Оценки числа решений теоретико-числовых уравнений, используемых в криптографии

Е. А. Гречников

Пусть p — нечётное простое число. В докладе мы рассмотрим следующие уравнения по модулю p:

$$g^x \equiv x \pmod p, \quad x \in \{0, \dots, p-1\}, g \text{ — примитивный корень} \tag{1}$$

$$y^2 \equiv f(x) \pmod p, \quad x, y \in \mathbb{F}_p, f \in \mathbb{F}_p[x], 2 \nmid \deg f \tag{2}$$

Вопрос о существовании решений уравнения (1) при каком-нибудь примитивном g — это проблема Бризолиса, которая была решена в 2003 году в [1] (решения существуют при всех $p > 3$). Интересной особенностью этого уравнения является то, что для числа решений в среднем по g довольно легко получить достаточно хорошую асимптотическую нижнюю оценку (из чего следует решение проблемы Бризолиса для больших p; трудности, преодолённые в [1], касаются хороших явных оценок и малых p), но трудно получить хорошую верхнюю оценку. В докладе очень кратко будет обрисовано доказательство нижней оценки $1 - C(\varepsilon)p^{-\frac{1}{4}+\varepsilon}$ и верхней оценки $\exp\left(C' \operatorname{Li}\left((\ln p)^{c\frac{\ln\ln\ln p}{\ln\ln p}}\right)\right)$.

Если в уравнении (2) f — многочлен третьей степени без кратных корней, то множество его решений вместе с одним «бесконечно удалённого» образует абелеву группу. Рассмотрение всех решений над $\overline{F}_p$, а не только над $\mathbb{F}_p$, приводит к эллиптической кривой. Теория эллиптических кривых исключительно обширна (её основы прекрасно изложены в книге [2]) и, в частности, позволяет подсчитывать решения конкретного уравнения вида (2) над $\mathbb{F}_p$ за полиномиальное (от $\log p$) время, а также перечисляет возможные варианты для всех таких уравнений (теорема Дойринга–Ватерхауза). В докладе будет кратко описан один из методов построения уравнения вида (2) с предписанным числом решений.

Если в уравнении (2) f — многочлен нечётной степени, большей 3, то можно ввести в рассмотрение гиперэллиптические кривые; общая теория даёт оценки числа решений и в этом случае, но здесь оценки можно уточнить элементарным методом (который, впрочем, не обобщается на случай произвольных конечных полей). Впервые более точную оценку доказал Коробов в [3]; в докладе будет обрисовано доказательство ещё чуть более точной оценки, основанное на тех же идеях. Кроме того, будет обрисовано построение уравнений вида (2) степени 5, дающих число решений, близкое к верхней оценке.

Список литературы

[1] Campbell M. E. On fixed points for discrete logarithms. Master's thesis, University of California at Berkeley, 2003.

[2] Silverman J. H. The arithmetic of elliptic curves. Second edition. Springer, 2009.

[3] Коробов П. М. Оценка сумм символов Лежандра // Доклады АН СССР. 1971. Т. 196, № 4. С. 764–767.