Pseudoprimalitá dei Repunit

Rosario Turco e Gabriele Di Pietro

24 ottobre 2010

1 Sommario

2 Introduzione

Un numero di Carmichael é un numero composto dispari n che soddisfa il piccolo teorema di Fermat

$$a^{n-1} \equiv 1 \; mod \; n \tag{1}$$

per ogni a relativamente primo con n cioé $(a, n) = 1$ con $1 < a < n$. In questo senso un numero di Carmichael é uno pseudoprimo per qualche base. L'unico modo per individuare che esso é composto consiste nel calcolare la (1) con $(a, n) \neq 1$ quindi nel trovare una base che permetta la fattorizzazione del numero stesso.
Una maniera per trovare numeri di Carmichael é quella di studiare la funzione $\lambda(n)$ detta funzione lambda di Carmichael.

Definizione 2.1 *La funzione lambda di Carmichael é il piú piccolo intero* $\lambda(n)$ *tale che* $k^{\lambda(n)} \equiv 1$ *mod* n *per tutti i* k *relativamente primi con* n. $\lambda(n)$ *é anche l'esponente del gruppo moltiplicativo* Z_n.

Essa si puó calcolare in maniera recursiva nel seguente modo

$$\begin{cases} \lambda(1) = 1 \\ \lambda(2) = 1 \\ \lambda(2^2) = 2 \\ \lambda(2^e) = 2^{e-2} \qquad e > 2 \\ \lambda(p^e) = (p-1)p^{e-1} \qquad p > 2 \; e \; primo \\ \lambda(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}) = lcm[\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \dots, \lambda(p_k^{e_k}))] \end{cases} \tag{2}$$

oppure utilizzando la funzione totiente $\phi(n)$

$$\lambda(n) = \begin{cases} \phi(n) \qquad n = p^\alpha \; con \; p = 2 \; e \; n \leq 2 \; oppure \; p > 2 \\ \phi(n)/2 \qquad n = 2^\alpha \; con \; \alpha \geq 3 \\ lcm[\lambda(p_i)^{\alpha_i}]_j \qquad n = \prod_j p_i^{\alpha_i} \end{cases} \tag{3}$$

dove lcm é il minimo comune multiplo.Per comoditá definiamo anche la funzione $\lambda_1(n)$ che utilizzeremo nella trattazione seguente

Definizione 2.2 *La funzione* $\lambda_1(n) = lcm(p_1 - 1, p_2 - 1, \dots, p_k - 1)$ *dove* $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$

da non confondere con la funzione $\lambda'(n)$ che nella letteratura é il minimo comune multiplo di tutti i fattori della funzione totiente $\phi(n)$.
Grazie a queste definizioni un numero di Carmichael n é tale che la sua funzione $\lambda(n)$ divide $n-1$ poiché in questo modo si verifica il piccolo teorema di Fermat (1); divide ma non é $n-1$ visto che solo per un numero primo $\lambda(n) = n - 1$.
Chiaramente $\lambda_1(n) | \lambda(n)$ quindi una condizione necessaria ma non sufficiente per cui un numero n sia di Carmichael é che $\lambda_1(n) | (n-1)$
Un numero Repunit é un numero composto da varie copie del singolo digit 1. In base 10 esso ha la forma

$$R_n = \frac{10^n - 1}{10 - 1} = \frac{10^n - 1}{9} \tag{4}$$

quindi n ci fornisce il numero di digit 1 di cui é composto il numero; in generale il discorso é valido per qualsiasi base b in questo caso il Repunit diventa

$$R_n^b = \frac{b^n - 1}{b - 1} \tag{5}$$

Una lista di probabili primi Repunit per giganteschi n é data dalla seguente tabella

n	scopritori	data
49081	H.Dubner	9 settembre 1999
86453	L.Baxter	26 ottobre 2000
109297	P.Bourdelais, H.Dubner	26-28 marzo 2007
270343	M.Voznyy and A. Budnyy	11 luglio 2007

essi soddisfano il piccolo teorema di Fermat, ma potrebbero essere in realtá numeri di Carmichael. Lo scopo di questo articolo é escludere questa ipotesi ed utilizzare i risultati ottenuti per estenderli anche ad altri pseudoprimi.
Poiché inoltre ci interessano solamente i Repunit che possono essere primi ci sará utile il seguente teorema di cui omettiamo la dimostrazione

Teorema 2.3 *Condizione necessaria ma non sufficiente affinchè R_n in base 10 sia primo e che n sia primo*

Per i Repunit in base 10 valgono inoltre le seguenti proprietá:

1. $\lambda(R_n) = \lambda_1(R_n)$
2. $\lambda(R_n) = \lambda(\frac{10^n-1}{9}) = \lambda(10^n - 1)$ oppure $\lambda(R_n) = \frac{\lambda(10^n-1)}{3}$
3. $\lambda_1(R_n) = \lambda_1(10^n - 1)$

3 Repunit-Carmichael un confronto diretto

Dalla sezione precedente la prima equazione che deve essere soddisfatta da un Carmichael- Repunit in base 10, se esiste, é

$$\frac{10^n - 1}{9} = k\lambda(n') + 1 \tag{6}$$

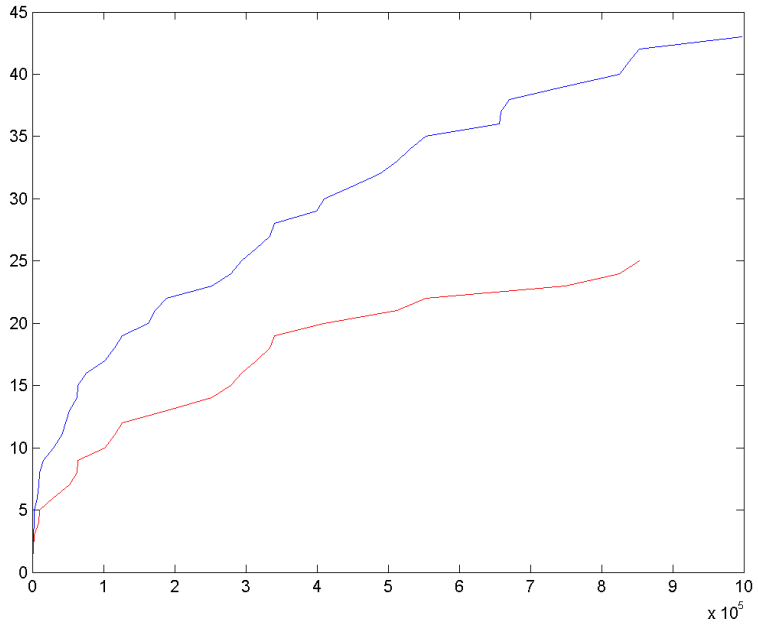
infatti se n' é di Carmichael allora $\lambda(n')|(n' - 1)$ quindi esiste un k tale che $n' = k\lambda(n') + 1$. Sviluppando la (6) otteniamo

$$k\lambda(n') = \frac{10^n - 1}{9} - 1 = \frac{10^n - 10}{9} = \frac{10(10^{n-1} - 1)}{9} = 10R_{n-1} \tag{7}$$

Ora alcune osservazioni ci permettono di dedurre quali siano i possibili valori di $\lambda(n')$

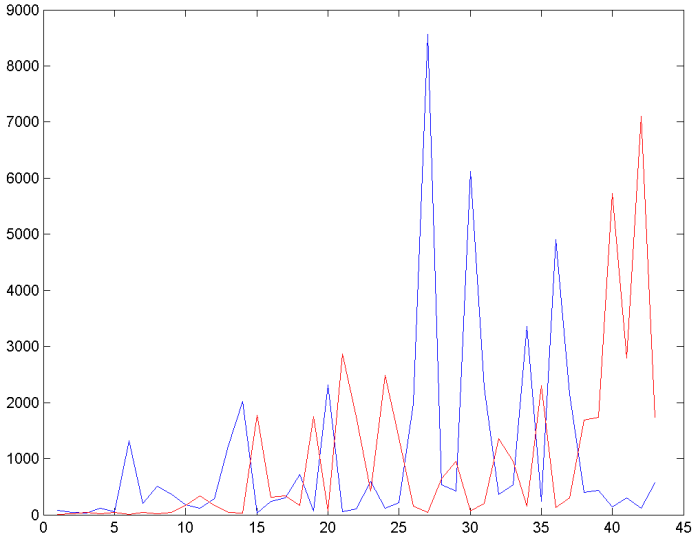
- R_{n-1} non contiene come fattori 2 e 5 poiché altrimenti il Repunit finirebbe con uno zero
- $\lambda(n')$ é pari (tranne alcuni casi banali) osservando la definizione recursiva poiché é il minimo comune multiplo di pari($p_i - 1$ dove p_i é primo e diverso da 2)

Quindi $\lambda(n')$ contiene sicuramente il numero 2 mentre k deve essere dispari visto che il 2 puó comparire una sola volta. Lo stesso discorso vale per il 5 puó essere contenuto una sola volta o da k o da $\lambda(n')$ e se avessimo maggiori informazioni sulla fattorizzazione di un Repunit potremmo enunciare altre condizioni necessarie. Necessarie, ma non sufficienti visto che implicitamente la vera condizione selezionante é che fissato k o fissato $\lambda(n')$ bisogna scegliere l'altro tale che si ottenga un Carmichael.
Giusto per avere un idea grafica possiamo costruire la funzione che al crescere di n' ci fornisce la frequenza con la quale le condizioni sul 2 e sul 5 vengono soddisfatte dai numeri di Carmichael



In blu la funzione che enumera i carmichael minori di 1 milione
In rosso i Carmichael che devono verificare le condizioni sul 2 e sul 5

Disegnamo inoltre anche la funzione λ e i suoi relativi k.



In blu la funzione λ per i Carmichael minori di 1 milione
In rosso il relativo valore di k

4 Primalitá dei Repunit

Passiamo adesso alla vera e propria dimostrazione della primalitá dei Repunit, cioé il fatto che essi non possono essere numeri di Carmichael. Ricordiamo dalla definizione della funzione λ e da quanto detto nell'introduzione che un numero n per essere di Carmichael deve verificare $\lambda(n)|(n-1)$. Poiché $\lambda_1(n)|\lambda(n)$ un'altra condizione necessaria é che $\lambda_1(n)|(n-1)$.

Teorema 4.1 *I Repunit R_n in base 10 composti, con n primo, hanno $\lambda_1(R_n)$ che non divide $R_n - 1$ quindi non possono essere numeri di Carmichael.*

Dimostrazione:
Consideriamo un Repunit R_n in base 10 composto quindi

$$R_n = \frac{10^n - 1}{9} = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \tag{8}$$

dove p_i $\forall i \in [1, k]$ sono tutti primi dispari visto che un Repunit in base 10 é sempre dispari ed in questo caso

$$\lambda_1(R_n) = lcm(p_1 - 1, p_2 - 1, \dots, p_k - 1) \tag{9}$$

é pari visto che é il minimo comune multiplo di numeri pari .Quindi possiamo scrivere $\lambda_1(R_n) = 2^k m$ per qualche intero m e qualche intero $k \geq 2$ infatti, per

la precisione, essendo tutti i $p_i - 1$ pari ($\forall i = [1, \ldots, k]$) essi contengono almeno un 2, quindi il numero di 2 del minimo comune multiplo é almeno pari al numero dei fattori p_i. In un Repunit composto i fattori sono almeno 2 (altrimenti non sarebbe composto) quindi $k \geq 2$.
Calcoliamo adesso

$$R_n - 1 = \frac{10^n - 1}{9} - 1 = \frac{10(10^n - 1)}{9} = 10R_{n-1} \tag{10}$$

dove chiaramente R_{n-1} é dispari. A questo punto se ci calcoliamo

$$\frac{R_n - 1}{\lambda_1(R_n)} = \frac{10R_{n-1}}{2^k m} = \frac{5R_{n-1}}{2^{k-1} m} \tag{11}$$

quindi essendo il numeratore dispari $\lambda_1(R_n) \not| R_n - 1$
$\diamond$
Naturalmente nel caso in cui un Repunit sia primo $\lambda_1(R_n)|(n-1)$ escludendo il Teorema 4.1 ed il Lemma 4.3 successivo.

Definizione 4.2 *Dato un primo p ed un generatore b del gruppo ciclico Z_p definiamo l'indice di a modulo p, indp(a), il piú piccolo intero m tale che*

$$b^m \equiv a \ mod \ p \tag{12}$$

quindi $indp(a) = m$.

Lemma 4.3 *Se $\lambda_1(n)$ non divide $n-1$, allora esistono due primi p e q tali che*

1. $p|n$
2. $p - 1 \not| (n - 1)$
3. $q^m|(p - 1)$
4. $q^m \not| (n - 1)$
5. *Se a non é il residuo q-esimo mod p allora $a^{n-1} \not\equiv 1 \ mod \ n$*

Dimostrazione.
Per il teorema fondamentale dell'aritmetica $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ dove i p_i $i \in [1, k]$ sono primi ed $e_i \in N$.
Se $\lambda_1(n)$ non divide $n - 1$ significa che $lcm(p_1 - 1, p_2 - 1, \ldots, p_k - 1) \not| (n - 1)$ quindi esiste i tale che $p_i - 1 \not|(n - 1)$. Ponendo $p = p_i$ abbiamo verificato la 1) e la 2).
Poiché per il punto 2) $p-1 \not|(n-1)$ per il teorema fondamentale dell'aritmetica esiste un intero m ed un q primo tale $q^m|(p-1)$ ma $q^m \not|(n-1)$. Questo significa che $p - 1$ non é *square free* soddisfando la 3) e la 4).
Supponiamo per assurdo che $a^{n-1} \equiv 1 \ mod \ n$, poiché dalla 1) $p|n$ allora é anche

$$a^{n-1} \equiv 1 \ mod \ p \tag{13}$$

se inoltre b é il generatore di un gruppo ciclico Z_p per la (12) abbiamo

$$b^{indp(a)} \equiv a \ mod \ p \tag{14}$$

mettendo insieme la (13) e la (14) otteniamo

$$b^{indp(a)(n-1)} \equiv 1 \ mod \ p \tag{15}$$

Ma Z_p ha ordine $p-1$ quindi $p-1|indp(a)(n-1)$. Ora affinché a non sia i q-esimo residuo modulo p, q non deve essere un divisore di $indp(a)$. Infatti se cosí non fosse si ha $indp(a) = ql$ per qualche l cosí $b^{ql} \equiv a \ mod \ p$ e quindi $(b^l)^q \equiv a \ mod \ p$, ma cosí a é il residuo q-esimo modulo p giungendo ad una contraddizione.
Poiché $q^m|(p-1)$ significa che $q^m|indp(a)(n-1)$ e quindi poiché $q \not| \ indp(a)$ allora $q^m|(n-1)$. Ma questo contraddice la 4)che abbiamo giá dimostrato quindi anche il punto 5) é vero.
$\diamond$

Corollario 4.4 *Un Repunit in base 10 composto possiede almeno un non residuo q-esimo modulo p per p e q definiti dal lemma precedente.*

Dimostrazione:
Utilizzando il Teorema 4.1 ed il lemma 4.3 i Repunit in base 10 non essendo di Carmicheal devono possedere un a che non verifica il piccolo teorema di Fermat cioé

$$a^{R_n-1} \not\equiv \ 1 \ mod \ R_n. \tag{16}$$

Utilizzando il punto 5) del lemma 4.3 questo a non puó essere un residuo q-esimo per i p e q del lemma 4.3.
$\diamond$
Seguendo la dimostrazione del teorema 4.1 é inoltre possibile fornire una versione generalizzata ad un qualsiasi Repunit in base b.

Teorema 4.5 *Sia R_n^b un Repunit composto in base b secondo la definizione (5). Dato $\lambda_1(R_n^b) = 2^k n$ per qualche $k \geq 2$ ed un intero dispari n se $b = 2^i m$ per qualche intero $i \geq 1$ ed m dispari tale che $i < k$ oppure se b é dispari e $R_{n-1}^b = 2^j v$ per qualche intero $j \geq 0$ e v dispari tale che $j < k$ allora il Repunit non é un Carmichael.*

Dimostrazione.
Seguendo la dimostrazione del teorema 4.1 si puó affermare che esiste $k \geq 2$ tale che $\lambda_1(R_n^b) = 2^k m$. A questo punto basta calcolare la quantitá

$$R_{n-1}^b = \frac{b^n - 1}{b-1} - 1 = \frac{b^n - b}{b-1} = bR_{n-1}^b \tag{17}$$

Come prima esaminiamo il rapporto ed otteniamo

$$\frac{R_n^b - 1}{\lambda_1(R_n^b)} = \frac{bR_{n-1}^b}{\lambda_1(R_n^b)} = \frac{bR_{n-1}^b}{2^k m}. \tag{18}$$

A questo punto bisogna riflettere sulla paritá del numeratore e distinguere i vari casi. Se b é pari allora R_n^b e R_{n-1}^b sono dispari perché si ottengono per definizione dal rapporto di numeri dispari $b-1$, b^n-1 e $b^{n-1}-1$; quindi possiamo scrivere $b = 2^i m$ per qualche intero $i \geq 1$ ed m dispari. Se b é dispari R_n^b potrebbe essere dispari oppure no tutto dipende dal numero di 2 presenti nel rapporto $\frac{b^n-1}{b-1}$. In ogni caso anche R_{n-1}^b potrebbe essere o pari o dispari quindi possiamo in generale scrivere $R_{n-1}^b = 2^j v$ per qualche intero $j \geq 0$ e v dispari. In entrambi i casi se vengono rispettate le condizioni $i < k$ e $j < k$, dopo la semplificazione il denominatore rimane con qualche 2 quindi é pari mentre il numeratore é dispari quindi $\lambda_1(R_n^b) \not| (R_n^b - 1)$ dichiarando l'impossibilitá di essere un Carmichael.
$\diamond$
Nel teorema 4.1 $b = 10$ quindi $i = 1$ e siccome $k \geq 2$ allora sicuramente non é un Carmichael.
Uno pseudoprimo forte di Fibonacci, grazie agli studi di Müller e Oswald, ha la proprietá di essere un Carmichael. Il teorema precedente ci permette di affermare il seguente corollario.

Corollario 4.6 *Un Repunit composto in base b nelle condizioni del teorema 4.5 non puó essere uno pseudoprimo forte di Fibonacci*

Definizione 4.7 *Uno pseudoprimo di Eulero in base c é un numero n che soddisfa*

$$c^{\frac{(n-1)}{2}} \equiv \pm 1 \ mod \ n \tag{19}$$

Definizione 4.8 *Uno pseudoprimo di Eulero-Jacobi in base c é un numero n che soddisfa*

$$c^{\frac{n-1}{2}} \equiv \left(\frac{c}{n}\right) \ mod \ n \tag{20}$$

dove $\left(\frac{c}{n}\right)$ *é il simbolo di Jacobi.*

Teorema 4.9 *Un Repunit* R_n^b *composto che soddisfa le condizioni del teorema 4.5 non puó essere uno pseudoprimo di Eulero o uno pseudoprimo di Eulero-Jacobi per qualche base c tale che* $(c, R_n^b) = 1$

Dimostrazione.
Dal teorema 4.5 un Repunit composto non puó essere un numero di Carmichael quindi esiste una base c tale che $(c, R_n^b) = 1$ che non verifica il piccolo teorema di Fermat

$$c^{R_n^b - 1} \not\equiv 1 \ mod \ R_n^b \tag{21}$$

Questo seguiva dal fatto che $\lambda_1(R_n^b) \not| \ (R_n^b - 1)$, ma a maggior ragione $\lambda_1(R_n^b) \not| \ \frac{R_n^b - 1}{2}$ quindi per la stessa base c vale anche

$$c^{\frac{R_n^b - 1}{2}} \not\equiv 1 \ mod \ R_n^b \tag{22}$$

Se adesso per assurdo

$$c^{\frac{R_n^b-1}{2}} \equiv -1 \; mod \; R_n^b \tag{23}$$

elevando al quadrato otteniamo

$$c^{R_n^b-1} \equiv 1 \; mod \; R_n^b \tag{24}$$

contraddicendo la (22).
Un altro modo diretto per verificare che non é uno pseudoprimo di Eulero é osservare che

$$c^{\frac{R_n^b-1}{2}} c^{\frac{R_n^b-1}{2}} = c^{R_n^b-1} \not\equiv 1 \; mod \; R_n^b \tag{25}$$

da cui l'impossibilitá del termine $c^{\frac{R_n^b-1}{2}}$ di poter essere congruente a 1 o -1.
Per definizione il simbolo di Jacobi é data dalla produttoria dei simboli di Legendre quindi puó assumere i valori $1, -1$ e 0. Abbiamo giá dimostrato che per i valori 1 e -1 il Repunit non verifica la (24). Ora rimane da dimostrare che

$$c^{\frac{R_n^b-1}{2}} \not\equiv 0 \; mod \; R_n^b \tag{26}$$

Se per assurdo (28) non fosse vera avremmo che $R_n^b | c^{(R_n^b-1)/2}$, ma $(c, R_n^b) = 1$ quindi non contiene fattori di R_n^b e non puó essere diviso da esso.
$\diamond$

5 Alcuni esempi

In questa sezione proponiamo una carrellata di esempi che esplicano i risultati ottenuti nel capitolo precedente.
Iniziamo con un Repunit in base $b = 20 = 2^2 5$. Cerchiamo di valutare se per $n = 4$ digit verifica il teorema 4.5. Essendo b pari sicuramente R_n^b e R_{n-1}^b sono dispari quindi non dobbiamo preoccuparci di essi. Calcolando si ha $\lambda_1(R_n^b) = 1200 = 2^4 5^2 3$ in questo caso $i = 2 < k = 4$ quindi ci troviamo nelle ipotesi del teorema 4.5, quindi il Repunit non puó essere un Carmichael.
Esiste quindi una base per cui il Repunit non é di Eulero ne di Eulero-Jacobi. Per trovarla calcoliamoci alcuni residui come verrá mostrato nell'esempio successivo ed utilizziamo il lemma 4.3.
Le coppie che verificano il lemma sono $q = 2$, $p = 401$ e $q = 5$, $p = 401$ ed il numero 3 non compare nelle due liste quindi sicuramente $a = 3$ non verifica la (1). Inoltre $R_n^b = 8421$ da cui

$$3^{8420/2} \equiv 7116 \; mod \; 8421 \tag{27}$$

quindi non é un numero di Eulero o Eulero-Jacobi in base 3.
La seguente tabella invece mostra per vari digit n di Repunit in base 10 il relativo $\lambda_1(R_n)$ ed il resto che si ottiene da $\frac{R_n-1}{\lambda_1(R_n)}$

digit di R_n	$\lambda_1(R_n)$	$resto$	$factor(R_n)$
2	10	0	11 (primo)
3	36	2	$3 \cdot 37$
4	100	10	$11 \cdot 101$
5	1080	310	$41 \cdot 271$
6	180	50	$3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$
7	79016	4886	$239 \cdot 4649$
8	30600	3311	$11 \cdot 73 \cdot 101 \cdot 137$
9	667332	333998	$3 \cdot 3 \cdot 37 \cdot 333667$
10	109080	22230	$11 \cdot 41 \cdot 271 \cdot 9091$
11	12317712	534886	$21649 \cdot 513239$
12	9900	5510	$3 \cdot 7 \cdot 11 \cdot 13 \cdot$ $\cdot 37 \cdot 101 \cdot 9901$
13	796114956	530747490	$53 \cdot 79 \cdot 265371653$
14	5130903960	2704037710	$11 \cdot 239 \cdot 4649 \cdot 909091$
15	26155440	3359030	$3 \cdot 31 \cdot 37 \cdot 41 \cdot$ $\cdot 271 \cdot 2906161$
16	7499998800	1288888710	$11 \cdot 17 \cdot 73 \cdot 101 \cdot$ $\cdot 137 \cdot 5882353$
17	326797227818148	5365294078	$2071723 \cdot 5363222357$
18	9746383860	5721368570	$3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot$ $\cdot 37 \cdot 52579 \cdot 333667$
19	$R_n - 1$	0	R_n (primo)
20	7497613800	4809600910	$11 \cdot 41 \cdot 101 \cdot 271 \cdot$ $3541 \cdot 9091 \cdot 27961$
21	1055243824992	825715740134	$3 \cdot 37 \cdot 43 \cdot 239 \cdot 1933 \cdot$ $\cdot 4649 \cdot 10838689$
22	253929632880	198026063190	$11^2 \cdot 23 \cdot 4093 \cdot 8779 \cdot$ $\cdot 21649 \cdot 513239$
23	$R_n - 1$	0	R_n (primo)
24	1699830000	955461110	$3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot$ $\cdot 73 \cdot 101 \cdot 137 \cdot 9901 \cdot$ $\cdot 99990001$
25	67494884397696000	64933811109319110	$41 \cdot 271 \cdot 21401 \cdot 25601 \cdot$ $\cdot 182521213001$
26	297048951989429640	111778679247214990	$11 \cdot 53 \cdot 79 \cdot 859 \cdot$ $\cdot 265371653 \cdot 1058313049$
27	38091589646193660780	1059005097073533230	$3^3 \cdot 37 \cdot 757 \cdot$ $\cdot 333667 \cdot 440334654777631$
28	18553630919077800	14345027772130710	$11 \cdot 29 \cdot 101 \cdot 239 \cdot 281 \cdot 4649 \cdot$ $\cdot 909091 \cdot 121499449$
29	490722978939462772580	464826702870565344870	$3191 \cdot 16763 \cdot 43037 \cdot$ $\cdot 62003 \cdot 77843839397$
30	18491896080	16027574870	$3 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 37 \cdot$ $\cdot 41 \cdot 211 \cdot 241 \cdot 271 \cdot 2161 \cdot$ $\cdot 9091 \cdot 2906161$

Diamo ora qualche esempio per il corollario 4.4.
Consideriamo il Repunit a 3 digit $R_n = 111$ che é composto. In particolare $111 = 3 \cdot 37$ cosí ad esempio abbiamo $p = 37$ e $q = 3$ che soddisfano il lemma 4.3 infatti $p|R_n$, $(p-1) \nmid (R_n - 1)$,$q^2|(p-1)$ e $q^2 \nmid (R_n - 1)$; oppure $p = 37$ e $q = 2$. Per la prima coppia i residui q-esimi sono dati da

$$1\ 8\ 27\ 27\ 14\ 31\ 10\ 31\ 26\ 1\ 36\ 26\ 14\ 6\ 8\ 26\ 29\ 23$$
$$14\ 8\ 11\ 29\ 31\ 23\ 11\ 1\ 36\ 11\ 6\ 27\ 6\ 23\ 10\ 10\ 29\ 36\ 0$$

mentre per la seconda coppia da

$$1\ 4\ 9\ 16\ 25\ 36\ 12\ 27\ 7\ 26\ 10\ 33\ 21\ 11\ 3\ 34\ 30\ 28$$
$$28\ 30\ 34\ 3\ 11\ 21\ 33\ 10\ 26\ 7\ 27\ 12\ 36\ 25\ 16\ 9\ 4\ 1\ 0$$

In entrambe le sequenze di residui non compaiono i numeri $2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35$, ma tra questi possiamo prendere solo quelli coprimi con $R_n = 111$. Essi sono $2, 5, 13, 17, 19, 20, 22, 32, 35$ che per il corollario 4.4 non verificano la (16).
Consideriamo il Repunit a 4 digit $R_n = 1111 = 11 \cdot 101$ .La prima coppia accettabile é $p = 101$ e $q = 2$ infatti in questo caso $p|R_n$, $(p-1) \nmid (R_n - 1)$, $q^2|(p-1)$ e $q^2 \nmid (R_n - 1)$. La seconda é $p = 101$ e $q = 5$; i residui q-esimi sono

$$1\ 4\ 9\ 16\ 25\ 36\ 49\ 64\ 81\ 100\ 20\ 43\ 68\ 95\ 23\ 54\ 87\ 21\ 58\ 97\ 37\ 80\ 24\ 71\ 19\ 70$$
$$22\ 77\ 33\ 92\ 52\ 14\ 79\ 45\ 13\ 84\ 56\ 30\ 6\ 85\ 65\ 47\ 31\ 17\ 5\ 96\ 88\ 82\ 78\ 76\ 76\ 78\ 82$$
$$88\ 96\ 5\ 17\ 31\ 47\ 65\ 85\ 6\ 30\ 56\ 84\ 13\ 45\ 79\ 14\ 52\ 92\ 33\ 77\ 22\ 70\ 19\ 71\ 24\ 80\ 37$$
$$97\ 58\ 21\ 87\ 54\ 23\ 95\ 68\ 43\ 20\ 100\ 81\ 64\ 49\ 36\ 25\ 16\ 9\ 4\ 1\ 0$$

e

$$1\ 32\ 41\ 14\ 95\ 100\ 41\ 44\ 65\ 10\ 57\ 69\ 17\ 100\ 57\ 95\ 100\ 60\ 84\ 17\ 65\ 6\ 17\ 87\ 36\ 39$$
$$39\ 69\ 69\ 6\ 95\ 10\ 14\ 69\ 57\ 1\ 84\ 62\ 91\ 39\ 10\ 60\ 14\ 91\ 14\ 39\ 65\ 57\ 65\ 41\ 60\ 36\ 44$$
$$36\ 62\ 87\ 10\ 87\ 41\ 91\ 62\ 10\ 39\ 17\ 100\ 44\ 32\ 87\ 91\ 6\ 95\ 32\ 32\ 62\ 62\ 65\ 14\ 84\ 95$$
$$36\ 84\ 17\ 41\ 1\ 6\ 44\ 1\ 84\ 32\ 44\ 91\ 36\ 57\ 60\ 1\ 6\ 87\ 60\ 69\ 100\ 0$$

I numeri che non compaiono nelle due liste sono $2, 3, 7, 8, 11, 12, 15, 18, 26, 27, 28, 29, 34, 35, 38, 40, 42, 46, 48, 50, 51, 53, 55, 59, 61, 63, 66, 67, 72, 73, 74, 75, 83, 86, 89, 90, 93, 94, 98, 99$ e tra questi devo considerare solo i numeri coprimi con R_n quindi dalla lista precedente dobbiamo scartare $11, 66, 99$.
La lista rimanente non soddisfa il piccolo teorema di Fermat come assicurato dal corollario 4.4.

6 Software utilizzato

Per quanto riguarda il software utilizzato quí di seguito vengono riportati dei programmi scritti in Matlab e Pari/Gp.

6.1 carmichael.m

```
function [y,vettlamb,thek]=carmichael(inizio,fine)
y=[];
vettlamb=[];
thek=[];
for k=inizio:fine
j=mod(k-1,lambda(k));
l=isprime(k);
p=(k-1)/lambda(k);
if j==0 & l==0
y=[y,k];
vettlamb=[vettlamb,lambda(k)];
thek=[thek,p];
end
end
```

La funzione carmichael.m restituisce tutti i numeri di Carmichael compresi tra i due parametri inizio e fine memorizzandoli nel vettore y. Calcola anche λ del numero di Carmichael e il relativo valore da assegnare a k.

6.2 lambda.m

```
function mcm=lambda(n)
vettore=factor(n);
maxind=length(vettore);
 indice=1;
temp=[];
while indice<=maxind
contatore=1;
while indice<maxind & vettore(indice)==vettore(indice+1)
contatore=contatore+1;
indice=indice+1;
end
if vettore(indice)==2 & contatore>2
temp=[temp,totient(2^contatore)/2];
else
temp=[temp,totient(vettore(indice)^contatore)];
end
indice=indice+1;
end
lunghezza=length(temp);
mcm=1;
for j=1:lunghezza
mcm=lcm(mcm,temp(j));
end
```

La funzione lambda.m restituisce il valore $\lambda(n)$ di un numero n utilizzando la definizione ricorsiva (3) dove compare la funzione totiente.

6.3 totient.m

```
function o=totient(n)
f=factor(n);
k=1;
l=length(f);
p=ones(2,l);
p(1,k)=f(1);
for j=2:l;
if f(j)~=f(j-1)
k=k+1;
p(1,k)=f(j);
else
p(2,k)=p(2,k)+1;
end
end
o=1;
for j=1:k
o=o*(p(1,j)-1)*p(1,j)^(p(2,j)-1);
end
```

La funzione totient.m restituisce la funzione totiente $\phi(n)$ di un numero n.

6.4 lambda1.m

```
function mcm=lambda1(n)
vettore=factor(n);
maxind=length(vettore);
indice=1;
temp=[];
while indice<=maxind
while indice<maxind & vettore(indice)==vettore(indice+1)
indice=indice+1;
end
temp=[temp,vettore(indice)-1];
indice=indice+1;
end
lunghezza=length(temp);
mcm=1;
for j=1:lunghezza
mcm=lcm(mcm,temp(j));
end
```

La funzione lambda1.m restituisce la funzione $\lambda_1(n)$ della Definizione 2.2.

6.5 residui.m

```
function v=residui(q,p)
for i=1:p
v(i)=mod(i^q,p);
end
```

La funzione residui.m restituisce i possibili q-esimi residui modulo p

6.6 lambda

```
lambda(n)= local(i=0,j=0); {
len=matsize(factor(n));
f=matrix(len[1],len[2]);
f=factor(n);
v=vector(len[1]);
if( len[1] == 1 & f[1,1]==2,
v[1] = (f[1,1])^(f[1,2]-2);
);
if(f[1,1]!=2,
for(j=1,len[1],
v[j] = (f[j,1]-1)*(f[j,1]^(f[j,2]-1));
);
);
print("factors : ",f);
print("lambda : ",lcm(v));
return(lcm(v));}
```

La funzione scritta in Pari/Gp restituisce la funzione $\lambda(n)$.

6.7 lambda1

```
lambda1(n)= local(i=0,j=0); {
len=matsize(factor(n));
f=matrix(len[1],len[2]);
f=factor(n);
v=vector(len[1]);
for(j=1,len[1],
v[j] = f[j,1]-1;
);
return(lcm(v));}
```

La funzione restituisce la funzione $\lambda_1(n)$

References

[1] Baxter, L. "R86453 Is a New Probable Prime Repunit." 26 Oct 2000. http://listserv.nodak.edu/scripts/wa.exe?A2=ind0010&L=nmbrthry&P=2557.

[2] Guy, R. K. "Pseudoprimes. Euler Pseudoprimes. Strong Pseudoprimes." A12 in Unsolved Problems in Number Theory, 2nd ed. New York: Springer-Verlag, pp. 27-30, 1994.

[3] Dubner, H. "New prp Repunit R(49081)." 9 Sep 1999. http://listserv.nodak.edu/scripts/wa.exe?A2=ind9909&L=nmbrthry&P=740.

[4] Dubner, H. "New Repunit R(109297)." 3 Apr 2007. http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0704&L=nmbrthry&T=0&P=178.

[5] Ribenboim, P. "Repunits and Similar Numbers." 5.5 in The New Book of Prime Number Records. New York: Springer-Verlag, pp. 350-354, 1996.

[6] Voznyy, M. and Budnyy, A. "New PRP Repunit R(270343)." 15 Jul 2007. http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0707&L=nmbrthry&T=0&P=1086.

[7] Yates, S. "Peculiar Properties of Repunits." J. Recr. Math. 2, 139-146, 1969.

[8] Pinch, R. G. E. "The Carmichael Numbers up to 10^{15}." Math. Comput. 61, 381-391, 1993a.

[9] Guy, R. K. "Carmichael Numbers." A13 in Unsolved Problems in Number Theory, 2nd ed. New York: Springer-Verlag, pp. 30-32, 1994.

[10] Grantham, J. "Pseudoprimes/Probable Primes." http://www.clark.net/pub/grantham/pseudo/.

[11] Hardy, G. H. and Wright, E. M. An Introduction to the Theory of Numbers, 5th ed. Oxford, England: Clarendon Press, 1979.

[12] Berlekamp, E. R. Algorithmic Coding Theory. New York: McGraw-Hill, 1968.

[13] Abramowitz, M. and Stegun, I. A. (Eds.). "The Euler Totient Function." 24.3.2 in Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, 9th printing. New York: Dover, p. 826, 1972.

[14] Sloane, N. J. A. Sequence A006970/M5442 in "The On-Line Encyclopedia of Integer Sequences."

[15] Riesel, H. Prime Numbers and Computer Methods for Factorization, 2nd ed. Boston, MA: Birkhäuser, 1994.