УДК 512(076.1)

Конечные поля. Аспекты применения в науке и образовании

Липницкий В.А., Королева М.Н.
Белорусский национальный технический университет

Конечные поля – алгебраические системы, допускающие 4 арифметические действия и имеющие лишь конечное число элементов. Впервые введены в научный обиход гениальным 21-летним парижским математиком-самородком Эваристом Галуа в 1831 году. Поэтому они приобрели название-синоним – поля Галуа. Они оказались необходимым компонентом при выводе необходимых и достаточных условий разрешимости уравнений в радикалах. С 60-х годов XX века конечные поля вновь оказались в центре внимания, теперь уже прикладной математики - как основной инструмент задания линейных помехоустойчивых кодов. Последние необходимы в цифровых системах передачи, хранения и обработки информации для её защиты от помех и разного рода «шумов», неизбежных в реальных каналах связи. В XXI веке защита информации от несанкционированного доступа постепенно уходит от модулярной арифметики к вычетно-полиномиальной, то есть опять-таки к арифметике конечных полей. На полях Галуа базируется ныне действующий американский стандарт шифрования AES, разрабатывались криптосистемы МакЭлиса-Сидельникова, EKCTR-криптосистемы, системы шифрования на эллиптических кривых.

Защита информации от несанкционированного доступа затрагивает не только государственные интересы. Она необходима в банковской сфере, нужна практически всем серьёзным фирмам. Диспетчер любой локальной компьютерной сети так или иначе должен заботиться о безопасности своих сотрудников. Проблемы защиты информации так или иначе должны быть в сфере интересов любого специалиста, а следовательно, в сфере интересов высшей школы. В ближайшем будущем каждый специалист с дипломом ВУЗа должен получить определённый образовательный пакет по защите информации. Касательно инженерных специальностей этот пакет должен иметь конкретную математическую базу, куда должно входить и практическое освоение арифметики полей Галуа. Это неизбежно влечёт за собой изучение цикла разделов современной алгебры: теории чисел, теории групп, теории колец, теории полей и полей Галуа; освоение ряда математических и криптографических алгоритмов; практическую компьютерную реализацию этих алгоритмов.

Новые знания неизбежно требуют освоения новых разделов математики. Соответствующие лекционные курсы являются относительно новыми, многие из них находятся в динамике становления или развития в соответствии с технологической революцией и требованиями времени.