Cromagnon child (DV, 5.5.2016)

On fournit ci-dessous un programme d'une simplicité enfantine qui permet de savoir si un nombre est premier ou pas. Le titre provenait de l'écoute d'une conférence de Mikhaïl Gromov à la rencontre Abel in Paris 2015, je le trouvais chouette. Euh, il ne pouvait mieux tomber en fait puisque pour ce texte, j'ai perdu beaucoup de temps à réinventer la poudre, à retrouver que $\varphi(p) = p - 1 \iff p$ *est premier*. Le gamin de Cromagnon, sûr, n'y aurait pas passé la journée.

Ce programme calcule le produit de $\frac{1}{4}$ par le cardinal d'ensemble suivant :

$$R(n) = \#\{(x, y) \textit{ tels que } 2 \leqslant x \leqslant n-2 \textit{ et } 2 \leqslant y \leqslant n-2 \textit{ et } xy \equiv 1 \ (mod\ n)\}$$

Par exemple, $R(39) = 5.5$ car il y a 22 produits congrus à 1 modulo 39 qui sont $2 \times 20, 4 \times 10, 5 \times 8, 7 \times 28, 8 \times 5, 10 \times 4, 11 \times 32, 14 \times 14, 16 \times 22, 17 \times 23, 19 \times 37, 20 \times 2, 22 \times 16, 23 \times 17, 25 \times 25, 28 \times 7, 29 \times 35, 31 \times 34, 32 \times 11, 34 \times 31, 35 \times 29, 37 \times 19$ et parce que $\frac{1}{4} \times 22 = 5.5$. Constatons qu'il est important de distinguer par exemple le produit 7×28 du produit 28×7.

```
#include <iostream>
#include <cmath>

int main (int argc, char* argv[]) {
  int n, x, y ;
  float compteur ;

  for (n = 7 ; n <= 100 ; n=n+2) {
     compteur = 0.0 ;
     std::cout << n << " -> " ;
     for (x = 2 ; x <= n-2 ; ++x)
        for (y = 2 ; y <= n-2 ; ++y)
           if ((x*y) % n == 1)
        compteur = compteur+1 ;
     std::cout << (float) compteur/4.0 << "\n" ;
  }
}
```

Présentons le résultat de ce programme dans un tableau en séparant les nombres impairs de la forme $4k+3$ (colonnes bleues) des nombres impairs de la forme $4k+1$ (colonnes jaunes).

n	$R(n)$	n	$R(n)$	n	$R(n)$	n	$R(n)$
7	1	55	9.5	9	1	57	8.5
11	2	59	14	13	2.5	61	14.5
15	1.5	63	8.5	17	3.5	65	11.5
19	4	67	16	21	2.5	69	10.5
23	5	71	17	25	4.5	73	17.5
27	4	75	9.5	29	6.5	77	14.5
31	7	79	19	33	4.5	81	13
35	5.5	83	20	37	8.5	85	15.5
39	5.5	87	13.5	41	9.5	89	21.5
43	10	91	17.5	45	5.5	93	14.5
47	11	95	17.5	49	10	97	23.5
51	7.5	99	14.5	53	12.5		

Que constate-t-on ?

D'une part, on constate que pour les nombres impairs de la forme $4k+3$, si $R(n)$ est entier et s'il est égal à $\frac{n-3}{4}$, n est premier ; il est composé sinon.

D'autre part, pour les nombres impairs de la forme $4k+1$, si $R(n) = \frac{n-3}{4}$, n est premier ; il est composé sinon.

L'étude amène à comprendre que le nombre de produits xy qui sont congrus à l'unité modulo un nombre donné n et tels que x et y sont compris entre 2 et $n-2$, ces produits étant comptés doublement lorsque $x \neq y$ mais simplement lorsque $x = y$, est égal à $\frac{\varphi(n)-2}{4}$. Ce fait permet de distinguer aisément les nombres premiers des nombres composés. Il permet d'établir un lien entre le caractère de primalité de n et le nombre de points appartenant à la courbe d'équation $xy \equiv 1$ dans $\mathbb{Z}/n\mathbb{Z}$.
$(\frac{\varphi(n)-2}{4} = \frac{n-3}{4} \iff \varphi(n) = n-1)$.