УДК 512.624.95:378.147.091.3

# Методические аспекты применения китайской теоремы об остатках в современных криптографических системах

Крупенкова Т.Г., Липницкий В.А.*
Белорусский национальный технический университет
Военная академия Республики Беларусь*

Впервые она рассматривалась в «Учебнике математики мастера Сана». Современная формулировка теоремы такова:

Теорема. Пусть $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ разложение натурального числа в произведение взаимно простых множителей. Тогда кольцо $Z/mZ$ изоморфно прямому произведению $Z/m_1Z \times Z/m_2Z \times \ldots \times Z/m_nZ$.

Установленный изоморфизм означает, что арифметические действия с числами по модулю $m$ можно заменить на такие же, но с CRT-представлениями этих чисел. Теорема дает прямое средство для распараллеливания вычислений. Это весьма важно для всех задач, требующих для своего решения масштабных вычислительных ресурсов. Для операций с целыми числами большой разрядности, выходящей за общепринятый в применяемых компьютерах диапазон, такой подход приносит существенный выигрыш в количестве операций. Примерно, двукратный-трехкратный. Ещё больший выигрыш – примерно, четырёхкратный – получается при возведении целых чисел в натуральные степени с помощью приведенной теоремы.

Для современной криптографии характерны сложные арифметические действия с целыми числами в 100 – 300 десятичных знаков, требующие огромных компьютерных ресурсов. Особенно вязкими в вычислительном плане являются наиболее популярные на сегодняшний день криптографические системы RSA, Эль-Гамаля, Рабина, а также их разнообразные модификации, ставшие национальными стандартами шифрования в различных странах мира.

Эти криптосистемы впрямую базируются на вычислениях в кольцах классов вычетов. Для реализации этих криптосистем особенно важны и актуальные любые подходы, снижающие сложность реализации тех или иных алгоритмов, не снижая при этом их криптографической стойкости.

Китайская теорема об остатках прочно вошла в арсенал средств современных вычислителей, пользователей современными криптографическими ресурсами.

Соответствующее место обязана занять эта теорема и в образовании инженеров соответствующих специальностей.