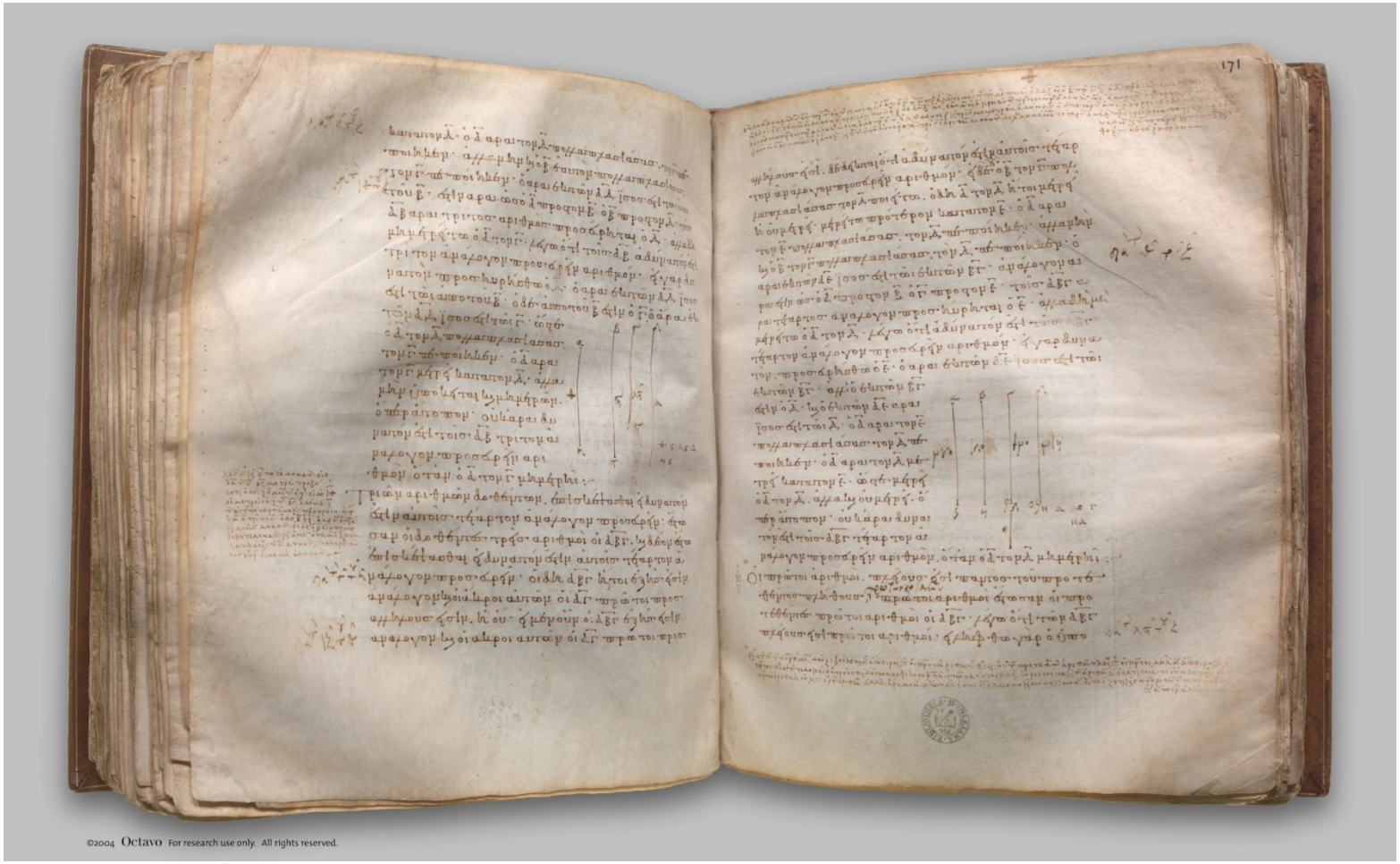
But 1 is not a considered a prime:

$6 = 2 \times 3 = 2 \times 3 \times 1 = 2 \times 3 \times 1 \times 1 \ldots$

Euclid's theorem

(*Elements*, Book IX, Prop 20)

The list of primes goes on for ever


©2004 Octavo For research use only. All rights reserved.

Euclid's theorem

The list of primes goes on for ever

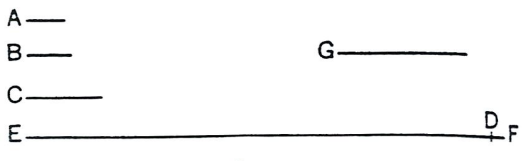
PROPOSITION 20

Prime numbers are more than any assigned multitude of prime numbers.

Let A, B, C be the assigned prime numbers;
I say that there are more prime numbers than A, B, C.

For let the least number measured by A, B, C be taken,
and let it be DE;
let the unit DF be added to DE.

Then EF is either prime or not.



First, let it be prime;
then the prime numbers A, B, C, EF have been found which are more than A, B, C.

Next, let EF not be prime;
therefore it is measured by some prime number. [VII. 31]
Let it be measured by the prime number G.
I say that G is not the same with any of the numbers A, B, C.
For, if possible, let it be so.
Now A, B, C measure DE;
therefore G also will measure DE.
But it also measures EF.
Therefore G, being a number, will measure the remainder, the unit DF:
which is absurd.
Therefore G is not the same with any one of the numbers A, B, C.
And by hypothesis it is prime.
Therefore the prime numbers A, B, C, G have been found which are more than the assigned multitude of A, B, C. Q. E. D.

Euclid's theorem

The list of primes goes on for ever

For suppose that the ONLY primes are
$p_1, p_2, p_3, \ldots, p_n$, and consider the number

$$N = (p_1 \times p_2 \times p_3 \times \ldots \times p_n) + 1.$$

Then N cannot be divided by any of these primes.
So N must be a new prime, or a product of new primes.
This contradicts the fact that we could list them all.

Examples:

- If the only known primes were 2, 3, 5 and 7,
then $N = (2 \times 3 \times 5 \times 7) + 1 = 211$ (a new prime)
- If the only known primes were 2, 3, 5, 7, 11, 13,
then $N = (2 \times 3 \times 5 \times 7 \times 11 \times 13) + 1$
$= 30{,}031 = 59 \times 509$ (two new primes)

Generalising Euclid's result

Using Euclid's method, we can prove that:

There are infinitely many primes of the form $4n + 3$:

3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, . . .

We can also prove that:

There are infinitely many primes of the form $4n + 1$:

5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, . . . ,

. . . but not of the form $4n + 2$, because these are all divisible by 2.

Dirichlet's theorem (1837)

So we can prove that:

There are infinitely many primes of the form $4n + 3$:

and also that:

There are infinitely many primes of the form $4n + 1$:

but not of the form $4n + 2$.

Dirichlet's theorem: If a and b have no factors in common, then there are infinitely many primes of the form $an + b$.

For example, when $a = 10$ and $b = 9$:

there are infinitely many primes of the form $10n + 9$

– that is, there are infinitely many primes ending with 9

[19, 29, 59, 79, 89, 109, 139, . . .]

Mersenne primes

Mersenne numbers are numbers of the form $2^n - 1$.

Some Mersenne numbers are prime:

$2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$, . . .

Others are not:

$2^4 - 1 = 15$, $2^6 - 1 = 63$, $2^8 - 1 = 255$, $2^9 - 1 = 511$, . . .

Is it true that $2^n - 1$ is prime if and only if n is prime?

If n is not prime, then nor is $2^n - 1$.

But if n is prime, must $2^n - 1$ be prime?

NO: if $n = 11$, then $2^{11} - 1 = 2047 = 23 \times 89$.

All recently found primes are Mersenne primes.

51 Mersenne primes are known: the latest (2018) is

$2^{82,589,933} - 1$ with almost 25 million digits.

Perfect numbers

A number N is *perfect* if it's the sum of all its proper factors.

6 is perfect because $6 = 1 + 2 + 3$,

28 is perfect because $28 = 1 + 2 + 4 + 7 + 14$,

The next two perfect numbers are 496 and 8128,

and then there are no more until 33,550,366.

Now $6 = 2 \times 3 = 2^1 \times (2^2 - 1)$; $28 = 4 \times 7 = 2^2 \times (2^3 - 1)$;

$496 = 16 \times 31 = 2^4 \times (2^5 - 1)$; $8128 = 64 \times 127 = 2^6 \times (2^7 - 1)$;

$33{,}550{,}336 = 4096 \times 8191 = 2^{12} \times (2^{13} - 1)$

Euclid: if $2^n - 1$ is prime, then $N = 2^{n-1} \times (2^n - 1)$ is perfect.

Does this give us *all* perfect numbers?

Euler: It gives us all *even* perfect numbers

but no-one knows whether there are any *odd* perfect numbers.

Fermat primes

Let $F(n) = 2^N + 1$, where $N = 2^n$

Conjecture: $F(n)$ is prime for all n

$F(0) = 2^1 + 1 = 3$

$F(1) = 2^2 + 1 = 5$

$F(2) = 2^4 + 1 = 17$

$F(3) = 2^8 + 1 = 257$

$F(4) = 2^{16} + 1 = 65{,}537$

But is $F(5) = 2^{32} + 1 = 4{,}294{,}967{,}297$ prime?

Fermat primes

Let $F(n) = 2^N + 1$, where $N = 2^n$

Conjecture: $F(n)$ is prime for all n

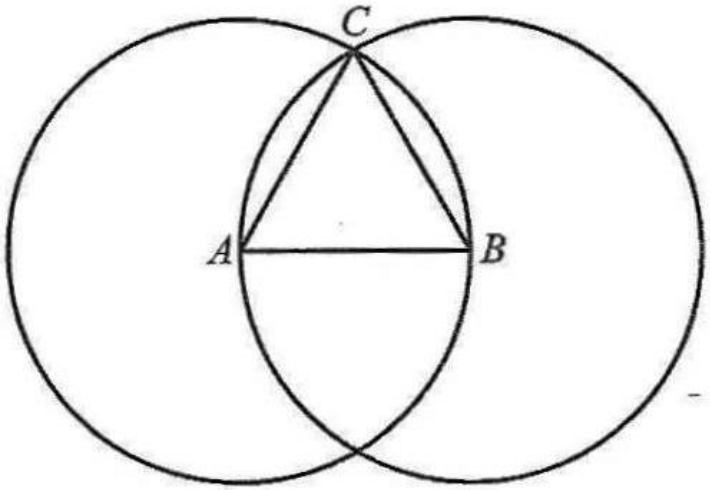
$F(0) = 3$, $F(1) = 5$, $F(2) = 17$, $F(3) = 257$,
$F(4) = 65{,}537$.

But is $F(5) = 2^{32} + 1 = 4{,}294{,}967{,}297$ prime?

Euler: No, it is $641 \times 6{,}700{,}417$

Moreover, no other Fermat primes
have ever been found . . .

Constructing triangles



Constructing an equilateral triangle

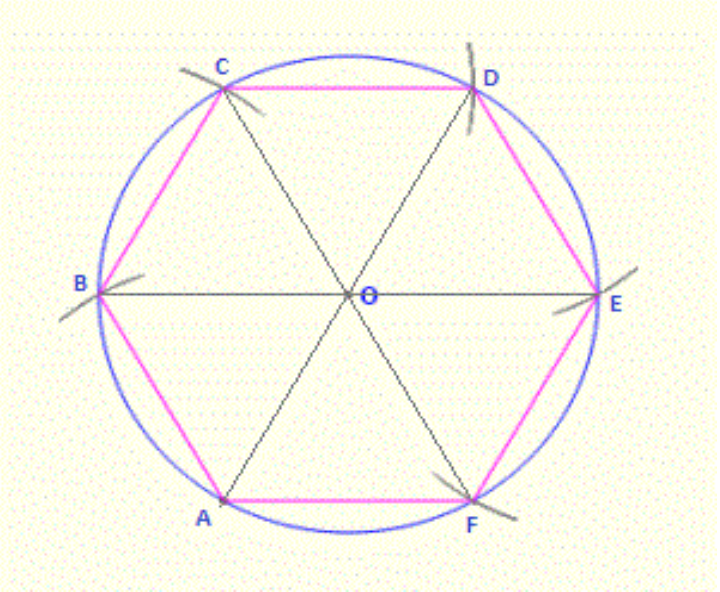
Given the line *AB*, draw the circle with centre *A* and radius *AB*, and the circle with centre B and radius *BA*.

These circles meet at the point *C*.

Draw the lines *AC* and *BC*.

Then *ABC* is an equilateral triangle.

Constructing hexagons



Constructing a regular hexagon

Draw a circle with centre *O* and radius *OA*.

With the point of the compasses at *A* and radius *OA*, mark the point *B* on the circle.

Repeat to get the points *C*, *D*, *E*, *F* .

Then *ABCDEF* is a regular hexagon.

Which polygons can we draw?

We can draw regular polygons with n sides

when $n = 3,\ 4,\ 5,\ 6,\ 8,\ 10,\ 12,\ 15,\ 16,\ 20,\ 24,\ \ldots$

but not when $n = 7,\ 9,\ 11,\ 13,\ 14,\ 18,\ 19,\ \ldots$

Gauss then drew $n = 17$, and proved:

One can draw a regular polygon with n sides if and only if n is a power of 2 × *unequal* Fermat primes.

[3, 5, 17, 257, 65537]

Yes: $30 = 2 \times 3 \times 5$, $32 = 2^5$, $34 = 2 \times 17$, $40 = 2^3 \times 5$, . . .

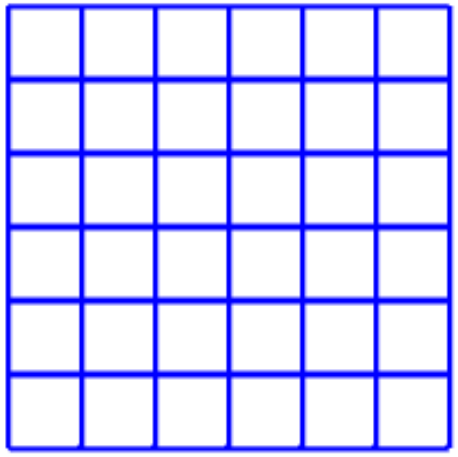
No: $35 = 5 \times 7$, $36 = 2^2 \times 3^2$, 37, . . . , $100 = 2^2 \times 5^2$.

So we cannot draw a regular polygon with 100 sides.

Perfect squares

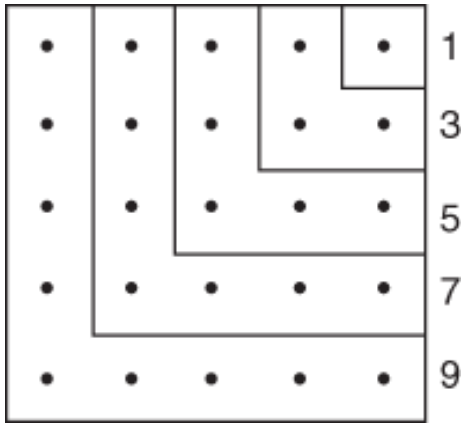
$1^2 = 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 16,$
$5^2 = 25,\ 6^2 = 36,\ 7^2 = 49,\ 8^2 = 64,$
$9^2 = 81,\ 10^2 = 100$

No squares end in 2, 3, 7 or 8.



Adding the first few odd numbers always gives a square

(1 , 1+3, 1+3+5, . . .)



Perfect squares

Every square has the form $4n$ or $4n + 1$.

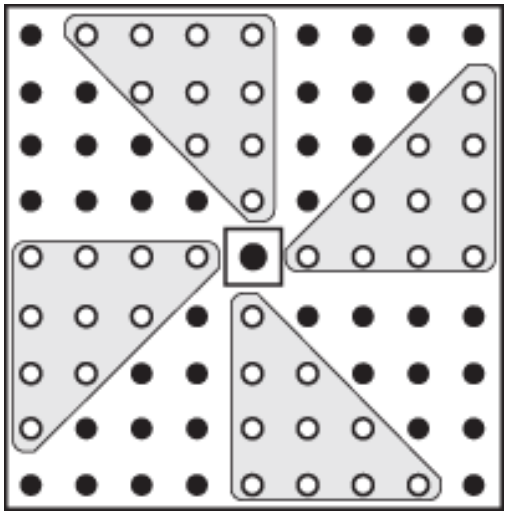
N even: $N = 2k$, so $N^2 = 4 \times k^2$.

N odd: $N = 2k + 1$, so $N^2 = 4 \times k(k+1) + 1$.

So 11, 111, 1111, 11111, . . . aren't squares, as they have the form $4n + 3$.

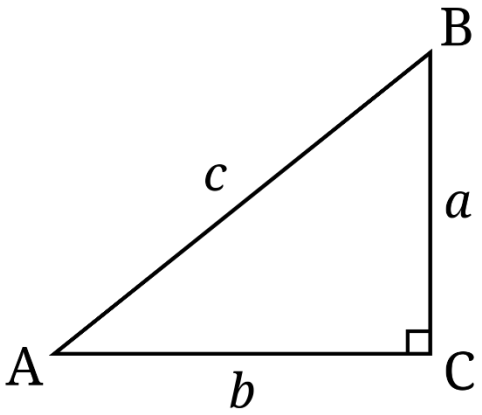
Moreover, if N is odd,

then N^2 has the form $8n + 1$.



Right-angled triangles

Pythagoras: If the sides are a, b, c, then $a^2 + b^2 = c^2$



Examples: $3^2 + 4^2 = 5^2$; $5^2 + 12^2 = 13^2$; $15^2 + 8^2 = 17^2$

Can we find all examples with whole-number sides?

We'll ignore scalings: $30^2 + 40^2 = 50^2$; $6^2 + 8^2 = 10^2$

so we assume that a, b, c have no factors in common.

Answer: $a = x^2 - y^2$, $b = 2xy$, $c = x^2 + y^2$,

where $x > y$, x and y have no common factors, and one is even and the other odd.

Listing all right-angled triangles

$$a = x^2 - y^2, \quad b = 2xy, \quad c = x^2 + y^2,$$

where $x > y$, x and y have no common factors,
and one is even and the other odd.

Examples: $x = 2, y = 1$: $a = 3, b = 4, c = 5$: $3^2 + 4^2 = 5^2$

$x = 3, y = 2$: $a = 5, b = 12, c = 13$: $5^2 + 12^2 = 13^2$

$x = 5, y = 2$: $a = 21, b = 20, c = 29$: $21^2 + 20^2 = 29^2$

Right-angled triangles with a side of length 29

$a = x^2 - y^2, \quad b = 2xy, \quad c = x^2 + y^2$

Example: $x = 5, \ y = 2$:

$a = 21, \ b = 20, \ c = 29 : \quad 21^2 + 20^2 = 29^2$

How many right-angled triangles with whole-number sides have a side of length 29?

Either $29 = x^2 + y^2$, so $x = 5, y = 2$: $a = 21, \ b = 20, \ c = 29$

or $29 = x^2 - y^2 = (x + y)(x - y) = 29 \times 1,$

so $x + y = 29, \ x - y = 1,$ giving $x = 15, \ y = 14,$

and $a = 29, \ b = 420, \ c = 421$.

Sums of squares

Which numbers can be written as the sum of two squares?

***Fermat's* 4*n* + 1 *theorem*:**

Every *prime number* of the form 4*n* + 1 (such as 5, 13, 17, 29, 41, . . .) is the sum of two squares (and in only one way).

$5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$,
$29 = 5^2 + 2^2$, $41 = 5^2 + 4^2$, . . .

Fermat's 'last theorem'

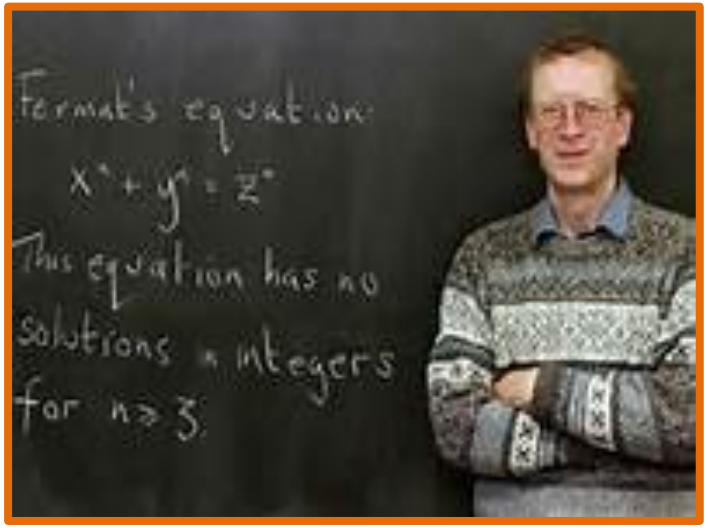
We've found a, b, c, so that
$a^2 + b^2 = c^2$.

Can we find a, b, c, so that
$a^3 + b^3 = c^3$?
or $a^4 + b^4 = c^4$? or . . .

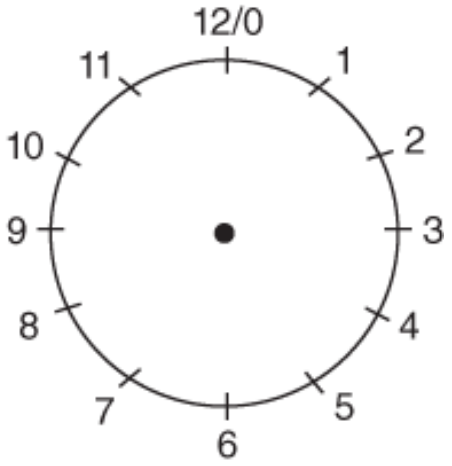
Fermat believed that:

For any $n > 2$, $a^n + b^n = c^n$
has no solutions.

Proved by Andrew Wiles,
1995.



Clock arithmetic

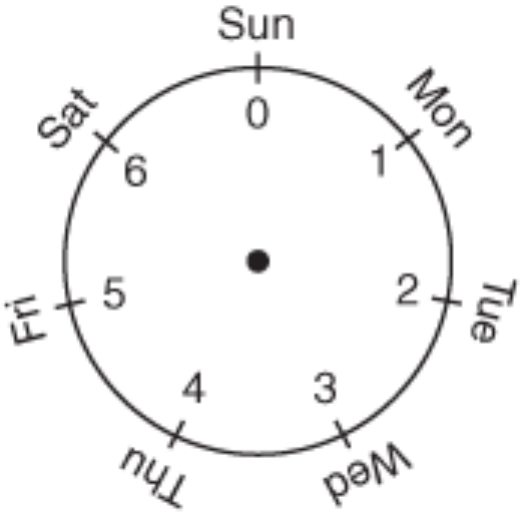


9 o'clock + 6 hrs = 3 o'clock: $9 + 6 \equiv 3 \pmod{12}$

10 o'clock + 7 hrs = 5 o'clock: $10 + 7 \equiv 5 \pmod{12}$

8 o'clock + 4 hrs = 12 o'clock: $8 + 4 \equiv 0 \pmod{12}$.

$a \equiv b \pmod{n}$ if a and b leave the same remainder when divided by n : that is, if $a - b$ is divisible by n.



Thursday + four days = Monday

Saturday + three days = Tuesday

Sunday = 0; Monday = 1; Tuesday = 2;

Wednesday = 3; Thursday = 4; Friday = 5;

Saturday = 6. Working (mod 7), we have

$4 + 4 \equiv 1 \pmod{7}$; $6 + 3 \equiv 2 \pmod{7}$

Carroll's method for finding the day of the week for any given date

Take the given date in 4 portions, viz. the number of centuries, the number of years over, the month, the day of the month.

Compute the following 4 items, adding each, whenever found, to the total of the previous items. When an item or total exceeds 7, divide by 7, and keep the remainder only.

The Century-Item: Divide by 4, take overplus from 3, multiply remainder by 2.

The Year-Item: Add together the number of dozens, the overplus, and the number of 4's in the overplus.

The Month-Item: If it begins or ends with a vowel, subtract the number, denoting its place in the year, from 10. This, plus its number of days, gives the item for the following month. The item for January is "0"; for February or March (the third month), "3"; for December (the 12th month), "12."

The Day-Item: is the day of the month.

The total, thus reached, must be corrected, by deducting "1" (first adding 7, if the total be "0"), if the date be January or February in a Leap Year: remembering that every year, divisible by 4, is a Leap Year, excepting only the century-years, in New Style, when the number of centuries is *not* so divisible (*e.g.* 1800).

The final result gives the day of the week, "0" meaning Sunday, "1" Monday, and so on.

Finding the day of the week

(C. L. Dodgson: Lewis Carroll)

Lewis Carroll's method

Add the following four numbers:

***Century number*. Divide the first two digits of the year by 4, subtract the remainder from 3, and double.**

***Year number*. Divide the last two digits of the year by 12, and add the quotient, the remainder, and the number of times 4 divides into the remainder.**

***Month number*. Carroll's method gives:**

Jan: 0 Feb: 3 Mar: 3 Apr 6 May: 1 Jun: 4 Jul: 6
Aug: 2 Sep: 5 Oct: 0 Nov: 3 Dec: 5

***Day number*: This is the day of the month.**

[Finally, subtract 1 if the date falls in January or February of a leap year.]

Lewis Carroll's method

Add the following numbers:

Century number. Divide the first two year digits by 4, subtract the remainder from 3, and double.

Year number. Divide the last two year digits by 12, and add the quotient, the remainder, and the number of times 4 divides into the remainder.

Month number.

Jan: 0	Feb: 3	Mar: 3	Apr 6
May: 1	Jun: 4	Jul: 6	Aug: 2
Sep: 5	Oct: 0	Nov: 3	Dec: 5

Day number: This is the day of the month.

28 September 2020

Century number

Divide 20 by 4: remainder 0; subtract 0 from 3 to give 3, and double to give 6

Year number

Divide 20 by 12 giving 1, remainder 8; 4 divides 8 2 times, giving 1 + 8 + 2 = 11

Month number Sep = 5

Day number 28

The sum is 6 + 11 + 5 + 28 = 50 ≡ 1 (mod 7) = Monday

Five Sundays in February?

The five Sundays must be 1, 8, 15, 22, 29 February, so the year must be a leap year.

Now 1 January 2001 was a Monday,

so 1 February 2001 was a Thursday,

1 February 2002 was a Friday (as $365 \equiv 1 \pmod 7$),

1 February 2003 was a Saturday,

1 February 2004 was a Sunday.

Also, the cycle of days repeats every 28 years

as $(28 \times 365) + 7 \equiv 0 \pmod 7$, so the years are

2004, 2032, 2060, 2088.

Fermat's 'little theorem'

For any number a and any prime number p,

$a^p - a$ is divisible by p

for example, $8^{37} - 8$ is divisible by 37

Another version (divide by a) is:

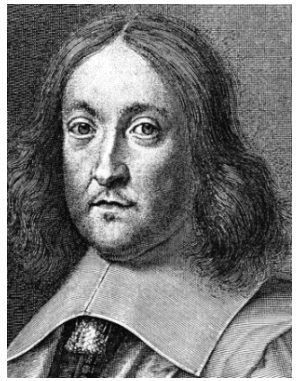
$a^{p-1} - 1$ is divisible by p

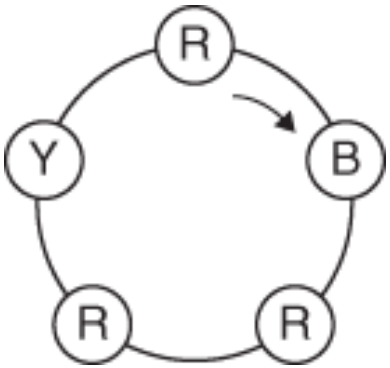
for example, $2^{52} - 1$ is divisible by 53,

or $2^{52} \equiv 1 \pmod{53}$

Counting necklaces

For any number *a* and any prime *p*,
$a^p - a$ is divisible by *p*



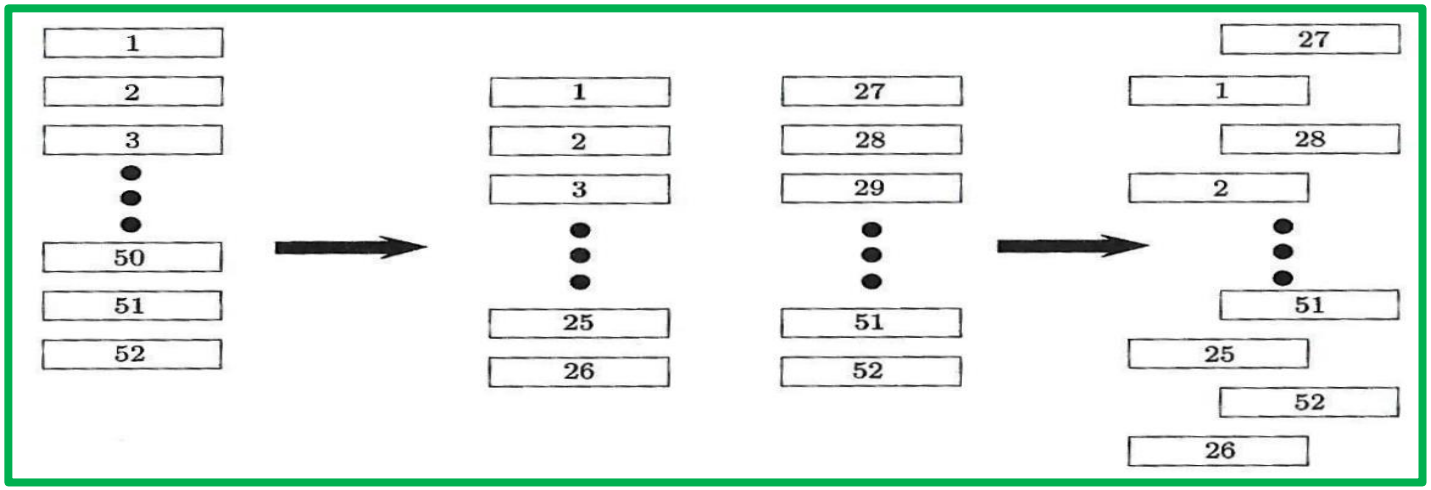


RBRRY
= BRRYR
= RRYRB
= RYRBR
= YRBRR

How many different coloured necklaces with p beads and a colours are there, using at least two colours?

There are a^p possible strings of beads, or $a^p - a$ when we exclude the 1-colour ones (such as RRRRR).
So there are $(a^p - a)/p$ *different* ones, and so $a^p - a$ is divisible by *p*.

How many shuffles are needed to restore a pack of cards to its original order?



Now the card in position x → position $2x$ (mod 53),

and after n shuffles → position $2^n x$ (mod 53).

So $2^n x \equiv x$ (mod 53), giving $2^n \equiv 1$ (mod 53).

But, by Fermat's theorem, $2^{52} \equiv 1$ (mod 53).

So the pack is restored after 52 shuffles.

[mod 53: $2^2 \equiv 4$, $2^4 \equiv 16$, $2^{13} \equiv 30$, $2^{26} \equiv 52$]

Shuffling a pack with two Jokers

We now have 54 cards, and in the same way we get

$2^n \equiv 1 \pmod{55}$.

But 55 isn't a prime number, so we can't use Fermat's theorem to give us $n = 54$ shuffles.

But if 55 divides $2^n - 1$, then so do 5 & 11.

So $2^4 \equiv 1 \pmod{5}$ and $2^{10} \equiv 1 \pmod{11}$.

So $2^{20} \equiv 1 \pmod{5}$ and $2^{20} \equiv 1 \pmod{11}$,

so $2^{20} \equiv 1 \pmod{55}$.

So the pack is restored after 20 shuffles.

Euler's theorem

If p does not divide a,

then $a^{p-1} - 1$ is divisible by p:

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

But what can we say if p isn't prime?

Euler's theorem: $a^{\varphi(n)} \equiv 1 \pmod{n}$,

where $\varphi(n)$ counts the numbers up to n
with no factors in common with n:

e.g. $\varphi(10) = 4$ [1, 3, 7, 9]; $\varphi(12) = 4$ [1, 5, 7, 11];

$\varphi(p) = p - 1$; $\varphi(pq) = (p - 1) \times (q - 1)$:

e.g. $1073 = 29 \times 37$, so $\varphi(1073) = 28 \times 36 = 1008$.

RSA public key cryptography

Alice wishes to send a secret message to Bob.

Bob first selects two primes, p, q, calculates $N = pq$. $N = 29 \times 37 = 1073$

and chooses e so that gcd $(e, \varphi(N)) = 1$. $\varphi(N) = 1008$, $e = 11$

He publicly announces e and N, but not p and q.

The numbers e and N are then the *public key,* known to all.

Alice now converts her message to numerical form and calls it M.

Knowing e and N, she calculates $E \equiv M^e \pmod{N}$ and sends it to Bob.

Using the fact that gcd $(e, \varphi(N)) = 1$, Bob calculates m and n for which

$me + n\,\varphi(N) = 1$, and so $me \equiv 1 \pmod{\varphi(N)}$. $11m \equiv 1 \pmod{1008}$

Now, by Euler's theorem, $M^{\varphi(N)} \equiv 1 \pmod{N}$, so $m = 275$

so $E^m \equiv (M^e)^m = M^{me} = M^{1 - n\varphi(N)} \equiv M \pmod{N}$.

Bob calculates $E^m \pmod{N}$ to retrieve Alice's original message M.

$M \equiv E^{275} \pmod{1073}$

RSA public key cryptography

Alice wishes to send a secret message to Bob.

Bob first selects two primes, p, q, calculates $N = pq$.

$N = 29 \times 37 = 1073$, $\varphi(N) = 1008$,

and chooses e so that gcd $(e, \varphi(N)) = 1$. $e = 11$

He then publicly announces e and N, but not p and q.

The numbers e and N are the *public key,* known to all.

Alice now converts her message to numerical form

and calls it M. Knowing e and N, she calculates

$E \equiv M^e \pmod{N}$ and sends it to Bob.

RSA public key cryptography

Alice calculates $E \equiv M^e \pmod{N}$ and sends it to Bob.

Using the fact that gcd $(e, \varphi(N)) = 1$,

Bob calculates m and n for which

$me + n\,\varphi(N) = 1$, and so $me \equiv 1 \pmod{\varphi(N)}$.

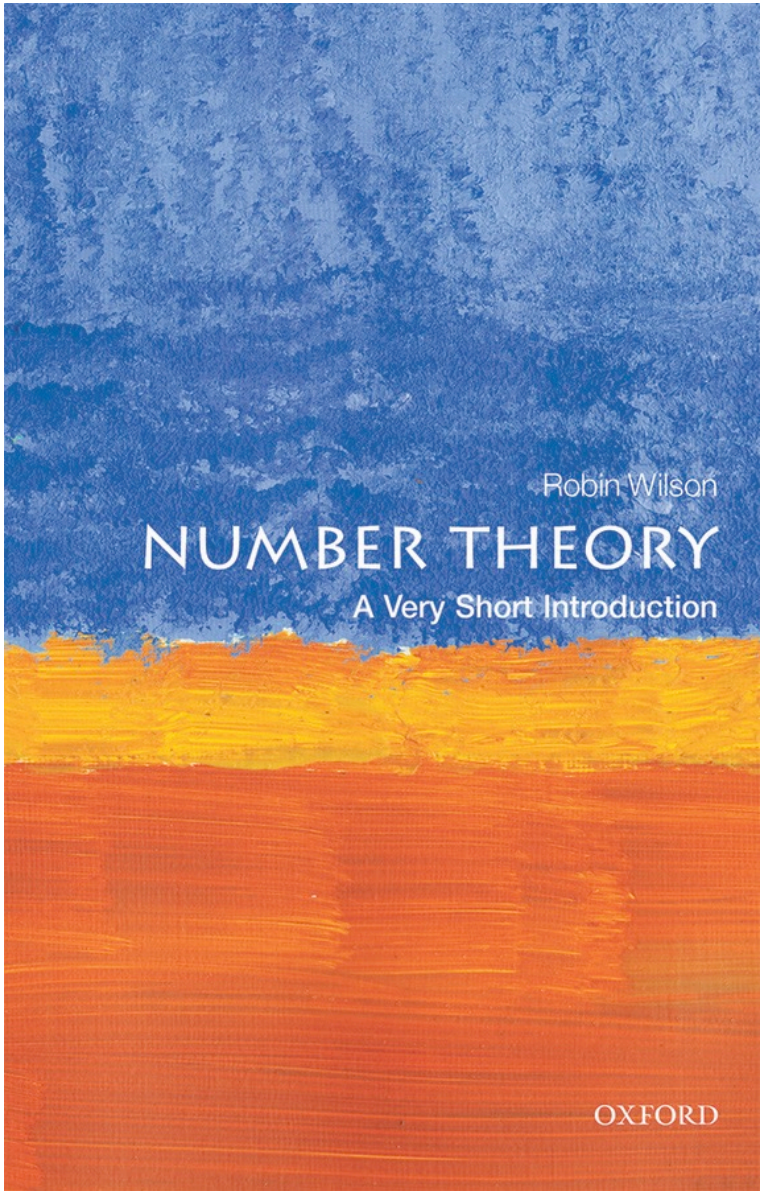
$11m \equiv 1 \pmod{1008}$, so $m = 275$

By Euler's theorem, $M^{\varphi(N)} \equiv 1 \pmod{N}$,

so $E^m \equiv (M^e)^m = M^{me} = M^{1 - n\varphi(N)} \equiv M \pmod{N}$.

Bob calculates $E^m \pmod{N}$ to retrieve Alice's original message M.

$M \equiv E^{275} \pmod{1073}$



Robin Wilson

NUMBER THEORY

A Very Short Introduction

(no. 636 in the series)

Published in May 2020 by Oxford University Press

ISBN: 978-0-19-879809-5

Price: £8.99

[US $11.95]