Moyenne des résidus quadratiques et moitié des nombres (Denise Vella-Chemla, 21.8.2017)

On poursuit ici nos expérimentations numériques en programmant de nouveaux calculs sur les résidus quadratiques modulaires des entiers.

On calcule pour chaque nombre x entre 3 et 100 la moyenne des résidus quadratiques des nombres inférieurs à la moitié de x. Illustrons cela par deux exemples :

- pour $x = 11, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 5, 5^2 = 3$, la moyenne vaut $\frac{1+4+9+5+3}{5} = \frac{22}{5} = 4.4$;
- pour $x = 13, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 3, 5^2 = 12, 6^2 = 10$, la moyenne vaut $\frac{1+4+9+3+12+10}{6} = \frac{39}{6} = 6.5$;

Attention à l'ordre dans lequel les opérations doivent être effectuées : effectuer d'abord la somme des carrés, puis la réduction modulaire n'aboutit pas au même résultat qu'effectuer d'abord les réductions modulaires, puis sommer les résultats (pour 13, la somme des carrés aurait abouti au nombre $91 = 1+4+9+16+25+36$ *et la réduction modulaire sur le résultat 91 aurait abouti à 0 puisque* $91 = 13 \times 7$ *; les réductions modulaires effectuées d'abord sur chaque carré indépendamment n'ont permis de soustraire que* 4×13 *à 91 (*1×13 *soustraite de 16,* 1×13 *soustraite de 25 et* 2×13 *soustraites de 36) et sommer les réductions modulaires a alors comme résultat 39 (différent du 0 obtenu en effectuant les opérations dans l'ordre inverse).*

Le programme de calcul des moyennes en C++ est fourni en annexe.

Voici le résultat de ce programme (pour les nombres x inférieurs ou égaux à 20, on a détaillé entre parenthèses les calculs des résidus quadratiques des nombres inférieurs à $\frac{x-1}{2}$).

```
3 ->
   (1,1),
   1
4 ->
   (1,1),(2,0),
   0.5
5 ->
   (1,1),(2,4),
   2.5
6 ->
   (1,1),(2,4),(3,3),
   2.66667
7 ->
   (1,1),(2,4),(3,2),
   2.33333
8 ->
   (1,1),(2,4),(3,1),(4,0),
   1.5
9 ->
   (1,1),(2,4),(3,0),(4,7),
   3
10 ->
   (1,1),(2,4),(3,9),(4,6),(5,5),
   5
11 ->
   (1,1),(2,4),(3,9),(4,5),(5,3),
   4.4
12 ->
   (1,1),(2,4),(3,9),(4,4),(5,1),(6,0),
   3.16667
```

```
13 ->
   (1,1),(2,4),(3,9),(4,3),(5,12),(6,10),
   6.5
14 ->
   (1,1),(2,4),(3,9),(4,2),(5,11),(6,8),(7,7),
   6
15 ->
   (1,1),(2,4),(3,9),(4,1),(5,10),(6,6),(7,4),
   5
16 ->
   (1,1),(2,4),(3,9),(4,0),(5,9),(6,4),(7,1),(8,0),
   3.5
17 ->
   (1,1),(2,4),(3,9),(4,16),(5,8),(6,2),(7,15),(8,13),
   8.5
18 ->
   (1,1),(2,4),(3,9),(4,16),(5,7),(6,0),(7,13),(8,10),(9,9),
   7.66667
19 ->
   (1,1),(2,4),(3,9),(4,16),(5,6),(6,17),(7,11),(8,7),(9,5),
   8.44444
20 ->
   (1,1),(2,4),(3,9),(4,16),(5,5),(6,16),(7,9),(8,4),(9,1),(10,0),
   6.5
```

$21 \to 9.1$	$41 \to 20.5$	$61 \to 30.5$	$81 \to 35.1$
$22 \to 10$	$42 \to 19.6667$	$62 \to 28$	$82 \to 41$
$23 \to 8.36364$	$43 \to 20.4762$	$63 \to 25.0645$	$83 \to 38.4634$
$24 \to 6.16667$	$44 \to 16.5$	$64 \to 21.5$	$84 \to 33.1667$
$25 \to 10.4167$	$45 \to 19.0909$	$65 \to 32.5$	$85 \to 42.5$
$26 \to 13$	$46 \to 20$	$66 \to 31.6667$	$86 \to 42$
$27 \to 11.0769$	$47 \to 18.3913$	$67 \to 32.4848$	$87 \to 37.093$
$28 \to 10.5$	$48 \to 14.1667$	$68 \to 28.5$	$88 \to 35.5$
$29 \to 14.5$	$49 \to 20.4167$	$69 \to 31.1176$	$89 \to 44.5$
$30 \to 12.6667$	$50 \to 23$	$70 \to 32$	$90 \to 41.6667$
$31 \to 12.4$	$51 \to 23.12$	$71 \to 28.4$	$91 \to 42.4667$
$32 \to 9.5$	$52 \to 22.5$	$72 \to 24.1667$	$92 \to 38.5$
$33 \to 15.125$	$53 \to 26.5$	$73 \to 36.5$	$93 \to 43.1304$
$34 \to 17$	$54 \to 24.6667$	$74 \to 37$	$94 \to 42$
$35 \to 14.4118$	$55 \to 22.4074$	$75 \to 31.0811$	$95 \to 38.4043$
$36 \to 11.1667$	$56 \to 19.5$	$76 \to 32.5$	$96 \to 32.1667$
$37 \to 18.5$	$57 \to 27.1429$	$77 \to 36.4737$	$97 \to 48.5$
$38 \to 18$	$58 \to 29$	$78 \to 34.6667$	$98 \to 45$
$39 \to 15.0526$	$59 \to 26.4483$	$79 \to 34.4359$	$99 \to 45.1224$
$40 \to 13.5$	$60 \to 21.1667$	$80 \to 27.5$	$100 \to 40.5$

On constate que la moyenne des restes pour les nombres premiers de la forme $p = 4k + 1$ (que sont 5, 13, 17, 29, 37, 41, 53, 61, 73, 89 et 97) est égale à $\frac{n}{2}$. Cela reste à prouver.

On constate qu'il en est de même pour les doubles des nombres premiers en question que sont 10, 26, 34, 58, 74 et 82.

Cette propriété ne semble pas vérifiée par une grosse majorité des nombres de la forme $4k + 1$ qui ne sont pas premiers : 9, 21, 25, 33, 45, 49, 57, 65, 69, 77, 81, 93 ; elle est cependant vérifiée par les nombre 65 et 85 qui sont chacun produits de 2 nombres premiers de la forme $4k + 1$: $65 = 5 \times 13$ et $85 = 5 \times 17$. On confirme en exécutant "plus loin" que la moyenne des restes quadratiques pour les nombres n suivants vaut $n/2$: 130 ($= 2 \times 5 \times 13$), 145 ($= 5 \times 29$), 170 ($= 2 \times 5 \times 17$), 185 ($= 5 \times 37$) ou 205 ($= 5 \times 41$), les factorisations de tous ces nombres contenant exclusivement deux nombres premiers de la forme $4k+1$ (soit aucun premier de la forme $4k + 3$), et parfois un facteur 2. On le confirme encore en trouvant $n/2$ comme moyenne des résidus quadratiques pour les nombres 481 ($= 13 \times 37$), 485 ($= 5 \times 97$), 493 ($= 17 \times 29$), 505

$(= 5 \times 101)$, 533 $(= 13 \times 41)$, 545 $(= 5 \times 109)$, 565 $(= 5 \times 113)$, 629 $(= 17 \times 37)$, 685 $(= 5 \times 137)$, 689 $(= 13 \times 53)$, 697 $(= 17 \times 41)$, 745 $(= 5 \times 149)$, 785 $(= 5 \times 157)$, 793 $(= 13 \times 61)$, 865 $(= 5 \times 173)$, 901 $(= 17 \times 53)$, 905 $(= 5 \times 181)$, 949 $(= 13 \times 73)$, 965 $(= 5 \times 193)$, 985 $(= 5 \times 197)$ ou enfin $2 \times 965 = 1930$, ce qui semble ne pas pouvoir être fortuit.

A première vue, il aurait pu sembler que les $n = 20k + 11$ premiers que sont 11, 31, 71 ont leur moyenne des restes quadratiques égale à $\frac{2n}{5}$ alors que cela n'est pas le cas des $n = 20k + 11$ composés que sont 51 et 91 mais on infirme cette hypothèse pour $n = 131$.

Ainsi, aucune formule évidente ne semble se dégager pour les nombres premiers (ou pas) de la forme $4k+3$.

Annexe : programme de calcul des moyennes des résidus quadratiques modulaires

```
#include <iostream>
#include <stdio.h>
#include <cmath>

int prime(int atester) {
  bool pastrouve=true;
  unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else
      if ((atester % k) == 0) return 0 ;
      else k++;
  }
}

int puiss(int n,int k,int m) {
  int result ;

  if (k == 0) result = 1;
  else result = (n * puiss(n,k-1,m)) % m;
  return result;
}

int main (int argc, char* argv[])
{
  int n, x, sommeres, bout, tempo ;

  for (n = 3 ; n <= 100 ; ++n) {
    std::cout << n << " -> " ;
    if (n <= 20) std::cout << "\n " ;
    sommeres = 0 ;
    if ((n % 2) == 0) bout = n/2 ; else bout=(n-1)/2 ;
    for (x = 1 ; x <= bout ; ++x) {
      tempo = puiss(x,2,n) ;
      if (n <= 20) std::cout << "(" << x << "," << tempo << ")," ;
      sommeres = sommeres+tempo ;
    }
    if (n <= 20) std::cout << "\n " ;
    std::cout << (float) sommeres / (float) bout << "\n" ;
  }
}
```