

Primality test. My contribution.

Dante Servi

Abstract

The starting point is given by Fermat's little theorem.

It seems almost magical to discover the presence of (a) among the factors of $2^a - 2$ only if (a) is prime.

Unfortunately it should also be noted in $2^a - 2$ the presence of many prime factors lower than (a); this can ruin the magic when (a) is a number made up of some of the factors that make up $2^a - 2$.

I imagined that $(2^a - 2)/a$ can be considered as the comparison between two sequences with different growth rates.

The first sequence I call (a) contains numbers in natural order ($a = a + 1$) starting from 1.

The second sequence I call (b) contains numbers that result from $b = 2^{a-2}$; for $a = 1$ $b = 2^{a-2} = 0$.

Therefore, calculated in this way the values of (b) are a function of the values of (a).

Without thinking about what Jacques Binet had already done with the Fibonacci sequence, I did the opposite operation; I found a way to obtain for each value of (a) a value identical to that resulting from $b = 2^{a-2}$ without having to use the value of (a).

After having released the values of (b) from the values of (a), I made two small changes to the growth rate of the values of (b); I think I got an interesting result with the second modification.

This article is written in English and Italian, the original language is Italian which is my language, the translation into English was done using the Google translator.

What have I done.

The first sequence that I call (a) contains numbers in natural order ($a = a + 1$) starting from 1.

The second sequence that I call (b) starts from 0 and contains numbers with a growth reason $b = 2b + 2$; where (2b) means twice the previous value of (b).

In the following table you can find the first seven numbers of the two sequences in question, to which I have matched the comparison (b/a) and the prime factorization of (b).

a	$b = 2b + 2$	b/a	factor(b)
1	0	0	0
2	$0 + 2$	1	2
3	$4 + 2$	2	2×3
4	$12 + 2$	3,...	2×7
5	$28 + 2$	6	$2 \times 3 \times 5$
6	$60 + 2$	10,...	2×31
7	$124 + 2$	18	$2 \times 3 \times 3 \times 7$

Returning to the initial formula that links the values of (b) to the values of (a).

Having noticed the constant (and useless starting from 3) presence of the factor 2, I halved (divided by 2) $b = 2^{a-2}$ obtaining $b = 2^{(a-1)-1}$; the version in which the values of (b) are not a function of (a) has become $b = 2b + 1$.

Now the two sequences both start from 3; it will be possible to verify that the comparison (b/a) is absolutely equivalent for the four versions.

a	$b = 2b + 1$	b/a	factor(b)
3	3	1	3
4	$6 + 1$	1,...	7
5	$14 + 1$	3	3×5
6	$30 + 1$	5,...	31
7	$62 + 1$	9	$3 \times 3 \times 7$

Given the results, I wanted to try to slightly modify the latest version of the reason for growth of (b).

With reference to the following table, I specify that by $b=b+b+1$ I mean that the values of (b) are obtained by adding the two previous values of (b) then adding 1; the first two values of (b) are fixed, the calculation starts from the third.

I was not inspired by the Fibonacci sequence, I just wanted to try to do something different (but not too much) compared to (2b); I noticed the similarity only later, and as I will explain it came in handy.

a	b=b+b+1	b/a	factor(b)
2	2	1	2
3	3	1	3
4	6	1,...	2x3
5	10	2	2x5
6	17	2,...	17
7	28	4	2x2x7

At this point I used PARI/GP to see if b/a continued to distinguish prime numbers from composite numbers, as happens in these first cases.

The following command lines for PARI/GP are used to calculate and write the two sequences (a) and (b) and also their comparison (b/a) from $a=4$ to $a=50000$.

Note: The limit of 50000 is due to the size of about 1 Gb that the pari.log file reaches; beyond this dimension Notepad cannot open the file.

Those who are able to create programs for PARI/GP can avoid writing the two values $m=b$ and $b_0=m$ to the file, greatly reducing the size of the file with the same maximum value of (a).

`default(log,1) → To write the results on pari.log.`

`a=3`

`b0=2`

`b=3`

`for(i=1, 49997, print("a=" a=a+1 " ; " m=b " ; b=" b=b+b0+1 " ; b0=" b0=m " ; b/a=" b/a))`

These are the first 20 results obtained.

`a=4 ; 3 ; b=6 ;b0=3 ; b/a=3/2`

`a=5 ; 6 ; b=10 ;b0=6 ; b/a=2`

`a=6 ; 10 ; b=17 ;b0=10 ; b/a=17/6`

`a=7 ; 17 ; b=28 ;b0=17 ; b/a=4`

`a=8 ; 28 ; b=46 ;b0=28 ; b/a=23/4`

`a=9 ; 46 ; b=75 ;b0=46 ; b/a=25/3`

`a=10 ; 75 ; b=122 ;b0=75 ; b/a=61/5`

`a=11 ; 122 ; b=198 ;b0=122 ; b/a=18`

`a=12 ; 198 ; b=321 ;b0=198 ; b/a=107/4`

`a=13 ; 321 ; b=520 ;b0=321 ; b/a=40`

`a=14 ; 520 ; b=842 ;b0=520 ; b/a=421/7`

`a=15 ; 842 ; b=1363 ;b0=842 ; b/a=1363/15`

`a=16 ; 1363 ; b=2206 ;b0=1363 ; b/a=1103/8`

`a=17 ; 2206 ; b=3570 ;b0=2206 ; b/a=210`

`a=18 ; 3570 ; b=5777 ;b0=3570 ; b/a=5777/18`

`a=19 ; 5777 ; b=9348 ;b0=5777 ; b/a=492`

`a=20 ; 9348 ; b=15126 ;b0=9348 ; b/a=7563/10`

`a=21 ; 15126 ; b=24475 ;b0=15126 ; b/a=24475/21`

`a=22 ; 24475 ; b=39602 ;b0=24475 ; b/a=19801/11`

`a=23 ; 39602 ; b=64078 ;b0=39602 ; b/a=2786`

To be usable as a primality test (as long as its validity is confirmed) it is necessary to calculate the value of (b) corresponding to any value of (a).

At this point I remembered the similarity with the Fibonacci sequence and I discovered that fortunately Jacques Binet came up with a valid formula for the Fibonacci sequence.

$$F_n = \left(\frac{(1 + \sqrt{5})}{2} \right)^n - \left(\frac{(1 - \sqrt{5})}{2} \right)^n \div \sqrt{5}$$

Inspired by this formula, I built by trial and error a formula that works (even if it should be improved); the calculation does not result in an integer value of (b) and therefore a rounding is required.

Here is my formula for calculating (b) as a function of (a).

$$b=((1+\sqrt{5})/2)^a-1$$

Being $(1+\sqrt{5})/2=\phi$ (golden ratio)

The formula can be written $b=\phi^a-1$

I checked.

- The correspondence of the results with the sequences (a) and (b) obtained with $a=a+1$ and $b=b+b+1$ up to $a=279000$.
- All numbers from 3 up to over 500 and sample groups of prime and composite numbers up to 279000; this is the maximum value of (a) for which I have calculated the corresponding value of (b) calculated with $b=b+b+1$.
- Some prime numbers up to 982451653, and also the two possible prime numbers before and after 982451653.

$a=982451649$

$b/a=...625/327483883$

$a=982451653$

$b/a=...66040$

$a=982451659$

$b/a=...548/982451659$

$a=982451651$

$b/a=...998/982451651$

$a=982451657$

$b/a=...970/982451657$

I also checked 124 composite numbers that are not recognized as such by $(2^a-2)/a$; I purposely considered only Carmichael numbers ending in 1, 3, 7 or 9.

341, 561, 1179, 1387, 1729, 2047, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, 10261, 12801, 13741, 13747, 13981, 14491, 15709, 15841, 18721, 19951, 23001, 23377, 25761, 29341, 30121, 30889, 31417, 31609, 31621, 33153, 41041, 46657, 49141, 52633, 63973, 75361, 83333, 88561, 90751, 93961, 101101, 104653, 115921, 126217, 162401, 172081, 176149, 188461, 204001, 226801, 228241, 252601, 276013, 282133, 294409, 314821, 334153, 340561, 399001, 410041, 488881, 512461, 530881, 534061, 552721, 563473, 574561, 622909, 653333, 656601, 658801, 665281, 670033, 748657, 838201, 852841, 997633, 1033669, 1082809, 1398101, 1569457, 1773289, 2100901, 2113921, 2433601, 2508013, 3828001, 4463641, 5148001, 6313681, 6733693, 6840001, 7207201, 11921001, 17098369, 19384289, 19683001, 22369621, 23382529, 26719701, 56052361, 64774081, 79411201, 82929001, 83966401, 84350561, 87318001, 90698401, 100427041, 172290241, 189941761, 230996949, 295643089, 809883361, 1150270849.

Of these 124 numbers $(\phi^a-1)/a$ did not recognize the following 11 as being composed.

228241, 252601, 399001, 512461, 852841, 2100901, 3828001, 5148001, 6840001, 87318001, 100427041.

It can be seen that all composite numbers not recognized as such end with 1; I wonder if composite numbers ending in 3, 7 or 9 are always recognized.

Using (phi) means dealing with infinite decimal numbers.

It is immediately evident that the connection with prime numbers derives from the decimals of (phi); considering to use a prime number as the value of (a), the larger the prime number, the more decimals it takes to obtain an almost perfectly integer number as a result.

It will be worth it, I'm sure someone will improve my formula.

In my tests I limited myself to testing numbers up to 1150270849 due to the number of decimals required for (phi) and the consequent memory required.

To test the number 1150270849 I set for (phi) 500000000 decimal places; abounding but not too much.

This is how the number of decimals of (phi) that occurs as a function of the value of (a) roughly increases; to show what inaccuracy it is, I deliberately did not round the value of (b) obtained.

`gp > \p50` `realprecision = 57 significant digits (50 digits displayed)`

`gp > phi=(1+sqrt(5))/2 = 1.6180339887498948482045868343656381177203091798058`

```
gp > a=101 (prime number)
gp > (phi^a-1)/a = 12689084558141989250.00000000000000000007725506

gp > a=307 (numero primo)
gp > (phi^a-1)/a = 4.6996680242086290838522874176898577466575420582103 E61 (more decimals required)

gp > \p100      realprecision = 115 significant digits (100 digits displayed)

gp > phi=(1+sqrt(5))/2
=1.6180339887498948482045868343656381177203091798057628621354486227052604628189024497072072041893
91137

gp > a = 307 (prime number)
gp > (phi^a-1)/a
=46996680242086290838522874176898577466575420582103405554559404.00000000000000000000000000000000
00000

gp > a=503 (prime number)
gp > (phi^a-1)/a
=2.6255183664668766678115783871878929225333122652447806841886329115683404091915256574448050195623
36855 E102 (more decimals required)

gp > \p150      realprecision = 154 significant digits (150 digits displayed)

gp > phi=(1+sqrt(5))/2
=1.6180339887498948482045868343656381177203091798057628621354486227052604628189024497072072041893
9113748475408807538689175212663386222353693179318006077

gp > a = 503 (prime number)
gp > (phi^a-1)/a
=262551836646687666781157838718789292253331226524478068418863291156834040919152565744480501956233
6854626.00000000000000000000000000000000000000000000000000000000
```

Dante Servi
Bressana Bottarone (PV)) Italy
dante.servi@gmail.com

Test di primalità. Il mio contributo.

Dante Servi

Abstract

La base di partenza è data dal piccolo teorema di Fermat.

Sembra quasi magico scoprire la presenza di (a) tra i fattori di 2^a-2 solo se (a) è primo.

Purtroppo si deve anche notare in 2^a-2 la presenza di molti fattori primi inferiori ad (a) ; questo può rovinare la magia quando (a) è un numero composto da alcuni dei fattori che compongono 2^a-2 .

Ho immaginato che $(2^a-2)/a$ si può considerare come il confronto tra due successioni con ragione di crescita diversa.

La prima successione che chiamo (a) contiene numeri in ordine naturale $(a=a+1)$ partendo da 1.

La seconda successione che chiamo (b) contiene numeri che risultano da $b=2^a-2$; per $a=1$ $b=2^1-2=0$.

Quindi calcolati in questo modo i valori di (b) sono in funzione dei valori di (a) .

Senza pensare a quello che aveva già fatto Jacques Binet con la successione di Fibonacci, ho fatto l'operazione contraria; ho trovato il modo di ottenere per ogni valore di (a) un valore identico a quello risultante da $b=2^a-2$ senza dover utilizzare il valore di (a) .

Dopo aver svincolato i valori di (b) dai valori di (a) ho eseguito due piccole modifiche alla ragione di crescita dei valori di (b) ; credo di aver ottenuto un risultato interessante con la seconda modifica.

Questo articolo è scritto in Inglese ed Italiano, la lingua originale è l'Italiano che è la mia lingua, la traduzione in Inglese è stata fatta utilizzando il traduttore di Google.

Cosa ho fatto.

La prima successione che chiamo (a) contiene numeri in ordine naturale $(a=a+1)$ partendo da 1.

La seconda successione che chiamo (b) parte da 0 e contiene numeri con una ragione di crescita $b=2b+2$; dove $(2b)$ significa due volte il valore precedente di (b) .

Nella seguente tabella si trovano i primi sette numeri delle due successioni in questione, ai quali ho fatto corrispondere il confronto (b/a) e la scomposizione in fattori primi di (b) .

a	$b=2b+2$	b/a	factor(b)
1	0	0	0
2	0+2	1	2
3	4+2	2	2x3
4	12+2	3,...	2x7
5	28+2	6	2x3x5
6	60+2	10,...	2x31
7	124+2	18	2x3x3x7

Tornando alla formula iniziale che lega i valori di (b) ai valori di (a) .

Avendo notato la costante (ed inutile a partire da 3) presenza del fattore 2 ho dimezzato (diviso per 2) $b=2^a-2$ ottenendo $b=2^{(a-1)}-1$; la versione nella quale i valori di (b) non sono in funzione di (a) è diventata $b=2b+1$.

Ora le due successioni iniziano entrambi da 3; si potrà verificare che il confronto (b/a) è assolutamente equivalente per le quattro versioni.

a	$b=2b+1$	b/a	factor(b)
3	3	1	3
4	6+1	1,...	7
5	14+1	3	3x5
6	30+1	5,...	31
7	62+1	9	3x3x7

Visti i risultati ho voluto provare a modificare leggermente l'ultima versione della ragione di crescita di (b).

Con riferimento alla tabella seguente, preciso che con $b=b+b+1$ intendo che i valori di (b) si ottengono sommando i due valori precedenti di (b) aggiungendo poi 1; i primi due valori di (b) sono fissi, il calcolo inizia dal terzo.

Non mi sono ispirato alla successione di Fibonacci, volevo solo provare a fare qualcosa di diverso (ma non troppo) rispetto a (2b); mi sono accorto della somiglianza solo in seguito, e come spigherò mi è tornata utile.

a	$b=b+b+1$	b/a	factor(b)
2	2	1	2
3	3	1	3
4	6	1,...	2x3
5	10	2	2x5
6	17	2,...	17
7	28	4	2x2x7

A questo punto ho utilizzato PARI/GP per vedere se b/a continuava a distinguere i numeri primi dai numeri composti, come succede in questi primi casi.

Le seguenti righe di comando per PARI/GP servono a far calcolare ed a far scrivere in pari.log le due successioni (a) e (b) ed anche il loro confronto (b/a) da $a=4$ fino ad $a=50000$.

Nota: Il limite di 50000 è dovuto alla dimensione di circa 1 Gb alla quale arriva il file pari.log; oltre questa dimensione Notepad non riesce ad aprire il file.

Chi è in grado di realizzare programmi per PARI/GP può evitare di scrivere nel file i due valori $m=b$ e $b_0=m$ riducendo di molto la dimensione del file a parità del massimo valore di (a).

default(log,1) → Per scrivere su pari.log i risultati.

a=3

b0=2

b=3

for(i=1, 49997, print("a=" a=a+1 " ; " m=b " ; b=" b=b+b0+1 " ; b0=" b0=m " ; b/a=" b/a))

Questi sono i primi 20 risultati ottenuti.

a=4 ; 3 ; b=6 ;b0=3 ; b/a=3/2

a=5 ; 6 ; b=10 ;b0=6 ; b/a=2

a=6 ; 10 ; b=17 ;b0=10 ; b/a=17/6

a=7 ; 17 ; b=28 ;b0=17 ; b/a=4

a=8 ; 28 ; b=46 ;b0=28 ; b/a=23/4

a=9 ; 46 ; b=75 ;b0=46 ; b/a=25/3

a=10 ; 75 ; b=122 ;b0=75 ; b/a=61/5

a=11 ; 122 ; b=198 ;b0=122 ; b/a=18

a=12 ; 198 ; b=321 ;b0=198 ; b/a=107/4

a=13 ; 321 ; b=520 ;b0=321 ; b/a=40

a=14 ; 520 ; b=842 ;b0=520 ; b/a=421/7

a=15 ; 842 ; b=1363 ;b0=842 ; b/a=1363/15

a=16 ; 1363 ; b=2206 ;b0=1363 ; b/a=1103/8

a=17 ; 2206 ; b=3570 ;b0=2206 ; b/a=210

a=18 ; 3570 ; b=5777 ;b0=3570 ; b/a=5777/18

a=19 ; 5777 ; b=9348 ;b0=5777 ; b/a=492

a=20 ; 9348 ; b=15126 ;b0=9348 ; b/a=7563/10

a=21 ; 15126 ; b=24475 ;b0=15126 ; b/a=24475/21

a=22 ; 24475 ; b=39602 ;b0=24475 ; b/a=19801/11

a=23 ; 39602 ; b=64078 ;b0=39602 ; b/a=2786

Per essere utilizzabile come test di primalità (sempre che ne sia confermata la validità) occorre poter calcolare il valore di (b) corrispondente ad un qualsiasi valore di (a).

A questo punto mi sono ricordato della somiglianza con la successione di Fibonacci ed ho scoperto che fortunatamente Jacques Binet ha ideato una formula valida per la successione di Fibonacci.

$$F_n = \left(\frac{(1 + \sqrt{5})}{2} \right)^n - \left(\frac{(1 - \sqrt{5})}{2} \right)^n \div \sqrt{5}$$

Ispirandomi a questa formula ho costruito per tentativi una formula che funziona (anche se andrebbe migliorata); dal calcolo non risulta un valore intero di (b) e quindi occorre un arrotondamento.

Ecco la mia formula per calcolare (b) in funzione di (a).

$$b=((1+\sqrt{5})/2)^a-1$$

Essendo $(1+\sqrt{5})/2=\phi$ (sezione aurea)

La formula può essere scritta $b=\phi^a-1$

Ho verificato.

- La corrispondenza dei risultati con le successioni (a) e (b) ottenute con $a=a+1$ e $b=b+b+1$ fino ad $a=279000$.
- Tutti i numeri da 3 fino ad oltre 500 ed a campione gruppi di numeri primi e composti fino a 279000; questo è il massimo valore di (a) per il quale ho calcolato il corrispondente valore di (b) calcolato con $b=b+b+1$.
- Alcuni numeri primi fino a 982451653, ed anche i due possibili numeri primi precedenti e successivi a 982451653.

$a=982451649$

$b/a=...625/327483883$

$a=982451653$

$b/a=...66040$

$a=982451659$

$b/a=...548/982451659$

$a=982451651$

$b/a=...998/982451651$

$a=982451657$

$b/a=...970/982451657$

Ho anche verificato 124 numeri composti che non vengono riconosciuti come tali da $(2^a-2)/a$; ho volutamente considerato solo i numeri di Carmichael che terminano per 1, 3, 7 o 9.

341, 561, 1179, 1387, 1729, 2047, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, 10261, 12801, 13741, 13747, 13981, 14491, 15709, 15841, 18721, 19951, 23001, 23377, 25761, 29341, 30121, 30889, 31417, 31609, 31621, 33153, 41041, 46657, 49141, 52633, 63973, 75361, 83333, 88561, 90751, 93961, 101101, 104653, 115921, 126217, 162401, 172081, 176149, 188461, 204001, 226801, 228241, 252601, 276013, 282133, 294409, 314821, 334153, 340561, 399001, 410041, 488881, 512461, 530881, 534061, 552721, 563473, 574561, 622909, 653333, 656601, 658801, 665281, 670033, 748657, 838201, 852841, 997633, 1033669, 1082809, 1398101, 1569457, 1773289, 2100901, 2113921, 2433601, 2508013, 3828001, 4463641, 5148001, 6313681, 6733693, 6840001, 7207201, 11921001, 17098369, 19384289, 19683001, 22369621, 23382529, 26719701, 56052361, 64774081, 79411201, 82929001, 83966401, 84350561, 87318001, 90698401, 100427041, 172290241, 189941761, 230996949, 295643089, 809883361, 1150270849.

Di questi 124 numeri $(\phi^a-1)/a$ non ha riconosciuto come composti i seguenti 11.

228241, 252601, 399001, 512461, 852841, 2100901, 3828001, 5148001, 6840001, 87318001, 100427041.

Si può notare che tutti i numeri composti non riconosciuti come tali terminano con 1; mi chiedo se i numeri composti che terminano con 3, 7 o 9 vengono sempre riconosciuti.

Utilizzare (ϕ) significa avere a che fare con infiniti numeri decimali.

Risulta subito evidente che il collegamento con i numeri primi deriva proprio dai decimali di (ϕ) ; considerando di utilizzare come valore di (a) un numero primo, più è grande il numero primo e più decimali occorrono per ottenere come risultato un numero quasi perfettamente intero.

Se ne varrà la pena, sono certo che qualcuno migliorerà la mia formula.

Nelle mie verifiche mi sono limitato a testare numeri fino a 1150270849 a causa del numero di decimali necessari per (ϕ) e della conseguente memoria necessaria.

Per testare il numero 1150270849 ho impostato per (ϕ) 500000000 cifre decimali; abbondando ma non troppo.

Ecco come approssimativamente cresce il numero di decimali di (ϕ) occorrenti in funzione del valore di (a); per mostrare di quale imprecisione si tratta, volutamente non ho arrotondato il valore di (b) ottenuto.

`gp > \p50` `realprecision = 57 significant digits (50 digits displayed)`

`gp > phi=(1+sqrt(5))/2 = 1.6180339887498948482045868343656381177203091798058`

