**Вопросы к лабораторной работе №3**

1. **Дать определение понятий: целое число, натуральное число, делимость чисел, собственный делитель, НОД.**

Целыми числами называются все натуральные числа, все числа противоположные им по знаку и нуль. Обозначается множество целых чисел Z Z={…,−3,−2,−1,0,1,2,3,…}).

Натуральные числа — это числа, начиная с 1, получаемые при счете предметов. 1, 2, 3, 4, 5…

Делимость чисел – это отношение, связь между целыми числами. Целое число а делится на целое число b, если существует целое число q, такое что а = bq. При этом число b считается отличным от нуля. Число а называется делимым, b называется делителем, а число q называется частным. Также говорят: "a кратно b".

Собственным делителем числа называется всякий его делитель, отличный от самого числа. У простых чисел существует ровно один собственный делитель — единица.

Наибольшее целое число, которое делит без остатка числа a и b называется наибольшим общим делителем этих чисел, НОД (m, n).

1. **Сформулировать основную теорему арифметики. Представить примеры ее применения.**

Всякое натуральное число (кроме 1) можно представить как произведение простых множителей.

Так, например, разложение числа 210 на простые множители может иметь вид 210 = 2 · 5 · 3 · 7 или 210 = 2 · 3 · 7 · 5

1. **Пояснить сущность проблемы факторизации и ее связь с прикладной криптографией.**

Факторизацией целого числа называется его разложение в произведение простых сомножителей. Такое разложение, согласно основной теореме арифметики, всегда существует и является единственным (с точностью порядка следования множителей).

Проблема факторизации напрямую связана с определением криптостойкости RSA, которое базируется на предположении, что не существует быстрых алгоритмов факторизации, которые за короткое время позволили бы взломать код, а если через некоторое время и получится это сделать, то данные потеряют свою актуальность.

1. **Найти НОД: пар чисел: 333и100;56и200;99и200;61и987;123и456; трех чисел: 21, 43, 342; 57, 31, 200; 42, 11, 98.**

НОД(333,100)=1, НОД(56,200)=8, НОД(99,200)=1, НОД(61,987)=1, НОД(123,456)=3, НОД(21,43,342)=1, НОД(57,31,200)=1, НОД(42,11,98)=1

1. **Записать каноническое разложение чисел: 2770, 3780, 6224.**

2770 = 2 · 5 · 277

3780 = 2 · 2 · 3 · 3 · 3 · 5 · 7 = 22 · 33 · 5 · 7

6224 = 2 · 2 · 2 · 2 · 389 = 24 · 389

1. **Записать соотношение Безу. Показать пример его практического использования.**

Соотношение Безу — представление наибольшего общего делителя целых чисел в виде их линейной комбинации с целыми коэффициентами.

Формулировка. Пусть a, b — целые числа, хотя бы одно из которых не нуль. Тогда существуют такие целые числа x,y, что выполняется соотношение: НОД(a,b)=x⋅a+y⋅b, которое называется соотношением Безу (для чисел a и b), а также леммой Безу или тождеством Безу. При этом целые числа x,y называются коэффициентами Безу.

Пример. НОД(12,30) = 6. Соотношение Безу имеет вид 6 = 3 · 12 + (-1) · 30.

1. **Подсчитать число взаимно простых чисел с числами 2770, 3780, 6224.**

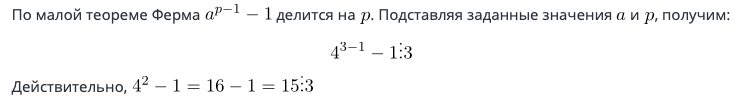
1104, 864, 3104

1. **Сформулировать малую теорему Ферма. Показать примеры ее практического применения.**

Если p- простое число и a− целое число, не делящееся на p, то a p−1−1 делится на p, т.е.



Пример. p=3 и a=4



1. **Сформулировать основные свойства модулярной арифметики.**

Первое свойство: (a + b) mod n = [(a mod n) + (b mod n)] mod n

Второе свойство: (a – b) mod n = [(a mod n) - (b mod n)] mod n

Третье свойство: (a x b) mod n = [(a mod n) x (b mod n)] mod n

1. **Пояснить порядок операций на основе расширенного алгоритма Евклида.**

Находим НОД (7,40) – прямая прогонка (алгоритм Евклида):

40 = 7·5 + 5,

7 = 5·1 + 2,

5 = 2·2 + 1, т. е. НОД (7,40) = 1.

1=5–2·2=5–2(7–5·1)=5·3+7(-2)=(40–7·5)3+7(-2) = 40·3+7(-17) = kn + ху=1(mod

n), или 7(-17) = 7y, так как -17 mod 40 = 23, то у=23: число 23 является обратным числу 7 по модулю 40.

Таким образом, сначала представляем первое число через второе плюс остаток, зачем представляем второе число через остаток предыдущего и подобное повторяем до получения остатка 1. Затем идем от последнего выражения до первого, выражая значения через разность, результатом которой будет 1, проводим данное действие пока не получим уравнение вида xy + kn =1

1. **Найти числа обратные к а по модулю n: a=41,n=143; a=13, n=71.**

7, 11