

### Вариант 1

1. Чему равно значение выражения в системе счисления с основанием 16?

$$1011,01_2 + 24,6_8$$

В ответе укажите только число, основание системы счисления указывать не нужно.

2. В алгоритме шифрования RSA на одном из этапов формирования пары ключей используется формула:

$(d \cdot e) \% f(n) = 1$ , где операция « % » — это остаток от деления.

Значение функции  $f(n)$  вычисляется по формуле  $f(n) = (p - 1) \cdot (q - 1)$ .

**Определите наибольшее значение числа  $d$ , которое меньше 40, если известно, что  $p = 5$ ,  $q = 7$ ,  $e = 11$ .**

3. Для хранения целых чисел со знаком в памяти компьютера существует два подхода. Первый заключается в замене первого бита на единицу. Несмотря на свою простоту, он не применяется в компьютерах для представления целых чисел, т. к. действия над числом выполняются по-разному для разных сочетаний знаков чисел. Второй подход заключается в построении дополнительного кода путём инверсии битов числа и операции сложения с единицей. Он позволяет выполнять арифметические действия с положительными и отрицательными числами по одному и тому же алгоритму.

**Постройте восьмибитный двоичный дополнительный код к числу -38.**

### Вариант 2

1. Вычислите значение выражения в системе счисления с основанием 8:

$$1101,01_2 - 34,6_8$$

В ответе укажите только число в восьмеричной системе, основание указывать не нужно.

2. В криптосистеме Эль-Гамала используется формула:

$y \equiv g^x \bmod p$  где:

$p = 23$  (простое число)

$g = 5$  (первообразный корень по модулю  $p$ )

$x = 7$  (секретный ключ)

**Найдите значение  $y$ .** В ответе укажите только число.

3. Для хранения целых чисел со знаком в памяти компьютера существует два подхода. Первый заключается в замене первого бита на единицу. Несмотря на свою простоту, он не применяется в компьютерах для представления целых чисел, т. к. действия над числом выполняются по-разному для разных сочетаний знаков чисел. Второй подход заключается в построении дополнительного кода путём инверсии битов числа и операции сложения с единицей. Он позволяет выполнять арифметические действия с положительными и отрицательными числами по одному и тому же алгоритму.

**Постройте восьмибитный двоичный дополнительный код к числу -125.**

### Вариант 3

1. Чему равно значение выражения в системе счисления с основанием 8?

$$1101,01_2 - 12,3_4$$

В ответе укажите только число, основание системы счисления указывать не нужно.

2. В алгоритме Диффи-Хеллмана для обмена ключами используется формула:

$$K = (g^a \bmod p)^b \bmod p, \text{ где } a \text{ и } b \text{ — секретные числа участников.}$$

Определите общий ключ  $K$ , если:

$$p = 23, g = 5,$$

секретное число Алисы  $a = 6$ ,

секретное число Боба  $b = 15$ .

3. Для хранения целых чисел со знаком в памяти компьютера существует два подхода. Первый заключается в замене первого бита на единицу. Несмотря на свою простоту, он не применяется в компьютерах для представления целых чисел, т. к. действия над числом выполняются по-разному для разных сочетаний знаков чисел. Второй подход заключается в построении дополнительного кода путём инверсии битов числа и операции сложения с единицей. Он позволяет выполнять арифметические действия с положительными и отрицательными числами по одному и тому же алгоритму.

**Постройте восьмибитный двоичный дополнительный код к числу -44.**