XXXIII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V: С.140, 2005.

УДК 50.41.00, 50.37.23

А.К.Полякова (4 курс, каф. ИБКС), Е.Б.Маховенко, к.т.н., доц.

МЕХАНИЗМЫ УМНОЖЕНИЯ ТОЧКИ НА ЧИСЛО НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Все большее распространение для построения криптографических алгоритмов получают эллиптические кривые над конечными полями. Самой трудоемкой и длительной операцией здесь является умножение точки на число. Существует несколько приемов умножения, одним из которых является способ, заключающийся в замене удвоения точки двойным умножением ее на $\sqrt{-2}$ с помощью изогении степени 2. Было выявлено, что такое комплексное умножение быстрее обычного примерно в три раза.

Пусть K — алгебраическое замыкание поля F_p. Тогда кольцо эндоморфизмов кривой E(K) изоморфно кольцу $\mathbf{Z}[\sqrt{-2}]$. Если r – простой порядок группы точек кривой $E(F_p)$, то имеет место разложение на простые множители в кольце $\mathbf{Z}[\sqrt{-2}]$: $r = \rho\bar{\rho}$, и изоморфизм конечных полей $\mathbf{F}_r \cong \mathbf{Z}[\sqrt{-2}]/(\rho)$. Для использования комплексного умножения можно либо использовать этот изоморфизм, либо разработать алгоритмы арифметики в евклидовом кольце $\mathbf{Z}[\sqrt{-2}]$ и конечном поле $\mathbf{Z}[\sqrt{-2}]/(\rho)$. Наибольший интерес представляет расширенный алгоритм Евклида в этом кольце.

Для разработки алгоритма деления использовалось гомоморфное вложение кольца $\mathbf{Z}[\sqrt{-2}]$ в неевклидово кольцо Z[x]. Нетривиальность решаемой задачи была обусловлена различием алгебраических свойств этих колец. Рассматривались два варианта деления: начиная с младших степеней полиномов и со старших. При реализации алгоритма Евклида и процесса деления все коэффициенты полинома, равные 2, заменялись полиномом $-x^2$. Алгоритм выполнялся до тех пор, пока степень делимого больше либо равна степени делителя, и норма делимого как элемента кольца $\mathbf{Z}[\sqrt{-2}]$ больше нормы делителя. Эксперимент показал, что алгоритм, начинающий работу со старших степеней, выигрывает по скорости примерно в три раза.

При тестировании в некоторых случаях алгоритм зацикливался. Кроме того, возникала ситуация, когда степень делимого была меньше степени делителя, в то время как норма делимого была больше нормы делителя. Это объяснялось тем, что представление числа в системе счисления с основанием $\sqrt{-2}$ неоднозначно, в частности, $x^2 + 1 = -1$. После установления однозначности представления алгоритм стал работать корректно.

Параллельно велась работа по разработке расширенного алгоритма Евклида для чисел, представленных в системе счисления по основанию $\sqrt{-2}$, который базировался на описанном выше методе деления. По сравнению с классической постановкой, входными значениями которой были два числа a и b, были внесены некоторые изменения. Если, при делении числа b на полином $x^2 + 1$ остаток от деления равен 0, то b приравнивается к частному деления с противоположным знаком. Это позволяет избежать лишних вычислений, связанных с неоднозначностью представления чисел.

Указанная корректировка представления числа позволила реализовать $\sqrt{-2}$-арный аналог бинарного расширенного алгоритма Евклида.