О. В. Шемякина (Санкт-Петербург, РЦЗИ «ФОРТ»). **О перемешивающих свойствах операций в конечном поле.**

Рассматривается действие каждой из операций в поле $\mathbf{GF}\,(q^n)$, где q — степень простого числа, $n \in \mathbf{N}$, на смежные классы относительно второй операции. Для факторгруппы $\mathbf{GF}\,(q^n)^*/\mathbf{GF}\,(q)^*$ справедливо следующее: а) каждый элемент суммы двух одинаковых смежных классов либо равен нулю, либо принадлежит этому же классу; нуль встречается в этой сумме $q-1$ раз, каждый ненулевой элемент встречается $q-2$ раза; б) все элементы суммы двух разных смежных классов различны и составляют объединение всех элементов $q-1$ различных смежных классов, отличных от данных.

При $n=2$ сумма двух различных смежных классов является объединением всех остальных смежных классов.

Для факторгруппы группы $\mathbf{GF}\,(q^2)^*$ по подгруппе порядка $q+1$ в зависимости от четности q и конкретных смежных классов возможны следующие варианты суммы двух смежных классов.

1. Элементы суммы попадают в $(q+1)/2$ смежных класса, при этом в каждый из них попадает $2(q+1)$ элементов.

2. Элементы суммы попадают в $(q+3)/2$ смежных класса, при этом в два класса попадает по $q+1$ элементов, в каждый из остальных — по $2(q+1)$ элементов.

3. Среди элементов суммы содержится $q+1$ нулей, остальные элементы попадают в $(q+1)/2$ смежных класса, при этом в один класс попадает $q+1$ элементов, в каждый из остальных — по $2(q+1)$ элементов.

4. Элементы суммы попадают в $q/2+1$ смежных класса, при этом в один класс попадает $q+1$ элемент, в каждый из остальных — по $2(q+1)$ элементов.

5. Среди элементов суммы содержится $q+1$ нулей, остальные элементы попадают в $q/2$ смежных класса, при этом в каждый из этих классов попадает $2(q+1)$ элементов.

Для факторгруппы $\mathbf{GF}\,(q^n)/\mathbf{GF}(q)$ справедливо: а) все элементы произведения $\mathbf{GF}\,(q)\cdot\mathbf{GF}\,(q)$ принадлежат смежному классу $\mathbf{GF}\,(q)$; каждый ненулевой элемент $\mathbf{GF}\,(q)$ встречается в этом произведении $q-1$ раз, нуль встречается $2q-1$ раз; б) произведение двух смежных классов, из которых, по крайней мере, один отличен от $\mathbf{GF}\,(q)$, содержит либо по q элементов из q различных смежных классов, либо по одному элементу из q^2 различных смежных классов.

При $n=2$ произведение различных смежных классов содержит q элементов из каждого смежного класса.

Если в смежный класс попадает больше одного элемента, то эти элементы не обязательно различны и справедливо следующее.

1. Все попадающие в $\mathbf{GF}\,(q)$ элементы произведения $\mathbf{GF}\,(q)$ на любой другой смежный класс равны нулю. Все остальные элементы этого произведения различны.

2. При нечетном q попадающие в один смежный класс элементы произведения двух смежных классов, отличных от $\mathbf{GF}\,(q)$, принимают $(q+1)/2$ значений. При этом $(q-1)/2$ из них встречаются по два раза.

3. При четном q попадающие в один из смежных классов элементы произведения двух смежных классов, отличных от $\mathbf{GF}\,(q)$, различны, а элементы, попадающие в остальные смежные классы, разбиваются на пары совпадающих.

Таким образом, сложение в конечном поле хорошо перемешивает смежные классы по мультипликативной группе любого подполя, и наоборот. Сложение в поле $\mathbf{GF}\,(q^2)$ равномерно перемешивает смежные классы по мультипликативной подгруппе порядка $q+1$. Это снижает эффективность использования метода гомоморфизмов.