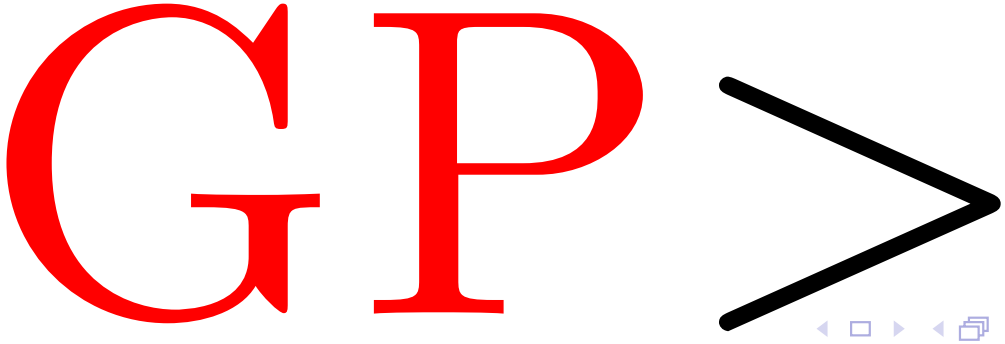
Utilisation de PARI/GP pour la théorie algébrique des nombres.

Bill Allombert

Université Montpellier 2 LIRMM/I3M
(avec Karim Belabas, Université Bordeaux 1)

22/01/2010



Le système de calcul formel PARI/GP

Un système de calcul formel pour des calculs orientés vers des applications en théorie des nombres.

Auteurs	Originellement écrit en 1987 by Henri Cohen et ses collaborateurs àl'université de Bordeaux. Maintenu par Karim Belabas depuis 1995.
License	GNU General Public License depuis 2000.
Web site	http ://pari.math.u-bordeaux1.fr

Les composantes de PARI/GP

PARI/GP contient plusieurs composantes :

- La bibliothèque C PARI (libpari)
- L'interpréteur de commande GP (gp)
- Le compilateur GP2C (gp2c) (distribué séparément)
- La documentation
- Des bases de données optionnelles

Dernières versions :

- PARI/GP Stable version : 2.3.4
- PARI/GP Development version : 2.4.3
- GP2C version : 0.0.5pl8

Le code source code

- Écrit en C ANSI avec utilisation optionelle d'assembleur en ligne pour les architectures suivantes : amd64, alpha, hppa, hppa64, ia64, ix86, m68k, ppc, ppc64, sparc
- Support optionnel pour la bibliothèque GMP (pour une arithmétique plus rapide avec les grands nombres).
- Très portable.
- Utilisation modeste des ressources.

Que peut faire PARI/GP

- calculs entiers et flottants en précision arbitraire.
- factorisation et test de primality, fonctions arithmétique usuelle.
- fonctions transcendantes (ζ, Γ).
- analyse numérique (intégration numérique, somme de series, algèbre linéaire).
- polynomes univariés et séries formelles.
- factorisation de polynomes sur $\mathbb{C}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, un corps de nombres).
- Algèbre linéaire sur $\mathbb{Z}$, $k[X]$, ou un corps ;
- réduction de réseau et applications (plus court vecteur, reconnaissance des nombres algébriques).
- corps de nombres, théorie du corps de classes, théorie de Galois.
- courbles elliptiques.

Réduction LLL de réseau et applications

qflll/qfllllgram : Réduction de réseau LLL.

Applications

- matkerint : $\mathbb{Z}$-base du noyau d'une matrice à coefficients entiers.
- lindep, algdep : Relation linéaire entre flottants.
- qfminim : trouver un vecteur minimal dans un réseau.
- polredabs : polynôme canonique définissant un corps de nombre

Fonctions transcendantes

- zeta : fonction ζ de Riemann par la sommation d'Euler-Maclaurin.
- 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.

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
- nfsubfields : Calcul des sous-corps
- galoisinit : Groupe de Galois explicite
- galoisfixedfield : Calcul de corps fixes
- galoissubgroups : Calcul des sous-groupes du groupe de Galois
- galoisidentify : Classe d'isomorphisme du groupe de Galois
- polsubcyclo,galoissubcyclo : calcul de polynômes sous-cyclotomiques.

Équations diophantienne

Formes quadratiques

qfbsolve : Résoud $q(x, y) = p$ ou p est premier.

Équation aux normes

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

Équation de Thué

thueinit/thue : Résoud une équation de Thué.

Courbes elliptiques

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

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

ellap : Algorithme de Schoof-Elkies-Atkin.

Factorisation de 38 en produit d'irreductibles dans le corps $K = \mathbb{Q}(\sqrt[3]{7})$.

$$\begin{aligned} 38 &= 2 \times 19 \\ &= (\sqrt[3]{49} + 3\sqrt[3]{7} + 3)(3\sqrt[3]{49} - \sqrt[3]{7} - 6) \\ &= (\sqrt[3]{49} + \sqrt[3]{7} - 1)(\sqrt[3]{49} + 4\sqrt[3]{7} - 3) \end{aligned}$$