Powers*permet de calculer a^k mod n en dcomposant k en base 2.*

Powers := **proc**(*nak*)**local** *X*, *Z*, *r*, *Y*, *A*, *i*, *j*; *X* := *convert*(*k*, *'base'*, 2); *Z* := *convert*(*X*, *array*);

while 2^*r*&*lek* **do** *r* := *r* + 1 **end do**;; *A* := *Matrix*(1, *r*); *A*[1, 1] := *a*; **for** *i* **from** 2 **to** *r* **do** *A*[1, *i*] := *mod*(*A*[1, *i* +

Algorithme p-1 de Pollard

; *a* := 3; **for** *d* **from** 2 **to** *factorial*(1000) **do** *b* := *Powers*(*n*, *a*, *d*); *g* := *gcd*(*b* + −1, *n*); **if** 1 < *g* **then** **retur**

Exemple du livre de Silverman section 4.4

Pollard (1715761513)

26927

double*permet de calculer kP avec P=(x1,y1) et la courbe elliptique donne par y^2=x^3+bx+c*

mod(−*lambda* ∗ *A*[1, 2 ∗ *j* + 1] − *nu*, *n*) **else** **return** *max*(*gcd*(*A*[1, 2 ∗ *j*], *n*), *gcd*(4 ∗ *A*[1, 2 ∗ *j* + −1]^3 + 4 ∗ *b* ∗ *A*[1, 2 ∗ *j* +

Factorisation de Lenstra par les courbes elliptiques ou ECM

; **for** *p* **from** 2 **to** *factorial*(1000) **do** *Q* := *double*(*factorial*(*p*), *x*1, *y*1, *b*, *c*, *n*); **if** *Q* :: *integer* **then** **return** *Q* **en**

Exemple du livre de Silverman Section 4.4

Lenstra (1715761513)

26927

− (*a* + 2) ∗ *P*[1, 1] ∗ *P*[1, 2]), *n*); *Q*[1, 1] := *h*[1, 1]; *Q*[1, 2] := *h*[1, 2]; *P*[1, 1] := *m*[1, 1]; *P*

to 300000000 **do** *Q* := *echelle*(*p*, *x*1, *a*, *b*, *n*); *a* := *rand*(); *x*1 := *rand*(); **if** *Q* :: *integer* **then** **return** *Q*

with (*numtheory*)

ssqrfree, *ithrational*, *jacobi*, *kronecker*, *λ*, *legendre*, *mcombine*, *mersenne*, *migcdex*, *minkowski*, *mipolys*, *mlog*, *mobius*, *mroot*, *msqrt*, *nearestp*,

, *y*, *s*; *s* := 0; **for** *x* **from** 0 **to** *p* + −1 **do** *y* := *x*^3 + *a* ∗ *x*^2 + *b* ∗ *x* + *c*; *s* := *s* + 1 + *numtheory* : −*legendre*(*y*, *p*) **end**

card (1525453, 45646, 166, 11)