MATHEMATICS OF COMPUTATION
Volume 70, Number 236, Pages 1755-1759
S 0025-5718(01)01400-4
Article electronically published on May 22, 2001

REVIEWS AND DESCRIPTIONS OF TABLES AND BOOKS

14[94-02, 94A60, 14H52] *Elliptic curves in cryptography* by Ian Blake, Gadiel Seroussi, and Nigel Smart, Cambridge University Press, New York, NY, 1999, xv+204 pp., 23 cm. softcover $39.95

Elliptic curves have been studied for more than a century from the perspectives of modular forms, complex analysis, algebraic geometry, and number theory. Schoof's discovery [10, 1984], that there is a polynomial time algorithm for establishing the size of the elliptic curve group over any finite field opened the way to various computational applications of these groups.

One by one, most applications which were customary in the multiplicative group of finite fields were adapted to the elliptic curve group. In the space of a few years, elliptic curves emerged in primality proving [5], integer factoring [6], and cryptography [8]. The first two applications take advantage of the large variety of available groups of the chosen order of magnitude, while the interest of the latter is based on the fact that in general no subexponential algorithm for computing the discrete logarithm in the elliptic curve group is known or likely to be found. Such algorithms had been known for some time in the multiplicative groups. However, many practical questions were still asking for improvements and clarity, so the last 15 years have seen intense research in this domain of applications.

The book at hand is a welcome, in-depth treatment of the various research and improvements up to 1999. It offers a comprehensive presentation of both the deeper theoretical background of algorithmic developments and the implementational bottlenecks. Whoever wants to deal with algorithmal aspects of elliptic curves will find here an excellent and, in most cases, sufficient starting point. The book is therefore not intended either as primary didactical material (proofs are scarcely given) nor as a compendium of the various short or long lived cryprographical mechanisms related to elliptic curves. For the first, books such as [7] for the practical and [3] for the mathematical aspects, are recommendable. For the latter, the technical IEEE standard P1363, which has been meanwhile released, is the relevant source for those mechanisms which are likely to be spread in practice.

The first two chapters offer a succinct introduction to general ideas of public key cryptography and the underlying arithmetic in finite fields. The important third chapter introduces the arithmetic of elliptic curves together with the various connections to division polynomials, Weil pairing, and modular functions, which have found explicit use in applications. The fourth chapter gives an overview of efficient implementations of elliptic curves arithmetic for the practitioner, and the fifth treats the discrete logarithm problem on elliptic curves. From the sixth to the eighth chapters the authors discuss the determination of the group order, by Schoof's algorithm and its later improvements and by an a priori choice of the complex multiplication fields of the target curve. The book closes with an overview

of primality proving and integer factoring using elliptic curves in the ninth chapter, and with generalizations of cryptosystems to abelian varieties of higher genus in the tenth chapter.

Let $\mathbb{F}_q$ be a finite field with q elements. An elliptic curve E over $\mathbb{F}_q$ is defined by a *long Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$ are such that the equation is nonsingular. This is equivalent to saying that the *discriminant*

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 90b_2b_4b_6 \neq 0,$$

where $b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6, b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. From the definition of the discriminant, it follows that it has special behavior in fields of characteristic 2 or 3. In fact, most applications in finite fields are treated differently in characteristic $p \leq 3$ and $p > 3$. In the book the clear choice to deal only with the cases of characteristics 2 and prime fields $\mathbb{F}_p$ with $p > 3$ was made. It is customary to indicate by $E(\mathbb{F}_q)$ the set of points on $\mathbb{F}_q^2$ of the equation defining E together with an extra point $\mathcal{O}$ at infinity, which one may think of as lying on the top of the y-axis. For two points, $P_1 = (x_1, y_1), P_2(x_2, y_2) \in E(\mathbb{F}_q)$, the sum is $P_1 \oplus P_2 = (x_3, y_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \mu - a_3)$, where

$$(\lambda, \mu) = \begin{cases} \left(\frac{y_2-y_1}{x_2-x_1}, \frac{y_1x_2-y_2x_1}{x_2-x_1}\right) & \text{if } x_1 \neq x_2, \\ \left(\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_2x_1+a_3}, \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_2x_1+a_3}\right) & \text{if } x_1 = x_2. \end{cases}$$

This composition rule makes $(E(\mathbb{F}_q), \oplus)$ into a commutative group with $\mathcal{O}$ as its neutral element and $E(\mathbb{F}_q) \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z})$, where d_1 divides both d_2 and $q - 1$. The n-fold addition of P to itself is $[n]P$ and $E[n] \cong (\mathbb{Z}/(n \cdot \mathbb{Z}))^2$ is the n-torsion group of E over $\overline{\mathbb{F}}_q$. The x-coordinates of the n torsion points are zeroes of the division polynomials Ψ_n. These notions, together with the more subtle connections to modular functions and complex multiplication, which we shall not describe here, are introduced in the third chapter, yielding a self-sufficient base for the understanding of all algorithms treated subsequently. The fourth chapter is an extensive overview of the main practical aspects which the implementer will encounter, from arithmetic tricks to point compression—a technical term (in cryptography) for the idea that a point on the curve carries essentially the information of its x coordinate plus one bit allowing to distinguish a solution of a quadratic equation.

The problem of taking the discrete logarithm on elliptic curves is the door to cryptographic applications of these groups. The known general techniques are treated comprehensively in chapter five. In the following special cases, described in this chapter, more performant algorithms than the generic ones are possible: First, the supersingular curves for which the Weil pairing yields an isomorphism to the roots of unity of the ground field or a small extension thereof, where subexponential index calculus methods can be applied. Second, the recent algorithm of Smart for computing the discrete logarithms on curves with the number of points equal to the (prime) characteristic of the field over which they are defined.

Unsurprisingly, the problem of determining the number of points in the elliptic curve group, which brought curves into computational algebra, is covered in three

extensive chapters. The first short one gives an overview of naive approaches and problems related to subgroups of the elliptic curve group.

The sixth and seventh chapters cover the generic algorithm of Schoof and its ulterior improvements and adaptations to *tricky* characteristics (i.e., $p = 2, 3$, with special behavior of the discriminant). The basic algorithm of Schoof for computing $\#E(\mathbb{F}_q)$ (that we briefly outline being the first step in the journey of which the book is telling the story) is based on the fact that from Hasse's Theorem, namely $\#E(\mathbb{F}_q) = q + 1 - t$ with $|t| \leq 2\sqrt{q}$, it is enough to determine t modulo l for sufficiently many small primes l. More precisely, it suffices to take primes $l \leq l_{\max}$ with $\prod_{l \leq l_{\max}} l > 4\sqrt{q}$. One uses the fact that the Frobenius endomorphism ϕ satisfies the equation $\phi^2 - t\phi + q = 0$. Considering a nontrivial point $P = (x, y) \in E[l]$, one lets $q_l = q \bmod l$. Then $(x^{q^2}, y^{q^2}) + [q_l](x, y) = [\tau](x^q, y^q)$ must be satisfied exactly for $\tau = t \bmod l$. The value of τ can be found by computing symbolically $(x^{q^2}, y^{q^2}) + [q_l](x, y)$ modulo the l-division polynomials Ψ_l and comparing with the possible values of $[\tau](x^q, y^q)$, $(\tau = 1, \ldots, l)$. The computations are polynomially bounded by $O(\log q)$ and the degree $\frac{l^2-1}{2}$ of the l-division polynomials. This degree grows in practice quite fast, which makes the arithmetic modulo division polynomials the essential bottleneck in the original version of Schoof's algorithm.

However, the division polynomials are in general not irreducible and one can sensibly reduce the complexity by replacing Ψ_l by some smaller—not necessarily irreducible—factors. Since $E[l] \cong (\mathbb{Z}/(l \cdot \mathbb{Z}))^2$, there is a representation of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ in $GL_2(\mathbb{F}_l)$, which yields information on the factorization patterns of Ψ_l. This fact was basically exploited in the subsequent contributions due to Atkin, Elkies and worked out and implemented by F. Morain, some of his students, and V. Müller.

The applications of elliptic curves to factoring and primality proving are briefly outlined, for the sake of completeness, in the ninth chapter. The last chapter summarizes the main ideas about cryptographic use of hyperelliptic curves at the time the was book printed.

For the interested reader, it may be important to mention some of the outstanding results of the last few years, which are ulterior to the conception of this book and thus not covered by it.

Counting points on curves over fields of small characteristics p have been sensibly simplified by an algorithm of Satoh [9], based on p-adic logarithms. The algorithm has been implemented, and curves over the field $\mathbb{F}_{2^{8009}}$ can be currently treated; without Satoh's approach, the best methods could calculate the curve orders in extensions of $\mathbb{F}_2$ of degree up to 2000.

In the domain of implementation, a beautiful paper of H. Cohen, A. Miyaji, and T. Ono [2] studies a variety of curve representations, with the aim of optimizing the performance of group operations; this can certainly be of great help for implementors. Fields of odd characteristic which are adapted to machine world length—*medium Galois fields* or simply *extension fields*, according to different terminologies—receive some attention. A run time study, [12] by Smart, of implementations of elliptic curve operations over fields of characteristics of various sizes suggests that these fields may have interesting practical properties.

Finally, *Weil descents* have been proposed by G. Frey [4] as a possible method for solving special instances of the discrete logarithms problem. This has already

motivated a series of important research with pro and con arguments, and is likely to become an important research topic.

References

1. Blake, I. F.; Seroussi, G.; Smart, N. P.: *Elliptic curves in cryptography*. Reprint of the 1999 original. London Mathematical Society Lecture Note Series, 265. Cambridge University Press, Cambridge, 2000. CMP 2000:15
2. Cohen, H.; Miyaji, A.; Ono, T.: *Efficient elliptic curve exponentiation using mixed coordinates*, Asiacrypt 98, Lecture Notes in Comput. Sci., 1514, Springer, Berlin, 1998. CMP 2000:06
3. Cox, D. A.: *Primes of the form $x^2 + ny^2$*, Wiley & Sons, 1989. MR **90m:**11016
4. Frey, G.: *Applications of arithmetical geometry to cryptographic constructions*, Preprint.
5. Goldwasser, S.; Killian, J.: *Almost all primes can be quickly certified*, Proc. 18-th Annual ACM Symp. on Theory of Computing (1986), 316–329.
6. Lenstra, H. W.: *Factoring integers with elliptic curves*, Ann. of Math., **126** (1987), 649–673. MR **89g:**11125
7. Menezes, Alfred J.: *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993. MR **2000d:**94023
8. Miller, V.: *Use of elliptic curves in cryptography*, Advances in Cryptology, Proceedings of CRYPTO'85, Lecture Notes in Comput. Sci. **218**, Springer, Berlin, 1986, pp. 417–426. MR **88b:**68040
9. Satoh, T.: *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. **15** (2000), no. 4, 247–270. CMP 2001:05
10. Schoof, R.: *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44**, (1985), 483–494. MR **86e:**11122
11. Silverman, J. H.: *The arithmetic of elliptic curves*. Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1999. MR **95m:**11054
12. Smart, N.: *A comparison of different finite fields for use in elliptic curve cryptosystems*, University of Bristol, Department of Computer Science, June 2000 preprint.

Preda Mihăilescu,
M_EC Consulting and Gesamthochschule Paderborn,
Germany
E-mail address: preda@math.upb.de

F. Pappalardi
Dipartimento di Matematica
Università degli studi Roma Tre
Largo S. L. Murialdo 1
I-00146 Roma
Italy
E-mail address: pappa@mat.uniroma3.it