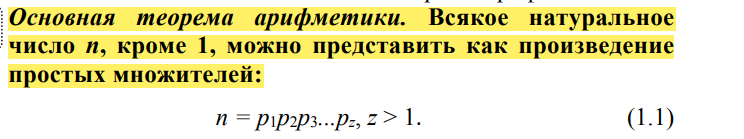
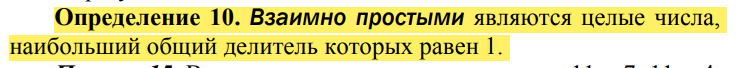
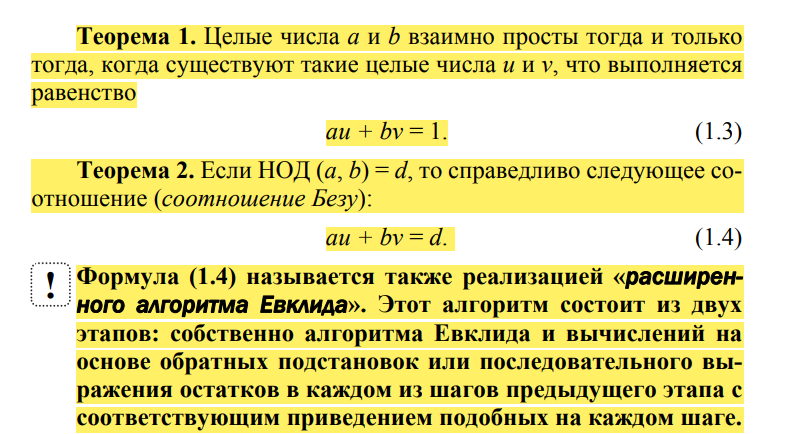
# 

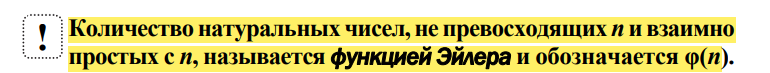


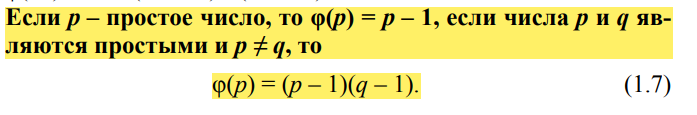
# 

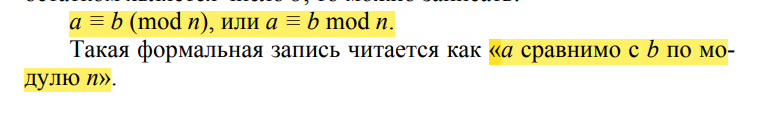


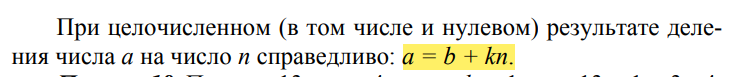


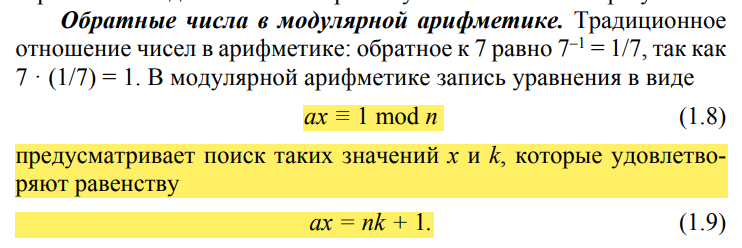
# Функция Эйлера

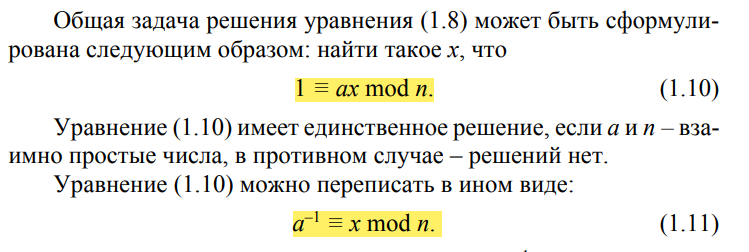


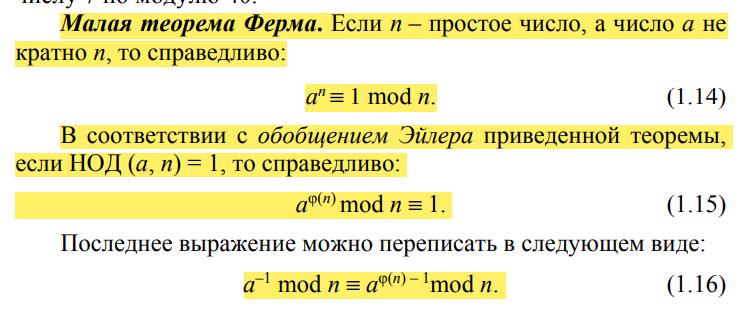












# 

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

**Целое число** - число, не содержащее дроби

**Натуральное число** - числа, возникающие естественным образом при счёте

**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* .

**Собственным делителем** числа называется всякий его делитель, отличный от самого числа.

**НОД** - наибольшим общим делителем для двух целых чисел m и n называется наибольший из их общих делителей.

# 2. Сформулировать основную теорему арифметики. Представить примеры ее применения.

Всякое натуральное число можно разложить на простые множители, т. е. однозначно записать его в виде произведения степеней простых чисел.

Например, число 12600 имеет такое разложение на простые множители: 

# 3. Пояснить сущность проблемы факторизации и ее связь с прикладной криптографией.

# 4. Найти НОД: пар чисел: 333 и 100; 56 и 200; 99 и 200; 61 и 987; 123 и 456; 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

# 5. Записать каноническое разложение чисел: 2770; 3780; 6224.

2770 = 2\*5\*277

3780 = 2\*2\*3\*3\*3\*5\*7

6224 = 2\*2\*2\*2\*389

# 6. Записать соотношение Безу. Показать пример его практического использования.

НОД(a,b) = d соотношение au + bv = d - наибольший общий делитель чисел a, b можно всегда представить как линейную комбинацию a и b с целыми коэффициентами.

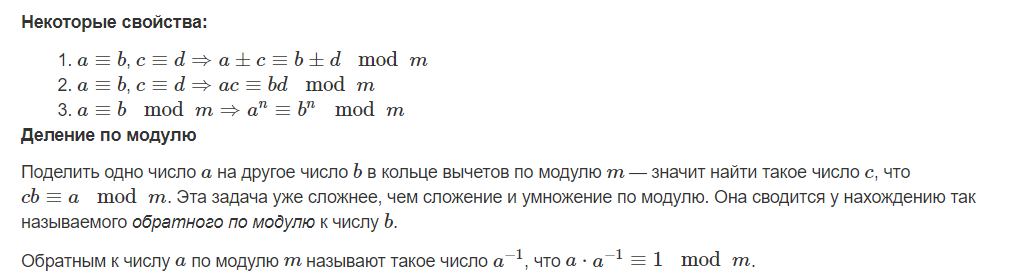
# 7. Подсчитать число взаимно простых чисел с числами 2770, 3780, 6224.

# 8. Сформулировать малую теорему Ферма. Показать примеры ее практического применения.

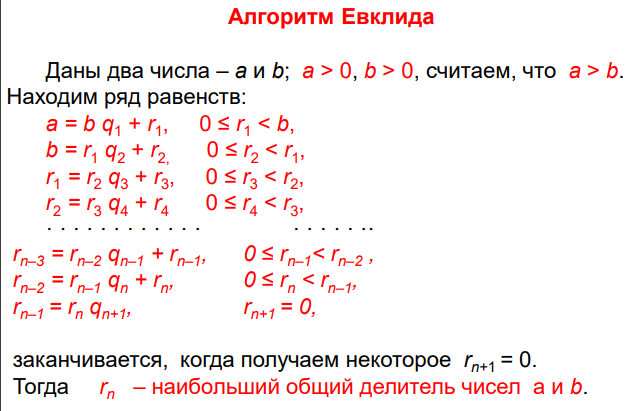
Малая теорема Ферма. Если n – простое число, а число а не кратно n, то справедливо:

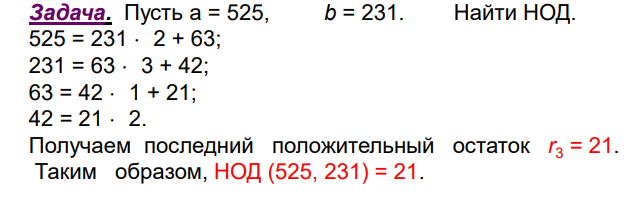


# 9. Сформулировать основные свойства модулярной арифметики.



# 10. Пояснить порядок операций на основе расширенного алгоритма Евклида.





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

a = 41 n = 143 - 7

a = 13 n = 71 - 11

Дистрибутивносить, коммутативность, ассоциативность