The Prime-Generating Algorithm (PGA)

Jacques Bienvenu[*]

April 29, 2010

Abstract

This article features a new type of algorithm whose goal is to give a better understanding of how prime numbers form themselves. It is called the *Prime-Generating Algorithm* or PGA.

[*] Professeur de mathématiques et Docteur ès lettres. Courriel: jybienvenu@wanadoo.fr

1 Introduction

This article features a new type of algorithm whose goal is not to find prime numbers like the Sieve of Eratosthenes, but to give a better understanding of how they form themselves. It is called the *Prime-Generating Algorithm* or PGA.

2 The length of numbers

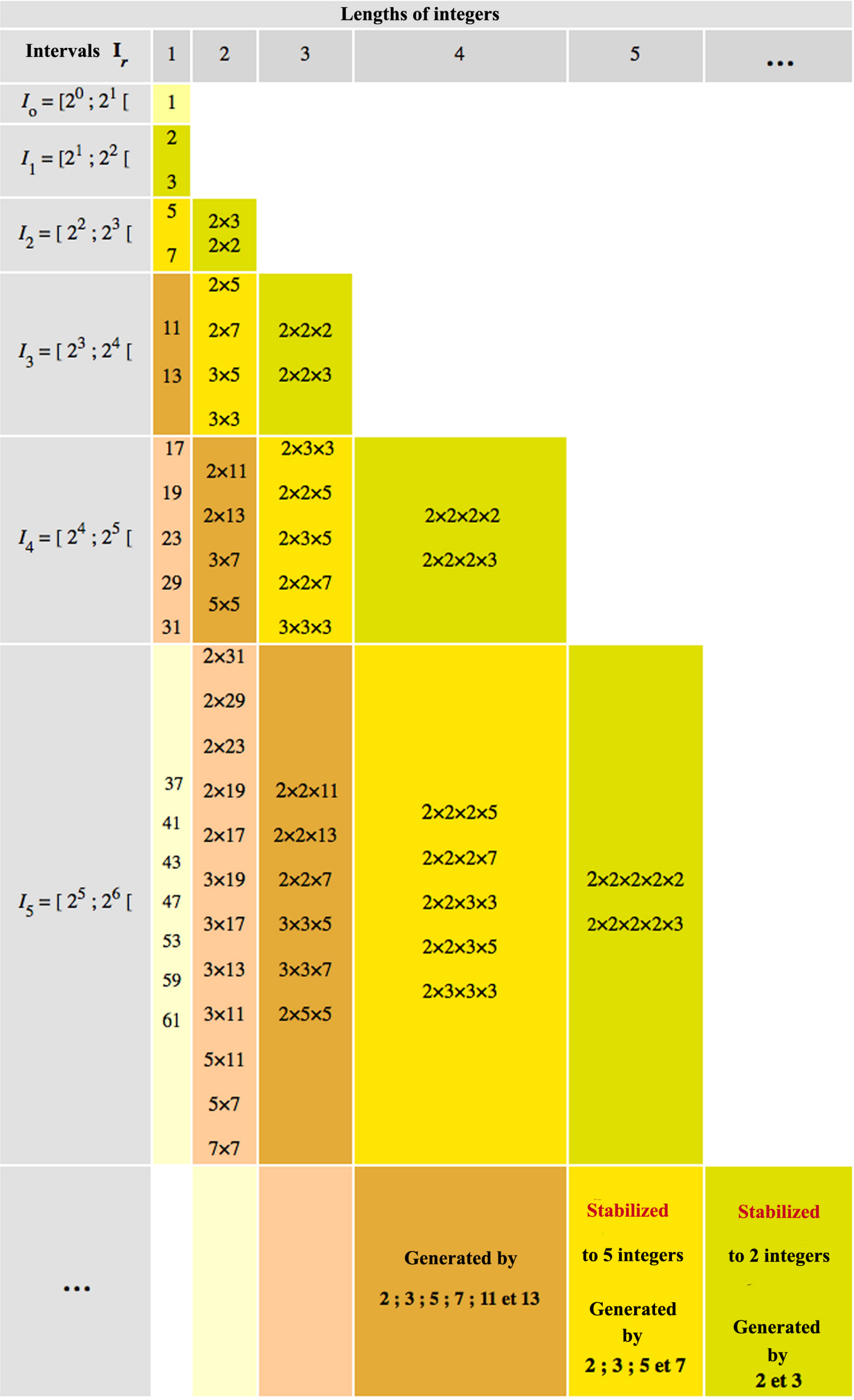
The series of integers is generated by the number "1" in an additive manner. In this succession of numbers, prime numbers seemingly appear without following a clear pattern. The definition of a prime number being relevant to multiplication, the main idea here is no longer to consider prime numbers as being additively generated by 1, but multiplicatively generated by prime numbers, and to sort them according to the prime number that features in the decomposition of an integer. First, the length of the integer must be defined : it's the number of prime numbers involved in the decomposition of one integer n into products of prime numbers (prime factorization). For example, $12 = 2 \times 2 \times 3$ has length 3. Likewise, the length of 5 is 1. According to this definition, prime numbers are integers whose length is 1.

Furthermore, integers can be placed in intervals limited by consecutive powers of 2. Hence, of the form $I_r = [2^r; 2^{r+1}[$. Notice that 2 is the smallest prime number. Therefore 2^r is the smallest integer of length r. Every integer in the interval I_r is smaller than 2^{r+1}, which is the smallest integer of length $r + 1$. From this it can be deduced that in the intervals I_r, integers have a maximum length of r. For the time being, we will allow that the integers' lengths take every value from 1 to r. This enables us to classify integers according to their lengths in each interval.

The following remarks can be made : the intervals I_r are all separate and form a partition of the set $\mathbb{N}$ of natural numbers. Furthermore, the number of elements in I_r doubles when going from r to $r + 1$. Our algorithm consists in writing integers according to this division.

3 The train will whistle p times

Consider the PGA chart (*Table* below) and observe the interval I_4 : each length of I_4 is generate by particular integers - the length 4 by 2 and 3 ; the length 5 by 2, 3, 5, 7; the length of 2 by 2, 3, 5, 7, 11, 13. The colors show that more of the same can be observed for the lengths of 5, 4 and 3 of I5 and the lengths of 2 and 3 for I_3. The algorithm could be represented in the following way : each interval I_r is a train. The new prime numbers are the engine, the old ones constitute the wagons. The last wagon I_4 is constituted by the prime numbers of the interval I_1, 2 and 3. Also note that the last wagon will always contain two elements regardless of the interval (in I_{1000}, there are two numbers whose length is 1000). The prime numbers of I_1 and I_2 constitute the first-to-last wagon of I_4 (the numbers with a length of 3). The number of integers in this wagon is five and it is stabilized, that is to say that the number of integers of the first-to-last wagon (the integers with a length of 4) of the next train I_5 is also five, as we can observe on the chart. Thus it can be shown that in I_{100} the last thirty-six wagons have a stabilized number of integers (see the *stabilization* theorem below).



Lengths of integers						
Intervals I_r	1	2	3	4	5	...
$I_o = [2^0 ; 2^1 [$	1					
$I_1 = [2^1 ; 2^2 [$	2 3					
$I_2 = [2^2 ; 2^3 [$	5 7	2×3 2×2				
$I_3 = [2^3 ; 2^4 [$	11 13	2×5 2×7 3×5 3×3	2×2×2 2×2×3			
$I_4 = [2^4 ; 2^5 [$	17 19 23 29 31	2×11 2×13 3×7 5×5	2×3×3 2×2×5 2×3×5 2×2×7 3×3×3	2×2×2×2 2×2×2×3		
$I_5 = [2^5 ; 2^6 [$	37 41 43 47 53 59 61	2×31 2×29 2×23 2×19 2×17 3×19 3×17 3×13 3×11 5×11 5×7 7×7	2×2×11 2×2×13 2×2×7 3×3×5 3×3×7 2×5×5	2×2×2×5 2×2×2×7 2×2×3×3 2×2×3×5 2×3×3×3	2×2×2×2×2 2×2×2×2×3	
...				Generated by 2 ; 3 ; 5 ; 7 ; 11 et 13	Stabilized to 5 integers Generated by 2 ; 3 ; 5 et 7	Stabilized to 2 integers Generated by 2 et 3

Table 1 : The Prime-Generating Algorithm (PGA)

4 Theorems originating from the PGA

We will only state two results here : a preliminary theorem that we will prove and a central theorem in this study, the theorem of stabilization, that will not be shown.

Consider the interval $I_r = [2^r; 2^{r+1}[$.

$L_{r,m}$ denotes the integers of length m belonging to I_r. The integer m varies therefore from 1 to r (a strictly positive integer). We denote by $P_r = L_{r,1}$ the prime numbers of I_r.

$Card(L_{r,m})$ designates the number of prime numbers in $L_{r,m}$.

Preliminary theorem

A) The prime numbers q which are factors of some integer in $L_{r,m}$ are such that : $q < 2^{r-m+2}$.

B) If q is a prime number such that $q < 2^{r-m+2}$, there exists at least one integer in $L_{r,m}$, with $2 \leq m \leq r$, that contains q as a factor.

Proof A)

Indeed, if $q < 2^{r-m+2}$, then $2^{m-1}q \geq 2^{r+1}$. However $2^{m-1}q$ is the smallest integer of length m that contains q. Thus there is no integer in $L_{r,m}$ containing q, and we necessarily get $q < 2^{r-m+2}$.

To prove B, we need the following lemma.

Lemma

For every real number $x \geq 2$, a prime number between x and $2x$ can always be found.

Proof

Bertrand's postulate states that for every integer $n > 1$, a prime number between n and $2n$ can always be found.

Consider a real number x, with $x \geq 2$ and let $E(x)$ be the integer part of x. We have $E(x) > 1$ and according to Bertrand, there exists a prime number p such as $E(x) < p < 2E(x)$, which implies $E(x) + 1 \leq p < 2E(x)$.

From $E(x) \leq x < E(x) + 1$, we deduce that $x < E(x) + 1 \leq p < 2E(x) \leq 2x$, which proves our assertion.

Proof B)

Consider now $q < 2^{r-m+2}$. If $2^{r-m+1} \leq q < 2^{r-m+2}$, then $2^r \leq 2^{m-1}q < 2^{r-1}$, and so, in the case of $2 \leq m \leq r$, there indeed exists at least one integer of $L_{r,m}$ that contains q as a factor.

If $q < 2^{r-m+1}$, then $2^{r-m+1}/q > 1$ and $2^{r-m+2}/q > 2$. Thus there exists a prime number p between $2^{r-m+2}/q$ and $2^{r-m+3}/q$. From this we deduce, using the lemma above, that in the case of $2 \leq m \leq r$, $2^{m-2}pq$ belongs to I_r and this number is indeed a integer of length m that contains q as a factor.

In other words, integers of length $2 \leq m \leq r$ of an interval I_r are the spawn of all the prime numbers less than or equal to those of the interval I_{r-m+1}. (It can be said that prime numbers generate a collection H of integers if all of these prime numbers are to be found in the decomposition of H's integers and if there are no other).

Stabilization theorem

For every r and $m \geq \frac{(r+1)ln2}{ln3}$ we have $card(L_{r,m}) = card(L_{r+n,m+n})$ for any natural number n. (Proof in the french version)

We can thus observe that for $r > 4$, for than a third of the length of an interval I_r have a cardinal number that stabilizes itself and therefore is also part of following intervals. To give an idea of this, in I_{100}, the last 36 lengths are stabilized. One can calculate stable lengths. Thus, for example, for every $r > 7$, it can easily be found that $L_{r,r} = 2$, $L_{r,r-1} = 5$, $L_{r,r-2} = 8$, *etc.*

5 Conclusion : Order rather than chaos

The PGA reveals a structure. In this algorithm, the intervals I_r appear to be generating cells of a collection of prime numbers which do not show in the decomposition of elements of I_r or of any of the previous intervals. On the other hand, these prime numbers will be used in the integers of the next intervals: the integers of length 2 in I_{r+1}, the integers of length 3 in I_{r+2} and so on until some length n is reached whose cardinal stabilizes. The interval I_r also appears to be related with the history of those prime numbers which have been constructed before. This clockwork looks closer to order than to chaos. This new order appears to be ruled by rigorously precise laws. Instead of focusing on a single prime number, one considers instead the collection of all such primes which belong to a given interval I_r. Therefore we promote the idea of studying prime numbers through the sieve provided by our intervals I_r. Our algorithm therefore connects to enumeration problems and thus to the paramount problem of estimating more precisely the density of prime numbers. Understanding the integers of length 2, as depicted in our PGA, is also relevant to cryptography problems. This glance towards the future is a proper way to conclude this article.

6 References

Jacques Bienvenu, "L'algorithme de génération des premiers (AGP)", Revue Tangente, n° 108, 2006

Chris Caldwell, Site Web "The primes pages", http://primes.utm.edu/.

Jean-Paul Delahaye, *Merveilleux nombres premiers. Voyage au cœur de l'arithmétique.* Éditions Belin/Pour la science, Paris, 2000.

Gilles Godefroy, *L'aventure des nombres*, Editions Odile Jacob, 1997.

Andrew Grandville, "Nombres premiers et chaos quantique", 2002.
online http://smf4.emath.fr/Publications/Gazette/2003/97/smf_gazette_97_29-44.pdf.

Edouard Lucas, *Théorie des nombres*, Gauthier-Villars, 1891, réédition Jacques Gabay, 1991.

M. Mendes France, G. Tenenbaum, *Les nombres premiers.* Que sais-je? vol. 571. Presses Universitaires de France, 1997.