УДК 512 624: 003.26

Аспекты формирования неприводимых полиномов над полями Галуа

Королёва М.Н., Липницкий В.А.
Белорусский национальный технический университет
Военная академия Республики Беларусь

Роль конечных полей (полей Галуа) в математике и в ее приложениях непрерывно растет. Минимальные поля Галуа как кольца классов вычетов по простому модулю – основной инструмент в современных криптосистемах: RSA, Рабина, Эль Гамаля и их модификациях. Расширения минимальных полей Галуа лежат в основе стандарта шифрования AES, эллиптической криптографии, XTR-криптосистем.

Всякое конечное поле $GF(p^m)$ имеет простую характеристику p, состоит из p^m элементов, при $m>1$ является $m-$мерным векторным пространством над своим подполем $GF(p)=Z/pZ$. С фиксированными параметрами p и m поле $GF(p^m)$ единственно и изоморфно фактор-кольцу $\hat{E}=(Z/pZ)[x]/<p(x)>$ кольца полиномов $(Z/pZ)[x]$ по максимальному идеалу $<p(\mathrm{x})>$, порожденному неприводимым над полем Z/pZ полиномом $p(\mathrm{x})$ степени m. Таким образом, неприводимые полиномы являются обязательным атрибутом формирования конечных полей. К сожалению, отсутствуют признаки, типа критерия Эйзенштейна для поля рациональных чисел, которые бы демонстрировали явный вид неприводимых полиномов тех или иных степеней над полями Галуа. Составители XTR-криптосистемы заметили и успешно применяют тот факт, что полином x^2+x+1 неприводим над бесконечным множеством полей Z/pZ, а именно, для всех p, таких, что $p\equiv 2(\mathrm{mod}\,3)$. Титов С.С. с учениками (Россия) уже в XXI веке установили неприводимость над полем $Z/2Z$ полинома $F(x)=x^n f(x+x^{-1})$, если неприводим над ним полином $f(x)=x^n+x^{n-1}+....+x+1$. Формирование неприводимых над Z/pZ полиномов является столь же открытой проблемой, как и формирование простых чисел. Эта задача решается рекуррентной процедурой, аналогичной решету Эратосфена, требующей значительных вычислительных усилий уже для значений $p=2$ и $k\geq 20$.