Liste de publications de Karim Belabas
(au 1 Décembre 2016)

Articles dans des revues à comité de lecture:

(1) (avec J.-F. Jaulent) The logarithmic class group package in PARI/GP, *Presses Mathématiques de Besançon*, à paraître.
(2) (avec C. Delaunay) Les travaux de Manjul Bhargava, *Gazette des Mathématiciens*, Vol. 143, pp. 6–15, 2015.
(3) (avec E. Friedman) Computing the residue of the Dedekind zeta function, *Mathematics of Computation*, Vol. 84, pp. 357–369, 2015.
(4) Algorithms for finite fields, *Panorama & Synthèses*, Vol. 36, pp. 1–17, 2013.
(5) (avec M. Bhargava et C. Pomerance) Error estimates for the Davenport-Heilbronn theorems, *Duke Mathematical Journal*, Vol. 153, pp. 173–210, 2010.
(6) (avec É. Fouvry) Discriminants cubiques et progressions arithmétiques, *International Journal of Number Theory*, Vol. 6 (7), pp. 1491–1529, 2010.
(7) (avec M. van Hoeij, J. Klüners et A. Steel) Factoring polynomials over global fields, *Journal de Théorie des Nombres de Bordeaux*, Vol. 21, pp. 15–39, 2009.
(8) (avec B. Allombert) Practical Aurifeuillian factorization, *Journal de Théorie des Nombres de Bordeaux*, Vol. 20, pp. 543–553, 2008.
(9) (avec F. Diaz y Diaz et E. Friedman) Small generators of the ideal class group, *Math. Comp.*, Vol. 77, pp. 1185–1197, 2008.
(10) Paramétrisation de structures algébriques et densité de discriminants, d'après Bhargava, *Astérisque* (séminaire Bourbaki), Vol. 299, pp. 267–299, 2005.
(11) Topics in computational algebraic number theory, *Journal de Théorie des Nombres de Bordeaux*, Vol. 16, pp. 19–63, 2004.
(12) A relative van Hoeij algorithm over number fields, *Journal of Symbolic Computation*, Vol. 37, pp. 641–668, 2004.
(13) (avec H. Gangl) Generators and relations for $K_2\mathcal{O}_F$, *K-theory*, Vol. 31, pp. 195–231, 2004.
(14) On quadratic fields with large 3-rank, *Math. Comp.*, Vol. 73, pp. 2061–2074, 2004.
(15) (avec F. Paulin et S. Hersonsky) Counting horoballs and rational geodesics, *Bull. London Math. Society*, Vol. 33, pp. 606–612, 2001.
(16) (avec L. Raïd) Quine critique de Peirce : vérité et convergence, *Philosophia Scientiae – Public@tions Électroniques* **1** (2001), 13 p.

(17) (avec H. Gangl) Determining $K_2\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ for $0 > d \geqslant -151$, *appendice à* Computing the tame kernel of quadratic imaginary fields, J. Browkin, *Mathematics of Computation*, Vol. 69, pp. 1681–1683, 2000.

(18) (avec É. Fouvry) Sur le 3-rang des corps quadratiques de discriminant premier ou pseudo-premier, *Duke Mathematical Journal*, Vol. 98, pp. 217–268, 1999.

(19) On the mean 3-rank of quadratic fields, *Compositio Mathematica*, Vol. 118, pp. 1–9, 1999 ; corrigendum *ibid* **140** (2004), p. 1221.

(20) (avec H. Cohen) Binary cubic forms and cubic number fields, in *Computational perspectives in Number Theory*, eds. D. Buell et J. Teitelbaum, 1998.

(21) A fast algorithm to compute cubic fields, *Mathematics of Computation*, Vol. 66, pp. 1213–1237, 1997.

(22) Crible et 3-rang des corps quadratiques, *Annales de l'Institut Fourier*, Vol. 46, pp. 909–949, 1996.

(23) Computing cubic fields in quasi-linear time, ANTSII, Bordeaux (1996), *in* LNCS 1122, Springer-Verlag, pp. 17–25.

(24) Variations sur un thème de Davenport et Heilbronn, *Séminaire de Théorie des Nombres de Paris*, 17 p. (1997). Arbitré et accepté pour publication, non paru suite à disparition de la collection.

Livres ou chapitres de livres:

(L1) (avec L. Raïd) L'analyse logique des probabilités selon Waismann, in *F. Waismann, Textures Logiques*, Cahiers de Philosophie du Langage, vol. 6, L'Harmattan, Paris, 2009, pp. 235–260.

(L2) L'algorithmique de la théorie algébrique des nombres, dans *Théorie algorithmique des nombres et équations diophantiennes* (N. Berline, A. Plagne, C. Sabbah, eds.). Ed. de l'École Polytechnique, pp. 85–153, 2005.

(L3) PARI-GP in *Handbook of Computer Algebra*, Eds. J. Grabmeier *et al.*, Springer, 2003, pp. 431–434.

Édition d'ouvrages:

(E1) *Explicit methods in number theory. Rational points and Diophantine equations*, 179 pages, *Panoramas et Synthèses* **36**, 179p., 2013.

Publications non cosignées issues des thèses encadrées: par principe, je ne cosigne pas les travaux réalisés par les étudiants que j'encadre.

(1) J. Brau et N. Jones Elliptic curves with 2-torsion contained in the 3-torsion field, *Proc. Amer. Math. Soc* Vol. 144, pp. 925–936, 2016.

(2) A. Page Computing arithmetic Kleinian groups, *Mathematics of Computation* Vol. 84, pp. 2361–2390, 2015.

(3) A. Page An algorithm for the principal ideal problem in indefinite quaternion algebras. *LMS J. Comput. Math.* Vol. 17, *ANTS XI*, pp. 366–384, 2014.

(4) N. Mascot Computing modular Galois representations *Rend. Circ .Mat. Palermo*, Vol. 62, No 3, pp. 451–476, 2013.
(5) A. Morra An algorithm to compute relative cubic fields, *Math. Comp.*, Vol. 284, pp. 2343–2361, 2013.
(6) A. Angelakis et P. Stevenhagen Imaginary quadratic fields with isomorphic abelian Galois groups, *ANTS X*, The Open Book Series vol. 1., Berkeley, pp. 21–39, 2013.
(7) C. Clavier, B. Feix, G. Gagnerot, C. Giraud, M. Roussellet et V. Verneuil, ROSETTA for Single Trace Analysis, *Progress in Cryptology - Indocrypt 2012*, LNCS vol. 7668, pp. 140–155, Springer, 2012.
(8) C. Clavier, B. Feix, G. Gagnerot, M. Roussellet et V. Verneuil, Square Always Exponentiation, *Progress in Cryptology - Indocrypt 2011*, LNCS vol. 7107, pp. 40–57, Springer, 2011.
(9) C. Clavier, B. Feix, G. Gagnerot, M. Roussellet et V. Verneuil, Improved Collision-Correlation Power Analysis on First Order Protected AES, *Cryptographic Hardware and Embedded Systems - CHES 2011*, LNCS vol. 6917, pp. 49–62, Springer, 2011.
(10) H. Cohen et A. Morra Counting cubic extensions with given quadratic resolvent, *J. Algebra*, Vol. 325, pp. 461–478, 2011.
(11) C. Clavier, B. Feix, G. Gagnerot, M. Roussellet et V. Verneuil, Horizontal Correlation Analysis on Exponentiation, *Information and Communications Security (ICICS 2010)*, LNCS vol. 6476, pp. 46–61, Springer, 2010.