1° Test di primalità di VincS

Siamo nel dominio dei numeri naturali escluso lo 0. Possiamo dire che il nostro test è simile a quello di Wilson ma è anche assimilabile ad un crivello quale quello di Eratostene.

Per il crivello di Eratostene, 1 (il primo dei numeri naturali che si incontra nel dominio definito) **deve** essere escluso dai numeri primi per definizione (altrimenti i suoi multipli azzererebbero tutta la mappa dei successivi primi). Nel nostro crivello, 1 potrebbe essere incluso nel conteggio (ma NON nei numeri primi per l'impossibilità di essere determinato quale tale) solo per darci la sicurezza che 2 è il più piccolo numero primo (mentre per Eratostene è un dogma).

Ma, per similitudine ad Eratostene e per comodità, stabiliamo che 2 è il più piccolo numero primo, così come riportano le più recenti definizioni:

"In matematica, un ***numero primo*** *(in breve anche primo) è un numero naturale maggiore di 1 che sia divisibile solamente per 1 e per sé stesso." (da Wikipedia)*

Sia x il numero di cui vogliamo testare la (NON) primalità. Siano p_i solo numeri primi. Definiamo P_k come la produttoria di tutti i primi inferiori ad x ovvero …

$$P_k = \prod_{i=1}^{k} p_i \qquad [1]$$

… tale per cui …

$$p_k < x \leq p_{k+1} \qquad [2]$$

In pratica il test consiste nello scoprire se x è pari a p_{k+1} ovvero se è o NON è il prossimo numero primo. Tutto questo senza, in pratica, conoscere il valore di p_{k+1}.

Esempio: utilizzando il nostro test, ed essendo noto che 2,3,5 e 7 sono tutti numeri primi, con la produttoria … $P_3 = 2 \cdot 3 \cdot 5$ … possiamo dimostrare che 6 è un numero composto e che 7 è il numero primo successivo a 5. Per conoscere i prossimi numeri composti e trovare il prossimo numero primo dobbiamo ricorrere (come in un crivello) alla produttoria … $P_4 = 2 \cdot 3 \cdot 5 \cdot 7$.

Sia q il resto di P_k **diviso** x ovvero …

$$P_k \equiv q \pmod{x} \qquad [3]$$

… e possiamo anche scrivere, utilizzando l'operatore **mod**ulo, …

$$q = P_k \bmod x \qquad [4]$$

Possiamo dividere il resto in tre tipologie (il perché sarà chiaro più avanti a dimostrazione completa):

A. Se $q=0$, x **è composto**!

   Dimostrazione:
   se il resto di P_k/x è pari a 0, è anche implicitamente dimostrato che x è un numero composto dal prodotto di alcuni dei primi che compongono anche P_k, tutti con esponente pari ad 1 (altrimenti il denominatore non sarebbe riducibile ad 1), e quindi che x NON è primo! x non può essere costituito da uno solo dei primi che compongono P_k per la stessa definizione di x e di P_k che abbiamo dato in partenza.

   Esempio:
   $x=6$ … quindi … $P_3 = 2 \cdot 3 \cdot 5 = 30$ … quindi …
   $q = 30 \bmod 6 = 0$ … quindi … x è composto!

B. Se $q \neq 0$ e $q \neq 1$, possiamo fare l'ipotesi iniziale che x sia composto e poi, se non lo è (per esclusione), arrivare alla conclusione dimostrata che x è primo! Vediamo come.

   Nota: scartiamo, da questa tipologia di resto, anche $q=1$ per comodità di dimostrazione in quanto arriveremo a dimostrare, per esclusione dai casi precedenti, che, se $q=1$, allora x deve essere necessariamente un numero primo.

Per verificare se x è un numero composto (in modo ovviamente diverso da quello descritto in A. che escludiamo essendo appunto $q \neq 0$) è sufficiente reiterare, ponendo inizialmente $t_{j=0}=q$, …

$$t_{j+1} = [q \cdot t_j] \bmod x \qquad [5]$$

… fino a quando succede una delle seguenti quattro evenienze.

Nota: per velocizzare la ricerca della prova di primalità forse vedremo che si può anche reiterare (sostituendo la [5]), ponendo sempre inizialmente $t_{j=0}=q$ …

$$t_{j+1} = [t_j \cdot t_j] \bmod x \qquad [6]$$

… e mantenendo le stesse considerazioni finali. Non tratteremo questa formula in questo testo se non per qualche accenno. Quindi, quando si parlerà di t_{j+1} , si parlerà sempre di quello definito nella [5].

1. $t_{j+1}=0$ ed in tal caso x **è un numero composto**!

   Dimostrazione:
   nel caso che la reiterazione finisse con $t_{j+1}=0$, per dimostrare che x è un numero composto è sufficiente dimostrare che il resto q della [5] è un multiplo dei primi componenti x ovvero dobbiamo dimostrare che …

   $$q = r \cdot p_c \cdots p_d \cdots p_f \qquad [7]$$

   … dove $p_c \cdots p_d \cdots p_f$ sono i numeri primi componenti x mentre r è un intero qualsiasi di cui per ora non ci interessiamo anche se potrebbe dare delle sorprese.

Per la nostra dimostrazione prendiamo il caso più completo di composizione di x (che rappresenta tutti i possibili tipi di fattorizzazione) in cui uno dei numeri primi, che chiameremo p_c, ha esponente 1 mentre $p_d{}^u \cdots p_f{}^z$, supponiamo con con $1<u<z$, rappresentano un gruppo di numeri primi che contribuiscono a comporre x con esponente appunto maggiore di 1. Questa dimostrazione mantiene la sua validità in tutte le sottospecie di composizione di x come, ad esempio, l'assenza di primi con esponente pari ad 1 oppure la presenza di molti di essi (rappresentati tutti da p_c) ed/oppure la presenza di uno solo dei primi con esponente maggiore di 1 (condizione minima necessaria per avere un resto $\neq 0$ altrimenti si ricade nella tipologia di resto A.).

Quindi …

$$x = (p_c \cdot p_d{}^u \cdots p_f{}^z) \qquad [8]$$

Per calcolare il resto q passiamo per la frazione …

$$\frac{P_k}{x} = \frac{p_1 \cdots p_c \cdot p_d \cdots p_f \cdots p_k}{p_c \cdot p_d{}^u \cdots p_f{}^z} \qquad [9]$$

… ed appare evidente che la migliore riduzione ai minimi termini che possiamo fare sarà …

$$\frac{P_k / (p_c \cdot p_d \cdots p_f)}{x / (p_c \cdot p_d \cdots p_f)} = \frac{p_1 \cdots \cdots p_k}{p_u{}^{u-1} \cdots p_f{}^{z-1}} \qquad [10]$$

Il risultato di questa divisione tra interi sarà sicuramente frazionaria ovvero con resto diverso da 0. Infatti tutti i termini al numeratore sono coprimi con esponente paria ad 1, abbiamo ridotto ai minimi termini ed abbiamo definito che almeno uno dei termini al denominatore abbia esponente maggiore di 1.

Possiamo quindi anche scrivere …

$$p_1 \cdots \cdots p_k = G_I \cdot (p_d{}^{u-1} \cdots p_f{}^{z-1}) + G_F \cdot (p_d{}^{u-1} \cdots p_f{}^{z-1}) \qquad [11]$$

… dove …
… G_I è la parte intera del risultato della divisione …
… G_F è la parte frazionaria (0,…..) del risultato della divisione …
… mentre tutto il resto lo conosciamo.

Chiamiamo R_R il "resto ridotto" della frazione che quindi sarà pari a …

$$R_R = G_F \cdot (p_d{}^{u-1} \cdots p_f{}^{z-1}) \qquad [12]$$

Se la [10] è frazionaria anche la [9] lo sarà è quindi alla stessa maniera possiamo scrivere …

$$p_1 \cdots p_c \cdot p_d \cdots p_f \cdots p_k = G_I \cdot (p_c \cdot p_d{}^{u} \cdots p_f{}^{z}) + G_F \ (p_c \cdot p_d{}^{u} \cdots p_f{}^{z}) \qquad [13]$$

… dove …
… G_I è sempre la parte intera del risultato della divisione …
… G_F è sempre la parte frazionaria (0,…..) del risultato della divisione …
… mentre tutto il resto lo conosciamo.

Chiamiamo R_P il "resto pieno" della frazione che quindi sarà pari a …

$$R_P = G_F \cdot (p_c \cdot p_d{}^{u} \cdots p_f{}^{z}) \qquad [14]$$

Se adesso dividiamo la [14] per la [12] otteniamo …

$$\frac{R_P}{R_R} = \frac{G_F \cdot (p_c \cdot p_d{}^{u} \cdots p_f{}^{z})}{G_F \cdot (p_d{}^{u-1} \cdots p_f{}^{z-1})} \qquad [15]$$

… e quindi …

$$R_P = R_R \cdot \ p_c \cdot p_d \cdots p_f \qquad [16]$$

Fatti i dovuti paralleli, ovvero $R_P=q$ ed $R_R=r$, la [16] dimostra vera l'ipotesi espressa in [7].

È facilmente dimostrabile che è sufficiente reiterare $z-1$ volte la [5], utilizzando la [7], per ottenere $t_{j+1}=0$, dimostrando così che x è un numero composto! Infatti, dopo aver reiterato $z-1$ volte, otteniamo (senza ricorrere al modulo ma tenendo comunque ben presenti la invarianza del modulo rispetto alle operazioni di moltiplicazione e, conseguentemente, di elevazione a potenza) …

$$q^z = (r^z \cdot \ {p_c}^{z-1} \cdot {p_d}^{z-u}) \cdot (\boldsymbol{p_c \cdot {p_d}^{u} \cdots {p_f}^{z}}) \qquad [17]$$

… quindi …

$$q^z = (r^z \cdot \ {p_c}^{z-1} \cdot {p_d}^{z-u} \cdots) \cdot \boldsymbol{x} \qquad [18]$$

… concludendo …

$$\boldsymbol{t_{j+1}} = q^z \ mod \ x = \boldsymbol{0} \qquad [19]$$

È altrettanto facilmente dimostrabile che se nelle precedenti, dalla [7] alla [18], sostituiamo p_c con il prodotto di due o più primi $p_m \cdots p_v$ la validità delle espressioni e delle conclusioni non cambia.

Appare evidente l'analogia dell'orologio con un quadrante di $[p_c \cdot {p_d}^u \cdot {p_f}^z]$ ore [pari ad x]. Infatti, dopo la reiterazione, è come far partire e far girare la lancetta $[r^z \cdot {p_c}^{z-1} \cdot {p_d}^{z-u} \cdots]$ volte sull'ora 0 (zero) riportandola sempre ed alla fine sull'ora 0 (zero). Con questa dimostrazione appare evidente che si può anche utilizzare anche la [6] per eseguire meno iterazioni (tratteremo in futuro più dettagliatamente questa analisi).

Riassumendo, possiamo dire di aver trattato **tutti** i casi in cui x può essere un numero composto. Abbiamo anche dimostrato i metodi con cui siamo venuti a conoscenza certa di ciò. Avendo usato questo ordine, da qui in poi, possiamo dimostrare per esclusione i casi in cui x è sicuramente un numero primo. Partendo dal calcolo del resto q nella [4]: con la A. abbiamo dimostrato subito, con $q=0$, che x **è un numero composto** dal prodotto di alcuni dei primi che compongono anche P_k, tutti con esponente **pari ad 1**; con la B.1. siamo partiti da $q \neq 0$ e $q \neq 1$ e, reiterando la [5], fino ad ottenere $t_{j+1}=0$, abbiamo dimostrato che x **è un numero composto** dal prodotto di alcuni dei primi che compongono anche P_k, di cui alcuni o tutti con esponente **maggiore di 1**.

Nota: tratteremo in futuro ed in separata sede una analisi della parte irriducibile del resto (r nella [7]). Vedremo se è possibile prevederne il valore ed altre considerazioni simili che non intaccano la validità di questo teorema ma lo possono solo arricchire.

2. t_{j+1} ***è pari ad uno dei*** t_j ***precedenti*** e quindi blocchiamo l'iterazione infinita perché abbiamo riconosciuto in anticipo un dominio di integrità come spiegheremo più avanti nella B.4.; ed in tal caso x **è un numero primo!**

3. $t_{j+1}=1$ e quindi blocchiamo l'iterazione infinita perché abbiamo riconosciuto in anticipo un dominio di integrità come spiegheremo più avanti nella B.4.; ed in tal caso x **è un numero primo!**

Dimostrazione aggiuntiva:
se il resto q è un multiplo di alcuni dei primi che compongono P_k e supponiamo che x sia composto, il risultato di qualsiasi iterazione della [5] non potrà essere inferiore ai primi di cui sopra. Essendo il più piccolo primo pari a 2, ne consegue che se $t_{j+1}=1$ allora x è per forza primo!

4. Vengono effettuate un numero di iterazioni superiori a quelle prevedibili senza giungere a nessuno dei precedenti casi:
   quindi x **è un numero primo!**

   Dimostrazione:
   la dimostrazione che x è un numero primo se le iterazioni durano all'infinito non è necessaria in quanto basta prendere un qualsiasi testo di algebra (citiamo Wikipedia).

   Da … http://it.wikipedia.org/wiki/Aritmetica_modulare ...
   … …
   "(gruppi ciclici finiti, anelli n.d.r.) Diversamente da quanto accade per i numeri interi, il prodotto di due elementi non nulli può essere nullo. Questo non succede però quando *n* è un numero primo: in questo caso infatti le classi formano un dominio d'integrità (e anche un campo)."

   Da … http://it.wikipedia.org/wiki/Dominio_d'integrità ...
   … …
   "In algebra, un **dominio d'integrità** è un anello commutativo con unità tale che $0 \neq 1$ in cui il prodotto di due qualsiasi elementi non-nulli è un elemento non nullo. I domini di integrità sono estensioni degli interi e forniscono un insieme naturale per lo studio della divisibilità."

Sono sufficienti queste considerazioni per affermare che, se x è un numero primo, il ciclo di reiterazione nella [5] o nella [6] continua all'infinito senza mai giungere a $t_{j+1}=0$.

Ma quante iterazioni dobbiamo eseguire prima di poter dire con certezza che siamo caduti in un dominio di integrità? Affermiamo che è comunque possibile calcolare il numero massimo di iterazioni da effettuare (diverso nella [5] dalla [6]) ed è quindi possibile ad un certo punto troncare il ciclo affermando che x è primo. Infatti l'ipotesi peggiore che possiamo fare è che x sia composto unicamente da una elevazione a potenza (z) del 2 (3 se scartiamo il test di x pari) e quindi il numero massimo di iterazioni che ci aspettiamo è $\log_2 x$ ($\log_3 x$ se scartiamo il test di x pari). Questo nel caso usiamo la [5] ma addirittura meno nel caso della [6]!

C. Se $q=1$, x **è primo**!

Dimostrazione:
per esclusione, possiamo dimostrare dalla A. e dalla B.1 che, se x è composto, il resto della divisione di P_k/x o è subito 0 oppure contiene, nella sua composizione, tutti i fattori primi di x presi almeno con esponente pari ad 1. E siccome il fattore primo più piccolo che può comparire è 2 ne viene di conseguenza che, se $q=1$, x NON è composto quindi x è primo! Come caso è forse assimilabile alla dimostrazione aggiuntiva della B.3 .

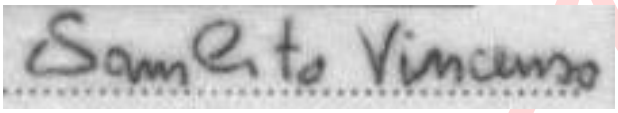
Esempio:
$x = 11$ … quindi … $P_4 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ … quindi …
$q = 210 \bmod 11 = 1$ … quindi … x è primo!

Concludendo, il **1° Test di primalità di VincS** dimostra che è possibile costruire un crivello di numeri primi consequenziali conoscendo solo che il più piccolo numero primo è 2.

Treviglio, l’ 11 Gennaio 2011 ore 22.20

In fede,

Vincenzo Sambito (VincS)



Firmato digitalmente da SAMBITO VINCENZO
ND: c=IT, o=NON PRESENTE, cn=SAMBITO VINCENZO, serialNumber=IT:SMBVCN65M22F205B, givenName=VINCENZO, sn=SAMBITO, dnQualifier=0151859
Motivo: Sono l'autore di questo documento
Data: 2011.01.12 00:09:24 +01'00'