

Nota sulla fattorizzazione dei numeri Repunit (R_n)

(e varie, per es. legge di conservazione del segno + o - della forma $p = 6k \pm 1$ della forma aritmetica dei numeri primi e dei semiprimi, nella funzione $s =$ somma cifre)

Osservando bene i numeri Repunit R_n e soprattutto i loro fattori e dei loro fattori, che come vedremo dipende dalle forme di $n = 6k$ (multipli pari di 3), $6k \pm 1$ (numeri dispari non multipli dispari di 3), $6k \pm 2$ (ossia numeri pari), $6k \pm 3$ (ossia multipli dispari di 3), abbiamo notato che i fattori di R_n dipendono, sia come grandezza che come numero, dalle forme di n , come nei seguenti possibili casi:

- a) se n è pari, tranne il 2 poiché $R_2 = 11$ è primo, R_n ha molti fattori primi piccoli (vedi tabella finale);
- b) se n è dispari, e specialmente se è anche numero primo, R_n ha pochi fattori primi, e che crescono di grandezza al crescere

di n; per es. $R_{17} = 2\ 071\ 723 \times 5\ 363\ 222\ 357$

P_n è primo per $n = 2, 19, 23, 317, 1031$ mentre per $n = 49081$ e 86453 è invece probabile primo (vedi Repunit – Wikipedia).

Notiamo pure (vedi Repunit (factors), su NationMaster, vedi in seguito) che R_{38} contiene come fattore primo, tra gli altri, anche R_{19} e così pure R_{46} contiene anche R_{23} , e così pure sarà per qualsiasi R_n con n multiplo di qualsiasi Repunit primo.

c) se n è multiplo dispari di 3, e quindi di forma $6k \pm 3$, R_n possiede molti fattori piccoli, e sempre il 37, con una particolare curiosità aritmetica: poiché $37 + 3 = 111 = R_3$ e $37/37 = 1$, succede che anche $R_6 = 111\ 111 / 3 = 37037$, e $37037 / 37 = 1001$; e così pure per R_9 :

$111\ 111\ 111 / 3 = 37037037$, che diviso 37 = 1001001;

più in generale,

$$R_{3k} = 3 \times 37 \times (10^{3k-3} + m)$$

dove m è il numero $R_{3k} / 3 \times 37 - 10^{3k}$ precedente

i valori successivi di m sono quindi 1, 1001, 1001001, ecc.

per es. $111/3 \times 37 = 1 \quad = m_1 = 10^0 + 1$
 $111111/3 \times 37 = 1001 \quad = m_2 = 10^3 + 1$
 $111111111/3 \times 37 = 1001001 \quad = m_3 = 10^6 + 1001$

Dove gli esponenti di m sono in successione, 0, 3 = 1 + 2, 6 = 1 + 2 + 3.

E quindi $R_{3k} = 3 \times 37 \times (10^{3k-3} + m)$:

k=1 $111 = 3 \times 37 \times 10^0 = 3 \times 37 \times 1 = 3 \times 37 \times 1$

k=2 $111111 = 3 \times 37 \times 1101 = 3 \times 37 \times (10^3 + 1) = 3 \times 37 \times (10^3 + 1)$
 $3 \times 37 \times (10^3 + 1) = 3 \times 37 \times (1000 + 1) = 3 \times 37 \times 1001 = 111111$

k=3 $111111111 = 3 \times 37 \times (10^6 + 1001) = 3 \times 37 \times (10^6 + 1001) =$
 $3 \times 37 \times (1000000 + 1001) = 3 \times 37 \times 1001001 = 111111111$

k=4 $111111111111 = 3 \times 37 \times (10^9 + 1001001) =$
 $3 \times 37 \times (10^9 + 1001001) = 3 \times 37 \times (1000000000 + 1001001)$

$= 3 \times 37 \times 1001001001 = 111111111111 = R_{12} = R_{3 \times 4} = R_{3k}$

d) se n è invece di forma 6k, e cioè pari e anche multiplo pari di 3, R_n ha pure molti piccoli fattori, compreso il 37,

e rientra nel caso c) ma ancora con più fattori primi ;

e) a volte, tutti i fattori di R_n terminano tutti con la cifra 1,

per esempio

$$R_{10} = 11 \times 241 \times 271 \times 9091$$

$$R_{20} = 11 \times 41 \times 101 \times 271 \times 3541 \times 19091 \times 27961$$

poiché per le cifre finali 1×1 fa sempre 1, mentre negli

altri casi abbiamo $3 \times 7 = 21$ terminante per 1, $9 \times 9 = 81$

terminante con 1, e così via anche per le altre cifre

terminali: $3 \times 5 = 15$, $7 \times 9 = 63$ ecc.

Ne consegue che tutti i multipli k dei Repunit, $k \times R_n$

(compresi i Repdigit tipo $333\ 333 = 3 \times 111\ 111$,

$9\ 999\ 999\ 999 = 9 \times 1\ 111\ 111\ 111$ ecc. e pure i multipli

k (con k fino a 9) dei Repdigit hanno anche gli stessi fattori

del Repunit di base, oltre ai fattori di k .

Per esempio $k \times R_5 = 13 \times 11\ 111 = 144\ 443$, e

dividendo un numero per i successivi R_n si può vedere se esso è un multiplo di un R_n ,

per es. il suddetto numero 144 443 diviso per i successivi Repunit 11, 111, 1111, dà numeri frazionari, mentre solo se diviso per 11 111 dà risultato il intero 13, poiché è multiplo di R_5 .

Ovviamente, ogni numero Repunit o Repdigit (Ripetizione di cifre) ha infiniti multipli, e anche qualche numero RSA potrebbe essere multiplo di Repunit, in tal modo facile da controllare perchè si conoscono i Repunit primi. Quindi si sconsigliano numeri primi Repunit per la crittografia RSA, mentre, viceversa, un numero RSA chiave pubblica, potrebbe essere benissimo un Repunit R_n con n numero primo molto grande, poiché in questi casi essi hanno pochi (o anche solo due) fattori primi molto grandi, e quindi più difficili da fattorizzare con le tecniche tradizionali (vedi parte finale).

Circa i numeri palindromi, essi si possono ottenere con

piccole potenze di Repunit (massimo il quadrato o il cubo)
per es.:

$$11^2 = 11 \times 11 = 121$$

$$11^3 = 11 \times 11 \times 11 = 1331$$

$$11^4 = 11 \times 11 \times 11 \times 11 = 14641$$

$$11^5 = 11 \times 11 \times 11 \times 11 \times 11 = 161051 \text{ non più}$$

numero palindromo;

$$111^2 = 111 \times 111 = 12321$$

$$111^3 = 111 \times 111 \times 111 = 1367631$$

$$111^4 = 111 \times 111 \times 111 \times 111 = 151807041 \text{ non più}$$

numero palindromo;

$$1111^2 = 1111 \times 1111 = 1234321$$

$$1111^3 = 1111 \times 1111 \times 1111 = 1371330631 \text{ non più}$$

numero palindromo;

$$11111 = \dots 123\ 454\ 321$$

$$11111 = \dots 1371700960631 \quad \text{non più palindromo};$$

$$111111 = \dots 12345654321$$

$$111111 = \dots 1371737997260631 \quad \text{non più palindromo};$$

e così via, ogni numero palindromo è il quadrato (o il cubo, ma solo per 11) di un Rapunit R_n , con al centro la cifra n.

$$\text{es. per } R_9 = 111\ 111\ 111,$$

$$111111111 = 12345678987654321, \text{ ma } n \text{ deve essere al}$$

massimo 9; per $n = 10$, al centro del numero palindromo si trova si trova 00:

$$1\ 111\ 111\ 111 = 123456789\underline{00}987654321; \text{ per } n > 10, \text{ non}$$

si ottengono più numeri palindromi, quadrati di Repunit

R_n solo se $n = 10$.

Lo stesso vale in genere per la ripetizione n volte di un numero primo (originando numeri che chiameremo

Rep-primes, che però saranno tutti composti, essendo

sempre multipli di p , e di forma $p \times (10^{2n} + m)$, dove n è il numero delle cifre di p . Per esempio, il numero 37 (con 2 cifre), se ripetuto due volte, diventa 3737, multiplo di 37 in quanto $3737 / 37 = 101 = 10^2 + 1$, mentre se è ripetuto tre volte diventa $373737 = 37 \times 10101$, con $10101 = 10^4 + 101$; e se ripetuto quattro volte, diventa $37373737 = 37 \times 1010101$, con $1010101 = 10^6 + 10101$, e si ritorna al caso dei Repunit. Lo stesso, ovviamente, con qualsiasi numero primo, di qualsiasi numero di cifre, per esempio $p = 7741$ ($n =$ quattro cifre), se ripetuto due volte, abbiamo 77417741 , e $77417741 / 7741 = 10001 = 10^4 + 1$, e così via per tutti gli altri numeri primi. Per cui qualsiasi numero dispari che ripete sempre lo stesso numero primo di base (37 e 7741 nei due esempi precedenti) non può mai essere anch'esso primo, poiché è un multiplo di quest'ultimo; oltre che il numero di cifre e la somma s

delle sue cifre sono rispettivamente multipli del numero di cifre di p , e della somma s delle cifre di p , per esempio per 77417741 abbiamo $n' = 8 = 4 \times 2$, ed $s' = 38 = 19 \times 2$, essendo $n = 4$ il numero delle cifre di p e 19 la somma delle cifre di p .

Vediamo ora la tabella dei fattori di R_n , in base alle forme di $n = 6k, 6k \pm 1, 6k \pm 2, 6k \pm 3$

TABELLA 1 : FATTORI DI REPUNIT

k	$n = 6k \pm$	\dots	R_n	Fattori primi	numero dei fattori
0	2	$6k + 2$	11	11	1
0	3	$6k + 3$	111	13, 37	2
1	4	$6k - 2$	1111	11, 101	2
1	5	$6k - 1$	11111	41, 271	2
1	6	$6k$	111111	3, 7, 11, 13, 37	5
1	7	$6k + 1$	1111111	239, 4649	2
1	8	$6k + 2$	11111111	11, 73, 101, 137 2	4
1	9	$6k + 3$	111111111	3, 37, 333 667	3

2	10	$6k-2$	1111111111	11, 41, 271, 9 091	4
2	11	$6k-1$	11111111111	21 649, 513 239	2
2	12	$6k$	111111111111	3, 7, 11, 13, 37,101, 9 901	7
2	13	$6k+1$	1111111111111	53, 79, 365 371 653	3
2	14	$6k+2$	11111111111111	11, 239, 4649, 909 891	4
2	15	$6k+3$	111111111111111	3, 31, 37, 41,271, 2 906 661	6
3	16	$6k-2$...	11, 17, 73, 101, 137, 5 882 353	6
4	17	$6k-1$...	2 071 723, 5 363 222 357	2
...

Come si vede, il numero dei fattori è sempre più alto per $n = 6k+3$ multiplo di 3 e a maggior ragione anche di $n = 6k$ multiplo di 6, ma anche con $n = 6k \pm 2$ e multipli di due, si hanno pure molti fattori, per es. $n = 6k + 2 = 8$ con 4 fattori, $n = 6k - 2 = 10$ con 4 fattori, $n = 6k - 2 = 16$ con 6 fattori, ma il maggior numero di fattori si ha come si vede, per $n = 6k$: 6 con 5 fattori, 12 con 7 fattori, 18 con 8 fattori, 30 con ben 13 fattori (per $n = 18$ ed $n = 30$ vedere tabella citata qui

di seguito)

Per R_n successivi, cioè con $n \geq 17$, vedi tabella sul sito

[http://www.nationmaster.com/encyclopedia/Repunit-\(factors\)](http://www.nationmaster.com/encyclopedia/Repunit-(factors))

che dà i fattori fino a $R_n = R_{50}$ e dove si vede anche che R_{19} ed R_{23} sono primi, e anche fattori primi di R_{38} ed R_{46} , con 38 e 46 multipli di 19 e 23, e quindi, di conseguenza, anche se n è un altro multiplo k di 19 o di 23; R_{k19} ed R_{k23} avranno come fattori anche R_{19} ed R_{23} , proprio come tutti i numeri R_n con n pari sono multipli di $11 = R_2$. Si nota anche infatti che se n' è multiplo di qualche n precedente, ha anche come fattori primi, i fattori primi di R_n precedente, per esempio $R_{15} = R_{5 \times 3}$ ha anche due fattori comuni a R_5 , 41 e 271, comuni anche a $R_{10} = R_{5 \times 2}$, così come i fattori 11 e 101 di R_4 sono comuni anche a R_8 , R_{12} ed R_{16} , con $n' = 8, 12$ e 16 multipli di $n = 4$. Notiamo anche che tutti i fattori primi di R_{k5} terminano tutti con la

cifra 1, cosa logica in quanto $1 \times 1 \times 1 \dots = 1$, così come i fattori di R_n debbono terminare a due a due con le cifre 3 e 7 ($3 \times 7 = 21$, ultima cifra 1 di tutti i Repunit, oppure entrambi con la cifra 9, poichè $9 \times 9 = 81$ con cifra finale 1, per es .per R_{11} abbiamo 21649×513239 con cifra finale 9 per entrambi i fattori,; e quando i fattori sono più di due, le cifre finali 1, 3, 7, o 9, comunque ripetute o combinate tra loro, hanno sempre per prodotto un numero che termina per 1, cifra finale di tutti i Repunit.

Circa il sistema crittografico RSA, qualche numero RSA potrebbe anche essere un Repunit R_n con n primo (poiché può essere il prodotto di due numeri primi molto grande, ma si sconsiglia, come detto prima, usare numeri primi Repunit, perché già si conoscono, e sono facili da trovare.

Ora sarebbe interessante certificare la primalità dei

numeri Repunit R₄₉₀₈₁ e R₈₆₄₅₃, R₁₀₉₂₀₇ ed R₂₇₀₃₄₃ dati per probabili primi dalla voce “Repunit” di Wikipedia, che riporta anche la congettura, ancora non dimostrata, che ci siano infiniti Repunit primi (cosa possibile), ed altre varie considerazioni su tale argomento che qui per il momento non ci interessano, essendo questo piccolo lavoro dedicato soltanto alla fattorizzazione dei Repunit (e di conseguenza, dei palindromi, quadrati di Repunit, e di Repdigit, piccoli multipli k di Repunit, con $k \leq 10$).

Francesco Di Noto - Giovanni Di Maria

Caltanissetta 18.8.2008

Nota 1.

Quanto sopra può essere esteso anche a numeri non Repunit. Nei Repunit R_n , infatti, n non è altro che la somma di tutte le cifre 1 che lo compongono: se n è primo, talvolta anche R_n è primo, come nei casi di $n = 2, 23, 29$

ecc. Ciò succede anche per i numeri primi normali: se la somma di forma $6k \pm 1$ delle loro cifre è un numero primo (e quindi già non divisibile per 3 e quindi di forma $6k \pm 3$, anche il numero iniziale potrebbe essere un numero primo, o al massimo il prodotto di due numeri primi (semiprimo).

Facciamo qualche esempio:

7723 primo, somma delle cifre 19 (primo)

7817 primo, somma delle cifre 23 (primo)

7757 primo, somma delle cifre $26 = 2 \times 13$

1 183 411 primo, somma delle cifre 19 (primo)

Mentre $1\ 183\ 413 + 2 = 1183413$ con somma cifre 21 (e quindi divisibile per 3) è uguale a $3 \times 7 \times 11 \times 47 \times 109$;

$7727 \times 7793 = 60\ 216\ 511$ semiprimo, somma cifre $22 = 2 \times 11$

Quindi se per un numero N la somma delle sue cifre è un numero primo, N può essere anch'esso primo, o al massimo un semiprimo;

se invece la somma delle cifre non è divisibile per 3, può essere pari e prodotto di 2 per un numero primo, ed N può essere primo oppure un semiprimo (prodotto di due grossi numeri primi); se invece la somma delle cifre è divisibile per 3, N è prodotto di diversi fattori, tra cui ovviamente il 3 (vedi esempio per 1183413 con somma 21), o al minimo, di 3 e di un qualsiasi numero primo, per es. 23181, con somma 15 divisibile $\times 3$, è uguale a 3×7727 .

Un qualsiasi numero RSA, quindi, è un grandissimo semiprimo, (composto da qualche centinaio di cifre) prodotto di due grossi numeri primi; e in tutti e tre i numeri la somma delle cifre dovrà necessariamente essere o un numero primo, o il doppio di un numero primo, ma mai un multiplo di 3. Infine, notiamo che se la somma cifre è $s = 6k-1$, (oppure $6k+1$) lo è anche il numero primo N: per esempio $7727 = 1288 \times 6 - 1$, e anche la sua somma cifre $s = 7 + 7 + 2 + 7 = 23$, è della stessa forma, $6 \times 4 - 1 = 23$. Non sappiamo ancora se R_{270343} è primo, ma in base a quanto sopra possiamo già sapere che è di forma $6k+1$, poiché lo è anche

la forma della somma s delle sue cifre,

$$s = 2 + 7 + 0 + 3 + 4 + 3 = 19 \text{ che è di forma } 19 = 6 \times 3 + 1$$

(possiamo chiamare questa relazione “legge di conservazione

della forma aritmetica $s = 6k \pm 1$ ”, che si conserva anche per

R_2 (2 però non di forma $6k + 1$, ma $6 \times 0 + 2$, unica

eccezione), R_{19} di forma $6k + 1$, R_{23} di forma $6k - 1$, R_{317} di

forma $6k - 1$, R_{1031} di forma $6k - 1$, primi, e tutti i rimanenti

probabili primi, poiché lo sono anche la somma s della cifra 1

ripetuta n volte, e cioè :

$$19 = 6 \times 3 + 1, \quad 23 = 6 \times 4 - 1, \quad 29 = 6 \times 5 - 1, \quad 317 = 6 \times 53 - 1,$$

$$1031 = 6 \times 172 - 1.$$

Tutto ciò potrebbe, in futuro, e se studiato bene a fondo,

contribuire ad una migliore conoscenza dei numeri primi, della

loro distribuzione, e quindi potrebbe aiutare a risolvere problemi

non ancora risolti, come la congettura di Riemann, basati proprio

sulla distribuzione dei numeri primi.

Nota 2.

Si potrebbe scoprire ancora qualcosa facendo la somma cifre s di tutti i primi consecutivi p , cioè osservando l'andamento della funzione $s = \text{somma cifre di } p$

TABELLA 2

(legge di conservazione della forma e del segno per p ed s)

<u>p</u>	<u>s</u>	<u>s = primo</u>	
2	2	si	
3	3	si	
5	5	si	
7	7	si	
11	2	si	$2 = 3 - 1$, si conserva il segno - di $6 \times 2 - 1$
13	4	no	$4 = 3 + 1$, si conserva il segno + di $6 \times 2 + 1$
17	8	no	$8 = 9 - 1 = 3m - 1$, si conserva il segno -
19	10	no	$= 2 \times 5$
23	5	si	
29	11	si	
31	4	no	$4 = 3 + 1$, si conserva il segno +
37	10	no	$= 2 \times 5$; $10 = 9 + 1$, si conserva il segno +
41	5	si	
43	7...	si	
47	11	si	
57	13	si	
61	7	si	
67	13	si	

71	8	no	$8 = 9 - 1$, si conserva il segno -
73	10	no	$= 2 \times 5$; $10 = 9 + 1$, si conserva il segno +
79	16	no	$16 = 15 + 1$, si conserva il segno +
83	11	si	
89	17	si	
97	16	no	$16 = 15 + 1$, si conserva il segno +
101	2	si	$2 = 3 - 1$, si conserva il segno - di $6 \times 17 - 1$
103	4	no	$4 = 3 + 1$, si conserva il segno -
107	8	no
109	10	no	$= 2 \times 5$...
113	4	no	...
127	10	no	$= 2 \times 5$...
131	4	no	---
137	11	si	
139	13	si	

... ..

(quando s è primo, p ed s hanno la stessa forma $6k - 1$

oppure $6k + 1$); quando s è di forma 2^n , $s = 3m - 1$ ed $s = 3m + 1$

conservano il segno algebrico di $p = 6k \pm 1$): questa è la legge di

conservazione del segno da parte di $s = p$ oppure di forma $s = 2^n$,

da noi scoperta.

Al crescere di p , cresce discontinuamente anche s , anche se spesso ricomincia da 2; ma ad ogni ripetizione di numeri bassi, si

aggiunge qualche nuovo $s =$ numero primo più grande; s molto

spesso è anche una potenza di 2: $2, 4, 8, 16$, ecc., di forma 2^n : $2, 4, 6$

$2^n = 3m - 1$ (se n è pari), per es. $2^2, 2^4, 2^6 \dots$ oppure $3m + 1$ (se n è

dispari), per es. $2^1, 2^3, 2^5 \dots$ che, rispettivamente -1 e $+1$ danno multipli di 3 , con -1 e $+1$ il segno di p ed $s = 6k - 1$ e $+1$ per la legge di conservazione del segno.

I numeri primi (contrassegnati con “si”) hanno comunque sempre la maggioranza sui composti (contrassegnati con “no”).

Nota 3.

Connessione con i primi ostinati e con le “perle di numeri primi”
(Vedi Lavori del Prof. Di Maria)

La funzione s vale ovviamente anche per i numeri primi ostinati, e per le “perle” di numeri primi, ed è più facile calcolarla (e determinare anche la forma aritmetica di tali numeri, uguale alla forma di s).

Nel primo caso, un primo ostinato è formato da un numero primo di due cifre accostato ad un altro numero primi (o altri numeri

primi) di due cifre, e il numero risultante è anch'esso primo.

Esempi:

11 di forma $6 \times 1 - 1$, con $s = 1 + 1 = 2 = 2 - 3 = -1$

1117 di forma $6 \times 186 + 1$, e con $s = 10 = 10 - 9 = +1$

111773 di forma $6 \times 18629 - 1$ e con $s = 20 = 20 - 21 = -1$

11177359 di forma $6k + 1$ con somma $s = 34 = 34 - 33 = +1$

... ..

11177359794179 ... con somma $s = 71 = 71 - 72 = -1$

ma anche $7 + 1 = 8 = s - 3m = 8 - 9 = -1$, che conserva il segno
—

di $71 - 72 = -1$, e anche di $71 = 6 \times 12 - 1$.

Come si vede il segno viene conservato nella somma $s - 3m$, che

può essere -1 oppure $+1$, determinabile anche tramite la

somma s senza calcolare $k = (N \pm 1) / 6$, calcolo molto po'

laborioso lungo per N di tipo "perle" molto lunghi.

Nel secondo caso, facciamo un solo esempio: un primo "perla" è,

per esempio, il numero segnato come N°1, di 7809 cifre (

ripetizioni di 12, più l' 1 finale; per calcolarne la somma cifre s, basta moltiplicare $7\ 808 \times 12 = 93\ 696$, al quale aggiungere la cifra finale 1, per cui $93\ 696 + 1 = 93\ 697$; calcolando la somma cifre di questo numero, abbiamo $9 + 3 + 6 + 9 + 7 = 34$, e ancora $3 + 4 = 7$ di forma $6k + 1 = 6 \times 1 + 1 = 6 + 1 = 7$, e $6k + 1$ è anche la forma del suddetto numero ostinato, per via della legge di conservazione della forma sia per p che per s. Oppure calcolando la somma s solo per 12 (il numero ripetuto)

$s = 1 + 2 = 3$, più la cifra finale 1 e abbiamo 4, che è uguale a $3 + 1$, e quindi conserva il segno (legge di conservazione del segno). Stesso procedimento per gli altri numeri ostinati, per es.

quello contrassegnato con il N° 2, ripetizione della sequenza

12345678 più la sequenza parziale finale 1234567:

somma s di 12345678 = $1+2+3+4+5+6+7+8 = 36$

che si può eliminare perché multiplo di 3;

somma s di 1234567 = $1+2+3+4+5+6+7 = 28$

$36+28 = 64$; $6+4 = 10$, $10 = 9+1$, ma anche $28 - 3m = 28 - 27 = +1$

quindi Numero 2° ostinato è pure di forma $6k + 1$, per la legge di conservazione della forma e quindi anche del segno – oppure + per p ed s, legge che potrebbe eventualmente servire per ulteriori teoremi su questi argomenti, per es. per abbreviare calcoli, ecc..

FINE