Petit théorème de Fermat et nombres composés
Fermat's little theorem and composite numbers

Joël Héras
20 août 2022

En utilisant le Petit théorème de Fermat $a^p \equiv a \bmod p$, il est possible de factoriser presque tous les nombres composés se terminant par 1, 3, 7 ou 9, non multiples de 3.
Using the Fermat's little theorem $a^p \equiv a \bmod p$, it is possible to factorize into primes almost all composite numbers ending in 1, 3, 7 or 9 not multiples of 3.

Décomposition de la formule en p étapes dans le cas a = 2 et p = 6.
En utilisant la formule : $a^p = 2^6 = 64$ et 64 mod 6 = 4
Decomposition of the formula into p steps in the case a = 2 and p = 6.
Using the formula : $a^p = 2^6 = 64$ and 64 mod 6 = 4

En décomposant :
By breaking it down :

1 et 2) a * a = 2 * 2 = 4	4 mod 6 = 4
3) 4 * 2 = 8	8 mod 6 = 2
4) 2 * 2 = 4	4 mod 6 = 4
5) 4 * 2 = 8	8 mod 6 = 2
6) 2 * 2 = 4	4 mod 6 = 4

Décomposition de la formule en p étapes dans le cas a = 2 et p = 7.
En utilisant la formule : $a^p = 2^7 = 128$ et 128 mod 7 = 2
Decomposition of the formula into p steps in the case a = 2 and p = 7.
Using the formula : $a^p = 2^7 = 128$ and 128 mod 7 = 2

En décomposant :
By breaking it down :

1 et 2) a * a = 2 * 2 = 4	4 mod 7 = 4
3) 4 * 2 = 8	8 mod 7 = 1
4) 1 * 2 = 2	2 mod 7 = 2
5) 2 * 2 = 4	4 mod 7 = 4
6) 4 * 2 = 8	8 mod 7 = 1
7) 1 * 2 = 2	2 mod 7 = 2

Tableau 1

			a1	a2	a * a	%	a3	a * a	%	a4	a * a	%	a5	a * a	%	a6	a * a	%	a7	a * a	%
6	64	4	2	2	4	4	2	8	2	2	4	4	2	8	2	2	4	4			
7	128	2	2	2	4	4	2	8	1	2	2	2	2	4	4	2	8	1	2	2	2

Cela ce vérifie pour des "p" plus élevés
This holds true for higher "p".

Tableau 2

			a1	a2	a * a	%	a3	a * a	%	a4	a * a	%	a5	a * a	%	a6	a * a	%	a7	a * a	%	a8			a9			a10			a11			a12			a13		
6	64	4	2	2	4	4	2	8	2	2	4	4	2	8	2	2	4	4																					
7	128	2	2	2	4	4	2	8	1	2	2	2	2	4	4	2	8	1	2	2	2																		
8	256	0	2	2	4	4	2	8	0	2	0	0	2	0	0	2	0	0	2	0	0	2	0	0															
9	512	8	2	2	4	4	2	8	8	2	16	7	2	14	5	2	10	1	2	2	2	2	4	4	2	8	8												
10	1024	4	2	2	4	4	2	8	8	2	16	6	2	12	2	2	4	4	2	8	8	2	16	6	2	12	2	2	4	4									
11	2048	2	2	2	4	4	2	8	8	2	16	5	2	10	10	2	20	9	2	18	7	2	14	3	2	6	6	2	12	1	2	2	2						
12	4096	4	2	2	4	4	2	8	8	2	16	4	2	8	8	2	16	4	2	8	8	2	16	4	2	8	8	2	16	4	2	8	8	2	16	4			
13	8192	2	2	2	4	4	2	8	8	2	16	3	2	6	6	2	12	12	2	24	11	2	22	9	2	18	5	2	10	10	2	20	7	2	14	1	2	2	2

Si on fait un tableau de tous les modulos de la décomposition, on s'aperçoit qu'il y a parfois des séries de nombres qui se répètent.
Il est intéressant de se pencher sur les 2 qui sont toujours présents, en particulier à la fin des nombres pairs, ce qui correspond au Petit théorème de Fermat (en vert).
Les 2 sont toujours absents de 4 et des multiples de 4 (en jaune).
If we make a table of all the modulos of the decomposition, we realize that there are sometimes series of numbers which are repeated.
It is interesting to look at the 2 which are always present, in particular at the end of the even numbers, which corresponds to the Fermat's little theorem (in green).
2s are always absent from 4s and multiples of 4s (in yellow).

Tableau 3

3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
1	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
2	0	3	2	1	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	0	1	4	2	0	7	6	5	4	3	2	1	0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
		2	2	4	0	5	2	10	8	6	4	2	0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	32	32	32	32	32	32	32
			4	1	0	1	4	9	4	12	8	4	0	13	10	7	4	1	20	18	16	14	12	10	8	6	4	2	0	31	30	29	28	27	26	25
				2	0	2	8	7	8	11	2	8	0	9	2	14	8	2	18	13	8	3	24	20	16	12	8	4	0	29	26	23	20	17	14	11
					0	4	6	3	4	9	4	1	0	1	4	9	16	4	14	3	16	6	22	13	4	24	16	8	0	25	18	11	4	34	28	22
						8	2	6	8	5	8	2	0	2	8	18	12	8	6	6	8	12	18	26	8	19	2	16	0	17	2	22	8	31	18	5
							4	1	4	10	2	4	0	4	16	17	4	16	12	12	16	24	10	25	16	9	4	1	0	1	4	9	16	25	36	10
								2	8	7	4	8	0	8	14	15	8	11	2	1	8	23	20	23	4	18	8	2	0	2	8	18	32	13	34	20
									4	1	8	1	0	16	10	11	16	1	4	2	16	21	14	19	8	7	16	4	0	4	16	1	28	26	30	1
										2	2	2	0	15	2	3	12	2	8	4	8	17	2	11	16	14	2	8	0	8	32	2	20	15	22	2
											4	4	0	13	4	6	4	4	16	8	16	9	4	22	4	28	4	16	0	16	30	4	4	30	6	4
												8	0	9	8	12	8	8	10	16	8	18	8	17	8	27	8	1	0	32	26	8	8	23	12	8
													0	1	16	5	16	16	20	9	16	11	16	7	16	25	16	2	0	31	18	16	16	9	24	16
														2	14	10	12	11	18	18	8	22	6	14	4	21	2	4	0	29	2	32	32	18	10	32
															10	1	4	1	14	13	16	19	12	1	8	13	4	8	0	25	4	29	28	36	20	25
																2	8	2	6	3	8	13	24	2	16	26	8	16	0	17	8	23	20	35	2	11
																	16	4	12	6	16	1	22	4	4	23	16	1	0	1	16	11	4	33	4	22
																		8	2	12	8	2	18	8	8	17	2	2	0	2	32	22	8	29	8	5
																			4	1	16	4	10	16	16	5	4	4	0	4	30	9	16	21	16	10
																				2	8	8	20	5	4	10	8	8	0	8	26	18	32	5	32	20
																					16	16	14	10	8	20	16	16	0	16	18	1	28	10	26	1
																						7	2	20	16	11	2	1	0	32	2	2	20	20	14	2
																							4	13	4	22	4	2	0	31	4	4	4	3	28	4
																								26	8	15	8	4	0	29	8	8	8	6	18	8
																									16	1	16	8	0	25	16	16	16	12	36	16
																										2	2	16	0	17	32	32	32	24	34	32
																											4	1	0	1	30	29	28	11	30	25
																												2	0	2	26	23	20	22	22	11
																												0	0	4	18	11	4	7	6	22
																													8	2	22	8	14	12	5
																														4	9	16	28	24	10
																															18	32	19	10	20
																																28	1	20	1
																																	2	2	2
																																		4	4
																																			8

Tableau 4

n	p1	p2	p1 + p2	b
49	7	7	14	7
77	7	11	18	17
91	7	13	20	7
119	7	17	24	23
121	11	11	22	11
133	7	19	26	7
143	11	13	24	23
161	7	23	30	29
169	13	13	26	13
187	11	17	28	27
203	7	29	36	35
209	11	19	30	29
217	7	31	38	7
221	13	17	30	5
247	13	19	32	31
253	11	23	34	33
259	7	37	44	7
287	7	41	48	47
289	17	17	34	17
299	13	23	36	35
301	7	43	50	7
319	11	29	40	39
323	17	19	36	35
329	7	47	54	53
341	11	31	42	premier
343	7	49	56	49
361	19	19	38	19
371	7	53	60	59
377	13	29	42	41
391	17	23	40	39
403	13	31	44	43
407	11	37	48	47
413	7	59	66	65
427	7	61	68	7
437	19	23	42	41
451	11	41	52	11
469	7	67	74	7
473	11	43	54	53
481	13	37	50	13
493	17	29	46	45
497	7	71	78	77
511	7	73	80	7
517	11	47	58	57
527	17	31	48	7
529	23	23	46	23
533	13	41	54	53
539	11	49	60	119
551	19	29	48	47
553	7	79	86	7
559	13	43	56	55

On s'intéresse aux séries de nombres qui se répètent et qui se terminent par 2.
Si on compte combien il y a de nombres entre le dernier 2 et la fin, le 2 inclus on a :
Pour n = 3 <> b = 1, pour n = 4 il n'y a pas de 2, pour n = 5 <> b = 1, pour n = 6 <> b = 2 ...

m = le nombre entre le premier nombre de la série et le premier 2.
Donc b = p modulo m.

Si on liste ces nombre b, on s'aperçoit
1) b = 1 pour tous les nombres premiers, c'est normal, c'est le Petit théorème de Fermat.
2) Pour les nombres pairs, multiples de 3 et se terminant par 5 on va les laisser de coté, ça parait chaotique même si ce ne l'est pas vraiment si on en fait une étude plus approfondie.
3) Listons les nombres composée ni pairs ni multiples de 3 ni se terminant par 5 et comparons b avec leurs facteurs et la somme de ces facteurs. Voir tableau ci-contre.

b est soit égal à un facteur, soit égal à la somme des 2 facteurs moins 1, soit rarement avec un nombre ne correspondant à rien. Ces derniers sont plus rares avec des nombres plus grands.

b = p1 ou b = p2 ou b = p1 + p2

La fréquence des p1 + p2 augmente avec des nombres plus grands.

Tableau 4

n	p1	p2	p1 + p2	b
49	7	7	14	7
77	7	11	18	17
91	7	13	20	7
119	7	17	24	23
121	11	11	22	11
133	7	19	26	7
143	11	13	24	23
161	7	23	30	29
169	13	13	26	13
187	11	17	28	27
203	7	29	36	35
209	11	19	30	29
217	7	31	38	7
221	13	17	30	5
247	13	19	32	31
253	11	23	34	33
259	7	37	44	7
287	7	41	48	47
289	17	17	34	17
299	13	23	36	35
301	7	43	50	7
319	11	29	40	39
323	17	19	36	35
329	7	47	54	53
341	11	31	42	premier
343	7	49	56	49
361	19	19	38	19
371	7	53	60	59
377	13	29	42	41
391	17	23	40	39
403	13	31	44	43
407	11	37	48	47
413	7	59	66	65
427	7	61	68	7
437	19	23	42	41
451	11	41	52	11
469	7	67	74	7
473	11	43	54	53
481	13	37	50	13
493	17	29	46	45
497	7	71	78	77
511	7	73	80	7
517	11	47	58	57
527	17	31	48	7
529	23	23	46	23
533	13	41	54	53
539	11	49	60	119
551	19	29	48	47
553	7	79	86	7
559	13	43	56	55

We are interested in series of repeating numbers that end in 2.
If we count how many numbers there are between the last 2 and the end, including the 2, we have:
For n = 3 <> b = 1, for n = 4 not nomber 2, for n = 5 <> b = 1, for n = 6 <> b = 2 ...

m = the number between the first number in the series and the first 2.
So b = p modulo m.

If we list these numbers b, we see.
1) b = 1 for all prime numbers, it's normal, it's the Fermat's little theorem.
2) For even numbers, multiples of 3 and ending in 5 we will leave them aside, it seems chaotic even if it is not really if we do a more in-depth study.
3) Let's list the composite numbers neither even nor multiple of 3 nor ending in 5 and compare b with their factors and the sum of these factors.
See table opposite.

b is either equal to a factor, or equal to the sum of the 2 factors minus 1, or rarely with a number corresponding to nothing. The latter are rarer with larger numbers.

b = p1 or b = p2 or b = p1 + p2

The frequency of p1 + p2 increases with larger numbers.

Algorithme en Python qui liste tous les b sauf multiples de 4.
Algorithm in Python that lists all b except multiples of 4.

```
d = 1
while d < 100:
   p = d
   a = 2
   m = 0
   while m < p:
      a = a * 2
      a = a % p
      m = m + 1
      if a == 2:
         b = p % m
         print(d,",",b)
         m = p
   d = d + 1
```

Algorithme en Python qui extrait les facteurs premiers d'un nombre composé non pair, non multiple de 3 et ne se terminant pas par 5.
Algorithm in Python that extracts the prime factors of a composite number that is not even, not a multiple of 3 and not ending in 5.

```
import math
from math import sqrt
p=157544237              # = 2357*66841,  99996271 premier, 99996277 = 151*662227
a=2
m=0
while m < p:
   a = a*2
   a=a%p
   m = m + 1
   if a==2:
      b=p%m
      s = b +1
      if s < (sqrt(p)*2) :
         print(b)
         t = p // b
         print(t)
         if b==1:
            print("premier")
         break
      c = s // 2
      d = (c**2)-p
      #e = c + int (d**0.5)
      e = c + int(math.sqrt(d))
      f = s - e
      print(f)
      print(e)
      if b==1:
```

```
        print("premier")
    m=p
```

Conclusion :

Le petit théorème de Fermat est capable de générer soit un facteur soit la somme des facteurs des nombre entiers positifs, clairement sur les nombres se terminant par 1, 3, 7 ou 9.
The Fermat's little theorem is able to generate either a factor or the sum of the factors of positive integers, clearly on numbers ending in 1, 3, 7 or 9.

Les nombres premiers p ne sont qu'un cas particuliers car les facteurs sont 1 et p et la somme des facteurs est p, (p * 1).
*The primes numbers p are just a special case because the factors are 1 and p and the sum of the factors is p, (p * 1).*

Un cas particulier pour les nombres 4 et multiples qui n'ont pas les nombre 2 dans la décomposition en modulos.
A particular case for the multiples of 4 which never have the number 2 in the decomposition into modulos.

En première approximation :
As a first approximation :

Pour les nombres pairs, il génère toujours 0 ou un nombre pair.
For even numbers, it always generates 0 or an even number.

Pour les nombres divisibles par 3, il génère un nombre divisible par 3
For numbers divisible by 3, it generates a number divisible by 3.

Pour les nombres finissant par 5, il génère soit un nombre finissant par 5 soit la somme des facteurs.
For numbers ending in 5, it generates either a number ending in 5 or the sum of the factors.

Note :

Pour les nombres se terminant par 1, 3, 7 ou 9, il génère parfois un pseudo-premier.
For numbers ending in 1, 3, 7 or 9 it sometimes generates a pseudo-prime.

Il génère aussi parfois un nombre sans relation apparente avec le nombre composé dont il est issu.
It also sometimes generates a number with no apparent relationship to the composite number from which it is derived.

Pour les puissances de nombres premiers, il génère la valeur de la puissance inférieure.
For powers of primes, it generates the value of the lower power.

157544237 = 2357*66841, 99996271 premier, 99996277 = 151*662227
99996273 = 7841*12753; 12753 = 1417*9; 1417 = 13*109; 9 = 3*3.
99996273 = 3 * 3 *13 * 109 * 7841