Variazioni Goldbach: problemi con numeri primi

Alessandro Zaccagnini

Padova, 26 novembre 2004

http://www.math.unipr.it/∼zaccagni/psfiles/papers/Goldbach_I.pdf

http://www.math.unipr.it/∼zaccagni/psfiles/papers/LucidiGoldbach_I.pdf

Preludio: I Numeri Primi

Chiameremo *numeri primi* gli interi $n \geq 2$ che sono divisibili solo per 1 e per se stessi.

Sono numeri primi 2, 3, 5, 7, 11, 13, 17, 19, 23, . . .

Euclide dimostrò che ogni numero intero $n \geq 2$ è primo oppure può essere scritto come prodotto di numeri primi:

$$\begin{aligned} 91 &= 7 \cdot 13 \\ 257 &= 257 \\ 666 &= 2 \cdot 3 \cdot 3 \cdot 37 \\ 1001 &= 7 \cdot 11 \cdot 13 \end{aligned}$$

Euclide dimostrò anche che esistono infiniti numeri primi: se 2, 3, 5, . . . , p fossero i soli numeri primi, prendiamo il numero

$$N = 2 \cdot 3 \cdot 5 \cdots p + 1$$

N dà resto 1 quando diviso per questi numeri primi.

Quindi la nostra lista iniziale non può essere completa.

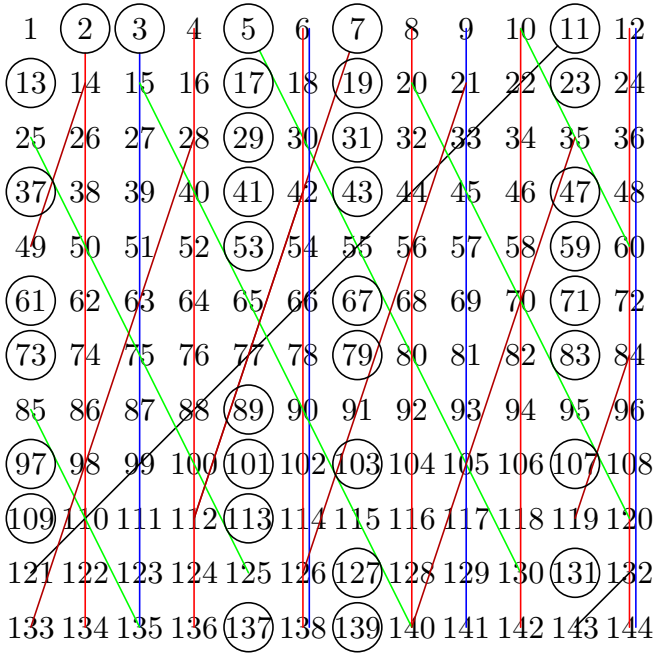
2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997

I numeri primi fino a 1000.

Come determinare i numeri primi?

1. Divisione per tentativi (esistono metodi migliori).

2. Crivello di Eratostene.



Il crivello di Eratostene: cancelliamo i multipli di 2 (rosso), i multipli di 3 (blu), i multipli di 5 (verde), i multipli di 7 (arancione) ed i multipli di 11 (nero).

Ma quanti sono i numeri primi?

Prendiamo un numero grande N. Quanti sono gli interi pari minori di N?

Quanti sono gli interi dispari minori di N e divisibili per 3?

Quanti sono gli interi non ancora eliminati e divisibili per 5?

. . . . . .

Quanti degli interi sopravvissuti al crivello finora rimangono quando eliminiamo i multipli di p?

Ad ogni passo togliamo circa $1/p$-esimo del totale degli interi rimasti.

Ci aspettiamo che la *proporzione* dei numeri rimasti sul totale sia approssimativamente

$$\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\cdots\left(1-\frac{1}{p}\right) \tag{1}$$

dove p indica il piú grande numero primo $\leq \sqrt{N}$.

Se N è un numero molto grande, questo prodotto vale approssimativamente

$$\frac{c}{\log N} \tag{2}$$

dove $c = 1.1229197\ldots$. Qui "log" indica la funzione *logaritmo naturale*, cioè in base $e = 2.718281828\ldots$

Ci potremmo aspettare che debbano esserci circa $cN/\log N$ numeri primi $\leq N$. Ma le cose non stanno esattamente cosí.

Nel 1896 Jacques Hadamard e Charles de la Vallée Poussin hanno dimostrato che

$$\pi(N) \sim \frac{N}{\log N}$$

dove $\pi(N)$ indica il numero dei numeri primi $p \leq N$.

Il simbolo $\sim$ indica che il rapporto fra le due quantità $\pi(N)$ ed $N/\log N$ è molto vicino ad 1 quando N è molto grande.

N	$\pi(N)$	$\pi(N) - \frac{N}{\log N}$	$\frac{\pi(N)\log N}{N}$
10	4	0	$0.921\ldots$
10^2	25	3	$1.151\ldots$
10^3	168	23	$1.161\ldots$
10^4	1229	143	$1.132\ldots$
10^5	9592	906	$1.104\ldots$
10^6	78498	6116	$1.084\ldots$
10^7	664579	44158	$1.071\ldots$
10^8	5761455	332774	$1.061\ldots$
10^9	50847534	2592592	$1.054\ldots$
10^{10}	455052511	20758029	$1.048\ldots$

Le differenze sono approssimate all'intero piú vicino.

Tema: il problema di Goldbach

Nel 1742 il matematico Christian Goldbach affermò che se n è un numero intero pari maggiore di 4 è possibile trovare due numeri primi dispari p_1 e p_2 in modo che

$$n = p_1 + p_2 \tag{3}$$

Per esempio, $10 = 3 + 7 = 5 + 5 = 7 + 3$.

Chiamiamo $r(n)$ il numero delle soluzioni dell'equazione (1) per n pari.

$r(4) = 1$ perché $4 = 2 + 2$: questo è l'unico caso in cui compare il numero primo 2.

n	$r(n)$	n	$r(n)$	n	$r(n)$	n	$r(n)$	n	$r(n)$
2	0	4	1	6	1	8	2	10	3
12	2	14	3	16	4	18	4	20	4
22	5	24	6	26	5	28	4	30	6
32	4	34	7	36	8	38	3	40	6
42	8	44	6	46	7	48	10	50	8
52	6	54	10	56	6	58	7	60	12
62	5	64	10	66	12	68	4	70	10
72	12	74	9	76	10	78	14	80	8
82	9	84	16	86	9	88	8	90	18
92	8	94	9	96	14	98	6	100	12
102	16	104	10	106	11	108	16	110	12
112	14	114	20	116	12	118	11	120	24
122	7	124	10	126	20	128	6	130	14
132	18	134	11	136	10	138	16	140	14
142	15	144	22	146	11	148	10	150	24

Valori di $r(n)$ per n pari fino a 150.

Domande:

1. Qual è l'ordine di grandezza di $r(n)$?

2. Come calcolare esattamente $r(n)$?

3. Perché $r(n)$ è cosí irregolare?

4. È vera la congettura di Goldbach, cioè è vero che $r(n) \geq 1$ per ogni n pari diverso da 2?

Daremo qualche risposta alle domande 1, 2, 3.

Prendiamo N molto grande, i $\pi(N)-1$ numeri primi dispari fino ad N, e tutte le loro possibili somme.

Le somme p_1+p_2 sono in totale

$$\big(\pi(N)-1\big)^2 \sim \frac{N^2}{(\log N)^2}$$

In media, per ogni intero pari $n \leq 2N$ ci sono approssimativamente $N/(\log N)^2$ soluzioni di (1) con p_1 e $p_2 \leq N$.

1	+	59		31	+	29	$\star$
3	+	57		33	+	27	
5	+	55		35	+	25	
7	+	53	$\star$	37	+	23	$\star$
9	+	51		39	+	21	
11	+	49		41	+	19	$\star$
13	+	47	$\star$	43	+	17	$\star$
15	+	45		45	+	15	
17	+	43	$\star$	47	+	13	$\star$
19	+	41	$\star$	49	+	11	
21	+	39		51	+	9	
23	+	37	$\star$	53	+	7	$\star$
25	+	35		55	+	5	
27	+	33		57	+	3	
29	+	31	$\star$	59	+	1	

Come calcolare $r(60)$. I multipli di 3 sono indicati in rosso, i multipli di 5 in blu. Le coppie (p_1, p_2) tali che $p_1 + p_2 = 60$ sono indicate da una $\star$.

1	+	61	
3	+	59	$\star$
5	+	57	
7	+	55	
9	+	53	
11	+	51	
13	+	49	
15	+	47	
17	+	45	
19	+	43	$\star$
21	+	41	
23	+	39	
25	+	37	
27	+	35	
29	+	33	
31	+	31	$\star$

33	+	29	
35	+	27	
37	+	25	
39	+	23	
41	+	21	
43	+	19	$\star$
45	+	17	
47	+	15	
49	+	13	
51	+	11	
53	+	9	
55	+	7	
57	+	5	
59	+	3	$\star$
61	+	1	

Come calcolare $r(62)$. La $\star$ indica le coppie (p_1, p_2) tali che $p_1 + p_2 = 62$.

Operiamo un “doppio crivello” sulle potenziali soluzioni dell’equazione (3), cancellando quelle in cui un addendo risulta divisibile per 3.

Attenzione: quando $n = 60$ i multipli di 3 compaiono alla stessa altezza, e quindi abbiamo cancellato solo $1/3$ delle soluzioni scritte all’inizio e ne sopravvivono $1 - 1/3 = 2/3$.

Quando $n = 62$ cancelliamo $2/3$ delle soluzioni scritte prima, lasciandone solamente $1 - 2/3 = 1/3$.

Come distinguere fra le due situazioni?

È molto semplice! Il numero primo 3 divide 60 ma non 62.

Naturalmente il numero 3 non è speciale: dobbiamo ripetere lo stesso procedimento per tutti i primi dispari $p \leq \sqrt{n}$.

Congettura: per n grande $r(n)$ vale circa

$$n \cdot \frac{1}{2} \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \cdot \left(1 - \frac{2}{q_1}\right) \cdots \left(1 - \frac{2}{q_s}\right)$$

dove $p_1, \ldots, p_r$ sono i primi dispari distinti che dividono n, mentre $q_1, \ldots, q_s$ sono gli altri primi dispari minori di $\sqrt{n}$.

Il fattore $\frac{1}{2}$ tiene conto del fatto che non ci sono addendi pari.

Tenendo conto del valore approssimato (2) per il prodotto sui numeri primi (1), possiamo semplificare la nostra congettura cosí:

$$r(n) \sim c' \cdot \frac{p_1 - 1}{p_1 - 2} \cdot \frac{p_2 - 1}{p_2 - 2} \cdots \frac{p_r - 1}{p_r - 2} \cdot \frac{n}{(\log n)^2}$$

per un'opportuna costante $c' = 1.3203\ldots$ detta *costante dei primi gemelli*.

Come si vede, questa quantità differisce dal valor medio *solo* per la presenza del prodotto sui fattori primi di n.

Per esempio, per $n = 60$ il prodotto sui fattori primi vale $8/3 = 2.6666\ldots$ mentre per $n = 62$ vale solamente $30/29 = 1.03448\ldots$

La nostra formula prevede dunque

$$r(60) = 12 \approx \frac{8}{3} \cdot c' \cdot \frac{60}{(4.094\ldots)^2} \approx 12.602\ldots$$

$$r(62) = 5 \approx \frac{30}{29} \cdot c' \cdot \frac{62}{(4.127\ldots)^2} \approx 4.972\ldots$$

Questi numeri sono abbastanza precisi, e questo ragionamento sembra suggerire il motivo per cui $r(60) = 12$ è piú del doppio di $r(62) = 5$.

Prendendo numeri piú grandi l'approssimazione migliora, ma in modo irregolare: dal punto di vista numerico, per n grande si ottengono approssimazioni migliori scrivendo $(\log n - 1)^2$ al posto di $(\log n)^2$.

Prima variazione

Qual è il problema corrispondente per i numeri dispari?

Tutti i numeri primi a parte 2 sono dispari: dobbiamo sommare tre numeri primi (dispari) per ottenere un altro numero dispari.

Congettura: per ogni numero dispari n sufficientemente grande, esistono tre numeri primi p_1, p_2 e p_3 tali che

$$n = p_1 + p_2 + p_3 \tag{4}$$

Chiamiamo $r_3(n)$ il numero delle soluzioni di questa equazione. Il ragionamento in media dà il numero molto piú grande

$$\frac{n^2}{(\log n)^3}$$

I. M. Vinogradov (1937): per n dispari sufficientemente grande l'equazione (4) ha sempre almeno una soluzione.

Inoltre, se n è un numero dispari sufficientemente grande

$$r_3(n) \sim c'' \cdot \frac{(p_1-1)(p_1-2)}{p_1^2-3p_1+3} \cdots \frac{(p_r-1)(p_r-2)}{p_r^2-3p_r+3} \cdot \frac{n^2}{(\log n)^3}$$

dove c'' è un'altra costante positiva, e $p_1, p_2, \ldots, p_r$ sono i fattori primi di n.

Cosa vuol dire “n dispari sufficientemente grande”?

Vuol dire che la proprietà che ci interessa vale per tutti gli interi dispari $n > N_0$, dove N_0 è un certo numero da determinare.

Per esempio, nel problema binario di Goldbach, congetturiamo che si possa prendere $N_0 = 2$.

Negli anni ’50 è stato dimostrato che nel problema ternario si può prendere $N_0 = 3^{3^{15}}$.

Ma è un numero enorme (ha quasi 7 milioni di cifre)!

Oggi sappiamo che si può prendere $N_0 = e^{100000}$, ma si tratta di un numero di oltre 43000 cifre!

Non è ancora possibile trattare i casi rimanenti con un calcolatore.

O. Ramaré (1995): *qualunque* sia il numero naturale $n \geq 2$, l'equazione

$$n = p_1 + p_2 + \cdots + p_r$$

è risolubile con i p numeri primi, ed $r \leq 7$.

Seconda variazione

Modifichiamo l'equazione (3) cambiando il segno $+$ in $-$:

$$n = p_1 - p_2$$

Ci sono soluzioni? Attenzione: potrebbero essere infinite!

Prendiamo un numero grande N e contiamo le soluzioni di questa equazione in cui $p_2 \leq N$.

n	π_n	n	π_n	n	π_n	n	π_n	n	π_n
2	205	4	203	6	411	8	208	10	270
12	404	14	245	16	200	18	417	20	269
22	226	24	404	26	240	28	248	30	536
32	196	34	215	36	404	38	213	40	267
42	489	44	227	46	201	48	409	50	270
52	221	54	410	56	240	58	212	60	535
62	206	64	201	66	458	68	209	70	318
72	401	74	206	76	220	78	428	80	272
82	205	84	493	86	207	88	217	90	531
92	218	94	208	96	400	98	232	100	260

Valori di $\pi_n(10000)$ per n pari fino a 100.

Anche qui sono evidenti delle irregolarità:

$\pi_{60} = 535$ è oltre il doppio di $\pi_{62} = 206$

Domanda: perché accade questo fenomeno?

1	61	1	63
3	63	3	65
5	65	5	67
7	67	7	69
9	69	9	71
11	71	11	73
13	73	13	75
15	75	15	77
. . . . .			
. . . . .			
. . . . .			
9991	10051	9991	10053
9993	10053	9993	10055
9995	10055	9995	10057
9997	10057	9997	10059
9999	10059	9999	10061

Una piccola parte della tavola per π_{60} e π_{62} con $N = 10000$.

Congettura: per n pari fissato ed N molto grande

$$\pi_n(N) \sim c' \cdot \frac{p_1 - 1}{p_1 - 2} \cdot \frac{p_2 - 1}{p_2 - 2} \cdots \frac{p_r - 1}{p_r - 2} \cdot \frac{N}{(\log N)^2}$$

dove $p_1, \ldots, p_r$ sono i fattori primi dispari di n e c' è la stessa costante di prima.

I numeri primi che hanno differenza 2 come 11 e 13 si chiamano tradizionalmente *primi gemelli*.

Altre variazioni

La domanda che ci siamo fatti prima è la seguente:

È vero che esistono infiniti numeri primi p per cui anche $p+2$ è un numero primo?

Ora ne facciamo un'altra simile:

Sarà vero che esistono infiniti numeri primi p per cui anche $p+2$ e $p+4$ sono numeri primi?

Nella tavola dei numeri primi questo accade solo quando $p=3$. Perché?

Perché *qualunque* sia il numero intero n, uno fra i numeri n, $n+2$ ed $n+4$ è divisibile per 3.

E che dire dei numeri p, $p+2$ e $p+6$? Possono essere tutti simultaneamente primi?

Sí! Succede in una grande quantità di casi: esistono ben 55 numeri primi $p < 10000$ tali che $p+2$ e $p+6$ sono ancora numeri primi.

Per esempio: (5,7,11), (11,13,17), (17,19,23).

Consideriamo le *costellazioni* di numeri primi: dati 2 numeri interi positivi distinti a e b, ci chiediamo:

È vero che esistono infiniti primi p tali che anche $p+a$ e $p+b$ sono simultaneamente primi?

Lo chiameremo “problema della costellazione (a,b).”

Come distinguere fra le costellazioni $(2,4)$ e $(2,6)$?

Abbiamo appena visto che queste sono radicalmente diverse.

Consideriamo il numero primo $q = 2$: se almeno uno dei numeri a e b non è pari, allora i numeri p, $p + a$, $p + b$ possono essere tutti primi solo se $p = 2$.

Per esempio, per la costellazione (3,5) questo accade solo quando $p = 2$, e per la costellazione (2,3) non accade mai.

Ora calcoliamo i resti di 0, a e b nella divisione per $q = 3$.

Se accade che i resti, in un qualche ordine, sono 0, 1, 2, allora i numeri p, $p + a$, e $p + b$ possono essere simultaneamente primi al massimo per un valore di p, e la costellazione (a, b) viene detta *non ammissibile*.

In caso contrario la costellazione si dice *ammissibile*.

Nell'esempio di prima, se $(a,b) = (2,4)$ quando $q = 3$ i resti valgono 0, 2, 1 rispettivamente.

Se $(a,b) = (2,6)$ quando $q = 3$ i resti valgono 0, 2, 0.

Congettura: se (a,b) è una costellazione ammissibile esistono infiniti primi p per cui anche $p+a$ e $p+b$ sono numeri primi.

Ma perché limitarci a considerare costellazioni di 3 primi?

Questo metodo funziona anche per studiare la distribuzione dei numeri primi p per cui $2p+1$ è un numero primo, e perfino per relazioni piú complicate di queste.

In realtà ci sono infiniti problemi di questo tipo, ma preferiamo concludere qui perché il tempo a disposizione è finito.

a	b	$\pi_{a,b}$	a	b	$\pi_{a,b}$	a	b	$\pi_{a,b}$	a	b	$\pi_{a,b}$
2	6	55	2	8	57	2	12	92	2	14	73
2	18	66	2	20	82	2	24	59	2	26	68
2	30	112	2	32	85	2	36	65	4	6	57
4	10	91	4	12	62	4	16	57	4	18	71
6	8	62	6	12	118	6	14	76	6	16	81
6	18	125	6	20	106	6	22	62	8	12	49
8	14	68	8	18	88	12	60	166	20	30	101
30	60	223	30	90	221	30	120	219	60	120	228

Conteggi per alcune costellazioni ammissibili di primi con $N = 10000$.