PROGETTO DI ECCELLENZA

L'UNIVERSITÀ A SCUOLA
A SCUOLA DI UNIVERSITÀ

UNIVERSITÀ CATTOLICA del Sacro Cuore

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

FONDAZIONE DELLA COMUNITÀ BRESCIANA ONLUS

Alessandro Musesti - Università Cattolica del Sacro Cuore

Un teorema è per sempre

a cura di Alessandro Musesti

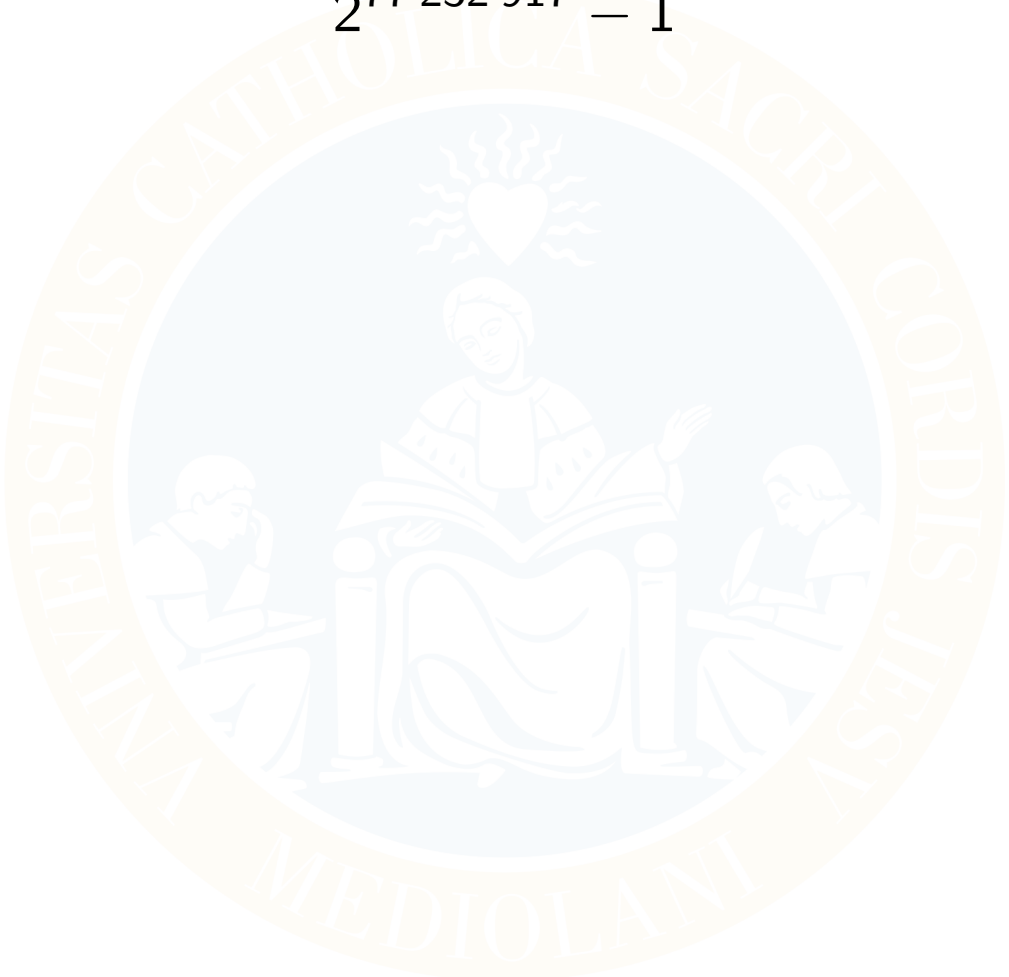
Università Cattolica del Sacro Cuore, Brescia

Advertisement

Breaking news

Il 26 dicembre 2017 è stato scoperto il più grande numero primo conosciuto:

$$2^{77\,232\,917} - 1$$



Breaking news

Il 26 dicembre 2017 è stato scoperto il più grande numero primo conosciuto:

$$2^{77\,232\,917} - 1$$

Tale numero ha 23 249 425 cifre:

Breaking news

Il 26 dicembre 2017 è stato scoperto il più grande numero primo conosciuto:

$$2^{77\,232\,917} - 1$$

Tale numero ha 23 249 425 cifre:

$$4673331833592310999883355855611155212513211028177 1$$

$$\vdots$$

$$(23\,249\,325 \text{ cifre})$$

$$\vdots$$

$$7989462799993961465921737113658273061806976217907 1$$

Breaking news

Il 26 dicembre 2017 è stato scoperto il più grande numero primo conosciuto:

$$2^{77\,232\,917} - 1$$

Tale numero ha 23 249 425 cifre:

$$46733318335923109998833558556111552125132110281771$$
$$\vdots$$
$$(23\,249\,325 \text{ cifre})$$
$$\vdots$$
$$79894627999939614659217371136582730618069762179071$$

Il precedente record $2^{74\,207\,281} - 1$ aveva 22 338 618 cifre (gennaio 2016)

"I promessi sposi" ha circa 1 310 000 caratteri...

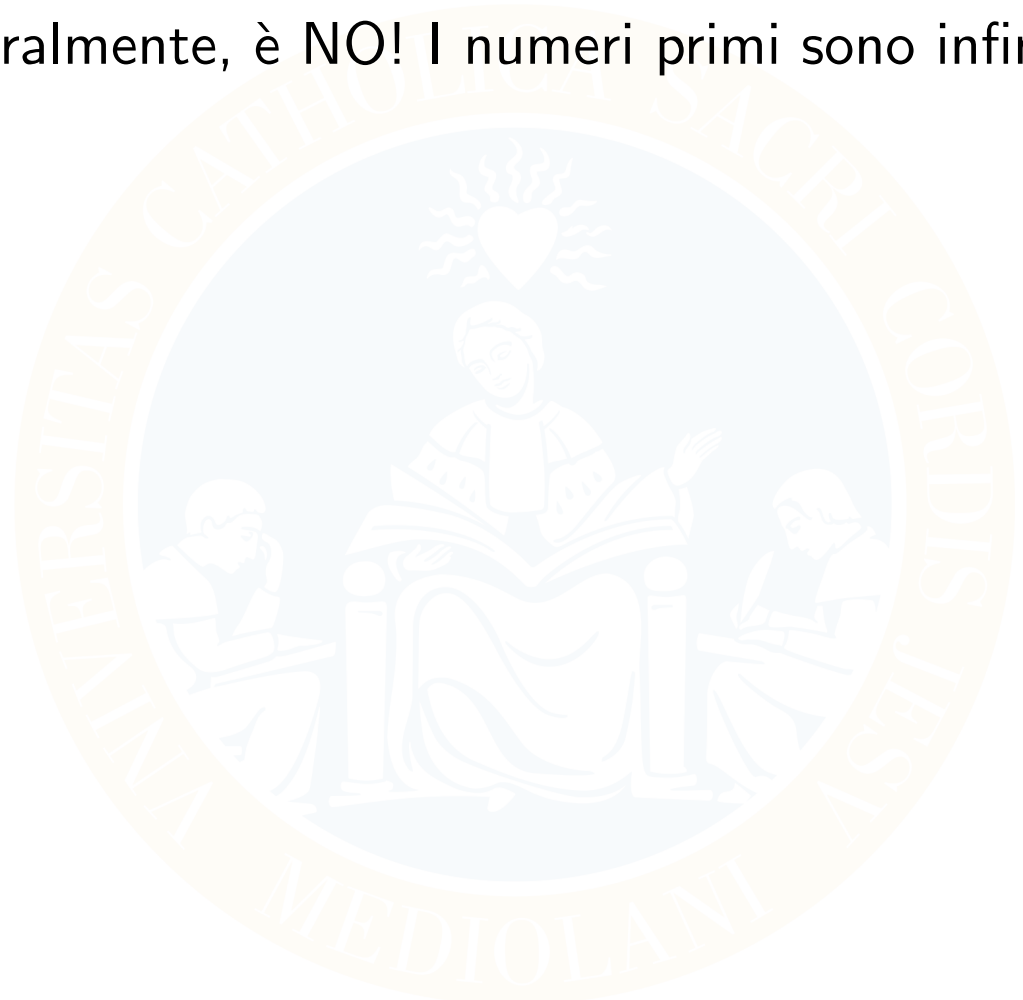
Numeri primi

Troveremo mai il numero primo più grande di tutti? Quello definitivo?

Numeri primi

Troveremo mai il numero primo più grande di tutti? Quello definitivo?

La risposta, naturalmente, è NO! I numeri primi sono infiniti.

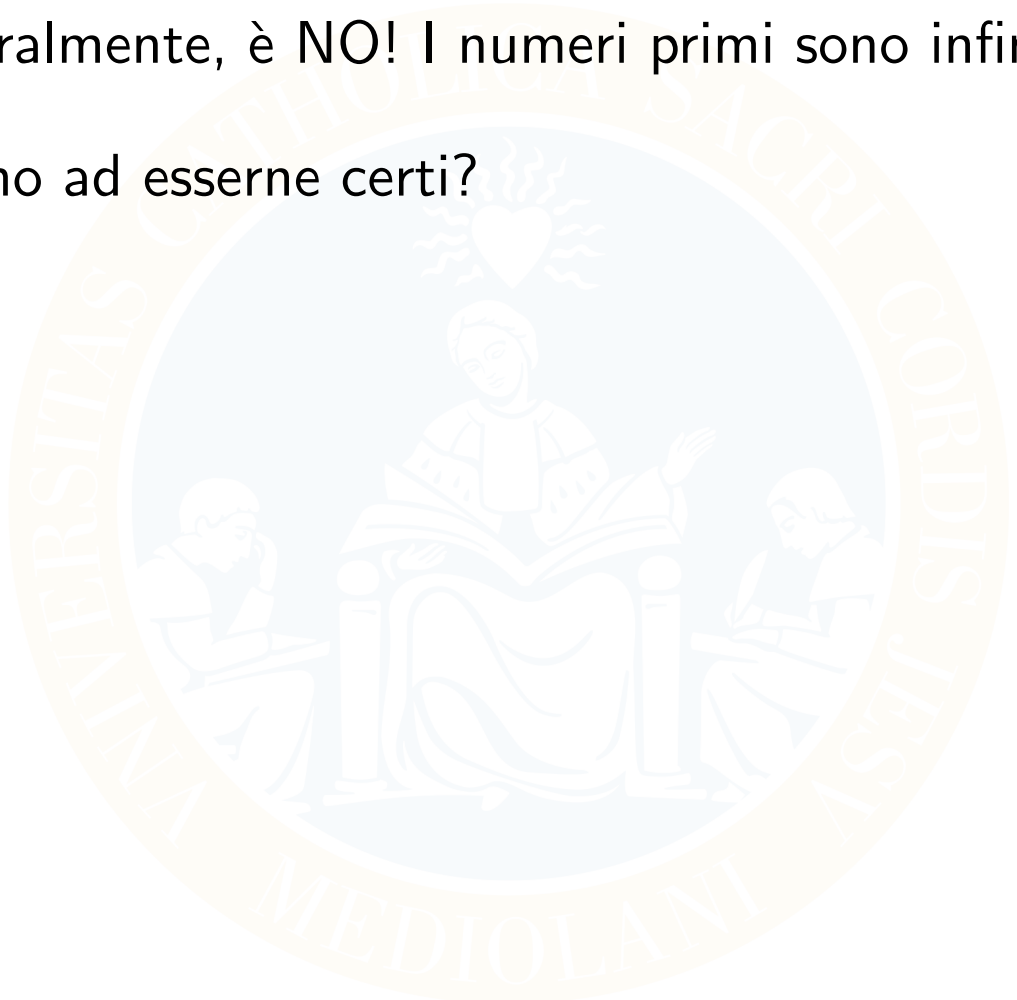


Numeri primi

Troveremo mai il numero primo più grande di tutti? Quello definitivo?

La risposta, naturalmente, è NO! I numeri primi sono infiniti.

Ma come facciamo ad esserne certi?



Numeri primi

Troveremo mai il numero primo più grande di tutti? Quello definitivo?

La risposta, naturalmente, è NO! I numeri primi sono infiniti.

Ma come facciamo ad esserne certi?

Lo possiamo dimostrare! Euclide lo ha fatto prima di noi, 2300 anni fa (e probabilmente non fu il primo).

Numeri primi

Troveremo mai il numero primo più grande di tutti? Quello definitivo?

La risposta, naturalmente, è NO! I numeri primi sono infiniti.

Ma come facciamo ad esserne certi?

Lo possiamo dimostrare! Euclide lo ha fatto prima di noi, 2300 anni fa (e probabilmente non fu il primo).

Ma noi possiamo seguire e capire la sua dimostrazione, o farne un'altra, se ne siamo capaci.

Numeri primi

Troveremo mai il numero primo più grande di tutti? Quello definitivo?

La risposta, naturalmente, è NO! I numeri primi sono infiniti.

Ma come facciamo ad esserne certi?

Lo possiamo dimostrare! Euclide lo ha fatto prima di noi, 2300 anni fa (e probabilmente non fu il primo).

Ma noi possiamo seguire e capire la sua dimostrazione, o farne un'altra, se ne siamo capaci.

Una volta che una proprietà è **dimostrata**, se il ragionamento è corretto e le ipotesi di partenza sono chiare, lo resterà per sempre.

Una dimostrazione dura per sempre, ben più di un diamante!

La dimostrazione di Euclide

Teorema

I numeri primi sono infiniti.

La dimostrazione di Euclide

Teorema

I numeri primi sono infiniti.

Dimostrazione

Prendiamo i numeri primi $p_1, p_2, \ldots, p_n$ e formiamo il numero

$$1 + p_1 \cdot p_2 \cdots p_n$$

La dimostrazione di Euclide

Teorema

I numeri primi sono infiniti.

Dimostrazione

Prendiamo i numeri primi $p_1, p_2, \ldots, p_n$ e formiamo il numero

$$1 + p_1 \cdot p_2 \cdots p_n$$

Tale numero non è divisibile per p_1, né per p_2, ... né per p_n, perché dà sempre resto 1.

La dimostrazione di Euclide

Teorema

I numeri primi sono infiniti.

Dimostrazione

Prendiamo i numeri primi $p_1, p_2, \ldots, p_n$ e formiamo il numero

$$1 + p_1 \cdot p_2 \cdots p_n$$

Tale numero non è divisibile per p_1, né per p_2, ... né per p_n, perché dà sempre resto 1.

Se lo fattorizziamo, troveremo quindi almeno un numero primo nuovo.

La dimostrazione di Euclide

Teorema

I numeri primi sono infiniti.

Dimostrazione

Prendiamo i numeri primi $p_1, p_2, \ldots, p_n$ e formiamo il numero

$$1 + p_1 \cdot p_2 \cdots p_n$$

Tale numero non è divisibile per p_1, né per p_2, ... né per p_n, perché dà sempre resto 1.

Se lo fattorizziamo, troveremo quindi almeno un numero primo nuovo.

Semplice, vero? Eppure questo semplice ragionamento ci garantisce che la caccia ai numeri primi grandi non finirà mai, almeno fino a quando ci sarà qualche essere interessato a trovarli.

La dimostrazione di Euclide

Teorema

I numeri primi sono infiniti.

Dimostrazione

Prendiamo i numeri primi $p_1, p_2, \ldots, p_n$ e formiamo il numero

$$1 + p_1 \cdot p_2 \cdots p_n$$

Tale numero non è divisibile per p_1, né per p_2, ... né per p_n, perché dà sempre resto 1.

Se lo fattorizziamo, troveremo quindi almeno un numero primo nuovo.

Semplice, vero? Eppure questo semplice ragionamento ci garantisce che la caccia ai numeri primi grandi non finirà mai, almeno fino a quando ci sarà qualche essere interessato a trovarli.
I moderni metodi crittografici si basano proprio su questo.

Il teorema di Pitagora

Teorema

Per un triangolo rettangolo di cateti a, b e ipotenusa c vale l'uguaglianza

$$a^2 + b^2 = c^2.$$

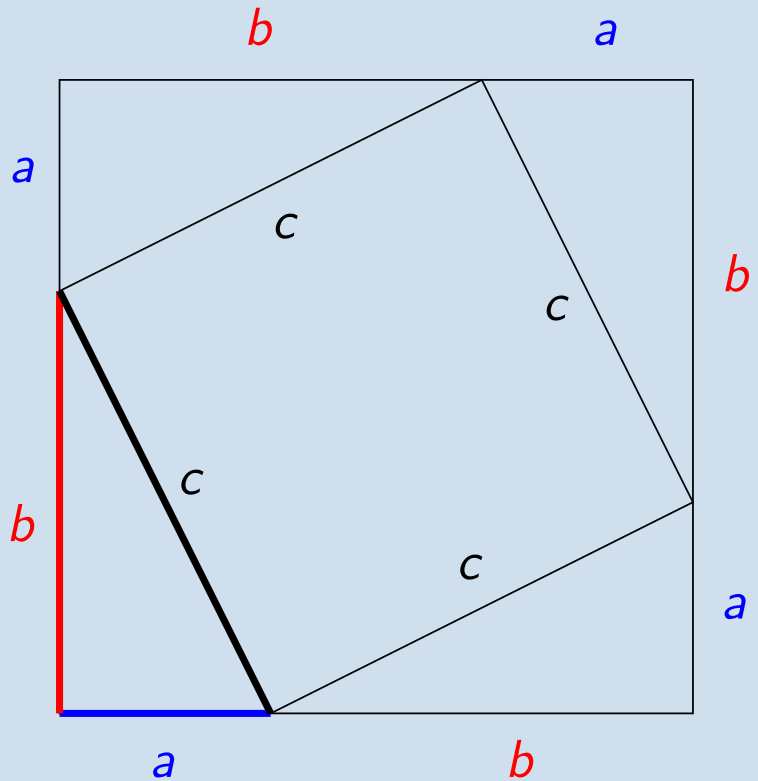
Il teorema di Pitagora

Teorema

Per un triangolo rettangolo di cateti a, b e ipotenusa c vale l'uguaglianza

$$a^2 + b^2 = c^2.$$

Dimostrazione



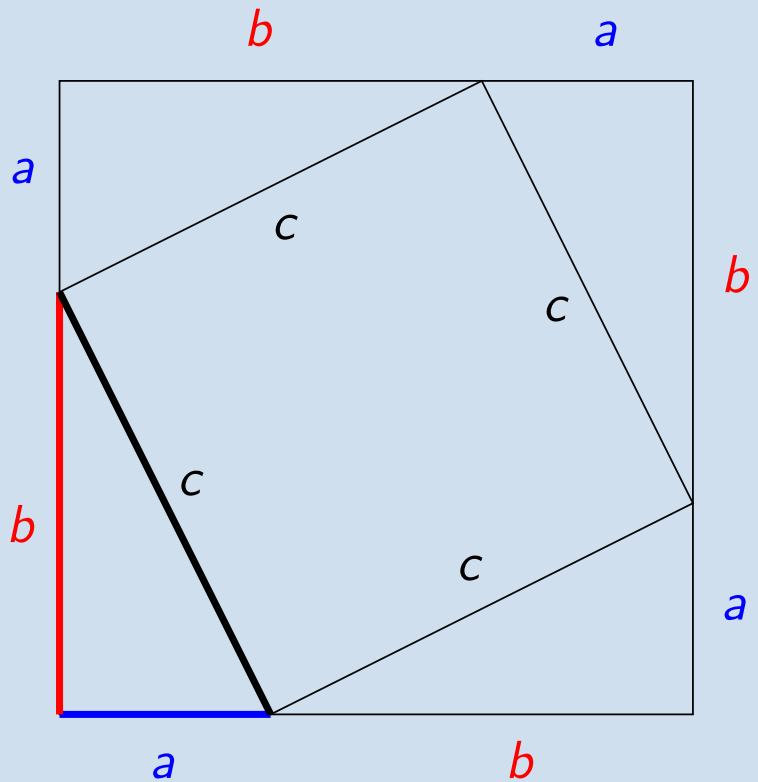
Il teorema di Pitagora

Teorema

Per un triangolo rettangolo di cateti a, b e ipotenusa c vale l'uguaglianza

$$a^2 + b^2 = c^2.$$

Dimostrazione



$$(a+b)^2 = 4 \cdot \frac{1}{2}ab + c^2$$

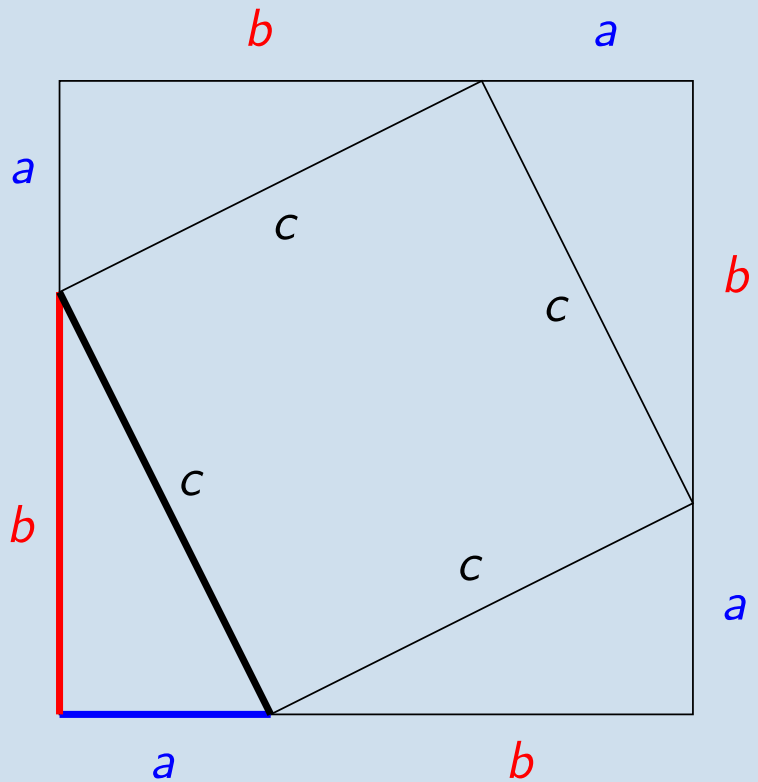
Il teorema di Pitagora

Teorema

Per un triangolo rettangolo di cateti a, b e ipotenusa c vale l'uguaglianza

$$a^2 + b^2 = c^2.$$

Dimostrazione



$$(a+b)^2 = 4 \cdot \frac{1}{2}ab + c^2$$

$$a^2 + 2ab + b^2 = 2ab + c^2$$

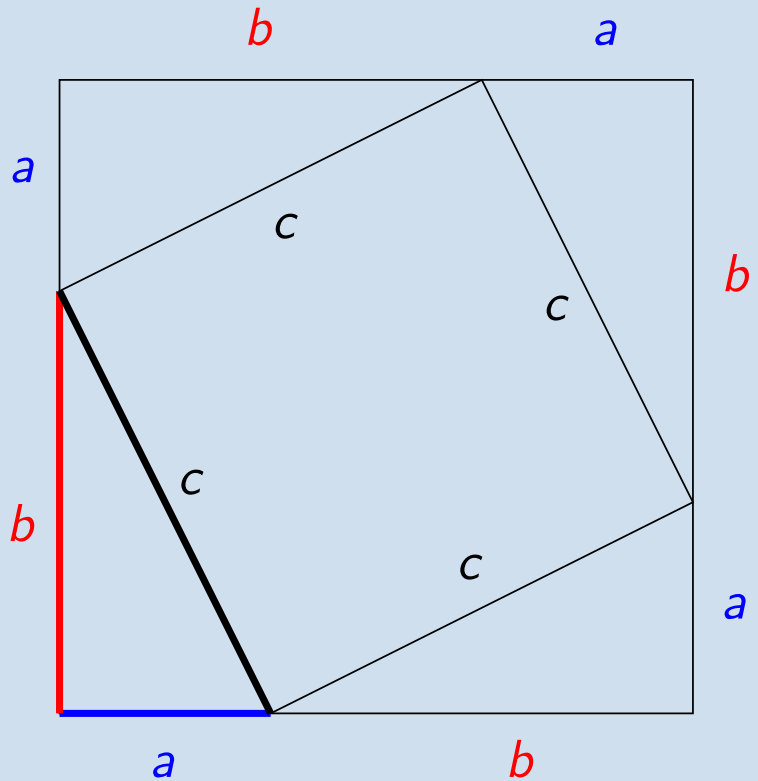
Il teorema di Pitagora

Teorema

Per un triangolo rettangolo di cateti a, b e ipotenusa c vale l'uguaglianza

$$a^2 + b^2 = c^2.$$

Dimostrazione



$$(a+b)^2 = 4 \cdot \frac{1}{2}ab + c^2$$

$$a^2 + 2ab + b^2 = 2ab + c^2$$

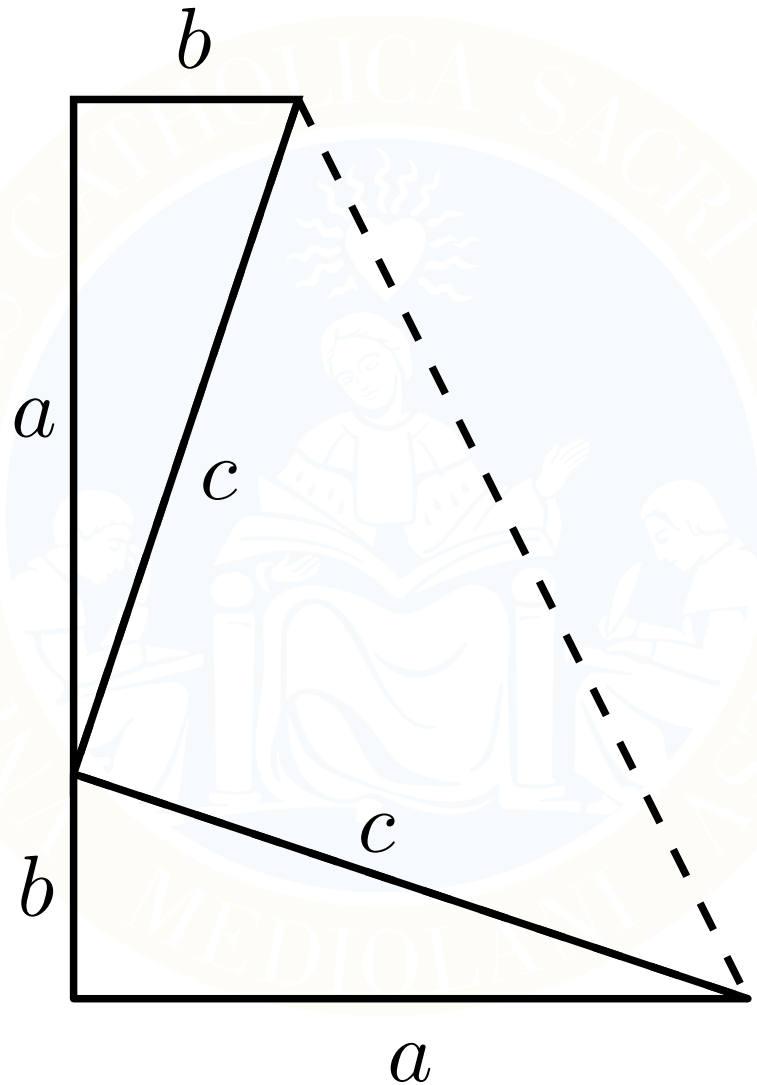
$$a^2 + b^2 = c^2$$

Il teorema di Pitagora

Il sito `http://www.cut-the-knot.org/pythagoras/` riporta 115 dimostrazioni diverse del Teorema di Pitagora!

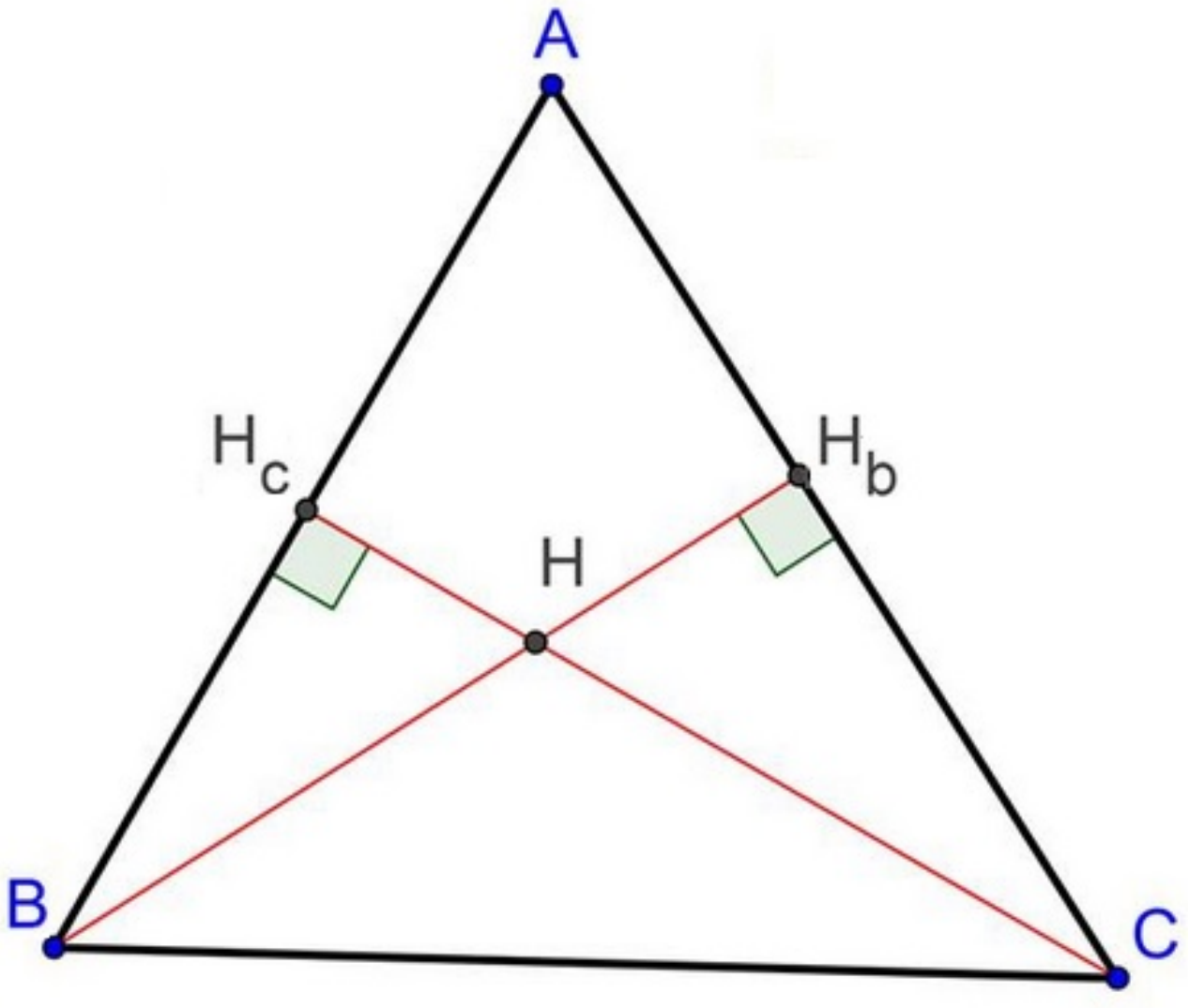
Il teorema di Pitagora

Il sito `http://www.cut-the-knot.org/pythagoras/` riporta 115 dimostrazioni diverse del Teorema di Pitagora!



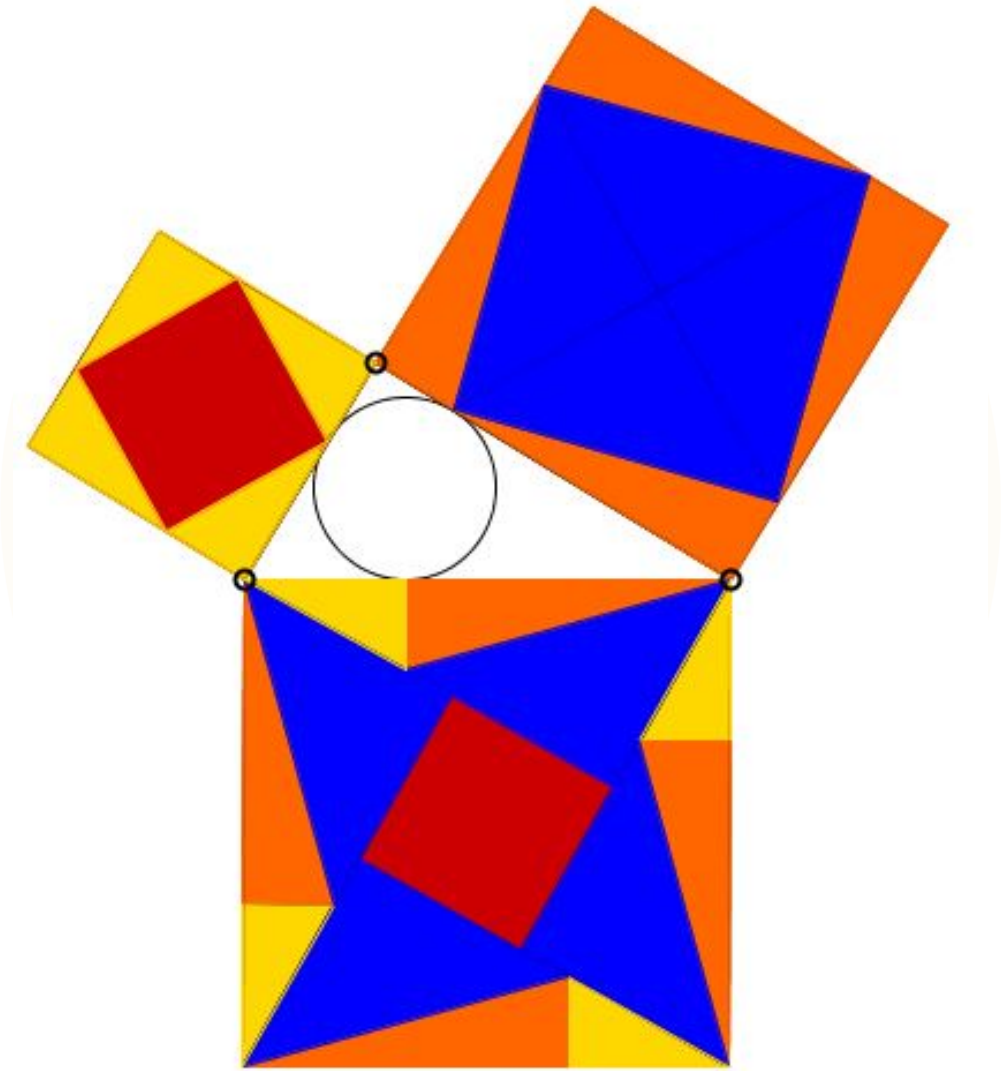
Il teorema di Pitagora

Il sito `http://www.cut-the-knot.org/pythagoras/` riporta 115 dimostrazioni diverse del Teorema di Pitagora!



Il teorema di Pitagora

Il sito `http://www.cut-the-knot.org/pythagoras/` riporta 115 dimostrazioni diverse del Teorema di Pitagora!



Il teorema di Pitagora

Il libro del 1927
The Pythagorean Proposition, di Elisha S. Loomis (1852–1940)
presenta 367 dimostrazioni diverse del teorema!

Il teorema di Pitagora

Il libro del 1927
The Pythagorean Proposition, di Elisha S. Loomis (1852–1940)
presenta 367 dimostrazioni diverse del teorema!

È senza dubbio uno dei teoremi più apprezzati della storia della Matematica, e ammette anche tante generalizzazioni: ad esempio, è vero anche il viceversa:

Teorema

Se per un triangolo di lati a, b, c vale l'uguaglianza

$$a^2 + b^2 = c^2,$$

allora il triangolo è rettangolo, con l'angolo retto tra a e b.

Il teorema di Pitagora

Il libro del 1927
The Pythagorean Proposition, di Elisha S. Loomis (1852–1940)
presenta 367 dimostrazioni diverse del teorema!

È senza dubbio uno dei teoremi più apprezzati della storia della Matematica, e ammette anche tante generalizzazioni: ad esempio, è vero anche il viceversa:

Teorema

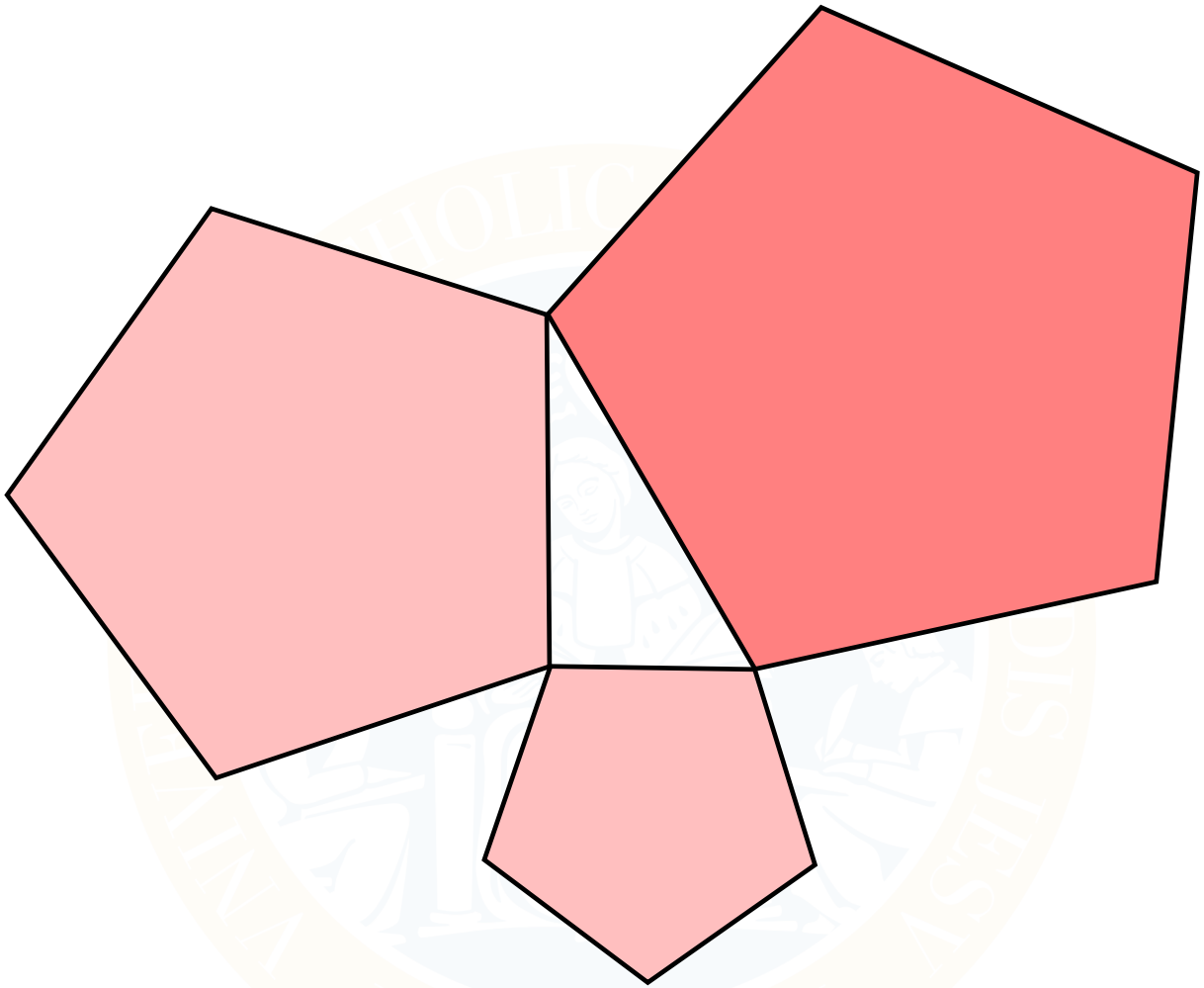
Se per un triangolo di lati a, b, c vale l'uguaglianza

$$a^2 + b^2 = c^2,$$

allora il triangolo è rettangolo, con l'angolo retto tra a e b.

Ed è valido per poligoni qualsiasi, basta che siano simili.

Il teorema di Pitagora generalizzato



Euclide, nella Proposizione VI.31, ha dimostrato anche questo teorema più generale.

L'ultimo teorema di Fermat

Sappiamo che esistono le *terne pitagoriche*, terne di numeri interi che soddisfano il teorema di Pitagora, ad esempio

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2$$

L'ultimo teorema di Fermat

Sappiamo che esistono le *terne pitagoriche*, terne di numeri interi che soddisfano il teorema di Pitagora, ad esempio

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2$$

Pierre de Fermat nel 1637 affermò che queste terne di numeri interi non esistono per potenze superiori, cioè non esistono numeri interi per cui

$$a^n + b^n = c^n, \qquad n \geq 3$$

L'ultimo teorema di Fermat

Sappiamo che esistono le *terne pitagoriche*, terne di numeri interi che soddisfano il teorema di Pitagora, ad esempio

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2$$

Pierre de Fermat nel 1637 affermò che queste terne di numeri interi non esistono per potenze superiori, cioè non esistono numeri interi per cui

$$a^n + b^n = c^n, \qquad n \geq 3$$

Purtroppo Fermat non scrisse la dimostrazione (che diceva però di avere).

L'ultimo teorema di Fermat

Sappiamo che esistono le *terne pitagoriche*, terne di numeri interi che soddisfano il teorema di Pitagora, ad esempio

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2$$

Pierre de Fermat nel 1637 affermò che queste terne di numeri interi non esistono per potenze superiori, cioè non esistono numeri interi per cui

$$a^n + b^n = c^n, \qquad n \geq 3$$

Purtroppo Fermat non scrisse la dimostrazione (che diceva però di avere).

Nonostante Fermat fosse un matematico di altissimo livello, in mancanza di una dimostrazione non gli si poteva credere sulla parola...

L'ultimo teorema di Fermat

Sappiamo che esistono le *terne pitagoriche*, terne di numeri interi che soddisfano il teorema di Pitagora, ad esempio

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2$$

Pierre de Fermat nel 1637 affermò che queste terne di numeri interi non esistono per potenze superiori, cioè non esistono numeri interi per cui

$$a^n + b^n = c^n, \qquad n \geq 3$$

Purtroppo Fermat non scrisse la dimostrazione (che diceva però di avere).

Nonostante Fermat fosse un matematico di altissimo livello, in mancanza di una dimostrazione non gli si poteva credere sulla parola...

Dopo secoli di tentativi Andrew Wiles, matematico britannico, ne pubblicò la prima dimostrazione nel 1995, oltre 350 anni dopo la sua formulazione.

Annals of Mathematics, **142** (1995), 443–551

Modular elliptic curves and Fermat's Last Theorem

By Andrew Wiles*

For Nada, Clare, Kate and Olivia

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Pierre de Fermat

Introduction

An elliptic curve over $\mathbf{Q}$ is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over $\mathbf{Q}$ with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular (in which case we say that the j-invariant is modular). A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over $\mathbf{Q}$ is modular. However, it only became widely known through its publication in a paper of Weil in 1967 [We] (as an exercise for the interested reader!), in which, moreover, Weil gave conceptual evidence for the conjecture. Although it had been numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many j-invariants were modular.

In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The precise mechanism relating the two was formulated by Serre as the ε-conjecture and this was then proved by Ribet in the summer of 1986. Ribet's result only requires one to prove the conjecture for semistable elliptic curves in order to deduce Fermat's Last Theorem.

Nascita di un teorema: la congettura

Quasi sempre un teorema nasce da una *congettura*, ovvero una proposizione che si ritiene possa essere vera, ma che ancora non è stata dimostrata.

Nascita di un teorema: la congettura

Quasi sempre un teorema nasce da una *congettura*, ovvero una proposizione che si ritiene possa essere vera, ma che ancora non è stata dimostrata.

Quello che abbiamo chiamato *Ultimo teorema di Fermat*, prima del 1995 avrebbe dovuto chiamarsi *congettura di Fermat* poiché, anche se si riteneva fosse vero, non ne esisteva dimostrazione.

Nascita di un teorema: la congettura

Quasi sempre un teorema nasce da una *congettura*, ovvero una proposizione che si ritiene possa essere vera, ma che ancora non è stata dimostrata.

Quello che abbiamo chiamato *Ultimo teorema di Fermat*, prima del 1995 avrebbe dovuto chiamarsi *congettura di Fermat* poiché, anche se si riteneva fosse vero, non ne esisteva dimostrazione.

Esistono tuttora notevoli congetture, in attesa di una dimostrazione: tra le più famose troviamo i sette *Millennium Problems*, del Clay Institute, ognuno dotato di un premio di un milione di dollari.

La congettura di Goldbach

Una congettura molto facile da enunciare è la seguente:

ogni numero pari più grande di 2 è la somma di due numeri primi.

La congettura di Goldbach

Una congettura molto facile da enunciare è la seguente:

ogni numero pari più grande di 2 è la somma di due numeri primi.

Essa è stata formulata in un carteggio tra Christian Goldbach e il grande Leonhard Euler nel 1742. Pur nella sua semplicità, tale proposizione non è stata tuttora né dimostrata né falsificata.

La congettura di Goldbach

Una congettura molto facile da enunciare è la seguente:

ogni numero pari più grande di 2 è la somma di due numeri primi.

Essa è stata formulata in un carteggio tra Christian Goldbach e il grande Leonhard Euler nel 1742. Pur nella sua semplicità, tale proposizione non è stata tuttora né dimostrata né falsificata.

Nel 2013, il matematico di origine peruviana Harald Helfgott ha annunciato la dimostrazione della cosiddetta *congettura debole di Goldbach*, secondo cui ogni numero dispari più grande di 5 è la somma di **tre** numeri primi.

La congettura di Goldbach

Una congettura molto facile da enunciare è la seguente:

ogni numero pari più grande di 2 è la somma di due numeri primi.

Essa è stata formulata in un carteggio tra Christian Goldbach e il grande Leonhard Euler nel 1742. Pur nella sua semplicità, tale proposizione non è stata tuttora né dimostrata né falsificata.

Nel 2013, il matematico di origine peruviana Harald Helfgott ha annunciato la dimostrazione della cosiddetta *congettura debole di Goldbach*, secondo cui ogni numero dispari più grande di 5 è la somma di **tre** numeri primi.

La sua dimostrazione però è ancora allo studio degli esperti che devono validarla.

La congettura di Goldbach

Esistono naturalmente delle grosse evidenze numeriche della congettura di Goldbach: con l'aiuto dei calcolatori elettronici la congettura è stata verificata per tutti i numeri pari fino a

$$4 \cdot 10^{18} = 4\,000\,000\,000\,000\,000\,000$$

(quattro miliardi di miliardi).

La congettura di Goldbach

Esistono naturalmente delle grosse evidenze numeriche della congettura di Goldbach: con l'aiuto dei calcolatori elettronici la congettura è stata verificata per tutti i numeri pari fino a

$$4 \cdot 10^{18} = 4\,000\,000\,000\,000\,000\,000$$

(quattro miliardi di miliardi).

Ma finché non ne verrà data una dimostrazione, non potremo mai sapere che l'affermazione è vera per *tutti* i numeri pari, neppure con l'uso dei computer più potenti.

La congettura di Goldbach

Esistono naturalmente delle grosse evidenze numeriche della congettura di Goldbach: con l'aiuto dei calcolatori elettronici la congettura è stata verificata per tutti i numeri pari fino a

$$4 \cdot 10^{18} = 4\,000\,000\,000\,000\,000\,000$$

(quattro miliardi di miliardi).

Ma finché non ne verrà data una dimostrazione, non potremo mai sapere che l'affermazione è vera per *tutti* i numeri pari, neppure con l'uso dei computer più potenti.

E pensare che per dimostrare che Goldbach si sbagliava basterebbe trovare un solo controesempio...

Attenzione alle cattive congetture!

Non tutte le congetture formulate nella storia si sono rivelate vere. Tra le più famose c'è la congettura sui numeri primi di Fermat:

$$2^{2^n} + 1 \quad \text{è un numero primo}$$

Attenzione alle cattive congetture!

Non tutte le congetture formulate nella storia si sono rivelate vere. Tra le più famose c'è la congettura sui numeri primi di Fermat:

$$2^{2^n}+1 \quad \text{è un numero primo}$$

Pierre de Fermat enunciò la congettura in base all'osservazione che

$$2^{2^0}+1=3$$
$$2^{2^1}+1=5$$
$$2^{2^2}+1=17$$
$$2^{2^3}+1=257$$
$$2^{2^4}+1=65\,537$$

che sono tutti numeri primi. Il numero successivo era troppo grande per essere trattato da Fermat.

I primi di Fermat

Ma un secolo dopo, ancora Euler, che era un abilissimo calcolatore, dimostrò che

$$2^{2^5} + 1 = 641 \cdot 6700417$$

falsificando così la congettura di Fermat.

I primi di Fermat

Ma un secolo dopo, ancora Euler, che era un abilissimo calcolatore, dimostrò che

$$2^{2^5} + 1 = 641 \cdot 6700417$$

falsificando così la congettura di Fermat.

La cosa buffa è che da allora non sono più stati scoperti altri numeri primi di Fermat, oltre ai primi cinque già noti, ed anzi oggi si è più orientati a pensare che non ce ne siano altri o che, se ce ne sono, debbano comunque essere in numero finito.

I primi di Fermat

Ma un secolo dopo, ancora Euler, che era un abilissimo calcolatore, dimostrò che

$$2^{2^5} + 1 = 641 \cdot 6700417$$

falsificando così la congettura di Fermat.

La cosa buffa è che da allora non sono più stati scoperti altri numeri primi di Fermat, oltre ai primi cinque già noti, ed anzi oggi si è più orientati a pensare che non ce ne siano altri o che, se ce ne sono, debbano comunque essere in numero finito.

La congettura di Fermat si è dunque rivelata grossolanamente falsa:
diffidate dal trarre conclusioni troppo frettolose!

Un'altra congettura: l'ipotesi cinese

Congettura

Un numero naturale $n > 2$ è primo se e solo se il resto della divisione

$$2^n : n$$

è esattamente 2.

Verifica - I

3	primo	2	28	non primo	16	53	primo	2
4	non primo	0	29	primo	2	54	non primo	28
5	primo	2	30	non primo	4	55	non primo	43
6	non primo	4	31	primo	2	56	non primo	32
7	primo	2	32	non primo	0	57	non primo	8
8	non primo	0	33	non primo	8	58	non primo	4
9	non primo	8	34	non primo	4	59	primo	2
10	non primo	4	35	non primo	18	60	non primo	16
11	primo	2	36	non primo	28	61	primo	2
12	non primo	4	37	primo	2	62	non primo	4
13	primo	2	38	non primo	4	63	non primo	8
14	non primo	4	39	non primo	8	64	non primo	0
15	non primo	8	40	non primo	16	65	non primo	32
16	non primo	0	41	primo	2	66	non primo	64
17	primo	2	42	non primo	22	67	primo	2
18	non primo	10	43	primo	2	68	non primo	16
19	primo	2	44	non primo	16	69	non primo	8
20	non primo	16	45	non primo	17	70	non primo	44
21	non primo	8	46	non primo	4	71	primo	2
22	non primo	4	47	primo	2	72	non primo	64
23	primo	2	48	non primo	16	73	primo	2
24	non primo	16	49	non primo	30	74	non primo	4
25	non primo	7	50	non primo	24	75	non primo	68
26	non primo	4	51	non primo	8	76	non primo	16
27	non primo	26	52	non primo	16	77	non primo	18

Verifica - II

78	non primo	64	103	primo	2	128	non primo	0
79	primo	2	104	non primo	48	129	non primo	8
80	non primo	16	105	non primo	92	130	non primo	114
81	non primo	80	106	non primo	4	131	primo	2
82	non primo	4	107	primo	2	132	non primo	4
83	primo	2	108	non primo	28	133	non primo	128
84	non primo	64	109	primo	2	134	non primo	4
85	non primo	32	110	non primo	34	135	non primo	53
86	non primo	4	111	non primo	8	136	non primo	120
87	non primo	8	112	non primo	16	137	primo	2
88	non primo	80	113	primo	2	138	non primo	64
89	primo	2	114	non primo	64	139	primo	2
90	non primo	64	115	non primo	78	140	non primo	116
91	non primo	37	116	non primo	16	141	non primo	8
92	non primo	16	117	non primo	44	142	non primo	4
93	non primo	8	118	non primo	4	143	non primo	85
94	non primo	4	119	non primo	60	144	non primo	64
95	non primo	13	120	non primo	16	145	non primo	32
96	non primo	64	121	non primo	112	146	non primo	4
97	primo	2	122	non primo	4	147	non primo	50
98	non primo	18	123	non primo	8	148	non primo	16
99	non primo	17	124	non primo	16	149	primo	2
100	non primo	76	125	non primo	57	150	non primo	124
101	primo	2	126	non primo	64	151	primo	2
102	non primo	64	127	primo	2	152	non primo	104

Verifica - III

153	non primo	53	178	non primo	4	203	non primo	186
154	non primo	16	179	primo	2	204	non primo	16
155	non primo	63	180	non primo	136	205	non primo	32
156	non primo	40	181	primo	2	206	non primo	4
157	primo	2	182	non primo	4	207	non primo	98
158	non primo	4	183	non primo	8	208	non primo	16
159	non primo	8	184	non primo	72	209	non primo	72
160	non primo	96	185	non primo	32	210	non primo	64
161	non primo	151	186	non primo	64	211	primo	2
162	non primo	82	187	non primo	161	212	non primo	16
163	primo	2	188	non primo	16	213	non primo	8
164	non primo	16	189	non primo	134	214	non primo	4
165	non primo	32	190	non primo	74	215	non primo	118
166	non primo	4	191	primo	2	216	non primo	136
167	primo	2	192	non primo	64	217	non primo	128
168	non primo	64	193	primo	2	218	non primo	4
169	non primo	80	194	non primo	4	219	non primo	8
170	non primo	4	195	non primo	8	220	non primo	56
171	non primo	170	196	non primo	128	221	non primo	32
172	non primo	16	197	primo	2	222	non primo	64
173	primo	2	198	non primo	190	223	primo	2
174	non primo	64	199	primo	2	224	non primo	32
175	non primo	93	200	non primo	176	225	non primo	107
176	non primo	64	201	non primo	8	226	non primo	4
177	non primo	8	202	non primo	4	227	primo	2

Verifica - IV

228	non primo	220	253	non primo	162	278	non primo	4
229	primo	2	254	non primo	4	279	non primo	233
230	non primo	104	255	non primo	128	280	non primo	16
231	non primo	134	256	non primo	0	281	primo	2
232	non primo	24	257	primo	2	282	non primo	64
233	primo	2	258	non primo	64	283	primo	2
234	non primo	64	259	non primo	128	284	non primo	16
235	non primo	173	260	non primo	256	285	non primo	107
236	non primo	16	261	non primo	251	286	non primo	218
237	non primo	8	262	non primo	4	287	non primo	46
238	non primo	30	263	primo	2	288	non primo	64
239	primo	2	264	non primo	16	289	non primo	155
240	non primo	16	265	non primo	32	290	non primo	154
241	primo	2	266	non primo	158	291	non primo	8
242	non primo	202	267	non primo	8	292	non primo	16
243	non primo	242	268	non primo	16	293	primo	2
244	non primo	16	269	primo	2	294	non primo	148
245	non primo	67	270	non primo	244	295	non primo	268
246	non primo	64	271	primo	2	296	non primo	256
247	non primo	193	272	non primo	256	297	non primo	161
248	non primo	8	273	non primo	239	298	non primo	4
249	non primo	8	274	non primo	4	299	non primo	280
250	non primo	124	275	non primo	43	300	non primo	76
251	primo	2	276	non primo	232	301	non primo	128
252	non primo	64	277	primo	2	302	non primo	4

Verifica - V

303	non primo	8
304	non primo	176
305	non primo	32
306	non primo	208
307	primo	2
308	non primo	256
309	non primo	8
310	non primo	94
311	primo	2
312	non primo	40
313	primo	2
314	non primo	4
315	non primo	8
316	non primo	16
317	primo	2
318	non primo	64
319	non primo	105
320	non primo	256
321	non primo	8
322	non primo	100
323	non primo	314
324	non primo	244
325	non primo	132
326	non primo	4
327	non primo	8
328	non primo	256
329	non primo	81
330	non primo	34
331	primo	2
332	non primo	16
333	non primo	179
334	non primo	4
335	non primo	233
336	non primo	64
337	primo	2
338	non primo	316
339	non primo	8
340	non primo	16
$341 = 11 \times 31$	non primo	2

Verifica - V

303	non primo	8
304	non primo	176
305	non primo	32
306	non primo	208
307	primo	2
308	non primo	256
309	non primo	8
310	non primo	94
311	primo	2
312	non primo	40
313	primo	2
314	non primo	4
315	non primo	8
316	non primo	16
317	primo	2
318	non primo	64
319	non primo	105
320	non primo	256
321	non primo	8
322	non primo	100
323	non primo	314
324	non primo	244
325	non primo	132
326	non primo	4
327	non primo	8
328	non primo	256
329	non primo	81
330	non primo	34
331	primo	2
332	non primo	16
333	non primo	179
334	non primo	4
335	non primo	233
336	non primo	64
337	primo	2
338	non primo	316
339	non primo	8
340	non primo	16
$341 = 11 \times 31$	non primo	2

La congettura è falsa!

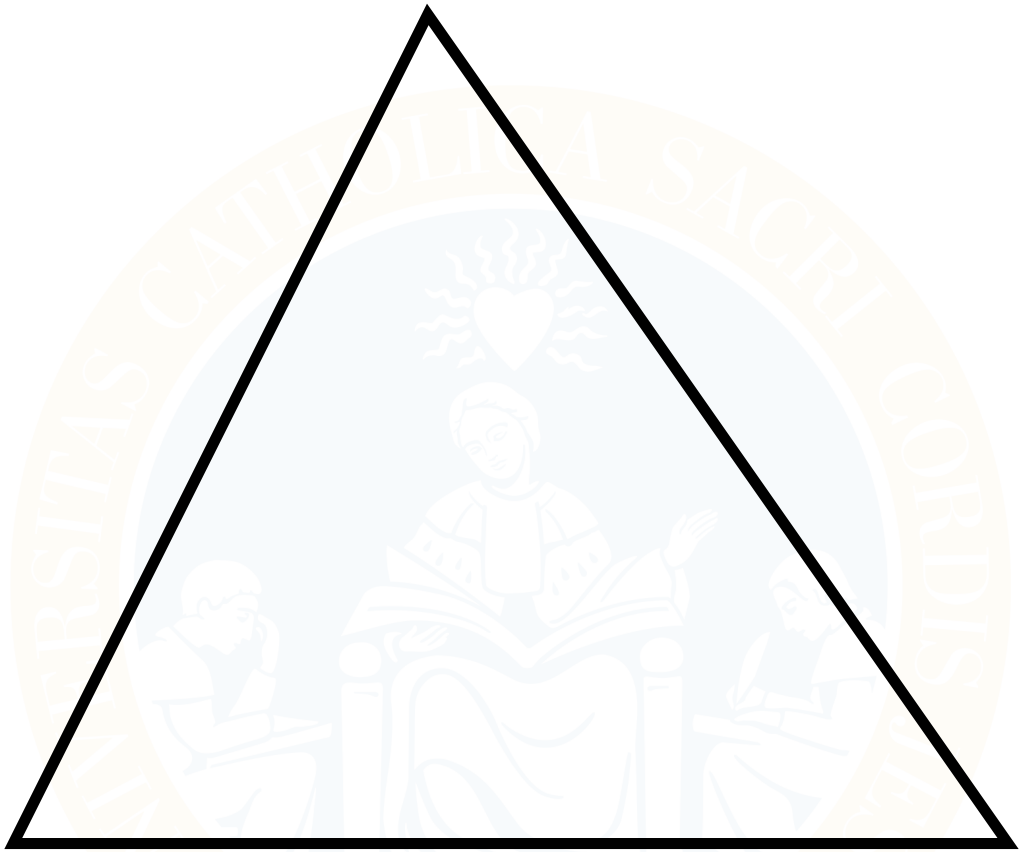
Verifica - V

303	non primo	8
304	non primo	176
305	non primo	32
306	non primo	208
307	primo	2
308	non primo	256
309	non primo	8
310	non primo	94
311	primo	2
312	non primo	40
313	primo	2
314	non primo	4
315	non primo	8
316	non primo	16
317	primo	2
318	non primo	64
319	non primo	105
320	non primo	256
321	non primo	8
322	non primo	100
323	non primo	314
324	non primo	244
325	non primo	132
326	non primo	4
327	non primo	8
328	non primo	256
329	non primo	81
330	non primo	34
331	primo	2
332	non primo	16
333	non primo	179
334	non primo	4
335	non primo	233
336	non primo	64
337	primo	2
338	non primo	316
339	non primo	8
340	non primo	16
$341 = 11 \times 31$	non primo	2

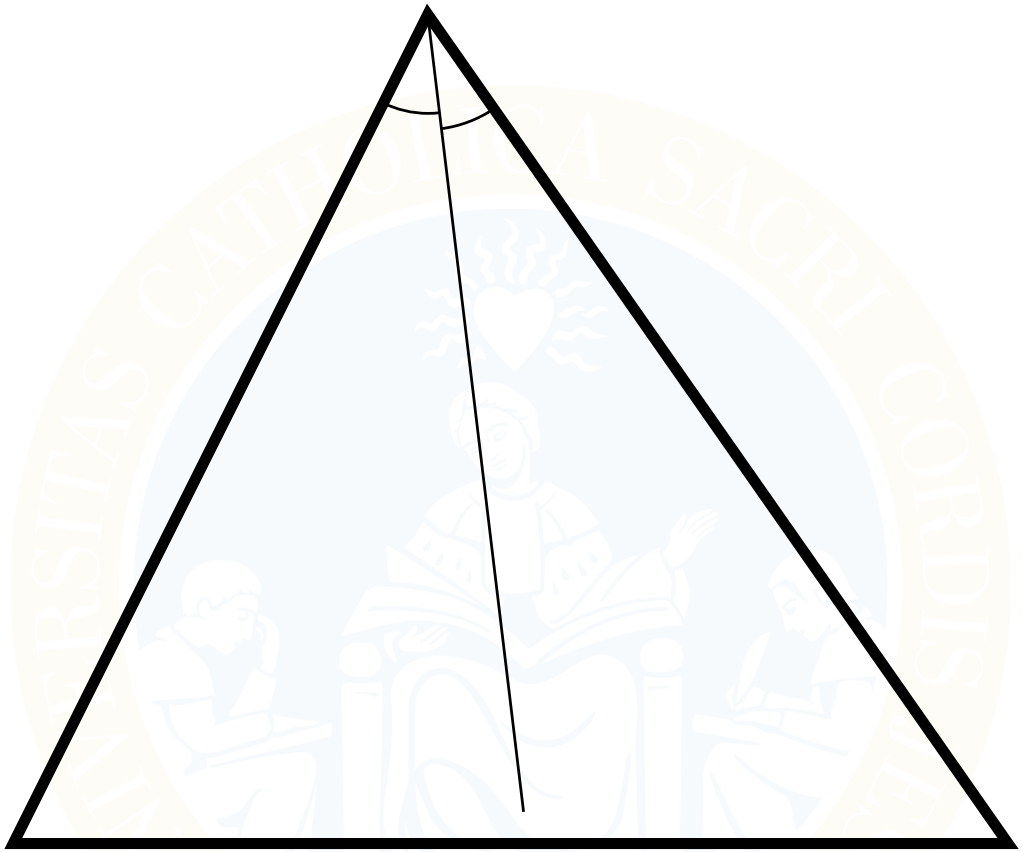
La congettura è falsa!

Nei primi 100000 numeri ce ne sono 79 falsi (e 9592 primi)

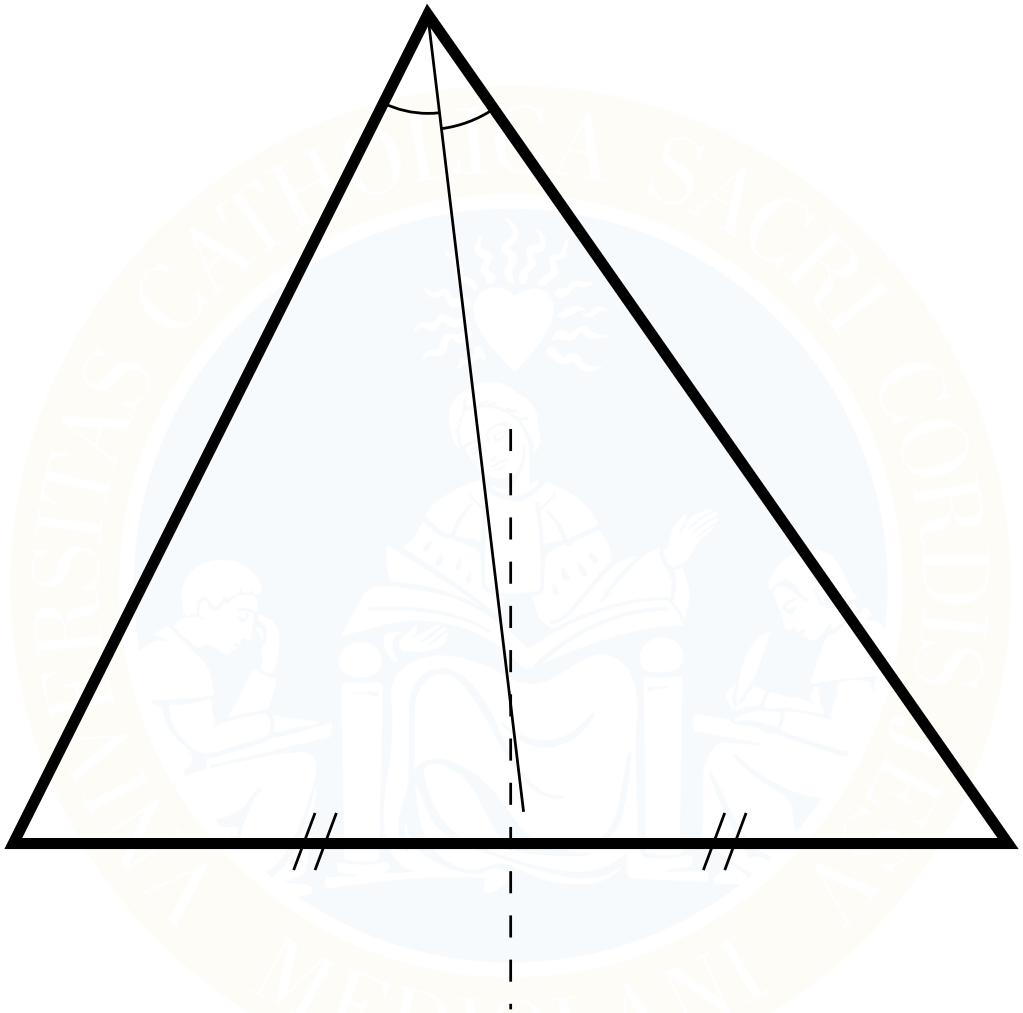
Attenzione alle dimostrazioni



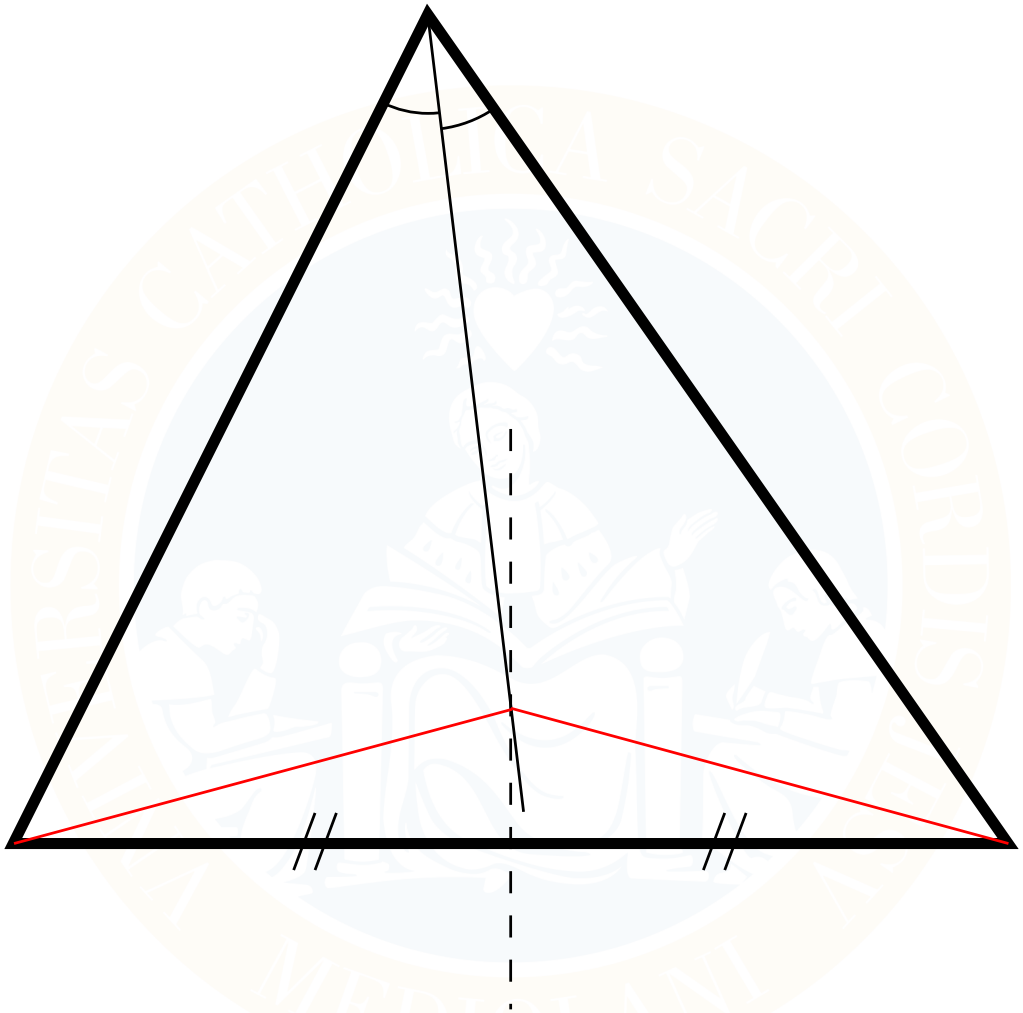
Attenzione alle dimostrazioni



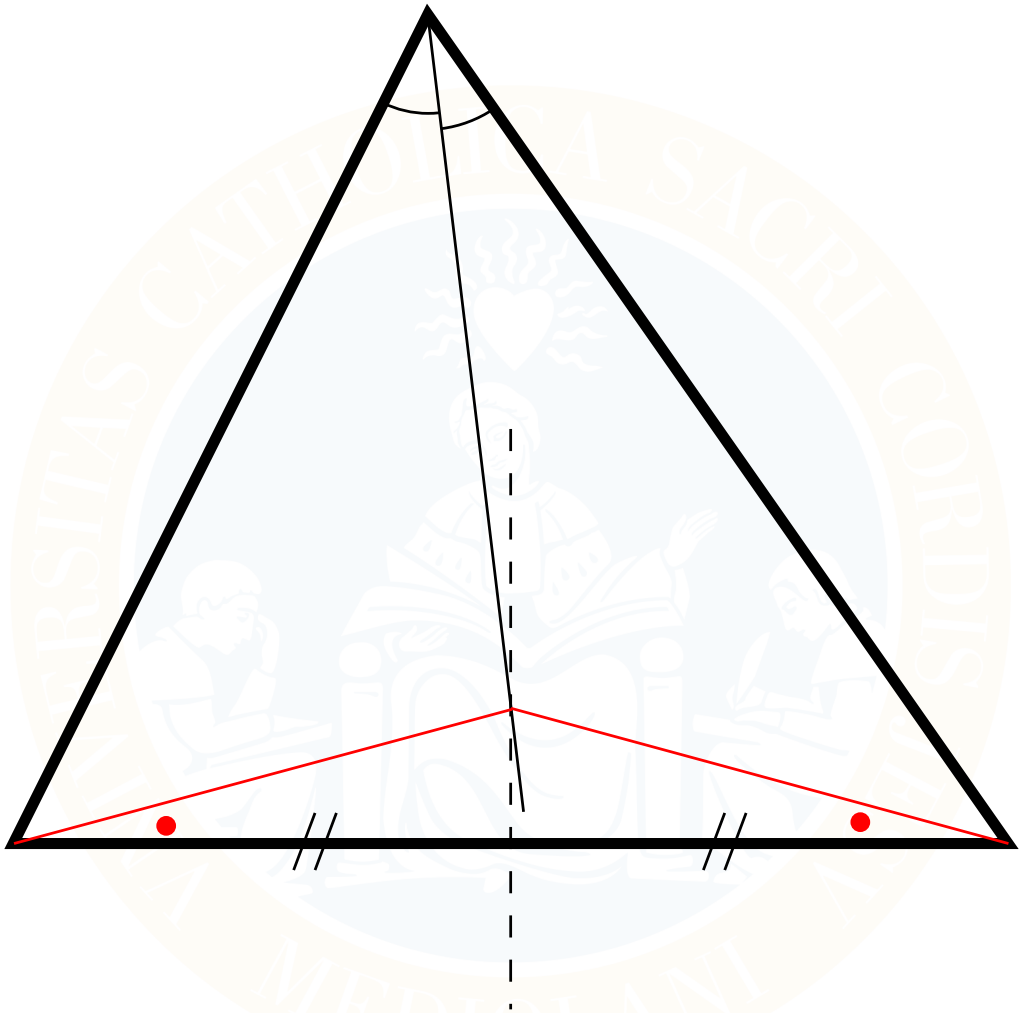
Attenzione alle dimostrazioni



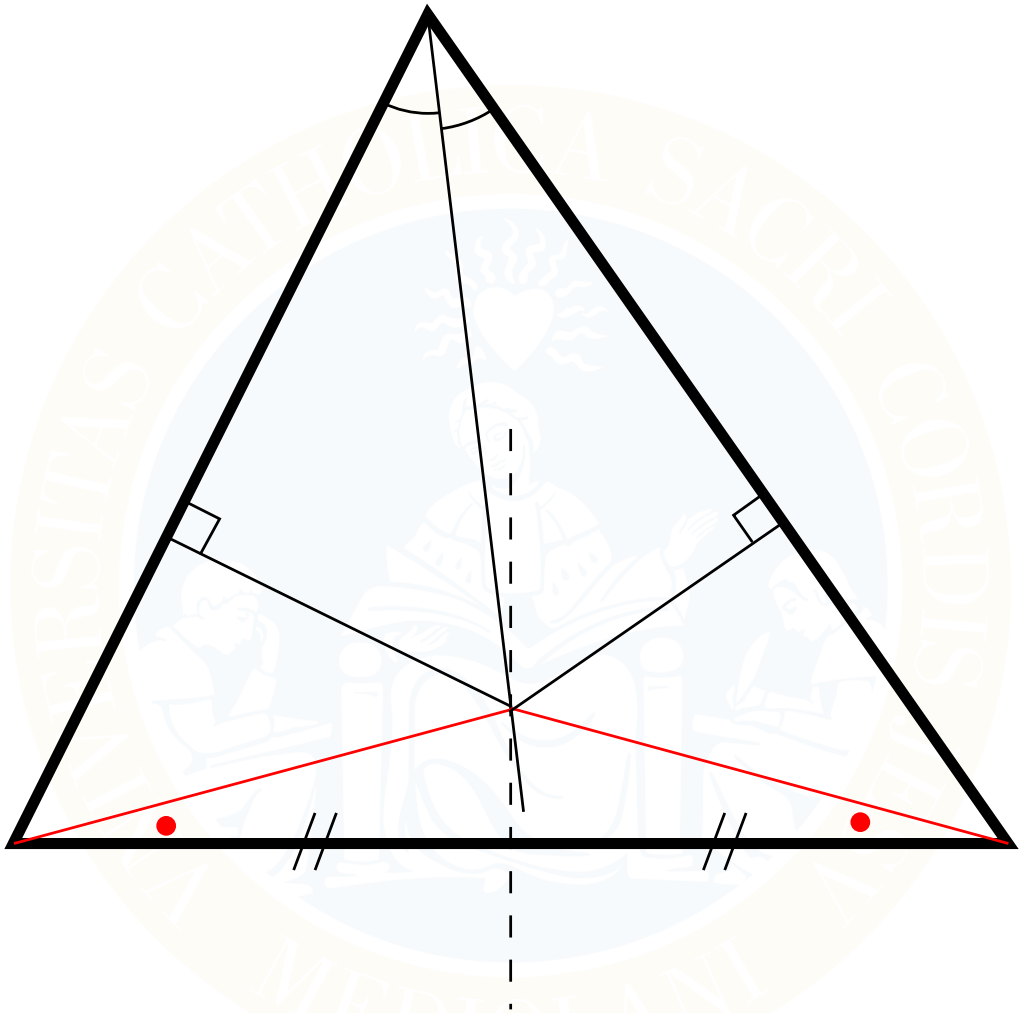
Attenzione alle dimostrazioni



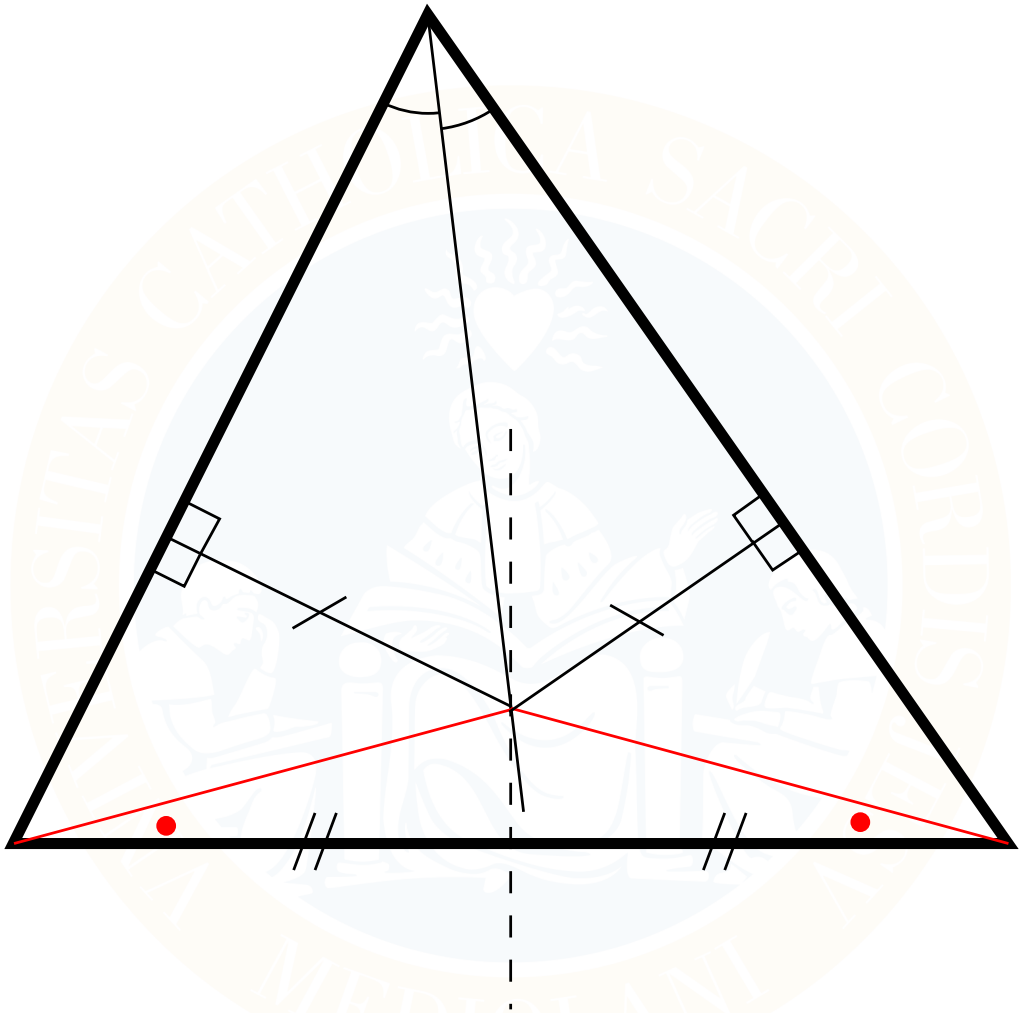
Attenzione alle dimostrazioni



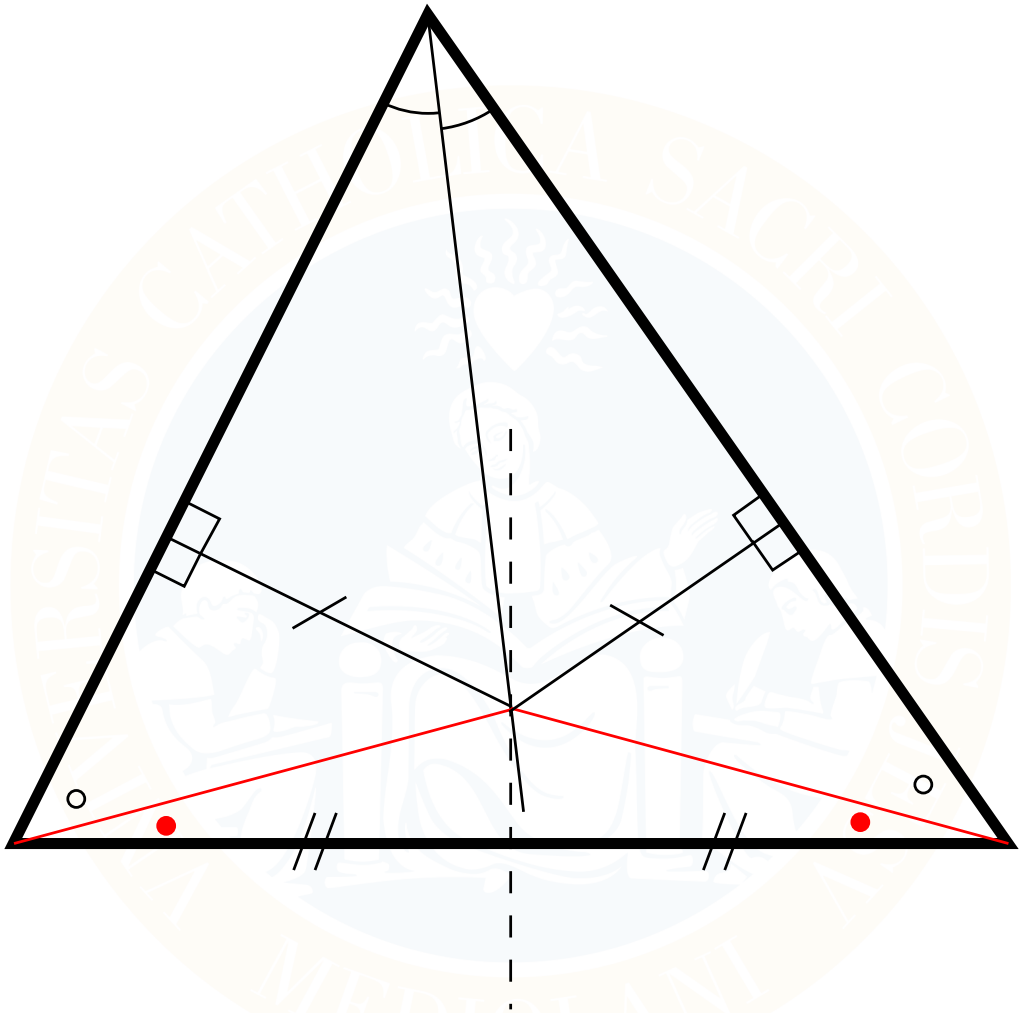
Attenzione alle dimostrazioni



Attenzione alle dimostrazioni



Attenzione alle dimostrazioni



Una citazione

Scopo della scienza non è tanto quello di aprire la porta all'infinito sapere, quanto quello di porre una barriera all'infinito errore.

B. Brecht, Vita di Galileo

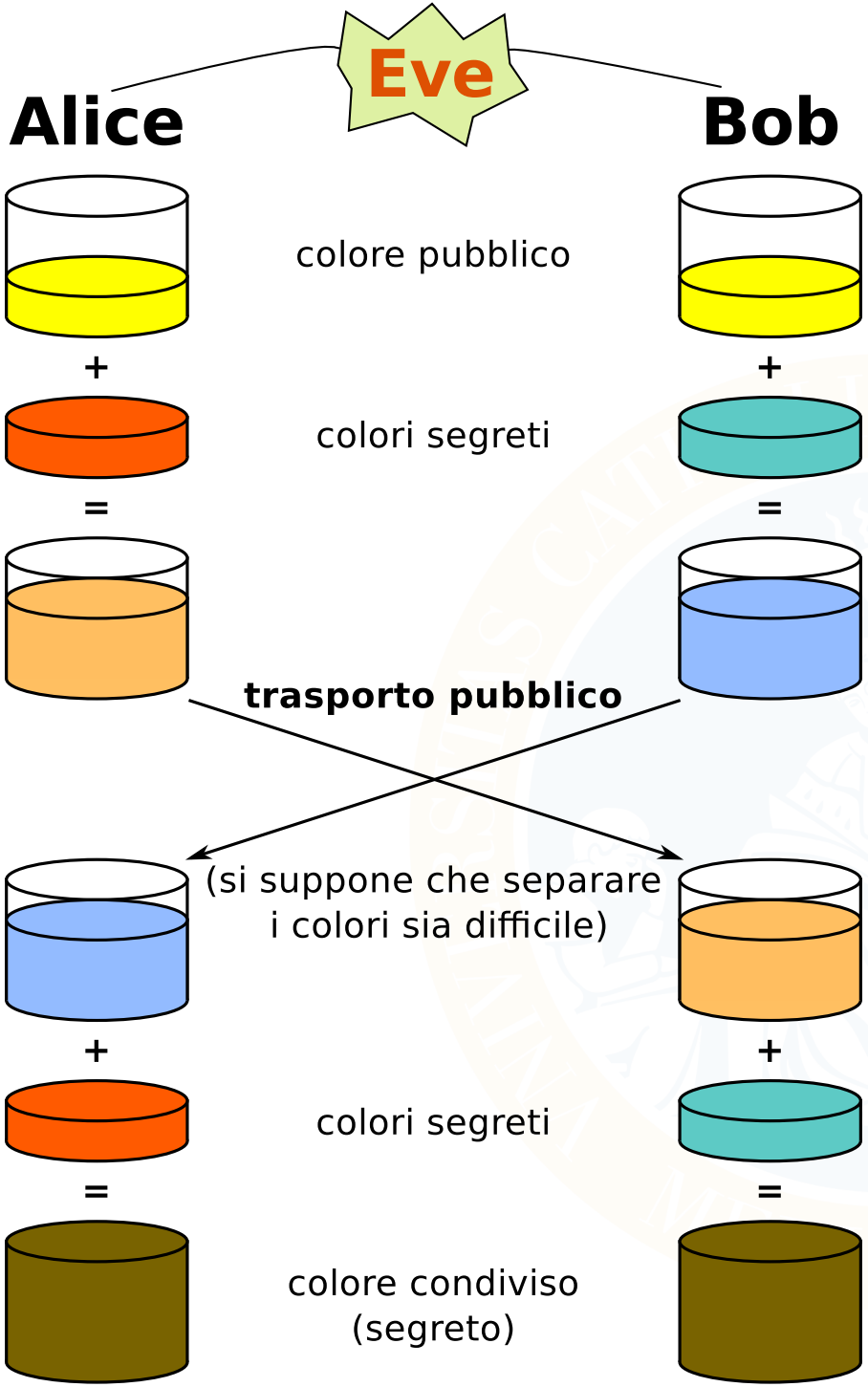
Un'applicazione alla crittografia

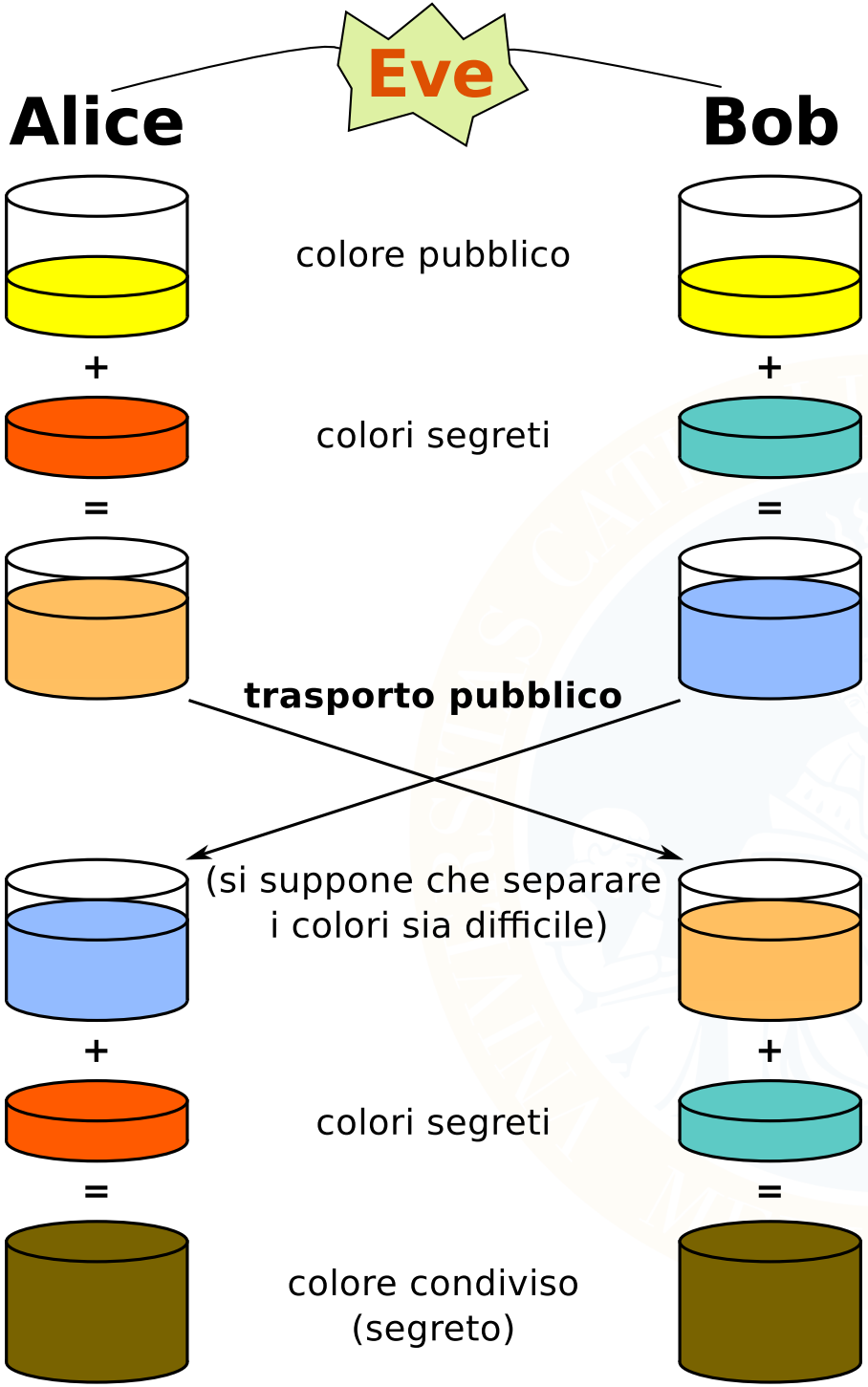
Alessandro Musesti - Università Cattolica del Sacro Cuore

Condivisione di una chiave: l'esempio con i colori

Alice e Bob vogliono poter scambiare messaggi senza che altri (rappresentati da Eve, il malvagio) li capiscano. Per fare questo devono entrambi avere una "chiave" che apra lo stesso lucchetto. Come possono fare a condividere questa chiave?

Vediamo un esempio, fatto coi colori, che si basa su un colore segreto (la chiave privata) e un colore noto a tutti (la chiave pubblica). Entrambi giungono a condividere un colore senza che Eve ne sia a conoscenza.


Eve
Alice
Bob
colore pubblico
+
colori segreti
=
trasporto pubblico
(si suppone che separare
i colori sia difficile)
+
colori segreti
=
colore condiviso
(segreto)



È **facile** mescolare i colori, ma è **difficile** capire quali colori formano una miscela.

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Provate a fattorizzare il numero 390900163...

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Provate a fattorizzare il numero 390900163...
E invece verificate, con la calcolatrice, quanto fa

$$14087 \times 27749$$

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Provate a fattorizzare il numero 390900163...
E invece verificate, con la calcolatrice, quanto fa

$$14087 \times 27749$$

Nelle attuali applicazioni informatiche si usano numeri di 1024 bit, che superano le 300 cifre decimali, e addirittura di 2048 bit!

RSA Factoring Challenge

Nel 1991 fu lanciato un concorso che chiedeva di fattorizzare alcuni numeri grandi, per stimolare la ricerca sulla sicurezza dell'algoritmo RSA, che si basa sulla fattorizzazione. Nel 2007 il concorso si è ufficialmente chiuso, ma tuttora alcuni gruppi stanno tentando di risolvere alcune delle sfide proposte.
Nel settembre del 2013 è stato fattorizzato il numero RSA-210, composto da 210 cifre decimali!

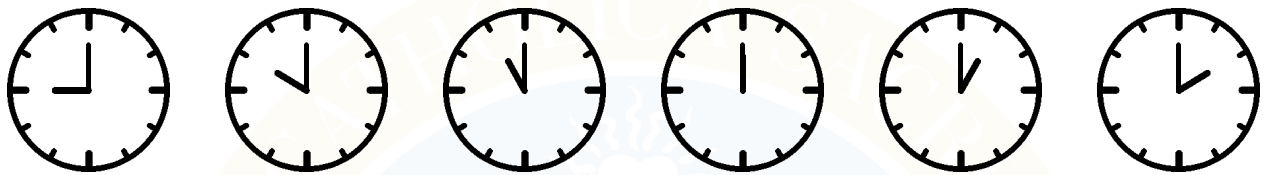
$$
\begin{aligned}
&2452466449002782119765176635730880184670267876783327597434144517150616\\
&0083003858721695220839933207154910362682719167986407977672324300560059\\
&2035631246561218465817904100131859299619933817012149335034875870551067 = \\
&\qquad 4359585683259407917999519653872144063854709102652201 9\\
&\qquad 6318705482144524085345275999740244625255428455944579 \times\\
&\qquad 5625457617268841037562770073044474817438769440075105 4\\
&\qquad 5104946851094548396577479473472146228550799322939273
\end{aligned}
$$

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?



Ovviamente, le 2.

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Ovviamente, le 2.
Se l'orologio segna le 5 si "moltiplica" quest'ora per 8, che ora risulterà?

Le 4, poiché $5 \times 8 = 40 = 12 \times 3 + 4$. Quindi la lancetta delle ore fa tre giri e finisce sulle 4.

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Ovviamente, le 2.
Se l'orologio segna le 5 si "moltiplica" quest'ora per 8, che ora risulterà?

Le 4, poiché $5 \times 8 = 40 = 12 \times 3 + 4$. Quindi la lancetta delle ore fa tre giri e finisce sulle 4.
Nell'aritmetica "dell'orologio" non interessa il numero dei giri, ma solo quello che avanza alla fine (il **resto** della divisione).

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Ovviamente, le 2.
Se l'orologio segna le 5 si "moltiplica" quest'ora per 8, che ora risulterà?

Le 4, poiché $5 \times 8 = 40 = 12 \times 3 + 4$. Quindi la lancetta delle ore fa tre giri e finisce sulle 4.
Nell'aritmetica "dell'orologio" non interessa il numero dei giri, ma solo quello che avanza alla fine (il **resto** della divisione).
Questa si chiama **aritmetica modulare**.

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5 (\mathrm{mod} 11),$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5 (\mathrm{mod} 11), \quad 5 \times 8 = 7 (\mathrm{mod} 11),$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5 (\mathrm{mod} 11), \quad 5 \times 8 = 7 (\mathrm{mod} 11), \quad 2^6 = 9 (\mathrm{mod} 11)$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5 (\mathrm{mod} 11), \quad 5 \times 8 = 7 (\mathrm{mod} 11), \quad 2^6 = 9 (\mathrm{mod} 11)$$

L'insieme dei numeri $\{0, 1, \ldots, p-1\}$ dotato di queste operazioni particolari si denota con $\mathbb{Z}_p$.

Generatori di $\mathbb{Z}_p$

Un **generatore** g in $\mathbb{Z}_p$ è un numero più piccolo di p tale che calcolando

$$g, g^2, g^3, \ldots, g^{p-2}, g^{p-1} (\mathrm{mod}\, p)$$

si esauriscano tutti i numeri tra 1 e $p-1$. Ad esempio, si può verificare che 2 è un generatore per $p = 11$, poiché

n	1	2	3	4	5	6	7	8	9	10
$2^n (\mathrm{mod} 11)$	2	4	8	5	10	9	7	3	6	1

Generatori di $\mathbb{Z}_p$

Un **generatore** g in $\mathbb{Z}_p$ è un numero più piccolo di p tale che calcolando

$$g, g^2, g^3, \ldots, g^{p-2}, g^{p-1} (\mathrm{mod}\, p)$$

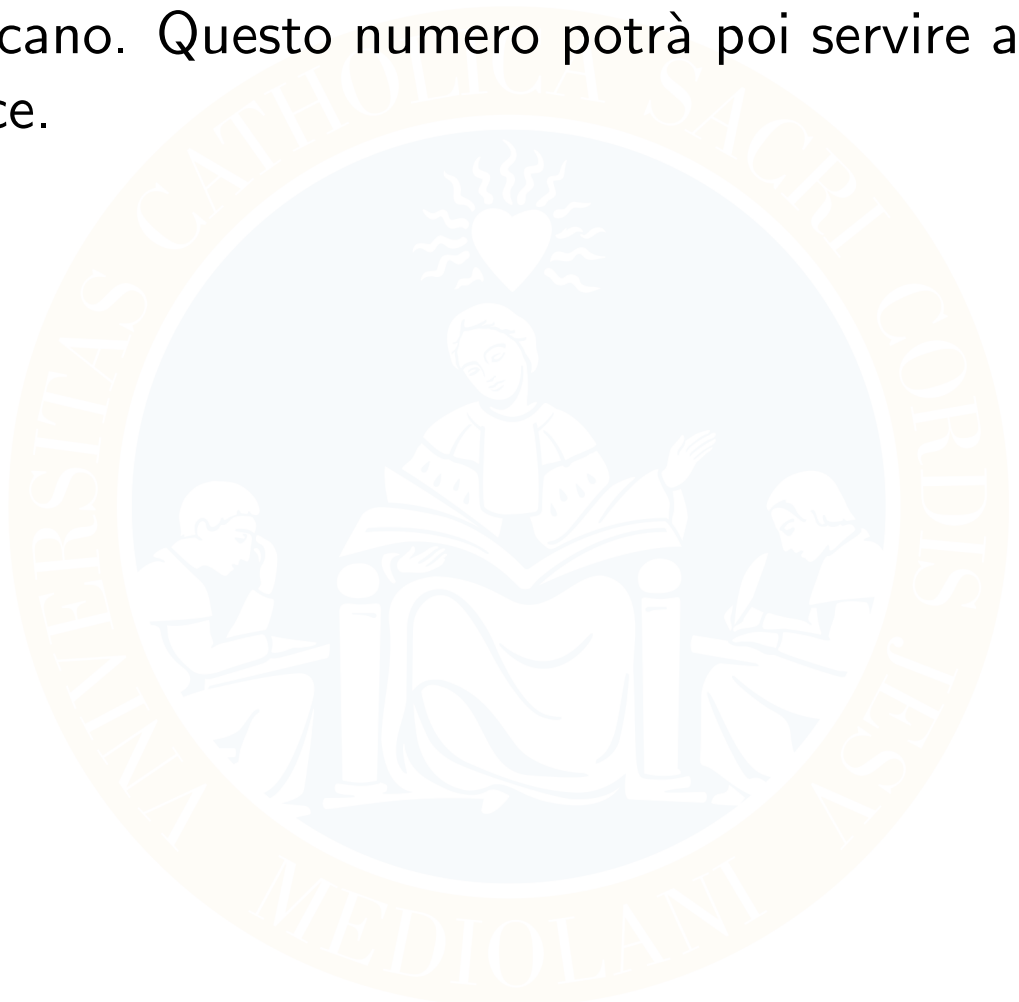
si esauriscano tutti i numeri tra 1 e $p-1$. Ad esempio, si può verificare che 2 è un generatore per $p = 11$, poiché

n	1	2	3	4	5	6	7	8	9	10
$2^n (\mathrm{mod} 11)$	2	4	8	5	10	9	7	3	6	1

Se p è primo, esiste sempre almeno un generatore in $\mathbb{Z}_p$, anche se potrebbe non essere semplice trovarlo.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.



Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.
È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.
È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.
Ad esempio, si verifica che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.
È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.
Ad esempio, si verifica che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Questi numeri p e g sono noti a tutti e decisi una volta per tutte. Nella pratica p è un numero molto grande (1024 bit), mentre g può anche essere piccolo.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.
È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$. Ad esempio, si verifica che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Questi numeri p e g sono noti a tutti e decisi una volta per tutte. Nella pratica p è un numero molto grande (1024 bit), mentre g può anche essere piccolo.

Poi si esegue la procedura seguente:

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod} p) = 6^{10} (\mathrm{mod} 17) =$

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod}\, 17) =$

6^n:	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod}\, 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod}\, 17) = 9$.

6^n:	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod} p) = 6^{10} (\mathrm{mod} 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod} p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

6^n:	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

3) Infine Alice prende la chiave pubblica di Bob, $B = 9$, e calcola $B^a (\mathrm{mod}\, p) = 9^{10} (\mathrm{mod} 17) = 13$.

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

3) Infine Alice prende la chiave pubblica di Bob, $B = 9$, e calcola $B^a (\mathrm{mod}\, p) = 9^{10} (\mathrm{mod} 17) = 13$.
Bob prende la chiave pubblica di Alice, $A = 15$, e calcola $A^b (\mathrm{mod}\, p) = 15^{14} (\mathrm{mod} 17) = 13$.

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod}\, 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod}\, 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

3) Infine Alice prende la chiave pubblica di Bob, $B = 9$, e calcola $B^a (\mathrm{mod}\, p) = 9^{10} (\mathrm{mod}\, 17) = 13$.
Bob prende la chiave pubblica di Alice, $A = 15$, e calcola $A^b (\mathrm{mod}\, p) = 15^{14} (\mathrm{mod}\, 17) = 13$.

È un caso che sia risultato lo stesso numero? Certamente no: si ha **sempre** $A^b = (g^a)^b = g^{ab} = (g^b)^a = B^a (\mathrm{mod}\, p)$.
Quindi Alice e Bob hanno una chiave in comune: il numero $\boxed{13}$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Scegliamo (a caso) le chiavi private: $a = 32359975$, $b = 6431846$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Scegliamo (a caso) le chiavi private: $a = 32359975$, $b = 6431846$.

Allora le chiavi pubbliche sono $A = g^a = 19135999$, $B = g^b = 5444512$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Scegliamo (a caso) le chiavi private: $a = 32359975$, $b = 6431846$.

Allora le chiavi pubbliche sono $A = g^a = 19135999$, $B = g^b = 5444512$.

E si ha $A^b = B^a = 18352668$, che è la chiave condivisa.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si può scoprire a: scorrendo tutta la tabella delle potenze del generatore si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si può scoprire a: scorrendo tutta la tabella delle potenze del generatore si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.

Ma allora dove sta la sicurezza della procedura? Nella realtà si usano numeri primi molto grandi, fatti da almeno 300 cifre, e la lista da scorrere per individuare l'esponente a a partire dalla conoscenza di g^a è molto, molto lunga!

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si può scoprire a: scorrendo tutta la tabella delle potenze del generatore si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.

Ma allora dove sta la sicurezza della procedura? Nella realtà si usano numeri primi molto grandi, fatti da almeno 300 cifre, e la lista da scorrere per individuare l'esponente a a partire dalla conoscenza di g^a è molto, molto lunga!

Questa operazione si chiama **logaritmo discreto**, ed è una funzione unidirezionale: è abbastanza facile calcolare $A = g^a$, ma è molto difficile scoprire l'esponente a conoscendo g e A. Anche i computer attualmente più potenti impiegherebbero centinaia di anni.