**Congetture sui numeri primi**

di Antonino Giambò

**1.** Su questa rubrica, a varie riprese e in più circostanze, mi sono occupato di numeri primi e di loro proprietà. Alcune di queste proprietà sono state dimostrate, altre solo enunciate ma dimostrabili, altre ancora solamente congetturate.

In questo contributo intendo occuparmi di alcune (solo alcune) di queste ultime, e precisamente di quelle proprietà che in tempi diversi sono state ipotizzate ma che nessuno è stato ancora in grado di dimostrare. Fanno parte del nutrito insieme di congetture sui numeri primi, che a loro volta sono parte delle cosiddette "questioni aperte" della Matematica.

Mostrerò pure come sia stata formulata una congettura che, qualora fosse dimostrata, implicherebbe la dimostrazione di altre congetture, sempre sui numeri primi.

**2.** La prima delle congetture di cui vado ad occuparmi non è in realtà una congettura poiché è stato dimostrato che è **falsa**: fu pronunciata da Fermat (Pierre de Fermat, 1601-1665) e recita che **sono primi tutti i numeri aventi la forma seguente: $2^{2^n}+1$, dove n è un numero naturale qualsiasi**.

In effetti, è così per i primi 5 numeri, ottenuti assegnando ad n i valori $0, 1, 2, 3, 4$. Ma, come provò Eulero (Leonhard Euler, 1707-1783) nel 1732, per $n=5$ si ottiene un numero composto.

I numeri della forma $2^{2^n}+1$ sono denominati *numeri di Fermat*. Ad oggi non si sa se esistono altri numeri primi di Fermat oltre ai cinque trovati dallo stesso Fermat.

Si congettura che **non esistano altri numeri primi di Fermat oltre ai cinque indicati.**

NOTA 1.

Qualche considerazione supplementare correlata a questi numeri.

In numeri $2^{2^n}$, con n intero positivo, sono chiaramente potenze di 2 con esponente $2^n$, ossia numeri siffatti:

$$2^2,\ 2^4,\ 2^8,\ 2^{16}, \dots, 2^{2^n}, \dots .$$

Ora, è evidente che questi numeri sono particolari numeri quadrati, ossia numeri della forma $m^2$.

Con riferimento all'esempio precedente, i numeri possono essere messi in questa forma:

$$(2^1)^2,\ (2^2)^2,\ (2^4)^2,\ (2^8)^2, \dots ,\quad \left(2^{2^{n-1}}\right)^2, \dots .$$

Pertanto i numeri di Fermat, $2^{2^n}+1$, purché sia $n>0$ e perciò fatta eccezione per il numero 3 ottenuto per $n=0$, sono particolari numeri della forma $m^2+1$, con m numero intero positivo.

Tra questi numeri alcuni sono i seguenti (quelli sottolineati sono numeri primi di Fermat):

$$2,\ \underline{5},\ \underline{17},\ 37,\ 101,\ \dots ,$$

ottenuti rispettivamente per $m=1$, $m=2$, $m=4$, $m=6$, $m=10$, … .

Si congettura che **l'insieme dei numeri primi della forma $m^2+1$ sia infinito**.

Si capisce facilmente che questi numeri primi, fatta eccezione per il numero 2 ottenuto per m=1, si ottengono attribuendo ad m valori pari.

**3.** Si era occupato di numeri primi, e precisamente dei numeri primi del tipo $2^n-1$, un contemporaneo di Fermat e con il quale Fermat era in corrispondenza, il monaco francese Marin Mersenne (1588-1648). Per questo i numeri aventi quella forma sono chiamati *numeri di Mersenne* e, quando sono primi, sono denominati ovviamente **numeri primi di Mersenne**.

Ma non era la prima volta che questi numeri comparivano nel panorama matematico. Figurano infatti nel teorema di Euclide sulla ricerca dei *numeri perfetti* (*Elementi*, libro IX, proposizione 36). Ad ogni buon conto, Mersenne non formulò alcuna ipotesi su tali numeri. Considerava infatti la formula $2^n-1$ semplicemente una formula generatrice di numeri primi. Così come Fermat considerava generatrice di numeri primi la formula $2^{2^n}+1$.

A tutt'oggi, benché se ne conosca un numero esiguo, poco più di cinquanta, si ipotizza, si congettura appunto **che i numeri primi di Mersenne siano in numero infinito**.

NOTA 2.

In realtà, oggigiorno si conoscono esattamente 52 numeri primi di Mersenne. Il 52° è stato scoperto recentissimamente nello scorso mese di ottobre. Si tratta del numero seguente:

$$2^{136.279.841} - 1 .$$

Questo numero ha circa 41 milioni di cifre.

Verosimilmente, il ricercatore, per stabilire che quel numero di Mersenne fosse primo, ha dovuto svilupparne la potenza. L'ha potuto fare perché ha avuto a disposizione potenti strumenti di calcolo automatico. Da questo sviluppo, qualora se ne abbia la necessaria pazienza, e ce ne vuole molta, si può contare il numero delle sue cifre.

A dire il vero, il numero di quelle cifre può essere calcolato anche senza conoscere lo sviluppo della potenza. Lo possiamo fare utilizzando apposite conoscenze sui logaritmi decimali.

Richiamiamo queste nozioni.

Il logaritmo decimale di un numero maggiore di 1 è di norma un numero decimale. La sua parte intera è denominata *caratteristica* del logaritmo decimale del numero.

Vale la seguente proprietà: La caratteristica del logaritmo decimale di un numero maggiore di 1 è uguale a tante unità quante sono le cifre della parte intera del numero, meno 1.

Per esempio:

- la caratteristica del logaritmo decimale del numero 437,96 è 2;
- sapendo che la caratteristica del logaritmo decimale di un numero incognito è 4, possiamo concludere che la parte intera del numero è formata da 5 cifre.

Passando allora al numero di Mersenne in questione, costatato che il numero delle sue cifre è uguale a quello del numero $2^{136.279.841}$, poniamo uguale a x questo numero e consideriamo il suo logaritmo decimale.

Per una nota proprietà dei logaritmi, si ha:

$$\log x = 136.279.841 \times \log 2 = 136.279.841 \times 0{,}30103 \approx 41.024.320 .$$

Il valore trovato, 41.024.320, è dunque la caratteristica del logaritmo decimale di x, cioè del numero di Mersenne. Come dire che questo numero è costituito da circa 41 milioni di cifre. Appunto.

**4.** Quella che forse è la più famosa congettura sui numeri primi e che a tutt'oggi non si sa se sia vera o falsa, è stata enunciata da un amico di Eulero, il prussiano Christian Goldbach (1690-1764), e per questo è conosciuta come **congettura di Goldbach**. Recita così:

**Ogni numero pari maggiore di 2 è la somma di due numeri primi** (non necessariamente distinti e non necessariamente per una sola coppia di numeri primi).

Per esempio:

$$4=2+2,\ \ 6=3+3,\ \ 8=3+5,\ \ 10=3+7=5+5,\ \ 12=5+7,\ \ 14=3+11=7+7,\ \ 16=3+13=5+11.$$

In realtà, questa formulazione della congettura, denominata *binaria*, è una rielaborazione della congettura, denominata *ternaria*, che sarebbe la congettura originaria di Goldbach, che recita così:

**Ogni numero intero maggiore di 5 è la somma di tre numeri primi** (non necessariamente distinti e non necessariamente per una sola terna di numeri primi).

Per esempio:

$$6=2+2+2,\ \ 10=2+3+5,\ \ 12=2+3+7=2+5+5,\ \ 15=3+5+7=5+5+5,\ \ 16=2+3+11.$$

NOTA 3.

È evidente che la formulazione ternaria vale se vale la formulazione binaria. Se infatti per ogni intero $n>2$ esistono due numeri primi p, q tali che $n=p+q$, allora per ogni intero $N>5$ esistono tre numeri primi p, q, r tali che $N=p+q+r$. Basta porre $r=3$.

Goldbach comunicò all'amico Eulero la sua congettura (nella formulazione ternaria) in una lettera del 1742. La risposta di Eulero fu la formulazione binaria. Formulazione che per questo è spesso denominata **congettura di Goldbach-Eulero**.

Entrambe le formulazioni compaiono nel volume *Meditationes Algebricae* del matematico inglese Edward Waring (1734-1793), pubblicato nel 1770.

**5.** Se si esamina la successione dei numeri primi a partire da 3:

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, eccetera,

e la successione dei numeri dispari sempre a partire da 3:

3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, eccetera,

si può costatare che a volte due numeri primi consecutivi sono anche numeri consecutivi nella successione dei numeri dispari, altre volte non lo sono.

Per esempio, fra i numeri minori di 100, le seguenti coppie di numeri primi consecutivi:

3-5, 5-7, 11-13, 17-19, 41-43, 59-61, 71-73

sono anche coppie di numeri dispari consecutivi.

Non sono invece coppie di numeri dispari consecutivi queste altre coppie di numeri primi consecutivi:

7-11, 13-17, 19-23, 23-29, 31-37, 37-41, 43-47, 47-53,
53-59, 61-67, 67-71, 73-79, 79-83, 83-89, 89-97.

Quando due numeri primi consecutivi sono anche numeri dispari consecutivi si dicono **numeri primi gemelli**.

Questo termine fu coniato dal matematico tedesco Paul Gustav Samuel Stäckel (1862-1919). Il termine originale, ovviamente in lingua tedesca, è *Primzahlzwilling*.

Mentre sappiamo fin dai tempi di Euclide che i numeri primi sono in quantità infinita, ancora oggi non sappiamo invece se costituiscono un'infinità o meno le coppie di numeri primi gemelli.

Si ipotizza che esse siano in numero infinito. Ma si tratta soltanto di un'ipotesi, chiamata **congettura dei numeri primi gemelli**, la cui formulazione più nota è la seguente:

**Esistono infiniti numeri primi p tali che anche p+2 è un numero primo.**

La congettura può essere enunciata anche nel modo seguente:

**Nella successione dei numeri primi esistono**
**infinite coppie di numeri p, q tali che $q-p=2$.**

Nel 1849 il matematico francese Alphonse de Polignac (1817-1890) generalizzò questa congettura, mettendo al posto di 2 un qualsiasi numero pari e formulò una nuova congettura, chiamata appunto **congettura di Polignac**, il cui enunciato è il seguente:

**Per ogni numero pari 2m, esistono, nella successione dei numeri primi,**
**infinite coppie di numeri *consecutivi* p, q tali che $q-p=2m$.**

Questa congettura racconta una storia veramente incredibile e stupefacente: anche se si pensa ad un numero pari H molto grande (diciamo mille miliardi di miliardi, ma solo per fissare le idee, poiché si possono immaginare numeri ben più grandi), la congettura di Polignac afferma che nella successione dei numeri primi esistono due numeri primi consecutivi p, q tali che $q-p$ è proprio quel numero H.

Il che vorrebbe dire che tra p e q, pur essendoci un'enormità di numeri (mille miliardi di miliardi nel nostro esempio), non ce n'è uno che sia primo. Veramente si può parlare di "solitudine dei numeri primi".

Due numeri primi consecutivi p, q tali che risulti $q-p=2m$ si denominano *numeri primi di Polignac distanti* 2m.

NOTA 4.

La congettura di Polignac, letta in altro modo, afferma che esistono catene di numeri composti consecutivi lunghe quanto si vuole.

Ma questo in verità, senza la pretesa però che agli estremi vi siano due numeri primi, può essere provato.

È possibile cioè costruire catene di numeri composti consecutivi lunghe quanto si vuole.

Per questo, dato un qualsiasi numero naturale $n>1$ basta considerare i seguenti numeri:

$$n!+2,\ n!+3,\ n!+4,\ \dots,\ n!+n.$$

Appurato che $n!=2\cdot3\cdot4\cdot\ldots\cdot n$, si costata che il primo di questi $n-1$ numeri è divisibile per 2, il secondo è divisibile per 3, il terzo per 4, … , l'ultimo è divisibile per n. Gli $n-1$ numeri sono pertanto numeri composti e inoltre, come si può costatare, sono numeri consecutivi.

Ribadisco: non bisogna concludere che i due numeri che racchiudono gli $n-1$ numeri, vale a dire $n!+1$ e $n!+n+1$, siano numeri primi.

Per esempio, se $n=5$, per cui $n!=120$, si ottiene la seguente successione di 4 numeri composti:

$$122,\ 123,\ 124,\ 125.$$

I numeri interi che li racchiudono sono 121 e 126, entrambi composti.

**6.** Nell'insieme dei numeri primi assumono una particolare rilevanza quei numeri $p_0$ tali che anche il numero $p_1=2p_0+1$ è un numero primo. Sono denominati **numeri primi di Germain**. Prendono il nome dalla matematica francese Marie Sophie Germain (1776-1831).

Qualche esempio di numeri primi di Germain e un controesempio:

- $p_0 = 3$ è un numero primo di Germain, poiché $p_1=2p_0+1=7$ è un numero primo.
- $p_0 = 5$ è un numero primo di Germain, poiché $p_1=2p_0+1=11$ è un numero primo.
- $p_0 = 7$ è un numero primo ma non di Germain, poiché $p_1=2p_0+1=15$ non è un numero primo.

Si ipotizza che i numeri primi di Germain formino un insieme infinito, ma si tratta di una congettura, denominata **congettura dei numeri primi di Germain**.

Mi sono occupato ampiamente di questo argomento in un articolo pubblicato su *Periodico di matematica* (N° 1-2, 2019). Qui mi limito a ricordare un interessante legame fra i numeri primi di Germain e i numeri primi di Polignac. In particolare, si dimostra che:

**Due numeri primi di Polignac distanti 2m sono anche numeri primi di Germain se e solo se m è multiplo di 3, vale a dire se la distanza fra i due primi di Polignac è 6 o 12 o 18 o 24 o … o 6k, qualunque sia l'intero positivo k.**

Fatta salva però la coppia $(3,5)$, che è l'unica coppia di numeri primi che non soddisfa a questa proprietà.

Due esempi:

- I due numeri primi di Polignac $(23, 29)$, distanti 6, sono anche numeri primi di Germain. Di fatto: $2\times23+1=47,\ 2\times29+1=59$ ed entrambi i numeri 47 e 59 sono numeri primi.
- I due numeri primi di Polignac $(1.499, 1.511)$, distanti 12, sono anche numeri primi di Germain. Di fatto: $2\times1.499+1=2.999,\ 2\times1.511+1=3.023$ ed entrambi i numeri 2.999 e 3.023 sono numeri primi.

Una congettura, che potremmo denominare **congettura dei numeri primi di Germain-Polignac**, afferma quanto segue:

**Per ogni numero naturale k non nullo, nell'insieme dei numeri primi di Polignac distanti 6k, esistono infinite coppie di numeri che sono anche numeri primi di Germain.**

Si capisce che, se fosse vera questa congettura, sarebbe vera di conseguenza la precedente congettura dei numeri primi di Germain.

**7.** C'è un aspetto dei numeri primi di Germain che ho appena sfiorato nell'articolo succitato. Mi propongo di approfondirlo per ciò che concerne lo scopo di questo contributo, vale a dire quello di elencare congetture non dimostrate sui numeri primi.

Allora, se $p_1$ è un numero primo di Germain, il numero $p_2 = 2\,p_1 + 1$ è certamente un numero primo. È forse quest'ultimo un numero primo di Germain? Lo è se il numero $p_3 = 2\,p_2 + 1$ è a sua volta un numero primo.

Proseguendo, se anche $p_2$, come $p_1$, è un numero primo di Germain, è forse pure $p_3$ un numero primo di Germain? Lo è evidentemente se il numero $p_4 = 2\,p_3 + 1$ è un numero primo.

E così via.

Si capisce allora che è possibile stabilire una gerarchia tra i numeri primi di Germain.

Ebbene, un numero primo di Germain $p_1$ si chiama numero primo di Germain di *n-esima specie* se i numeri $p_2 = 2\,p_1 + 1$, $p_3 = 2\,p_2 + 1$, … , $p_{n-1} = 2\,p_{n-2} + 1$ sono numeri primi di Germain, ma $p_n = 2\,p_{n-1} + 1$ è un numero primo senza essere un primo di Germain.

La successione di numeri primi:

$$p_1, p_2, p_3, \dots, p_n ,$$

dove, come detto sopra, $p_1, p_2, p_3, \dots, p_{n-1}$ sono numeri primi di Germain mentre $p_n$ è un numero primo ma non di Germain, si denomina *catena di Cunningham* [1] di lunghezza $n$.

Mostro, a titolo di esempio, una catena di Cunningham di lunghezza 6:

$$89 - 179 - 359 - 719 - 1439 - 2879.$$

Si pone la seguente domanda:

**Esistono catene di Cunningham di lunghezza qualsiasi?**

È stato dimostrato che:

**Non esistono catene di Cunningham di lunghezza infinita**.

Si ipotizza invece che:

**Per ogni naturale $n$, esistono infinite catene di Cunningham di lunghezza $n$**.

Ma questo non è stato ancora dimostrato ed è pertanto semplicemente una **congettura**. Ancora una questione aperta.

Ora, però, da qui a trovare una catena di Cunningham di lunghezza qualsiasi ce ne corre. In realtà, a tutt'oggi, almeno per quanto ne sappia, la catena più lunga di cui si ha conoscenza ha lunghezza 17 ed è stata trovata nel 2008 dal matematico Jarosław Wróblewski, dell'Istituto di Matematica dell'Università di Breslavia (Polonia). Il primo termine di questa catena è il numero 2.759.832.934.171.386.593.519.

Nello stesso anno 2008 Wróblewski ha scoperto altre catene di lunghezza 17.

In realtà, catene di lunghezza 2 o 3 è facile trovarne. Meno semplice è trovarne di lunghezza maggiore.

Mostro, a titolo di curiosità, il primo e l'ultimo termine delle catene di Cunningham delle lunghezze da 4 a 10. Ciascuna di queste catene, nella propria classe di lunghezze, ha il minore primo termine (tabella 1):

| Lunghezza n | Primo termine $p_1$ | n-esimo termine $p_n$ |
|---|---|---|
| 4 | 509 | 4.079 |
| 5 | 2 | 47 |
| 6 | 89 | 2.879 |
| 7 | 1.122.659 | 71.850.239 |
| 8 | 19.099.919 | 2.444.789.759 |
| 9 | 85.864.769 | 21.981.381.119 |
| 10 | 26.089.808.579 | 13.357.981.992.959 |

tabella 1 – Catene di Cunningham del 1° tipo

Sono tutte *catene complete*, nel senso che non possono essere estese con l'aggiunta di termini più piccoli del primo o più grandi dell'ultimo.

Per esempio, non è una catena completa la catena 5-11-23-47, di lunghezza 4, poiché può essere estesa con l'aggiunta del termine 2, facendola diventare di lunghezza 5.

Le catene di Cunningham prese in considerazione fin qui sono dette del *1° tipo*.

Esistono infatti catene di Cunningham del *2° tipo*. Precisamente, una catena siffatta, di lunghezza $n$, è una successione di numeri primi

$$p_1, p_2, p_3, \dots, p_n ,$$

dove ogni numero $p_i$ con $2 \le i \le n$, è tale per cui si ha: $p_i = 2\,p_{i-1} - 1$, mentre $p_{n+1} = 2p_n - 1$ non è un numero primo.

[1] Allan Joseph Champneys Cunningham, matematico britannico, 1842-1928.

Catene di questo tipo, di lunghezza 2 o 3, come dell'altro tipo, si trovano facilmente. Meno facile è trovarne di lunghezza maggiore. Come per le catene del 1° tipo, fornisco una tabella (tabella 2) contenente il primo e l'ultimo termine delle catene di Cunningham del 2° tipo, delle lunghezze da 4 a 10.

Ciascuna di queste catene (tabella 2), nella propria classe di lunghezze, è quella che ha il minore primo termine ed è una catena completa:

| Lunghezza n | Primo termine $p_1$ | n-esimo termine $p_n$ |
|---|---|---|
| 4 | 2.131 | 17.041 |
| 5 | 1.531 | 24.481 |
| 6 | 385.591 | 12.338.881 |
| 7 | 16.651 | 1.065.601 |
| 8 | 15.514.861 | 1.985.902.081 |
| 9 | 857.095.381 | 219.416.417.281 |
| 10 | 205.528.443.121 | 105.230.562.877.441 |

tabella 2 – Catene di Cunningham del 2° tipo

Per la cronaca, c'è da dire che ancora con il contributo determinante di Jarosław Wróblewski, nel 2014 è stata scoperta una catena di Cunningham del 2° tipo di lunghezza 19.

**8.** Un'altra congettura sui numeri primi fu formulata dal matematico francese Adrien-Marie Legendre (1752-1823) e per questo è conosciuta come **congettura di Legendre**. Afferma che **per ogni numero naturale n non nullo, esiste almeno un numero primo compreso fra $n^2$ e $(n+1)^2$**.

Ovvero, detta in termini equivalenti: **fra due numeri quadrati successivi è compreso almeno un numero primo**.

Per esempio, considerata la successione dei numeri quadrati:

$$1 - 4 - 9 - 16 - 25 - 36 - \dots,$$

si può controllare che fra 1 e 4 ci sono due numeri primi, 2 e 3; fra 4 e 9 ci sono due numeri primi, 5 e 7; fra 9 e 16 ci sono due numeri primi, 11 e 13; fra 16 e 25 ci sono tre numeri primi, 17, 19 e 23; e così via.

Per quanto mi risulta, ad oggi, le verifiche fatte mostrano che di numeri primi compresi fra due qualsiasi quadrati successivi ce ne sono almeno due.

Comunque la congettura rimane tale poiché non è stata ancora dimostrata.

**N**OTA 5.

Nel 1845 il matematico francese Joseph Bertrand (1822-1900) formulò la seguente congettura, simile alla precedente, passata alla storia come **postulato di Bertrand**:

**Per ogni numero n>1 esiste almeno un numero primo compreso fra n e 2n**.

Bertrand la verificò per ogni $n<3\times10^6$, ma non riuscì a dimostrarla.

La congettura fu però dimostrata pochi anni dopo, nel 1850, dal matematico russo Pafnuty Lvovich Chebyshev (1821-1894) e per questo la congettura, che a questo punto ovviamente non è più tale, è denominata **teorema di Chebyshev**.

Altre dimostrazioni furono fornite in seguito dall'ungherese Paul Erdös (1913-1996) e dall'indiano Srinivasa Ramanujan (1887-1920).

**9.** Fermiamo ora la nostra attenzione su due delle congetture segnalate e precisamente sulla congettura dei primi gemelli e sulla congettura dei primi di Germain.

Apparentemente non hanno nulla in comune.

In realtà sono entrambe conseguenze di un'altra congettura, nel senso che, ammessa questa per vera, quelle si possono dimostrare.

La congettura in questione è la **congettura di Dickson**, formulata nel 1904 dal matematico statunitense Leonard Eugene Dickson (1874-1954). Fin dall'età di 26 anni fu professore all'Università di Chicago ed è considerato uno dei fondatori della scuola algebrica americana.

**CONGETTURA DI DICKSON. Indicato con $s$ un intero positivo, siano le funzioni $f_i(n) = a_i n + b_i$ con $a_i, b_i$ numeri interi e $a_i$ positivi (per $i = 1, 2, \dots, s$). Supponiamo che non esista alcun intero maggiore di 1 che divida ciascuno dei seguenti prodotti:**

$$\prod_{i=1}^{s} f_i(n) = f_1(n) \cdot f_2(n) \cdots f_s(n) , \quad \forall n \in \mathbb{Z} .$$

**Allora esistono infiniti numeri naturali $n$ tali che $f_1(n), f_2(n), \dots, f_s(n)$ sono tutti numeri contemporaneamente primi.**

Andiamo dunque a vedere come, ammessa per valida questa congettura, si dimostrino le due congetture suddette.

- Dimostriamo la *congettura dei primi gemelli*:

***Esistono infinite coppie di numeri primi gemelli.***

DIMOSTRAZIONE.

Consideriamo le seguenti funzioni lineari del numero naturale p:

$$f_1(p) = p, \quad f_2(p) = p + 2 ,$$

dove p e $p+2$ sono entrambi numeri primi, con $p \geq 3$.

Sia $\Pi(p)$ il loro prodotto, vale a dire:

$$\Pi(p) = p \cdot (p + 2) .$$

Dimostriamo che non esiste un fattore comune a tutti i possibili prodotti $\Pi(p)$.

Per questo, basta trovare due prodotti particolari che non abbiano alcun fattore comune.

Poniamo dunque l'attenzione sui valori che $\Pi(p)$ assume per $p=3$ e per $p=11$, dopo aver costatato che questi due numeri sono entrambi numeri primi e che numeri primi sono anche i numeri 3+2=5 e 11+2=13. Si trova:

$$\Pi(3) = 3 \cdot 5 , \quad \Pi(11) = 11 \cdot 13 .$$

Non ci vuol molto a capire che non esiste alcun intero maggiore di 1 che sia fattore comune ai due prodotti.

Se vale allora la congettura di Dickson, dobbiamo concludere che esistono infinite coppie di numeri primi p, p+2, ossia infinite coppie di numeri primi gemelli.

- Dimostriamo la *congettura dei primi di Germain*:

***Esistono infiniti numeri primi di Germain.***

DIMOSTRAZIONE.

Consideriamo le seguenti funzioni lineari del numero naturale p:

$$f_1(p) = p, \quad f_2(p) = 2p + 1 ,$$

dove p è un numero primo di Germain, per cui $2p+1$ è un numero primo (non importa se primo di Germain o no).

Sia $\Pi(p)$ il loro prodotto, vale a dire:

$$\Pi(p) = p \cdot (2p + 1) .$$

Dimostriamo che non esiste un fattore comune a tutti i possibili prodotti $\Pi(p)$.

Come prima, basta trovare due prodotti particolari che non abbiano alcun fattore comune.

Per questo, poniamo l'attenzione sui valori che $\Pi(p)$ assume per $p=3$ e per $p=5$, dopo aver costatato che questi due numeri sono entrambi numeri primi di Germain. Si trova:

$$\Pi(3) = 3 \cdot 7 , \quad \Pi(11) = 5 \cdot 11 .$$

Si capisce subito che non esiste alcun intero maggiore di 1 che sia fattore comune ai due prodotti.

Se vale allora la congettura di Dickson, dobbiamo concludere che esistono infinite coppie di numeri primi p, $2p+1$. Come dire che esistono infiniti numeri primi di Germain.

- Altre congetture è possibile dimostrare come applicazione della congettura di Dickson.

Compresa la congettura sull'esistenza di catene di Cunningham di una qualsiasi lunghezza n, ma con ragionamenti più sofisticati e non ce ne occupiamo. Questo però se è richiesta una dimostrazione per una catena

di lunghezza generica. Se invece si ragiona su catene di una lunghezza particolare, la dimostrazione, condotta come nei due casi sopra descritti, si presenta abbastanza semplice, fatta salva la ricerca di due opportune datene di Cunningham. Ricerca in verità spesso complicata e a tutt'oggi non sempre con esito positivo,

Ma vediamo un esempio particolare.

*Esistono infinite catene di Cunningham del 1° tipo di lunghezza 4*.

DIMOSTRAZIONE.

Dato il numero primo p, supponiamo che siano numeri primi anche i numeri 2p+1, 2(2p+1)+1=4p+3 e 2(4p+3)=8p+7, mentre non sia un numero primo il numero 2(8p+7)+1=16p+15.

Si ha pertanto la seguente catena di Cunningham del 1° tipo, di lunghezza 4:

$$p_1 = p,\ \ p_2 = 2p_1 + 1,\ \ p_3 = 2p_2 + 1,\ \ p_4 = 2p_3 + 1.$$

Consideriamo allora le seguenti funzioni lineari di p:

$$f_1(p) = p, \quad f_2(p) = 2p + 1\,, \quad f_3(p) = 4p + 3\,, \quad f_4(p) = 8p + 7.$$

Sia $\Pi(p)$ il loro prodotto, vale a dire:

$$\Pi(p) = p \cdot (2p + 1) \cdot (4p + 3) \cdot (8p + 7)\,.$$

Troviamo che i numeri 509 e 1.229 generano due catene di Cunningham del 1° tipo della medesima lunghezza 4; precisamente le due catene:

$$509 - 1.019 - 2.039 - 4.079, \quad 1.229 - 2.459 - 4.919 - 9.839.$$

Risulta perciò, ovviamente:

$$\Pi(509) = 509 \cdot 1.019 \cdot 2.039 \cdot 4.079\,; \quad \Pi(1.229) = 1.229 \cdot 2.459 \cdot 4.919 \cdot 9.839\,.$$

Si costata che non esiste alcun fattore comune a questi due prodotti e quindi non esiste alcun fattore comune a tutti i possibili prodotti $\Pi(p)$.

Si può concludere, come nei due casi trattati in precedenza, che, se vale la congettura di Dickson, è dimostrata la proposizione in questione.

Ragionando alla stessa maniera si dimostra che

*Esistono infinite catene di Cunningham del 2° tipo di lunghezza 4*.

Basta trovare due catene di questa lunghezza e costatare che non hanno fattori comuni. Per esempio:

$$2.131 - 4.261 - 8.521 - 17.041, \quad 3.061 - 6.121 - 12.241 - 24.481.$$

**9.** Concludo con alcune curiosità, che poi altro non sono che nuove questioni aperte sui numeri primi.

- Se si prende in considerazione la successione dei numeri di Fibonacci:

$$1 - 1 - 2 - 3 - 5 - 8 - 13 - 21 - 34 - 55 - 89 - \cdots,$$

si può controllare facilmente che tra questi numeri ci sono dei numeri primi. Per esempio:

$$2 - 3 - 5 - 13 - 89 - \cdots.$$

Sono denominati *numeri primi di Fibonacci*.

La domanda è: **I numeri primi di Fibonacci sono in numero finito o infinito?**

Nessuno è stato in grado di stabilirlo. È una questione aperta.

- Se consideriamo i numeri primi $13, 17, 19, 37$. Possiamo costatare che sono numeri primi anche i numeri che si ottengono da essi scrivendoli al contrario, cioè i numeri $31, 71, 91, 73$.

I numeri che hanno questa caratteristica sono denominati *numeri primi reversibili*.

La domanda, alla quale ancora non è stata data risposta, è: **I numeri primi reversibili sono in numero finito o infinito?**

- Consideriamo i numeri primi $23, 113, 139, 4877$.

Possiamo costatare che sono numeri primi anche i numeri che si ottengono da essi cancellando la cifra delle unità, cioè i numeri $2, 11, 13, 487$.

I numeri che hanno questa caratteristica sono denominati *numeri primi caudati* (ovvero: *numeri primi con la coda*)

Possiamo costatare pure che sono ancora numeri primi i numeri che si ottengono da quelli assegnati cancellando la prima cifra a sinistra, cioè i numeri 3, 13, 39, 877.

I numeri che hanno questa caratteristica sono denominati *numeri primi decapitabili* (ovvero: *numeri primi ai quali è possibile tagliare la testa*)

Si può verificare agevolmente che esistono numeri primi che sono caudati ma non decapitabili oppure decapitabili ma non caudati oppure infine caudati e decapitabili.

La domanda, che ancora non ha avuto risposta, è la solita: **I numeri che hanno una di queste caratteristiche o che hanno entrambe le caratteristiche sono in numero finito o infinito?**

BIBLIOGRAFIA.

Wikipedia, libera enciclopedia on-line.