>

Racine carrée modulo un entier.

```
> restart;
> with(numtheory);
```

[*GIgcd*, *bigomega*, *cfrac*, *cfracpol*, *cyclotomic*, *divisors*, *factorEQ*, *factorset*, *fermat*, *imagunit*, *index*, *integral_basis*, *invcfrac*, *invphi*, *issqrfree*, *jacobi*, *kronecker*, λ, *legendre*, *mcombine*, *mersenne*, *migcdex*, *minkowski*, *mipolys*, *mlog*, *mobius*, *mroot*, *msqrt*, *nearestp*, *nthconver*, *nthdenom*, *nthnumer*, *nthpow*, *order*, *pdexpand*, ϕ, π, *pprimroot*, *primroot*, *quadres*, *rootsunity*, *safeprime*, σ, *sq2factor*, *sum2sqr*, τ, *thue*] (1)

Racine carrée modulo p premier impair.

>

Soit p un nombre premier impair. La procédure suivante rend q impair et i tels que p-1=q.2^i.

```
> impair:=proc(p)
  local i,q;
  i:=0;
  q:=p-1;
  while q mod 2 = 0 do
        i:=i+1;
        q:=q/2;
  od;
  [q,i];
  end;
```

impair := **proc**(*p*) (1.1)

local *i*, *q*;

i := 0;

q := *p* − 1;

while *mod*(*q*, 2) = 0 **do**

i := *i* + 1;

q := 1 / 2 * *q*

end do;

[*q*, *i*]

end proc

```
> impair(7);
```

[3, 1] (1.2)

```
> impair(13);
```

$$[3, 2] \tag{1.3}$$

Soit p un nombre premier impair tel que q est le plus grand facteur impair de p-1. La procédure gene rend un générateur du 2-Sylow de (Z/pZ)^*.

```
> gene:=proc(p,q)
  local n,h,z;
  h:=rand(2..p-1);
  n:=h();
  while legendre(n,p)=1 do
      n:=h() od;
  z:=n&^q mod p;
  end;
```

$$gene := \mathbf{proc}(p, q) \tag{1.4}$$

$$\mathbf{local}\ n, h, z;$$

$$h := rand(2..p - 1);$$

$$n := h();$$

$$\mathbf{while}\ (numtheory:-legendre)(n, p) = 1\ \mathbf{do}$$

$$n := h()$$

$$\mathbf{end\ do};$$

$$z := mod(n\ \&^\wedge\ q, p)$$

$$\mathbf{end\ proc}$$

```
>
```

Soit p un nombre premier impair et a un entier premier à p.
La procédure racine rend une racine carrée de a modulo p.

```
> racine:=proc(p,a)
  local x,y,z,q,e,r,b,v,c,t,m;
  v := impair(p) ;
  q := v[1];
  e := v[2];
  y := gene(p,q);
  r := e;
  x := a&^((q-1)/2) mod p;
  b := a*x^2 mod p;
  x := a*x mod p;
  while b mod p <> 1 do
      m := 1;
      c := b^2 mod p;
      while c mod p <> 1 do
          c := c^2 mod p;
          m := m+1;
      od;
      if m=r then RETURN('Erreur') fi;
      t := y&^(2^(r-m-1)) mod p;
```

```
        y := t^2 mod p;
        r := m;
        x := x*t mod p;
        b := b*y mod p;
    od;
    x;
    end;
```

```
racine := proc(p, a)                                                    (1.5)
    local x, y, z, q, e, r, b, v, c, t, m;
    v := impair(p);
    q := v[1];
    e := v[2];
    y := gene(p, q);
    r := e;
    x := mod(a &^ (1 / 2*q - 1 / 2), p);
    b := mod(a*x^2, p);
    x := mod(a*x, p);
    while mod(b, p) <> 1 do
        m := 1;
        c := mod(b^2, p);
        while mod(c, p) <> 1 do
            c := mod(c^2, p);
            m := m + 1
        end do;
        if m = r then
            RETURN('Erreur')
        end if;
        t := mod(y &^ (2^(r - m - 1)), p);
        y := mod(t^2, p);
        r := m;
        x := mod(x*t, p);
        b := mod(b*y, p)
    end do;
    x
```

```
end proc
```

```
> p:=ithprime(100);
```

$$p := 541 \tag{1.6}$$

```
> legendre(5,p);
```

$$1 \tag{1.7}$$

```
> racine(p,5);
```

$$345 \tag{1.8}$$

```
> 345^2 mod p;
```

$$5 \tag{1.9}$$

```
> legendre(6,p);
```

$$-1 \tag{1.10}$$

```
> racine(p,6);
```

$$\mathit{Erreur} \tag{1.11}$$

Racines carrées modulo p^n (p premier impair).

```
> racinepn:=proc(p,n,a)
  local x,t,q,i;
  x := racine(p,a);
  q := p;
  for i from 1 to n-1 do
      t := -(x^2-a)/q;
      t := t*(2*x)&^(-1) mod p;
      x := x+t*q mod q*p;
      q := q*p;
  od;
  [x,-x mod p^n];
  end;
```

$$\begin{aligned}
&\mathit{racinepn} := \mathbf{proc}(p, n, a) \\
&\quad \mathbf{local}\, x, t, q, i; \\
&\quad x := \mathit{racine}(p, a); \\
&\quad q := p; \\
&\quad \mathbf{for}\, i\, \mathbf{to}\, n-1\, \mathbf{do} \\
&\qquad t := -(x\text{^}2 - a)/q; \\
&\qquad t := \mathit{mod}(t*(2*x)\ \&\text{^}\ (-1), p); \\
&\qquad x := \mathit{mod}(x + t*q, q*p); \\
&\qquad q := q*p \\
&\quad \mathbf{end\ do};
\end{aligned} \tag{2.1}$$

```
    [x, mod(-x, p^n)]
end proc
```

```
> p;
```

$$541 \tag{2.2}$$

```
> r:=racinepn(p,7,5);
```

$$r := [9560255225038356431, 40035284820110109 50] \tag{2.3}$$

```
> p^7;
```

$$13563783707049367381 \tag{2.4}$$

```
> r[1]^2 mod p^7;
```

$$5 \tag{2.5}$$

Racines carrées modulo 2^n.

```
> racine2n:=proc(n,a)
  local x,i,q,t;
  q := 4;
  x := 3;
  for i from 3 to n-1 do
      t := -(x^2-a)/(2*q) mod 2;
      x := x+t*q mod 2*q;
      q := 2*q;
  od;
  [x,-x mod 2^n,x+2^(n-1) mod 2^n,-x+2^(n-1) mod 2^n];
  end;
```

$$racine2n := \mathbf{proc}(n, a) \tag{3.1}$$

```
    local x, i, q, t;
    q := 4;
    x := 3;
    for i from 3 to n - 1 do
        t := mod(-1 / 2 * (x^2 - a) / q, 2);
        x := mod(x + t * q, 2 * q);
        q := 2 * q
    end do;
    [x, mod(-x, 2^n), mod(x + 2^(n - 1), 2^n), mod(-x
    + 2^(n - 1), 2^n)]
end proc
```

```
> racine2n(6,41);
```

$$[19, 45, 51, 13] \tag{3.2}$$

```
> 13^2 mod 2^6;
```

41 (3.3)

```
>
```

Racines carrées modulo p^n (p premier quelconque).

```
> racinepuiss:=proc(p,n,a)
  if p=2 then racine2n(n,a)
  else racinepn(p,n,a) fi
  end;
```

racinepuiss := **proc**(*p*, *n*, *a*) (4.1)

if *p* = 2 **then**

racine2n(*n*, *a*)

else

racinepn(*p*, *n*, *a*)

end if

end proc

Racines carrées modulo un entier n quelconque.

```
> racinecarree:=proc(n,a)
  local i,f,t,v,m,tw,w,r,k;
  f := ifactors(n)[2];
  t := nops(f);
  v := [seq(racinepuiss(f[j][1],f[j][2],a),j=1..t)];
  m := x->convert(x,list);
  w := map(m,v[1]);
  tw := nops(w);
  for i from 2 to t do
      w := [seq([op(w[j]),v[i][1]],j=1..tw),seq([op(w[j]),v[i][2]]
  ,j=1..tw)];
      tw := 2*tw;
  od;
  r := [seq(chrem(w[j],[seq(f[l][1]^f[l][2],l=1..t)]),j=1..tw)];
  end;
```

racinecarree := **proc**(*n*, *a*) (5.1)

local *i*, *f*, *t*, *v*, *m*, *tw*, *w*, *r*, *k*;

f := (*ifactors*(*n*))[2];

t := *nops*(*f*);

v := [*seq*(*racinepuiss*((*f*[*j*])[1], (*f*[*j*])[2], *a*), *j* = 1..*t*)];

```
    m := proc(x)
        option operator, arrow;
        convert(x, list)
    end proc;
    w := map(m, v[1]);
    tw := nops(w);
    for i from 2 to t do
        w := [seq([op(w[j]), (v[i])[1]], j = 1..tw)
       , seq([op(w[j]), (v[i])[2]], j = 1..tw)];
        tw := 2*tw
    end do;
    r := [seq(chrem(w[j], [seq((f[l])[1]^(f[l])[2], l = 1..t)]), j = 1..tw)]
end proc
```

```
> rac:=racinecarree(144,73);
```

$$rac := [19, 109, 91, 37, 35, 125, 107, 53] \tag{5.2}$$

```
> for i from 1 to 8 do rac[i]^2 mod 144 od;
>
```

$$73$$
$$73$$
$$73$$
$$73$$
$$73$$
$$73$$
$$73$$
$$73 \tag{5.3}$$

Racines d'un polynôme P modulo un nombre premier p.

J'emploie ici la méthode naïve qui consiste à essayer tous les entiers entre 0 et p.

```
> racpol:=proc(f,p)
  local i,l;
  l := NULL;
  for i from 0 to p-1 do
```

```
        if subs(x=i,f) mod p = 0 then l:=l,i fi
    od;
    []];
    end;
```

$$racpol := \mathbf{proc}(f, p) \tag{6.1}$$

```
    local i, l;
    l := NULL;
    for i from 0 to p - 1 do
        if mod(subs(x = i, f), p) = 0 then
            l := l, i
        end if
    end do;
    [l]
end proc
```

```
> P:=x^6+x+1;
```

$$P := x^6 + x + 1 \tag{6.2}$$

```
> p:=ithprime(100);
```

$$p := 541 \tag{6.3}$$

```
> racpol(P,p);
```

$$[19] \tag{6.4}$$

```
> subs(x=19,P);
```

$$47045901 \tag{6.5}$$

```
> % mod p;
```

$$0 \tag{6.6}$$

```
> Pp:=diff(P,x);
```

$$Pp := 6\,x^5 + 1 \tag{6.7}$$

```
> subs(x=19,Pp) mod p;
```

$$194 \tag{6.8}$$

Racines d'un polynôme P modulo p^n.

```
>
```

On suppose avoir trouvé r tel que P(r)=0 mod p. On suppose que P'(r) est non nul modulo p.

```
> racpolpn:=proc(P,p,n,r)
  local t,q,i,Pp,s;
  Pp := diff(P,x);
  s := r;
```

```
    q := p;
    for i from 1 to n-1 do
        t := -subs(x=s,P)/q;
        t := t*subs(x=r,Pp)&^(-1) mod p;
        s := s+t*q mod q*p;
        q := q*p;
    od;
    s;
    end;
```

$$racpolpn := \mathbf{proc}(P, p, n, r) \tag{7.1}$$

$\mathbf{local}\ t, q, i, Pp, s;$

$Pp := diff(P, x);$

$s := r;$

$q := p;$

$\mathbf{for}\ i\ \mathbf{to}\ n - 1\ \mathbf{do}$

$t := -subs(x = s, P) / q;$

$t := mod(t * subs(x = r, Pp)\ \&^{\wedge}\ (-1), p);$

$s := mod(s + t * q, q * p);$

$q := q * p$

$\mathbf{end\ do};$

s

$\mathbf{end\ proc}$

```
> racpolpn(P,p,4,19);
```

$$11744480295 \tag{7.2}$$

```
> subs(x=%,P) mod 541^4;
```

$$0 \tag{7.3}$$

Fonctions de maple.

```
>
> msolve(x^2-5,541);
```

$$\{x = 345\}, \{x = 196\} \tag{8.1}$$

```
> 345^2 mod 541;
```

$$5 \tag{8.2}$$

```
> msqrt(5,541);
```

$$345 \tag{8.3}$$

```
> msqrt(5,541^10);
```

$$389348149595433174722613811 \tag{8.4}$$

```
> primroot(541^10);
```

$$2 \tag{8.5}$$

```
> mlog(5,2,541^10);
```

$$443956383514128568349099296 \tag{8.6}$$

```
> 2&^% mod 541^10; #  "&^" impose de faire les calculs
  intermédiaires
                   #  modulo 541^10.
```

$$5 \tag{8.7}$$

```
> mlog(5,2,7);
```

$$\mathit{FAIL} \tag{8.8}$$

```
> Donc on ne peut pas trouver y tel que 2^y=5 mod 7.
> 19^4
```

$$130321 \tag{8.9}$$

```
>
```