важнейшие (в частности, для криптографии) понятия: *наибольшего общего делителя* (НОД) и *взаимно простых чисел*.

Определение 9. Наибольшее целое число, которое делит без остатка числа a и b, называется ***наибольшим общим делителем*** этих чисел – НОД (a, b).

Пример 13. Делителями числа $a = 24$ являются: 1, 2, 4, 6, 8, 12, 24; делителями числа $b = 32$ являются: 1, 2, 4, 8, 16, 32. Как видим, НОД (24, 32) = 8.

Понятно, что значение НОД можно вычислять для неограниченного ряда чисел.

Простым и эффективным средством вычисления НОД (a, b) является *алгоритм Евклида* (примеры его использования приведены в [3]). В основе алгоритма лежит определение 5. В соответствии с этим определением используется цепочка вычислений двумя исходными (начальными) числами a и b:

$$a_i = b_i q_i + r_i,\ 0 \le r_i \le b_i. \quad (1.2)$$

При $i = 0$ в выражении (1.2) a_i и b_i соответствуют как раз числам a и b. Последний ненулевой остаток (r_i, $i \ge 0$) соответствует НОД (a, b).

Пример 14. Пусть $a = 1234$, $b = 54$. Найти НОД.

$1234 = 54 \cdot 22 + 46;$

$54 = 46 \cdot 1 + 8;$

$46 = 8 \cdot 5 + 6;$

$8 = 6 \cdot 1 + 2;$

$6 = 2 \cdot 3 + 0.$

Последний ненулевой остаток равен 2, поэтому НОД (1234, 54) = 2.

Чтобы найти НОД нескольких чисел (например, a, b, c), достаточно найти НОД двух чисел (например, НОД (a, b) = d), потом НОД полученного (НОД (a, b)) и следующего числа (НОД (c, d)), и т. д.

Таким образом, чтобы вычислить НОД k чисел, нужно последовательно вычислить (k – 1) НОД. Последнее вычисление дает искомый результат.

Определение 10. ***Взаимно простыми*** являются целые числа, наибольший общий делитель которых равен 1.

Пример 15. Взаимно простыми являются числа 11 и 7, 11 и 4, хотя число 4 само по себе не является простым.

Теорема 1. Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые числа u и v, что выполняется равенство

$$au + bv = 1. \tag{1.3}$$

Теорема 2. Если НОД $(a, b) = d$, то справедливо следующее соотношение (*соотношение Безу*):

$$au + bv = d. \tag{1.4}$$

! **Формула (1.4) называется также реализацией «*расширенного алгоритма Евклида*». Этот алгоритм состоит из двух этапов: собственно алгоритма Евклида и вычислений на основе обратных подстановок или последовательного выражения остатков в каждом из шагов предыдущего этапа с соответствующим приведением подобных на каждом шаге.**

Пример 16. Для демонстрации обратимся к примеру 14, который составляет первый из указанных этапов. Ниже приведена табл. 1.1, из которой можно легко понять, как по алгоритму Евклида вычисляются остатки.

Таблица 1.1

Реализация алгоритма Евклида для примера 14

1234 = 54 · 22 + 46	46 = 1234 – 54 · 22
54 = 46 · 1 + 8	8 = 54 – 46 · 1
46 = 8 · 5 + 6	6 = 46 – 8 · 5
8 = 6 · 1 + 2	2 = 8 – 6 · 1

Обратные подстановки, или проход вверх, начинаются от записи равенства в нижней строке правого столбца таблицы: $2 = 8 - 6 \cdot 1$. Далее вместо цифры 6 подставляется ее значение из равенства строкой выше: $2 = 8 - (46 - 8 \cdot 5) \cdot 1$ и т. д. Полная цепочка подстановок и преобразований выглядит так: $2 = 8 - (46 - 8 \cdot 5) \cdot 1 = 8 - 46 + 8 \cdot 5 = 8 \cdot 6 - 46 = (54 - 46) \cdot 6 - 46 = 54 \cdot 6 - 46 \cdot 6 - 46 = 54 \cdot 6 - 46 \cdot 7 = 54 \cdot 6 - (1234 - 54 \cdot 22) \cdot 7 = 54 \cdot 6 - 1234 \cdot 7 + 54 \cdot 154 = \mathbf{54 \cdot 160 + (-7) \cdot 1234} = 8640 - 8638$. Из выражения перед последним знаком равенства (выделено) следует, что для нашего примера $u = -7$ и $v = 160$ в соответствии с формой записи в выражении (1.4).