Программа спецкурса «Дискретное логарифмирование».

1. Задача дискретного логарифмирования на примере мультипликативной группы конечного поля. Метод индексного исчисления. [1, 2]
2. Эллиптические кривые. Закон сложения точек эллиптической кривой. [3]
3. Эллиптические кривые над конечными полями. [3]
4. Структура группы точек эллиптической кривой, определённой над конечным полем. [3]
5. Задача дискретного логарифмирования в группе точек эллиптической кривой, определённой над конечным полем. [3]
6. Методы Полига-Хелмана и Полларда вычисления дискретного логарифма. [4, 5]
7. Эллиптические кривые над p-адическими полями. [6]
8. Эллиптический логарифм. [7]
9. Решение задачи дискретного логарифмирования для эллиптических кривых порядка p над полем $\mathbb{F}_p$. [8, 9]
10. Кольцо эндоморфизмов эллиптической кривой. [3]
11. Дивизоры эллиптической кривой. Многочлены деления. [3]
12. Спаривания на эллиптических кривых. [10]
13. Алгоритм вычисления спаривания Вейля. [11]
14. Определение порядка и структуры группы точек эллиптической кривой, определённой над конечным полем. [11, 12]
15. Алгоритм Менезеса-Окамото-Ванстоуна нахождения дискретного логарифма на эллиптических кривых. [13, 14]
16. Суперсингулярные кривые. Дискретное логарифмирование на таких кривых. [3, 13]
17. Связь структуры группы эллиптической кривой, определенной над конечным полем с кольцом эндоморфизмов этой кривой. [15]
18. Быстрое вычисление структуры группы и дискретного логарифма на некоторых эллиптических кривых специального вида. [16]

Список литературы

[1] *Kraitchik M.* Théorie des Nombres. 1922. Vol. 1. Gauthier-Villars.

[2] *Kraitchik M.* Recherches sur la théorie des nombres. 1924. Gauthier-Villars.

[3] *Enge A.* Elliptic curves and their applications to cryptography: an introduction. Kluwer Academic Publishers. 1999.

[4] *Pohlig S. and Hellman M.* An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. IEEE Transactions on Information Theory. 1978. No 24. P. 106—110.

[5] *Pollard J.* Monte Carlo methods for index computation mod p. Mathematics of Computation. 1978. No 32. P. 918—924.

[6] *Milne J. S.* Elliptic curves. 2006.

[7] *Silverman J. H.* The Arithmetic Of Elliptic Curves. Springer-Verlag, GTM 106, 1986. Expanded 2nd Edition, 2009.

[8] *Smart N. P.* The discrete logarithm problem on elliptic curves of trace one. Hewlett-Packard Company. 1997.

[9] *Semaev I.* Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. Mathematics of Computation. 1998. No 67. P. 353—356.

[10] *Enge A.* Bilinear pairings on elliptic curves. 2012.

[11] *Miller V. S.* The Weil pairing and its efficient calculation. Journal of Cryptology. 2004. Vol. **17**. 235–261.

[12] *Schoof R. J.* Elliptic curves over finite fields and the computation of square roots $\pmod p$. Math. Comp. 1985. **44**. 483–494.

[13] *Menezes A., Okamoto T., Vanstone S.* Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory. 1993. No 39. P. 1639—1646.

[14] *Frey G., Rück H.* A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of Computation. 1994. No 62. P. 865—874.

[15] *Lenstra H. W. Jr.* Complex multiplication structure of elliptic curves. Journal of Number Theory. 1996. **56**. 227–241.

[16] *Айерленд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987, 416 с.