Глава 4. Элементы теории чисел и шифрование

«Математика — царица наук, а теория чисел — царица математики», — говорил Карл Фридрих Гаусс почти двести лет назад. Долгое время теория чисел считалась самой «чистой» из математических дисциплин — занимающейся ради красоты и никак не связанной с практикой. Сегодня, в эпоху Интернета, банковских карт и мессенджеров, эта наука оказалась едва ли не самой востребованной: без неё не отправить безопасное сообщение, не оплатить покупку и не зайти на сайт по защищённому соединению.

В этой главе мы пройдём путь от античного алгоритма Евклида до современных криптографических протоколов, обеспечивающих безопасность в Интернете. Один и тот же небольшой набор фактов о *делимости и сравнениях по модулю* окажется работающим везде — от шифрования RSA до структуры данных для подсчёта различных элементов в больших потоках.

Читатель встретит три «слоя» материала:

- **Теоретико-числовой фундамент**: алгоритм Евклида, малая теорема Ферма, функция Эйлера, тесты простоты — классические результаты, без которых не существует современной криптографии.
- **Криптографические протоколы**: симметричное и асимметричное шифрование, RSA и Диффи–Хеллман, электронная цифровая подпись, схемы электронного голосования.
- **Вероятностные алгоритмы**: универсальное хеширование, счётчики HyperLogLog, измерение «социального расстояния» в графах больших сетей.

Многие из изученных конструкций ежесекундно работают внутри устройств читателя: каждое HTTPS-соединение, каждый клик в банковском приложении, каждый запрос в поисковике — результат применения математических фактов, которым посвящена эта глава.