УДК 512.642.95:378.147.091.3

НЕПРИВОДИМЫЕ ПОЛИНОМЫ ШЕСТОЙ СТЕПЕНИ В КОЛЬЦЕ Z/2Z

Студент гр. 10404115 Русевич О. А
Науч. рук. Крупенкова Т. Г.
Белорусский национальный технический университет

Пусть P – поле, то есть произвольное коммутативное кольцо с единицей, у которого все элементы, отличные от нуля, обратимы, иными словами $P^* = P \setminus \{0\}$. Например, $P = Q, R, C, Z / pZ$.

Многочлен $f(x) \in P[x]$ степени $n \geq 1$ называется неприводимым в кольце если в любом его представлении в виде произведения $f(x) = g(x)q(x)$ сомножителей $g(x)$, $q(x) \in P[x]$ один из этих сомножителей является константой, то есть элементом поля P.

В кольце $(Z/pZ)[x]$ также существуют неприводимые полиномы любой степени n ≥1. Здесь произвольных полиномов степени n имеется лишь конечное множество (в количестве p^{n+1}), тем более неприводимых полиномов данной степени всегда конечно.

Для неприводимости полинома степени 2 или 3 в кольце $P[x]$ необходимо и достаточно, чтобы он не имел корней в поле P. Для неприводимости полинома степени 4 или 5 в кольце необходимо и достаточно, чтобы он не имел корней в поле $P[x]$ и не делился ни на какой (неприводимый) полином второй степени. Обычно неприводимость полинома над конечным полем определяется процедурой просеивания, напоминающей решето Эратосфена для целых чисел – последовательным делением на неприводимые (или все) меньшей степени от 1 до $[n / 2]$.

Для нахождения неприводимых полиномов шестой степени были найдены остатки от деления всех многочленов шестой степени ($p^{n+1} = 128$) на неприводимые полиномы до третьей степени, с помощью Wolfram Mathematica. Таким образом, было получено 18 полиномов:

$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$; $x^6 + x^5 + x^4 + x^3 + 1$; $x^6 + x^5 + x^4 + x^2 + 1$; $x^6 + x^5 + x^3 + x^2 + 1$; $x^6 + x^4 + x^3 + x^2 + 1$; $x^6 + x^5 + x^4 + x + 1$; $x^6 + x^5 + x^3 + x + 1$; $x^6 + x^4 + x^3 + x + 1$; $x^6 + x^5 + x^2 + x + 1$; $x^6 + x^4 + x^2 + x + 1$; $x^6 + x^3 + x^2 + x + 1$; $x^6 + x^5 + 1$; $x^6 + x^4 + 1$; $x^6 + x + 1$; $x^6 + x^3 + 1$; $x^6 + x^2 + 1$; $x^6 + x^2 + + 1$; $x^6 + x^3 + 1$.