37 Группа над кольцом

Задача. Боб разрабатывает криптосистему, стойкость которой базируется на сложности решения задачи дискретного логарифмирования в группе G. Эта группа составлена из элементов кольца R, операция в G задается многочленом $f(x, y)$ над кольцом R:

$$x * y = f(x, y).$$

Сколько способов выбора f имеется у Боба?

Решение. Предположим, что единицей G является 0 — нулевой элемент кольца R. Пусть $f_y(x)$ — многочлен, который задает результат операции $x*y$ при фиксированном y. Пусть y' и y'' — взаимно обратные элементы G. Тогда для любого $x \in R$:

$$f_{y''}(f_{y'}(x)) = x.$$

Это возможно только если многочлены $f_{y'}(x)$, $f_{y'}(x)$ являются линейными. Следовательно, степень $f(x, y)$ относительно x равняется 1. Аналогичным образом, степень $f(x, y)$ относительно y также равняется 1 и

$$f(x, y) = \alpha x + \beta y + \gamma xy.$$

Из условий $f(x, 0) = x$, $f(0, y) = y$ следует, что $\alpha = \beta = 1$. Более того, для любого $y \in R$ функция $x \mapsto f_y(x) = x+y+\gamma xy$ должна быть биективной, и поэтому $\gamma = 0$. Окончательно,

$$f(x, y) = x + y.$$

Предположим теперь, что единицей G является произвольный элемент O кольца R. Тогда многочлен $f^*(x, y) = f(x+O, y+O)-O$ задает новую групповую операцию с единицей 0. По доказанному выше $f^*(x, y) = x + y$ и, следовательно,

$$f(x, y) = x + y - O.$$

Таким образом, имеется $|R|$ способов выбора f.