УДК 519.7

Метод Диемитко формирования больших простых чисел

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

В современном информационном обществе как никогда актуализированы все проблемы, связанные с созданием и успешным функционированием IT-технологий, особенно вопросы защиты информации. Современные криптографические системы – RSA, Рабина, Эль Гамаля и их всевозможные модификации требуют для своего создания больших простых чисел размером порядка 512-1024 бита. Развиваемая с древних времен теория чисел оказалась неподготовленной к такому внешне простому вопросу. Систематизация теории сравнений привела к осознанию справедливости следующего утверждения.

Теорема 1. *Натуральное число* $n > 1$ *является простым тогда и только тогда, когда мультипликативная группа* Z / nZ^* *кольца классов вычетов* Z / nZ *по модулю* n *является циклической порядка* $n-1$.

Фактической переформулировкой теоремы о разложении любой конечной циклической группы в произведение своих примарных подгрупп является

теорема 2 (Тест Брилхарта-Лемера-Селфриджа, 1975). *Пусть* $n-1 = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_s^{r_s}$ *– разложение на простые множители. Пусть для каждого* i, $1 \le i \le s$, *существует такое целое* b_i, *что 1)* $b_i^{n-1} \equiv 1 (\mathrm{mod}\, n)$; *2)* $b_i^{(n-1)/p_i} \neq 1 (\mathrm{mod} n)$. *Тогда* n *– простое число.*

Следующий тест явился результатом длительных исследований нескольких поколений математиков.

Теорема 3 (Диемитко, 1988). *Пусть* $n = qR + 1 > 1$, *где* q *– нечетное простое число,* R *– четное и* $R < 4(q+1)$. *Если существует такое целое* a, *что* $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ *и* $a^{(n-1)/q} \neq 1 (\mathrm{mod}\, n)$, *то* n *– простое.*

Секрет теоремы Диемитко в том, что делители числа n, если бы и существовали, то они имели бы весьма специфический вид, что достаточно быстро проверяется. В силу означенного факта, теорема Диемитко долгое время была в основе стандарта формирования простых чисел Республики Беларусь и многих других стран.