

Une implémentation de la méthode de Shanks

emmanuel_____hallouin@univ-tlse2.fr_____http://www.math.univ-toulouse.fr/~hallouin/eh-agreg.html_____hallouin

Voici une implémentation en **maple** du calcul de racine carrée dans $\mathbb{Z}/p\mathbb{Z}$ avec la méthode de Shanks.

```

with(numtheory) ;

Shanks := proc(x, p)
## Calcul de la racine carree de x modulo p avec la methode de Shanks
  local r, alpha, g, G, y, sqrt_y, z, i, j, k ;

  r := p-1 ; alpha := 0 ;
  while irem(r, 2) = 0 do r := iquo(r,2) ; alpha := alpha + 1 ; od ;

  while true do g := rand(2..p-1)() ; if legendre(g, p) = -1
                                          then break ; fi ; od ;

  g := g&^r mod p ;
  # g est un generateur du 2-Sylow

  y := x&^r mod p ; sqrt_y := 1 ; G := g ; j := alpha ;
  # y appartient au 2-Sylow

  while true do
    i := 0 ; z := y ; # ordre(G) = 2^j
    while z <> 1 do z := z&^2 mod p ; i := i + 1 ; od ; # ordre(y) = 2^i

    for k from i to (j-2) do G := G&^2 mod p od ;
    sqrt_y := sqrt_y*G mod p ; G := G&^2 mod p ; y := y/G mod p ; j := i ;

    if y = 1 then break ; fi ;
  od ;
  RETURN(x&^((r+1)/2) / sqrt_y mod p) ;
end ;

p := nextprime(1200) ;

for i from 1 to 100 do
  p := nextprime(p) ;
  print(p) ;

  Carres := select(x -> legendre(x,p) = 1, [seq(i, i = 1..p-1)]) ;

  for x in Carres do if x - Shanks(x,p)^2 mod p <> 0 then print("Il y a une erreur !") ;
    break ; fi ; od ;

  printf("Tout est ok pour p = %d\n", p) ;
od ;

```
