

Programme de recherche des premiers par les propriétés quadratiques (Denise Vella-Chemla, 18.5.2019)

Le programme ci-dessous trouve, de façon très inefficace, les nombres premiers en testant la condition fournie par Gauss dans les Recherches arithmétiques.

Un nombre est premier si et seulement si son nombre de résidus quadratiques est égal à  $\frac{p-1}{2}$ .

```
#include <iostream>
#include <stdio.h>
#include <math.h>
#include <time.h>

int main (int argc, char* argv[])
{
    int x, y, z, p, nbsol ;
    bool marque[1000] ;
    float tps1, tps2 ;

    tps1 = clock() ;
    for (p = 7 ; p <= 1000 ; p=p+2)
    {
        nbsol = 0 ;
        for (x = 1 ; x <= p-1 ; ++x) marque[x] = false ;
        for (x = 1 ; x <= p-1 ; ++x)
        {
            for (y = 0 ; y <= p-1 ; ++y)
                for (z = 0 ; z <= p-1 ; ++z)
                    if (x*x-p*y-z == 0)
                        marque[x*x-p*y] = true ;
        }
        for (x = 1 ; x <= p-1 ; ++x)
            if (marque[x])
                nbsol = nbsol+1 ;
        if (nbsol == (p-1)/2)
            std::cout << p << "□□□" ;
    }
    tps2 = clock() ;
    std::cout << (float)(tps2-tps1)/CLOCKS_PER_SEC << "\n" ;
}
```

Voici le résultat de ce programme :

```
7 11 13 17 19 23 29 31 37 41 43 47 53 59
61 67 71 73 79 83 89 97 101 103 107 109 113
127 131 137 139 149 151 157 163 167 173 179 181
191 193 197 199 211 223 227 229 233 239 241 251
257 263 269 271 277 281 283 293 307 311 313 317
331 337 347 349 353 359 367 373 379 383 389 397
401 409 419 421 431 433 439 443 449 457 461 463
467 479 487 491 499 503 509 521 523 541 547 557
563 569 571 577 587 593 599 601 607 613 617 619
631 641 643 647 653 659 661 673 677 683 691 701
709 719 727 733 739 743 751 757 761 769 773 787
797 809 811 821 823 827 829 839 853 857 859 863
877 881 883 887 907 911 919 929 937 941 947 953
967 971 977 983 991 997
289.332
```