ПРИМЕНЕНИЕ ОСНОВНЫХ ЕДИНИЦ КВАДРАТИЧНЫХ ПОЛЕЙ К РЕШЕНИЮ ДИОФАНТОВЫХ УРАВНЕНИЙ

Белова Л.Ю.

Ярославский государственный университет им. П.Г. Демидова, математический ф-т, каф. компьютерной безопасности и математических методов обработки информации, Россия, 150000, Ярославль, Советская ул. 14

Рассматривается задача реализации алгоритма для получения всех целочисленных решений общего уравнения второго порядка от двух переменных:

$$a_1x^2+a_2xy+a_3y^2+b_1x+b_2y+c=0,\ a_1,\ a_2,\ a_3,\ b_1,\ b_2,\ c\in Z \quad (1)$$

Теоретическое решение этого классического вопроса, конечно, имеется, однако приемлемая программная реализация не проста.

Наметим основные этапы задачи (обоснования – см. [1]).

Сначала (1) сводится к рассмотрению уравнений более специального вида

$$N(z)=x^2-dy^2=k \quad (2)$$

Здесь $N(z)=z\cdot\bar{z}=(x+y\sqrt{d})(x-y\sqrt{d})$ -- норма числа $z=x+\sqrt{d}\,y$, $x,\ y\in Z$, (т.е. целые). Ясно, что $N(z)$ мультипликативна: $N(u\cdot v)=N(u)\cdot N(v)$.

Вещественным квадратичным полем $K=Q(\sqrt{d})$ называется множество действительных чисел вида: $z=a+b\sqrt{d}$, где $a,\ b\in Q$ (рациональные), $d\in Z$, $d>1$ и свободно от квадратов. Если рассмотреть внутри K множество D целых алгебраических чисел, то $D=Z[\omega]$, где $\omega=\sqrt{d}$ в случае $d\equiv 2,\ 3 \pmod 4$, и $\omega=1/2(1+\sqrt{d})$ в случае $d\equiv 1 \pmod 4$. Это значит, числа $z=a+b\cdot\omega\in D$ таковы, что $a,\ b\in Z$, а числа 1 и ω составляют канонический <u>целочисленный</u> базис. Внутри D обратимыми являются те и только те числа ε, норма которых ± 1, то есть $N(\varepsilon)=\pm 1$.

Среди всех обратимых элементов D имеется такое число ε_1, что остальные обратимые являются, с точностью до знака, его степенями: $\varepsilon=\pm(\varepsilon_1)^n$. Это число ε_1 называется <u>основной единицей поля</u> K. Для получения бесконечных серий решений уравнения (2) используется мультипликативность нормы и основная единица: $N(z\cdot(\varepsilon_1)^{2m})=N(z)N((\varepsilon_1)^{2m})=k$.

Имеется лишь конечное число «начальных» решений (2), из которых, с помощью указанного приёма получаются все бесконечные серии решений. Таким образом, имеется три этапа решения задачи (1): сведение исходной задачи к специальному виду (2), определение начальных решений и нахождение основной единицы. На втором третьем этапах привлекается разложение числа ω в непрерывную дробь. Эта часть работы наиболее трудоёмкая. Существуют результаты вычислений основных единиц до d=100. Мы стремились расширить таблицу хотя бы до d=200. Напомним, что для квадратичных иррациональностей непрерывная дробь периодична, и для получения ε_1 требуется взять подходящую дробь с «предпериодным» номером. Среди чисел $100<d<200$ имеются два числа со сверхдлинными периодами: для d=151 период равен 563 и для d=199 период равен 1257. Используя формулу Бине для чисел Фибоначчи, можно показать, что, если $\varepsilon_1=a+b\cdot\omega$, то a и b содержат, в случае d=151, не менее 150 десятичных знаков, а в случае d=199 – не менее 300. Эти два числа не были просчитаны до конца. Все остальные периоды меньше 22 и поддаются просчёту без привлечения специальных методов.