Quelques algorithmes implantés dans PARI/GP

GP>

Arithmétique entière

Il est nettement préférable d'utiliser la bibliothèque GMP pour l'arithmétique entière. Cette bibiliothèque fournit entre autre les algorithmes suivants :

1. Multiplication et division (Karatsuba, Toom-Cook, FFT)
2. Racine carré asymptotiquement rapide
3. PGCD et PGCD étendu sous-quadratique
4. Changement de base asymptotiquement rapide

Entiers

Factorisation

Fonction GP `factorint` Les algorithmes suivant sont implantés :
- ρ (Pollard-Brent)
- SQUFOF (Shanks)
- ECM (Lenstra)
- MPQS (Pomerance)

Primalité

- Crible d'Ératosthéne récursif.
- ispseudoprime : test de pseudo-primalité au sens de Baillie-Pomerance-Selfridge-Wagstaff
- isprime : Algorithmes de Selfridge et de Adleman-Pomerance-Rumely-Cohen-Lenstra

Calculs de PGCD

PGCD simple et étendu sur $\mathbb{Z}$

- gcd : Algorithme de Lehmer-Jebelean (utilisation des mots de têtes).
  Avec GMP : PGCD sous quadratique.
- bestappr : Algorithmes de reonnaissance des rationnels (réels et p-adique)

PGCD sur $\mathbb{Z}[X]$

Algorithme du PGCD modulaire classique

PGCD pour des polynômes sur un corps de nombre

Algorithme du PGCD modulaire de Encarnacion.

Résultants

Résultants sur $\mathbb{F}_p[X]$ et $\mathbb{F}_p[X, Y]$

Algorithme du sous résultant et algorithme d'interpolation.

Résultants sur $\mathbb{Q}[X]$ et $\mathbb{Q}[X, Y]$

Résultants modulaires à une ou deux variables

Résultants sur un anneau inexact

Utilisation de la matrice de Sylvester.

Résultants sur un anneau exact général

Algorithme sur sous-résultant de Lazard/Ducos.

Algèbre linéaire

Algèbre linéaire sur un corps

- matker/matimage/matsolve/matdet : Pivot de Gauss.
- matfrobenius : (réduite de Frobenius) Utilisation de la HNF polynomial

Forme normal de Hermite et de Smith

fonctions mathnf/matsnf :
- Algorithme naïf.
- Algorithme de Batut
- Algorithme HNFLLL
- Algorithme modulaire

Réduction LLL de réseau et applications

Algorithme L^2 de Phong Nguyen and Damien Stehlé qflll/qflllgram : Réduction de réseau LLL.

Applications

- matkerint : $\mathbb{Z}$-base du noyau d'une matrice à coefficients entiers.
- lindep, algdep : Relation linéaire entre flottants.
- qfminim : algorithme de Fincke-Pohst pour trouver un vecteur minimal dans un réseau.
- polredabs : polynôme canonique définissant un corps de nombre en utilisant Fincke-Pohst.
- zncoppersmith : algorithme de Coppersmith pour trouver une petite solution à une équation modulaire.

Factorisation de polynômes

Factorisation sur $\mathbb{Z}$

factor : Algorithme de van Hoeij.

Factorisation sur un corps de nombre

- nffactor : Algorithme de van Hoeij modifié.
- factornf : Méthode de Trager.

Recherche de racines sur $\mathbb{C}$

polroots : Algorithme de Schönhage/Gourdon (non heuristique).

Factorisation de polynômes sur $\mathbb{F}_p$

- factormod : Algorithme de Berlekamp.
- factorcantor : Algorithme de Cantor-Zassenhauss.

Factorisation de polynômes sur $\mathbb{F}_q$

Fonction GP factorff.

- Algorithme de Cantor-Zassenhauss.
- Algorithme de Berlekamp
- Algorithme de B.A. pour la factorisation sur $\mathbb{F}_q$ de polynômes définis sur $\mathbb{F}_p$ (factorisation relative).

Construction de polynômes irreductibles

ffinit : Algorithme déterministe de Adleman-Lenstra-B.A.

Fonctions transcendantes

- Pi, log : Utilisation de la moyenne arithmético-géométrique.
- zeta : fonction ζ de Riemann par la sommation d'Euler-Maclaurin.
- zetak : fonction ζ_K d'un corps de nombre, méthode de Tollis.
- besselh1, besselh2, besseli, besselj, besseljh, besselk, besseln : Fonctions de Bessel.

Sommations (heuristiques)

- intnum : Integration par la méthode dite 'doublement exponentielle'.
- intnumromb : Integration par la méthode de Romberg.
- sumalt : Algorithme de Cohen, Villegas et Zagier pour les séries alternées.

Groupes génériques

Algorithmes pour des groupes cyclique génériques :

- znlog/fflog : logarithme discret Algorithme de Pohlig-Hellman et algorithme ”pas de bébé/pas de géant” de Shanks.
- znorder/fforder : ordre d’un élément.
- znprimroot/ffprimroot : générateur.

Corps de nombres

calcul d'une $\mathbb{Z}$-base de l'anneau des entiers.

nfdisc/nfbasis : Algorithme Round 4 de Zassenhauss,Ford-Pauli-Roblot.

factorisation d'idéaux

idealprimedec/idealfactor : Algorithme de Buchmann-Lenstra.

Calcul du groupe de classes

– quadclassunit,bnfinit,bnfisprincipal : Algorithme de Buchmann (heuristique, sous GRH).
– bnfcertify : Permet de certifier le résulat inconditionnellement (lent).

Théorie du corps de classes

Calcul des groupes de rayons

- bnrinit/bnrisprincipal : algorithme de Cohen et al.
- rnfconductor : calcul du conducteur.

Calcul d'un polynôme definissant une extension abélienne

- rnfkummer : Utilisation de la théorie de Kummer et du théorème de Hecke.
- quadhilbert/quadray, cas imaginaire : Méthode de Schertz basé sur la réciprocité de Shimura.
- bnrstark, quadhilbert/quadray, cas réel : Utilisation des unités de Stark (Roblot).

Théorie de Galois

- polgalois : Classe de conjugaison du Groupe de Galois d'un polynôme (Méthode des résolvents de Stauduhar/Eichenlaub)
- nfsubfields : Calcul des sous-corps par l'algorithme de Klüners.
- galoisinit : Groupe de Galois explicite (Algorithme de B.A.)
- galoisfixedfield : Calcul de corps fixes par sommes de Newton (Algorithme de B.A.).
- galoissubgroups : Calcul des sous-groupes du groupe de Galois (Algorithme de B.A.).
- galoisidentify : Classe d'isomorphisme du groupe de Galois (méthode du calcul des traces des éléments et des classes d'isomorphismes des sous-groupes maximaux (B.A.)).
- polsubcyclo,galoissubcyclo : calcul de polynômes sous-cyclotomiques.

Équations diophantienne

Formes quadratiques

qfbsolve : Résoud $q(x, y) = p$ ou p est premier. Algorithmes de Gauss et de Cornacchia

Équation aux normes

- bnfisnorm : Résoud $N_K/\mathbb{Q}(x) = m$
- rnfisnorm : Résoud $N_L/K(x) = \alpha$ Algorithmes de Simon.
- bnfisintnorm : Résoud l'équation au norme en entiers algébriques.

Équation de Thué

thueinit/thue : Algorithme de Hanrot (parfois conditionnel)

Courbes elliptiques

- elladd,ellpow : Addition de points sur une courbe.
- ellglobalred : conducteur de la courbe.
- ellsearch : Interface avec la base de donnée de Cremona.

Nombre de point sur $\mathbb{F}_p$

ellap : les algorithmes suivants sont utilisés :

- Sommes de Jacobi,
- Détection des courbes à multiplication complexes par un ordre principal,
- Algorithme de Shanks-Mestre,
- Algorithme de Schoof-Elkies-Atkin.

Combinatoire

Factoriel

$n!$, binomial : Algorithme "diviser pour régner"

Nombres de Stirling

stirling : Nombres de Stirling de première et seconde espèces.

Nombre de partition

numbpart : Formule de Hardy-Ramanujan-Rademacher