TEOREMA DI CRISPIN-JAKOB (TCJ)

Il soggetto del teorema sono i numeri **Repunit e Repdigit,** in cui una stessa cifra viene ripetuta più volte. Nel caso più comune, dei Repunit, la cifra ripetuta è 1.
Questi numeri furono trattati a partire del xvii secolo e sono in certo senso una generalizzazione dei noti numeri di Mersenne, connessione che qui non viene sfruttata.
Il TCJ dimostra una notevole proprietà della fattorizzazione dei Repunit, la quale, a sua volta, porta a due algoritmi per la scoperta di nuovi numeri primi, maggiori di p, dove p è il numero (primo) di cifre del Repunit.
Questi algoritmi sono indubbiamente efficaci, e producono numeri sicuramente primi, non "probabilmente primi". Tuttavia, per mancanza di mezzi adeguati, non se ne è finora potuta confrontare l'efficacia con quella di altri algoritmi in uso.

1. Definizioni e notazioni

In una qualsiasi base di numerazione B (con B > 1), i numeri ottenuti ripetendo N volte una data cifra, c (evidentemente 0 < c < B), sono detti "repdigit" (abbreviazione di "repeat digit"). Ad esempio, in base 10, con c=5 ed N=6, un simile numero è 555555. Tra questi, i numeri ottenuti ripetendo la cifra 1 (che esiste in tutte le basi di numerazione) – ossia con c=1 - sono detti "repunit" (abbreviazione di "repeat unit"); sempre in base 10 e con N=6, un simile numero è 111111. Per indicare i numeri repdigit, e come caso particolare i numeri repunit, utilizzeremo la notazione c[N,B], in cui c, N e B

hanno i significati precedentemente definiti. A volte per i numeri "repunit" si utilizza anche la notazione $R_N^{(B)}$, ma questa simbologia risulta meno comoda quando B ed N diventano delle espressioni non banali.

Quindi gli esempi precedenti possono essere scritti come:
555555 = 5[6, 10] e 111111 = 1[6, 10]

In particolare, nella base B, la cifra più grande è (B-1); il numero (B-1)[N,B] può sempre essere scritto come

$$(B-1)[N,B] = B^N - 1 \qquad (1)$$

Ad esempio, in base 10, dove la cifra massima è 9, il numero 9[5, 10], ossia 99999, può essere scritto come $(10^5 - 1) = 100.000 - 1 = 99.999$.

È immediato verificare che il numero 1[N,B] può essere scritto come ((B-1)[N,B])/(B-1), ed allora c[N,B] può a sua volta essere scritto come c·((B-1)[N,B])/(B-1). Introducendo l'espressione (1) nelle due formule precedenti, si ha:

$$1[N,B] = \frac{B^N-1}{B-1} \qquad (2), \text{ e}$$

$$c[N,B] = c\,\frac{B^N-1}{B-1} \qquad (3).$$

Ad esempio, mantenendo ancora gli esempi precedenti in base 10, si ha: 1[6, 10] (ossia 111111) = 9[6, 10] (ossia 999999) diviso 9, e 5[6, 10] (ossia 555555) = 5 · 1[6, 10].

I numeri 1[N,B] e c[N,B] possono anche essere scritti rispettivamente come

$$\sum_{i=0}^{N-1} B^i \qquad (4)$$

e

$$\sum_{i=0}^{N-1} c \cdot B^i = c \cdot \sum_{i=0}^{N-1} B^i \qquad (5)$$

In base 10, 1[6, 10] = 111111 può essere scritto come $10^0 + 10^1 + 10^2 + 10^3 + 10^4 + 10^5$, e 5[6, 10] = 555555 può essere scritto come $5\cdot10^0 + 5\cdot10^1 + 5\cdot10^2 + 5\cdot10^3 + 5\cdot10^4 + 5\cdot10^5 = 5\cdot(10^0 + 10^1 + 10^2 + 10^3 + 10^4 + 10^5)$.

2. Il piccolo teorema di Fermat

Il piccolo teorema di Fermat, in una delle sue possibili enunciazioni, anzi proprio nell'enunciazione che ne diede Fermat in una lettera del 18 ottobre 1640 al suo confidente Frenicle, afferma che, se p è un numero primo e non è un divisore della base di numerazione B, il numero $(B^{p-1} - 1)$ è multiplo di p. Ma, in base all'espressione (1) precedente, $(B^{p-1} - 1)$ è il repdigit (B-1)[p-1,B], ovvero il numero composto da (p-1) cifre (B-1).

In base 10, ad esempio, poiché 7 è primo e non è un divisore della base 10, il piccolo teorema di Fermat afferma che il numero 10^6-1 = 999999 è divisibile per 7; questo può essere facilmente verificato.

Una immediata conseguenza del piccolo teorema di Fermat è la seguente proprietà.

Proprietà 1: Se un numero primo p, oltre a non essere un divisore di B, non è neppure un divisore di (B-1), allora

$$1[p-1,B] = \frac{(B^{p-1}-1)}{B-1} \qquad (6)$$

è ancora un multiplo di p, perché lo è il secondo membro dell'uguaglianza.

Proseguendo l'esempio precedente in base 10, poiché 7 non è divisore di 9 (il nostro B-1), possiamo concludere che 111111 è divisibile per 7.

Possiamo allora concludere che, per ogni base di numerazione B e per ogni numero primo p che non è divisore della base B o di (B-1), il repunit 1[p-1,B] è divisibile per p, e quindi sono divisibili per p tutti i repdigit c[p-1,B].

In base 10, siamo certi che 1[12, 10] (ossia 111111111111) è divisibile per 13; che 1[18, 10] (ossia 111111111111111111) è divisibile per 19; che 1[10, 10] (ossia 1111111111) è divisibile per 11; e così via. La stessa proprietà non vale invece ad esempio per il numero primo 3, che è un divisore di (B-1)=9; infatti 1[2, 10] = 11 non è divisibile per 3; e neppure per il numero primo 5, che è un divisore della base 10.

Se p non è divisore né di B né di (B-1), non è detto tuttavia che 1[p-1,B] sia il più piccolo repunit multiplo di p. Ad esempio, in base 10, il numero primo p=11 (che non è divisore né di B (ossia 10) né di (B-1) (ossia 9)) è già un repunit, ed è più piccolo di 1[10, 10], ovvero 1[p-1,10]. Lo stesso vale per p=13: si verifica facilmente che 1[6, 10] è multiplo di 13, ed è più piccolo di 1[12, 10]. È noto che il più piccolo repunit divisibile per un numero primo p (che non sia un divisore della base di numerazione B né di (B-1)) ha un numero di cifre che è uguale al numero di cifre del periodo del numero periodico che si ottiene dalla divisione (1/p).

Ci si può chiedere a questo punto se esistono dei repunit multipli di un numero primo p, se p è divisore di (B-1). A questa domanda risponde il seguente teorema.

Teorema 1: In una data base B, se il numero primo p è divisore di (B-1) (e quindi non è divisore di B), il più piccolo repunit divisibile per p è 1[p,B].

Dimostrazione: Applicando la formula (4) precedente, possiamo scrivere, per qualsiasi x:

$$1[x,B] = \sum_{i=0}^{x-1} B^i = 1 + \sum_{i=1}^{x-1} B^i = 1 + \sum_{i=1}^{x-1} ((B-1)+1)^i \qquad (7)$$

Sviluppando le potenze di ((B-1)+1) con la formula binomiale, si ottengono tutti addendi che contengono almeno un fattore (B-1), tranne (x-1) addendi uguali ad 1, che risultano dalle potenze del

termine "+1"; ossia, in definitiva 1[x,B] è la somma di termini che contengono almeno un fattore (B-1), più x addendi uguali ad 1 (il primo fuori dalla sommatoria, gli altri (x-1) dallo sviluppo binomiale delle potenze all'interno della sommatoria). Poiché p è un divisore di (B-1), possiamo anche affermare che 1[x,B] è la somma di termini che sono tutti divisibili per p (contengono il fattore (B-1)), più x addendi uguali ad 1, ovvero più x. Affinché questo numero sia divisibile per p, è necessario e sufficiente che x sia divisibile per p. Inoltre, il valore minimo di x che è divisibile per p è ovviamente proprio p. **C.v.d.**

> In base 10, il numero primo 3 è un divisore di 9 (il nostro (B-1)). Quindi, applicando il teorema precedente, 111 è divisibile per 3, cosa che è senz'altro vera.
>
> Come ulteriore verifica, in base 8, il primo repunit divisibile per 7 (= B-1) è 1111111, come si può facilmente verificare.

Quindi, ricapitolando la situazione, possiamo enunciare la seguente

Proprietà 2: Se p è un numero primo non divisore della base di numerazione B, esiste sempre almeno un repunit che è multiplo di p. Distinguiamo due casi:

1. p è divisore di (B-1). Il più piccolo repunit multiplo di p è 1[p,B].

2. p non è divisore di (B-1). Il repunit 1[p-1,B] è certamente divisibile per p, ma non è necessariamente il più piccolo che ha questa proprietà.

Invece per i numeri primi che sono divisori della base di numerazione B non esistono repunit che ne siano multipli.

> Questo è evidente in base 10. Non possono esistere repunit multipli di 2 o di 5.

3. Repunit e numeri non primi

A questo punto ci si potrebbe chiedere se e quando è possibile trovare un repunit che sia multiplo di un numero non primo. Per rispondere a questa legittima domanda servono alcune osservazioni e dimostrazioni preliminari.

Il teorema di Eulero, che è una generalizzazione del piccolo teorema di Fermat, afferma che per ogni modulo n ed ogni intero B coprimo rispetto ad n (ovvero che non ha divisori comuni con n), si ha:

$$B^{\varphi(n)} \equiv 1 \ (mod\ n) \qquad (8)$$

dove φ(n) indica la funzione phi di Eulero, che conta il numero di interi fra 1 ed n coprimi rispetto ad n. Si tratta di una generalizzazione in quanto, se n = p è un numero primo, allora φ(p) = p-1, ricadendo nell'enunciato del piccolo teorema di Fermat. Da questo teorema si può dedurre immediatamente che $(B^{\varphi(n)} - 1) = (B\text{-}1)\cdot 1[\varphi(n),B]$ è divisibile per n. Se poi n è coprimo rispetto a (B-1), si deduce che è il fattore 1[φ(n),B] che è divisibile per n.

Il teorema di Eulero non garantisce però che si tratti del più piccolo repunit divisibile per n.

Proprietà 3: Il repunit 1[kn,B], raggruppando le sue cifre n ad n, può essere scritto come

$$1[kn, B] = \sum_{i=0}^{k-1} 1[N, B] \cdot B^{ni} = 1[n,\ B] \cdot \sum_{i=0}^{k-1} B^{ni} \qquad (9)$$

Ad esempio 1[18, 10], raggruppando le cifre 6 a 6, può essere scritto come 1[6, 10]·(10^0 + 10^6 + 10^{12}) = 111111·(1 + 10^6 + 10^{12}).

Proprietà 4: Se a non è primo, il repunit 1[a,B] non è primo. Infatti, se a = b·c, in base alla Proprietà 3 precedente possiamo scrivere

$$1[a, B] = 1[b \cdot c, B] = 1[b,\ B] \cdot \sum_{i=0}^{c-1} B^{bi} = 1[c,\ B] \cdot \sum_{i=0}^{b-1} B^{ci} \qquad (10)$$

Quindi 1[a,B] è divisibile sia per 1[b,B] sia per 1[c,B].

Ad esempio, 1[6, 10] (= 111111) è divisibile sia per 1[2, 10] (= 11) sia per 1[3, 10] (= 111), come si verifica facilmente.

Teorema 2: Se 1[n,B] è il più piccolo repunit multiplo di un qualsiasi numero a (primo o non primo), tutti e soli i repunit dell'insieme 1[kn,B] sono multipli di a (con k > 0).

Dimostrazione: Infatti per la proprietà 3 si può scrivere:

$$1[kn, B] = 1[n,\ B] \cdot \sum_{i=0}^{k-1} B^{ni} \qquad (11)$$

in cui il primo fattore del secondo membro è divisibile per a, e quindi lo è anche 1[kn,B].

D'altra parte, se 1[x,B] è divisibile per a (ovviamente x ≥ n per non contraddire l'ipotesi), allora, posto y = x mod n, si può scrivere:

$$1[x, B] = \sum_{i=0}^{x-1} B^i = \sum_{i=0}^{x-y-1} B^i + \sum_{i=x-y}^{x-1} B^i = \sum_{i=0}^{x-y-1} B^i + B^{x-y} \sum_{i=0}^{y-1} B^i \qquad (12)$$

Abbiamo supposto che il primo membro di questa catena di uguaglianze sia divisibile per a, e lo è anche il primo addendo dell'ultima espressione (poiché y = x mod n, e quindi x-y è multiplo di n), per cui deve esserlo anche l'ultima sommatoria. Ma, per quanto appena dimostrato, questo è possibile solo se y=kn, per cui non esiste nessun y = x mod n maggiore di 0. **C.v.d.**

Da questo teorema possiamo dedurre ad esempio che, dato che 1[6, 10] è il più piccolo repunit multiplo di 13, tutti i repunit dell'insieme 1[6n, 10] sono multipli di 13; tra questi c'è, come c'era da aspettarsi in base alla Proprietà 1, anche 1[12, 10].

Teorema 3: Se p è un numero primo, e 1[n,B] è il più piccolo repunit multiplo di p, allora 1[np,B] è il più piccolo repunit multiplo di p^2.

Dimostrazione: In base alla Proprietà 3 possiamo scrivere:

$$1[np, B] = 1[n,\ B] \cdot \sum_{i=0}^{p-1} B^{ni} \qquad (13)$$

Possiamo scegliere una nuova base di numerazione, C = B^n; allora il secondo membro diventa:

$$1[n,\ B] \cdot \sum_{i=0}^{p-1} C^i = 1[n, B] \cdot 1[p, C] \qquad (14)$$

Nella base C, (C-1) = B^n-1, ed in base all'ipotesi è divisibile per p (infatti è (B-1)·1[n,B]); quindi si può applicare il Teorema 2, che afferma che 1[p,C] è il più piccolo repunit (in base C) divisibile per p. Visto che il primo fattore del prodotto a secondo membro, per ipotesi, è divisibile per p, possiamo concludere che il prodotto, e quindi 1[np,B], è divisibile per p^2. **C.v.d.**

> Ad esempio, in base 10, sappiamo che 1[6, 10] è il primo repunit divisibile per 13. Allora possiamo concludere, in base al teorema precedente, che il primo repunit divisibile per 13^2 è 1[6·13, 10] = 1[78, 10].

Questo teorema si può facilmente estendere al seguente

Teorema 3bis: Se p è un numero primo, e 1[np^{k-1},B] (k > 0) è il più piccolo repunit multiplo di p, allora 1[np^k,B] è il più piccolo repunit multiplo di p^{k+1}.

Dimostrazione: È sufficiente procedere per induzione, applicando in modo iterativo un ragionamento simile a quello applicato per dimostrare il Teorema 3 precedente. Per k > 0, se 1[np^{k-1},B] è multiplo di p^k, in base alla Proprietà 3 possiamo scrivere:

$$1[np^k, B] = 1[np^{k-1},\ B] \cdot \sum_{i=0}^{p-1} B^{np^{k-1}i} \qquad (15)$$

Possiamo scegliere una nuova base di numerazione, C = $B^{np^{k-1}}$; allora il secondo membro diventa:

$$1[np^{k-1},\ B] \cdot \sum_{i=0}^{p-1} C^i = 1[np^{k-1}, B] \cdot 1[p, C] \qquad (16)$$

dove il primo fattore è, per ipotesi, il più piccolo repunit multiplo di p^k. Nella base C, (C-1) = $B^{np^{k-1}} - 1$, ed in base all'ipotesi è divisibile per p (infatti è (B-1)·1[np^{k-1},B]); quindi si può applicare il Teorema 2, che afferma che 1[p,C] è il più piccolo repunit (in base C) divisibile per p. Visto che il primo fattore del prodotto a secondo membro, per ipotesi, è divisibile per p^k, possiamo concludere che il prodotto, e quindi 1[np^k,B], è divisibile per p^{k*1}. **C.v.d.**

> Quindi, in base 10, se 1[6, 10] è il più piccolo repunit multiplo di 13, in base al Teorema 3bis possiamo affermare che 1[78, 10] è il più piccolo repunit multiplo di 13^2=169; 1[1014, 10] è il più piccolo repunit multiplo di 13^3=2197; e così via.

Posiamo anche notare che, sempre in base 10, visto che 1[6, 10] è anche il più piccolo repunit multiplo di 7, in base al Teorema 3bis 1[42, 10] è il più piccolo repunit multiplo di 7^2=49, 1[294, 10] è il più piccolo repunit multiplo di 7^3=343, e così via.

In conclusione, dato un numero a non primo e di cui nessuno dei fattori primi è divisore della base di numerazione B, conoscendone la decomposizione in fattori, siamo in grado di trovare il repunit più piccolo che è multiplo di a. Se

$$a = a_1^{k_1} \cdot a_2^{k_2} \cdot a_3^{k_3} \cdot \ldots \cdot a_m^{k_m} = \prod_{i=1}^{m} a_i^{k_i} \qquad (17)$$

è la decomposizione di a in fattori primi, e se 1[n_i,B] è il minimo repunit multiplo di a_i, allora il numero di cifre del minimo repunit multiplo di a sarà, in base al Teorema 3bis precedente, e ricordando che gli a_i sono numeri primi, mentre gli n_i non lo sono necessariamente:

$$mcm(n_i, i = 1, \ldots, m) \cdot a_1^{k_1-1} a_2^{k_2-1} a_3^{k_3-1} \ldots a_m^{k_m-1} = mcm(n_i, i = 1, \ldots, m) \cdot \prod_{i=1}^{m} a_i^{k_i-1} \qquad (18)$$

dove mcm(n_i, i = 1, …, m) indica il minimo comune multiplo dei valori n_i, per i che varia da 1 ad m. Se non si conosce il più piccolo repunit multiplo di un fattore a_i, si può comunque trovare un repunit multiplo di a utilizzando nel calcolo precedente, per il fattore corrispondente, un repunit sicuramente multiplo di a_i, anche se non il più piccolo, in base alla Proprietà 2 precedente.

Ad esempio, operando in base 10, il numero 363 è decomponibile come $11^2 \cdot 3$. Il più piccolo repunit multiplo di 11 è proprio 11 (ovvero 1[2, 10]), ed il più piccolo repunit multiplo di 3 è 1[3, 10]. Il minimo comune multiplo tra 2 e 3 (i nostri n_1) è 6; il valore della produttoria è 11, in quanto rimane soltanto questo termine dal fattore 11^2. Quindi il più piccolo repunit multiplo di 363 sarà 1[66, 10], come si può verificare facilmente.

Come ulteriore esempio, operando in base 10, il numero 63 è decomponibile come $7 \cdot 3^2$, e dato che il più piccolo repunit multiplo di 3 è 1[3, 10] ed il più piccolo repunit multiplo di 7 è 1[6, 10], sappiamo che il più piccolo repunit multiplo di 63 è 1[18, 10] (infatti il minimo comune multiplo tra 3 e 6 è 6, che va ancora moltiplicato per la produttoria, che in questo caso si riduce a 3).

4. Repunit e numeri primi

Si sa con certezza che un certo numero di repunit sono numeri primi. In base 10 se ne conoscono con certezza cinque, e il più grande conosciuto in base 10 è 1[1031,10]. Altri sono classificati come "probabili primi". Si congettura che i repunit primi siano infiniti.

In una qualsiasi base di numerazione B, se p è un numero primo e non è divisore di (B-1), il repunit 1[p,B] potrebbe essere primo. In tutti gli altri casi non lo è; infatti se p è divisore di (B-1) il repunit 1[p,B] è divisibile per p in base alla Proprietà 2 precedente, e se p non è primo vale la Proprietà 4 precedente, per cui non lo è neppure 1[p,B].

Per approfondire lo studio sulla relazione tra repunit e numeri primi introduciamo un paio di osservazioni.

Proprietà 5: Se p è un numero primo maggiore di 2, in qualsiasi base di numerazione B il repunit 1[p,B] è un numero dispari.

Infatti, se p è primo e maggiore di 2, è ovviamente dispari. Scrivendo il repunit 1[p,B] nella forma (4), esso contiene p addendi, di cui uno è il numero 1, e gli altri (p-1) sono potenze di B. Poiché (p-1) è comunque pari, la somma di questi (p-1) addendi è comunque pari, sia che B sia pari o dispari, poiché tutte le potenze di B hanno la stessa parità di B, come si può verificare per induzione, e sommando il numero 1 si verifica che 1[p,B] è dispari.

Proprietà 6: In una qualsiasi base di numerazione B, se un numero primo p > 2 non è divisore di (B-1), il repunit 1[p,B] è sempre uguale a (2kp + 1) per un opportuno k > 0, ovvero (1[p,B] – 1) è divisibile per 2p.

Infatti:

$$(1[p,B] - 1) = \sum_{i=0}^{p-1} B^i - 1 = \sum_{i=1}^{p-1} B^i = B \sum_{i=0}^{p-2} B^i = B \cdot 1[p-1,B] \qquad (19)$$

e l'ultimo membro di questa catena di uguaglianze è divisibile per p, in base alla Proprietà 1 precedente se p non è un divisore di B, oppure, in caso contrario, perché il fattore B che vi compare è appunto divisibile per p, per cui possiamo scrivere 1[p,B] = hp + 1 per un opportuno h > 0.

Inoltre, in base alla Proprietà 5 precedente, poiché 1[p,B] è dispari e quindi (1[p,B] – 1) è pari, h·p è un numero pari, quindi h è pari e può essere scritto come 2k. Da cui infine:

1[p,B] = 2kp + 1 per un opportuno k > 0.

Si noti che la Proprietà 6 vale nella forma 1[p,B] = kp + 1 per un opportuno k > 0 se p=2 (l'unico passaggio del ragionamento precedente che viene meno è l'ultimo, che era basato sul fatto che p è dispari).

Proprietà 7: Dati due numeri a e b del tipo

a = 2np + 1 e b = 2mp + 1.

il numero a·b è ancora del tipo

ab = 2kp + 1

Infatti:

$ab = (2np + 1)\cdot(2mp + 1) = 4nmp^2 + 2np + 2mp + 1 = 2p\cdot(2nmp + n + m) + 1$

Disponiamo ora di tutti gli strumenti per dimostrare il seguente

Teorema di Crispin-Jakob: In una qualsiasi base di numerazione B, se p è un numero primo che non è un divisore di (B-1), per il repunit 1[p,B] si verifica una delle seguenti possibilità:

1. 1[p,B] è un numero primo, oppure

2. tutti i suoi fattori primi sono del tipo (2kp + 1), con k > 0.

Dimostrazione: Supponiamo che p_1 sia un divisore di 1[p,B] diverso da p. p_1 non può essere un divisore di B; se lo fosse, non potrebbe essere divisore di un repunit nella base B.

Intanto possiamo dimostrare che p_1 è sicuramente maggiore di p. Infatti, se per assurdo p_1 fosse minore di p, il repunit minimo che ne è multiplo sarebbe $1[n_1,B]$ con $n_1 < p_1$, oppure $1[p_1,B]$, rispettivamente secondo che p_1 non sia o sia un divisore di (B-1) (Proprietà 2 precedente). Allora, per il Teorema 2 precedente, tutti i repunit multipli di p_1, compreso quindi 1[p,B], avrebbero un numero di cifre multiplo rispettivamente di n_1 (minore di p_1) o di p_1. Ma questo è possibile solo se $n_1 = p$, poiché p (numero di cifre di 1[p,B]) è primo e minore di p_1. Quindi 1[p,B] è anche il più piccolo repunit multiplo di p_1. Come ulteriore conseguenza, in base al Teorema 1, p_1 non è divisore di (B-1).

In base alla Proprietà 1, poiché p_1 è primo e non è divisore né di B né di (B-1), il repunit $1[p_1-1,B]$ è un suo multiplo, mentre, per quanto visto subito sopra, 1[p,B] è il repunit minimo che ne è multiplo. Quindi, per il Teorema 2, $(p_1 – 1)$ è multiplo di p, per cui, per un opportuno numero intero k:

$$p_1 – 1 = kp \rightarrow p_1 = kp + 1.$$

Ma poiché p_1, per essere primo, deve essere dispari, come anche p, il numero k deve essere pari, per cui possiamo sostituirlo con 2h.

In definitiva, se p_1 è un fattore primo di 1[p,B], vale la relazione: $p_1 = 2hp + 1$. **C.v.d.**

> In base 10, ad esempio, da tavole disponibili, sappiamo che 1[11, 10] ammette due divisori, che sono 21.649 (=1.968·11+1) e 513.239 (=46.658·11+1), confermando la tesi del teorema di Crispin-Jakob.
>
> Dalle stesse tavole sappiamo anche che il repunit 1[19, 10] è primo, mentre 1[13, 10] ammette i divisori 53 (=4·13+1), 79 (=6·13+1), e 265.371.653 (=20.413.204·13+1), verificando ancora numericamente la correttezza del teorema precedente.
>
> Secondo Wikipedia (https://it.wikipedia.org/wiki/Numero_primo_di_Mersenne#cite_ref-1) "*In generale un numero del tipo* $M_n = 2^n - 1$ *viene detto "numero di Mersenne" (anche quando non è un numero primo di Mersenne). Si conoscono diverse proprietà dei fattori primi degli* M_p *composti con p primo. Ad esempio (e Fermat fu il primo ad evidenziare e usare questa proprietà) si può dimostrare che ogni fattore primo di* M_p*dev'essere del tipo 2kp + 1 con k intero positivo*". Il riferimento è al lavoro di Mauro Fiorentini "Numeri di Mersenne", che a sua volta non dà altre indicazioni (http://www.bitman.name/math/article/288). In questa luce, il TCJ è un'estensione a una base qualsiasi di questa proprietà notata da Fermat limitatamente a B=2.

Si noti che, in base alle ipotesi del teorema, l'unica condizione che deve essere soddisfatta, che lega p e B, è che p non sia divisore di (B-1). In particolare p può essere un divisore della base di numerazione B.

Infatti, in base 10, si verifica numericamente che 1[2, 10] = 11 è primo, mentre 1[5, 10] = 11111 ammette come divisori 41 (=8·5+1) e 271 (=54·5+1).

Dal teorema di Crispin-Jakob si ricava immediatamente la seguente proprietà.

Proprietà 8: Dato un qualsiasi numero primo p, esiste almeno un numero intero k > 0 tale per cui il numero $p_1 = (2kp+1)$ è primo. In particolare $p_1 \leq 1[p, 2]$ (ovvero il repunit con p cifre in base 2). Per dimostrare questa proprietà è sufficiente applicare il teorema nel caso particolare B=2, per cui è ovviamente verificata l'ipotesi che p non sia un divisore di (B-1)=1.

5. Algoritmo per verificare se un repunit è primo

In qualsiasi base di numerazione B, se p è un numero primo non divisore di (B-1), abbiamo dimostrato che il repunit 1[p,B] è primo oppure è il prodotto di fattori del tipo (2np + 1). In particolare, se p_1 è il più piccolo fattore primo di 1[p,B], indicando con (2mp + 1) il prodotto di tutti gli altri fattori primi (in base alla Proprietà 7, sarà ancora un numero dello stesso tipo), possiamo scrivere:

$$1[p,B] = (2np + 1)\cdot(2mp + 1) \qquad (20)$$

Algoritmo 1: Per verificare se 1[p,B] è primo, si può allora pensare di dividerlo in successione per tutti i numeri del tipo 2kp+1, per k = 1, 2, …. Se per un certo k_1 il risultato della divisione è intero, abbiamo trovato un p_1 ($=2k_1p+1$) che è divisore di 1[p,B], per cui quest'ultimo repunit non è primo. D'altra parte, in base al teorema di Crispin-Jakob, possiamo anche concludere che p_1 è primo; abbiamo quindi trovato un altro numero primo maggiore di p.

Se invece non si trova un tale k_1, possiamo concludere che 1[p,B] è primo.

Rimane da stabilire quando fermarsi nei calcoli, ovvero fino a che punto incrementare k prima di concludere che 1[p,B] è primo. È evidente, in base alla relazione (20), che quando il risultato della divisione (1[p,B])/(2kp+1) diventa minore di (2kp+1), il valore di tentativo (2kp+1) è diventato maggiore della radice quadrata di 1[p,B], per cui ci si può fermare senza dover calcolare a priori un valore limite di k.

Questa tecnica può essere utilizzata sia per verificare se un repunit è primo, sia per trovare certamente un altro numero primo maggiore di quello di partenza; inoltre è applicabile in qualsiasi base di numerazione B, con la sola condizione che p non sia divisore di (B-1). Per inciso, quest'ultima condizione è sempre verificata se si sceglie B=2, ossia si opera nella base binaria. Per verificare se un repunit è primo non è necessario affrontare la temuta scomposizione in fattori, ma è sufficiente eseguire in modo ripetitivo una "semplice" divisione (cosa che potrebbe non essere poi così semplice con l'aumentare del numero delle cifre).

È possibile dare una valutazione del numero massimo di operazioni, in particolare di divisioni, che occorre eseguire per portare a termine l'algoritmo. Il più grande divisore ($2k_{max}p+1$) da considerare, se non si trova prima un divisore del repunit 1[p,B], è la radice quadrata di 1[p,B], che, ricordando la formula (4), può essere approssimata con la radice quadrata dell'addendo più grande della sommatoria, che è B^{p-1}; si può allora scrivere:

$$2k_{max}p + 1 \cong B^{(p-1)/2} \qquad (21)$$

da cui, trascurando l'addendo +1, si può ricavare una valutazione di k_{max}:

$$k_{max} = \frac{B^{(p-1)/2}}{2p} \qquad (22)$$

Dal punto di vista computazionale l'algoritmo può ancora essere migliorato, come precisato nel paragrafo seguente.

6. Algoritmo per trovare almeno un numero primo p_1 maggiore di un altro numero primo p

Scegliamo una base di numerazione B tale che p non sia un divisore di (B-1), per cui sono soddisfatte le ipotesi del Teorema di Crispin-Jakob. Sapendo, dalla Proprietà 6, che 1[p,B] può essere scritto nella forma 2kp+1, ed applicando la formula (4) precedente:

$$1[p,B] = 2kp+1 = \frac{B^p - 1}{B-1} = \sum_{i=0}^{p-1} B^i \qquad (23)$$

possiamo ricavare k:

$$k = \left(\sum_{i=1}^{p-1} B^i \right) / 2p \qquad (24)$$

Notare che, dati p e B, questa operazione può essere fatta una volta per tutte.

Se 1[p,B] non è primo, in base al teorema di Crispin-Jakob esiste un numero primo p_1 del tipo (2mp+1) che è il più piccolo divisore di 1[p,B], ed il resto della divisione (altro divisore di 1[p,B]) è ancora un numero del tipo (2np+1). Possiamo allora scrivere:

$$1[p,B] = 2kp+1 = (2np+1)(2mp+1) \qquad (25)$$

Con alcuni semplici passaggi, ricavando ad esempio n, si ottiene:

$$n = \frac{k - m}{2mp+1} \qquad (26)$$

Ovviamente deve essere n > m.

A questo punto l'algoritmo per individuare un numero primo $p_1 > p$ diventa il seguente.

Algoritmo 2: Si calcola una volta sola k. Poi si considerano in successione i numeri interi m, a partire da 1. Se n, calcolato con la formula precedente, è intero, allora l'algoritmo termina, 1[p,B] non è primo e può essere decomposto, e (2mp+1) è sicuramente primo.

Quando n calcolato con la formula precedente risulta minore di m, l'algoritmo termina ed 1[p,B] è primo.

Il numero 2mp+1 eventualmente trovato per n intero è il più piccolo fattore primo del numero 1[p,B] ed è certo inferiore alla radice quadrata di quest'ultimo. Uno o più numeri primi maggiori di 2mp+1, sempre del tipo ($2m_1p+1$) in base al teorema di Crispin-Jakob, saranno quindi nascosti nel quoziente 1[p,B]/(2mp+1)=(2np+1), dove n è già stato calcolato al termine dell'algoritmo precedente. Poiché il nostro procedimento è basato sulla relazione (2mp+1)(2np+1)=(2kp+1), potremo usare lo stesso algoritmo con questo nuovo k_1 (ossia il numero n trovato a termine dell'algoritmo precedente) (assai più piccolo del precedente k) trovando così un numero primo $2m_1p+1$ maggiore del precedente. E così via, fino ad esaurimento della scomposizione del repunit iniziale, trovando sempre numeri primi maggiori dei precedenti e di p.

Formalmente, se ($2k_1p+1$) (k_1 è il numero n trovato al termine dell'algoritmo precedente) è decomponibile nel prodotto ($2m_1p+1$)($2n_1p+1$), la formula (6) precedente può essere riscritta come:

$$n_1 = \frac{k_1 - m_1}{2m_1p + 1} \qquad (26bis)$$

dove k_1 ha il significato sopra definito e ($2m_1p+1$) è l'eventuale nuovo fattore primo cercato. Questo calcolo è inoltre facilitato dal fatto che sappiamo che m_1 sarà maggiore di m, per cui, applicando l'algoritmo precedente alla formula (26bis), invece di partire con le iterazioni da $m_1=1$, si può iniziare con $m_1=m$.

Finora abbiamo interpretato B come base di numerazione, ma l'algoritmo precedente continua ad essere valido se B è un qualsiasi numero tale per cui p non sia divisore di (B-1), senza interpretarlo necessariamente come base di numerazione.

L'Algoritmo 2 precedente risulta più conveniente dell'Algoritmo 1 perché i calcoli da fare, ed in particolare la divisione, interessano numeri più piccoli, con un numero di cifre minore, e quindi più maneggevoli.

Si possono ancora introdurre delle semplificazioni dal punto di vista del calcolo. In particolare si può osservare che il numeratore della formula (26) precedente in una data iterazione può essere ottenuto da quello dell'iterazione precedente diminuito di un'unità, ed il denominatore è quello dell'iterazione precedente incrementato di 2p. Ulteriori considerazioni si possono fare per saltare iterazioni per cui risulta che (2mp+1) è divisibile per 3 (un'iterazione ogni tre), e così via.

Se l'obiettivo è quello di individuare un nuovo numero primo p_1 a partire da un dato numero primo p, si può sfruttare la scelta arbitraria di B per semplificare i calcoli, ad esempio scegliendo B=2 per operare nella base binaria. Ciò riduce la complessità del calcolo del termine k.

Si noti che, se il termine (2mp+1) non è divisore di 1[p,B], ciò non significa che esso non possa essere un numero primo.

Gli algoritmi esposti permettono di stabilire se un repunit è o non è primo, ed in quest'ultimo caso di individuare un altro numero primo maggiore di quello di partenza, per cui possono essere applicati in modo ripetitivo per costruire numeri primi sempre più grandi, con un numero di calcoli molto ridotto rispetto alla decomposizione in fattori primi, che è un'operazione molto pesante. Si noti tuttavia che non permettono in generale di stabilire se un dato numero, che non è un repunit, è o non è primo.

Ci si potrebbe infine chiedere se qualsiasi numero primo può essere rappresentato come un repunit 1[p,B], con p e B opportunamente scelti. Ciò è ovviamente vero, in quanto qualsiasi numero (eccetto 2) può essere ottenuto come 1[2,(r-1)] (quindi con p=2 e B=(r-1)); infatti questo numero diventa 11 nella base di numerazione (r-1), poiché 1+(r-1) = r). Per questo repunit non valgono però le Proprietà 5 e 6 precedenti, e quanto discende da queste Proprietà, in quanto non è verificata l'ipotesi p > 2 (infatti in questo caso p=2).