Ezome, Tony; **Lercier, Reynald**

Elliptic periods and primality proving. (English) Zbl 1310.11118

J. Number Theory 133, No. 1, 343-368 (2013).

From the text: We construct extension rings with fast arithmetic using isogenies between elliptic curves. As an application, we give an elliptic version of the AKS primality criterion.

The main restriction of classical Kummer theory is that not every ring R has a primitive d-th root of unity. One may look for an auxiliary extension $R' \supset R$ that contains such a primitive root, but this may result in many complications and a great loss of efficiency. Another approach, already experimented in the context of normal bases for finite fields extensions, consists in replacing the multiplicative group $\mathbb{G}_m$ by some well chosen elliptic curve E over R. We then look for a section $T \in E(R)$ of exact order d. Because elliptic curves are many, we increase our chances to find such a section. We call the resulting algebra S a ring of elliptic periods because of the strong analogy with classical Gauss periods.

The first half of the present work is devoted to the explicit study of Kummer theory of elliptic curves and, more specifically, to the algebraic and algorithmic description of the residue algebras constructed. The resulting elliptic functions and equations are not quite as simple as binomials. Still they can be described very explicitly and quickly, e.g. in quasi-linear time in the degree d. The geometric situation is summarized by Theorem 1 and the R-algebra S of elliptic periods is described by Theorem 2.

The second half of the paper proposes an elliptic version of the AKS primality criterion. A general, context free, primality criterion in the style of Berrizbeitia is first given in Theorem 3. This criterion involves an R-algebra S where $R = \mathbb{Z}/n\mathbb{Z}$ and n is the integer to be tested for primality. If we take S to be $R[x] = (x^d - \alpha)$, we recover results by Berrizbeitia and his followers. If we take S to be a ring of elliptic periods, we obtain the elliptic primality criterion of Corollary 2.

MSC:

11Y11 Primality
11Y16 Number-theoretic algorithms; complexity
14H52 Elliptic curves

Keywords:

elliptic curve; primality; Galois theory; probabilistic algorithms; ring theory

Software:

ECPP

Full Text: DOI arXiv

References:

[1] Agrawal, M.; Kayal, N.; Saxena, N., {\scprimes} is in {\scp}, Ann. of Math., 160, 781-793, (2004) · Zbl 1071.11070

[2] Ash, D. W.; Blake, I. F.; Vanstone, S. A., Low complexity normal bases, Discrete Appl. Math., 25, 191-210, (1989) · Zbl 0712.11073

[3] Atiyah, M.; McDonald, I. G., Introduction to commutative algebra, (1969), Addison-Wesley Publishing Company · Zbl 0175.03601

[4] R.M. Avanzi, P. Mihăilescu, Efficient quasi-deterministic primality test improving AKS, 2007; available at http://xwww.uni-math.gwdg.de/preda/.

[5] Bernstein, D. J., Proving primality in essentially quartic random time, Math. Comp., 76, 389-403, (2007) · Zbl 1144.11085

[6] Berrizbeitia, P., Sharpening "primes is in P" for a large family of numbers, Math. Comp., 74, 2043-2059, (2005) · Zbl 1071.11071

[7] Bourbaki, N., Algèbre commutative, Éléments de mathématiques, (2006), Springer, (Chapitres 5 à 7) · Zbl 0141.03501

[8] Cheng, Q., Primality proving via one round in ECPP and one iteration in AKS, J. Cryptology, 20, 375-387, (2007) · Zbl 1155.11362

[9] Couveignes, J. M.; Lercier, R., Elliptic periods for finite fields, Finite Fields Appl., 15, 1-22, (2009) · Zbl 1216.11106

[10] Enge, A., Elliptic curves and their applications to cryptography — an introduction, (1999), Kluwer · Zbl 1335.11002

[11] Gao, S.; Lenstra, H. W., Optimal normal basis, Des. Codes Cryptogr., 2, 315-323, (1992) · Zbl 0770.11055

[12] Joux, A.; Lercier, R., The function field sieve in the medium prime case, (Vaudenay, S., Advances in Cryptology — EUROCRYPT 2006, Lecture Notes in Comput. Sci., vol. 4004, (2006), Springer Berlin/Heidelberg), 254-270 · Zbl 1140.94349

[13] Katz, N. M.; Mazur, B., Arithmetic moduli of elliptic curves, Ann. of Math. Stud., vol. 108, (1985), Princeton University Press · Zbl 0576.14026

[14] Kedlaya, K. S.; Umans, C., Fast modular composition in any characteristic, (Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science, (2008), IEEE Computer Society), 146-155

[15] Lenstra, A. K.; Lenstra, H. W., Algorithms in number theory, (van Leeuwen, J., Handbook of Theoretical Computer Science, vol. A: Algorithms and Complexity (A), (1990), North-Holland), 673-716 · Zbl 0900.68250

[16] H.W. Lenstra, C. Pomerance, Primality testing with gaussian periods, Dartmouth, 2009; available at http://www.math.dartmouth.edu/~carlp/PDF

[17] Lercier, R.; Lubicz, D., Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time, (Biham, E., Advances in Cryptology — EUROCRYPT 2003, Lecture Notes in Comput. Sci., vol. 2656, (2003), Springer Berlin/Heidelberg), 360-373 · Zbl 1035.11067

[18] Liu, Q., Algebraic geometry and arithmetic curve, Oxford Sci. Publ., (2006)

[19] Morain, F., Implementing the asymptotically fast version of the elliptic curve primality proving algorithm, Math. Comp., 76, 493-505, (2007) · Zbl 1127.11084

[20] Mullin, R. C.; Onyszchuk, I. M.; Vanstone, S. A.; Wilson, R. M., Optimal normal bases in $\operatorname{GF}(p^n)$, Discrete Appl. Math., 22, 149-161, (1988-1989) · Zbl 0661.12007

[21] Schönhage, A. A., Schnelle multiplikation von polynomen über Körpern der charakteristik 2, Acta Inform., 7, 395-398, (1977) · Zbl 0362.65011

[22] Schönhage, A.; Strassen, V., Schnelle multiplikation großer zahlen, Computing, 7, 281-292, (1971) · Zbl 0223.68007

[23] Schoof, R., Four primality testing algorithms, (Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Math. Sci. Res. Inst. Publ., vol. 44, (2008), Cambridge Univ. Press Cambridge), 101-126, (Surveys in Number Theory) · Zbl 1196.11169

[24] Vélu, J., Isogénies entre courbes elliptiques, C. R. Acad. Sci. Sér. I, 273, 238-241, (1971) · Zbl 0225.14014

[25] Vélu, J., Courbes elliptiques munies d'un sous-groupe $\mathbb{Z} / n \mathbb{Z} \times \mu_n$, Mém. Soc. Math. Fr., 57, (1978) · Zbl 0433.14029

[26] Voloch, J. F., On some subgroups of the multiplicative group of a finite ring, J. Théor. Nombres Bordeaux, 16, 233-239, (2004) · Zbl 1078.11069