УДК 511.5

Распределение целых и рациональных точек на суперэллиптических кривых

Трелина Л. А.
Белорусский национальный технический университет

В приложениях требуется использовать эффективные алгоритмы специальных отображений множеств точек суперэллиптической кривой $y^m = f(x)$, $f(X) \in K[X]$, $m + \deg f > 4$, над конечным или числовым полем K.

Рассмотрены следующие два класса кривых и отображений.

Пусть $\{E\}_{R,C}$ – множество случайных эллиптических кривых E над $\mathbf{Q}$ (над $K \supseteq \mathbf{Q}$, $[K:\mathbf{Q}] < \infty$), таких, что дискриминанты $D_E \neq 0$ и наибольший простой делитель произведения (норм) всех D_E не превосходит некоторой границы C. Пусть, далее, $\mathrm{B} \subset K[t]$ – множество случайных двучленов не менее второй степени и со свободным членом, превосходящим по абсолютной величине вычисляемую в явном виде границу $\Omega = \Omega(C)$ $(\Omega = \Omega(C, K))$. Тогда отображения

$$\varphi_z : \{P\} \to \mathrm{B}, \quad x_p \mapsto x_p + z, \quad |z| > \Omega,$$

множества всех целых точек на кривых семейства $\{E\}_{R,C}$ в множество B инъективны для каждого z.

Можно рассматривать результанты $R(E_i, E_j)$ вместо дискриминантов D_E. Для суперэллиптических кривых границы зависят также от $m, \deg f$.

С помощью второго класса отображений устанавливается зависимость между порядком группы рациональных точек эллиптической кривой $y^2 = x^3 + ax + b$ над простым конечным полем $\mathbf{F}_p$ и свойствами периодических точек отображений $\Phi_1(z) = z^2 + A$, $\Phi_2(z,s) = (z^4 + s)/3\sqrt{3}$. Аналогично рассматриваются множества целых точек кривых $y^m = f(x)$ над числовыми полями.