

CONSERVAZIONE DELLE FORME E DEI SEGNI ANCHE NEI NUMERI SEMIPRIMI $N = p * q$

(con $p > 3$ e $q > 3$)

Gruppo ERATOSTENE

Le forme $6k \pm 1$ dei numeri primi e i segni + e - vengono conservati anche nei semiprimi, prodotti di due numeri primi maggiori di 3, e quindi con eccezione del 2 e del 3, che non sono di forma $6k \pm 1$.

Infatti, il prodotto di due numeri si può scrivere, in base alle tre possibilità come:

1a) Primo caso: segni uguali:

$$(6m - 1) (6n - 1) = 36mn - 6m - 6n + 1 = 36mn - 6(n-m) + \underline{1}$$

$$1b) 6(m + 1) (6n + 1) = 36mn + 6m + 6n + 1 = 36mn + 6(m+n) + \underline{1}$$

2a) Secondo caso : segni diversi

$$(6m - 1) (6n + 1) = 36mn + 6m - 6n - 1 = 36mn + (m - n) - \underline{1}$$

$$2b) (6m + 1) (6n - 1) = 36mn - 6m - 6n - 1 = 36mn - (n-m) - \underline{1}$$

Come si vede, nei casi 1a e 1b si conserva il +1 finale (prodotto di $+1 * +1 = +1$), mentre nei casi 2a e 2b si conserva il -1 finale, prodotto di $-1 * +1$ e di $+1 * -1$, per esempio:

$$1a) 17 * 29 = 493 = 6 * 82 + 1$$

$$1b) \quad 19 * 31 = 588 = 6 * 98 + 1$$

$$2a) \quad 17 * 31 = 527 = 6 * 88 - 1$$

$$2b) \quad 13 * 29 = 377 = 6 * 63 - 1$$

I numeri gemelli , essendo di segno diverso, rientrano nel caso 2°, essendo di forma $p = 6m - 1$ e $q = 6m + 1$, per essi infatti $m = n$ ma il segno algebrico diverso, e il loro

prodotto si semplifica in $N = p * q = 36m^2 - 1$, quale che sia m . Tutto ciò però non ci aiuta molto a fattorizzare un numero RSA, che essendo il prodotto di due numeri primi molto grandi, è anche un semiprimo, tranne che nel caso dei gemelli in cui $p = \sqrt{N} - 1$ e $q = \sqrt{N} + 1$: Per N non prodotto di numeri primi non gemelli, vedi “Fattorizzazione con algoritmo generalizzato con quadrati perfetti in ambito delle forme $6k + 1$ ” .

Nel caso 1b, $6(m + n) = 6(3 + 5) = 6 * 8 = 48 = 50 - 2$ si ha una connessione con la congettura di Goldbach, poiché: $19 + 31 = 50 = 6(3+5) + 2 = 50 = p + q$, e poiché trovare m ed n è ugualmente difficile come trovare p e q , la cosa non ci aiuta molto nella fattorizzazione di N , ed è meglio il contenuto del suddetto articolo “Fattorizzazione ...”.

Ma solo in tal caso, forse, qualcosa si potrebbe anche fare, poiché il rapporto $N/36$ è spesso circa il doppio della somma $p + q$;

per esempio se $N = 589$, $589/36 = 16,36 \approx 2(m + n)$, chè è circa il doppio di $m + n = 3+5 = 8$, e $6(m + n) = 6 * 8,1805555 = 49,08 \approx 50 = p + q$ da cui, con le coppie di Goldbach per almeno $N = 50$ (e numeri

pari successivi), si risale facilmente (almeno per N piccoli, di poche cifre) alla coppia 19 e 31 il cui prodotto è $19 * 31 = 589$; è una ricerca che riprenderemo eventualmente in seguito, per i numeri N di forma $6k + 1$ (lo stesso ragionamento si può fare anche con i numeri p e q di forma $6k - 1$; per es. $17 * 29 = 493$, $17 + 29 = 46$ e $493/36 = 13,69 \approx 2 * k$

$$= 2 * 6,847222; 6,847222 * 6 = 41,08 \approx 46 = 17 + 29) .$$

Il legame teorico tra somma e prodotto c'è anche qui (oltre che in Goldbach), ma forse non anche l'utilità pratica perché essa sarebbe comunque minore del metodo descritto in “ Fattorizzazione... in ambito delle forme $6k \pm 1$ ”, che permette di evitare la costruzione delle coppie di Goldbach per i numeri pari S (probabili somme $S = p + q$) superiori a $2n = 2\sqrt{N}$, e tanto meno superiori quanto più p e q sono vicini, fino a coincidere con $2n = 2\sqrt{N}$ per N quadrati perfetti o prodotti di due numeri primi gemelli, per es. $12 * 12 = 144$; $12 + 12 = 24 = 2n = 2\sqrt{144}$, e $N = 143 = 11 * 13$, con

$$11 + 13 = 24 = 2\sqrt{(143+1)} .$$

Insomma, anche i semiprimi conservano la forma dei loro fattori primi, e il segno + e - come già noto prodotto di segni: $- * - = +$, $- * + = -$, $+ * - = -$, $+ * + = +$.

Caltanissetta 1.7.2010