Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическое задание №6**

**Тема «Теория чисел»**

Руководитель: Ржеутская Н. В.

Выполнил:

Студент 2 курса 8 группы ФИТ

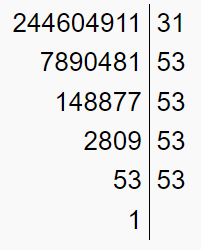
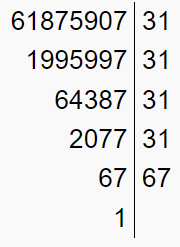
Солодкий Денис Викторович

Минск 2022

**Вариант №13**

**Задание №1**

Найти канонические разложения чисел а и b.

*а* = 244604911, *b* = 61875907, тогда  
  

Итого, 627 = 534 ∙ 31; 399 = 67 ∙ 314

**Задание №2**

Найти НОД (a, b) пользуясь:

a) алгоритмом Евклида,

б) разложением чисел на простые множители.

Алгоритм Евклида

*а* = 244604911, *b* = 61875907, тогда

244604911 = 61875907 ∙ 3 + 58977190  
61875907 = 58977190 ∙ 1 + 2898717  
58977190 = 2898717 ∙ 20 + 1002850  
2898717 = 1002850 ∙ 2 + 893017  
1002850 = 893017 ∙ 1 + 109833  
893017 = 109833 ∙ 8 + 14353  
109833 = 14353 ∙ 7 + 9362  
14353 = 9362 ∙ 1 + 4991  
9362 = 4991 ∙ 1 + 4371  
4991 = 4371 ∙ 1 + 620  
4371 = 620 ∙ 7 + 31  
620 = 31 ∙ 20 + 0

Разложение чисел на простые множители

Наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (244604911; 61875907) = 31

**Задание №3**

С помощью расширенного алгоритма Евклида найти целые u, v, удовлетворяющие соотношению Безу: au + bv = НОД (a, b)

31 = 4371 – 620∙7 = 4371 – (4991 – 4371)∙7 = 4371∙8 – 4991∙7 = (9362 – 4991)∙8 – 4991∙7 = 9362∙8 – 4991∙15 = 9362∙8 – (14353 – 9362)∙15 = 9362∙23 – 14353∙15 = (109833 – 14353∙7)∙23 – 14353∙15 = 109833∙23 - 14353∙176 = 109833∙23 – (893017 – 109833∙8)∙176 = 109833∙1431 – 893017∙176 = (1002850 – 893017)∙1431 – 893017∙176 = 1002850∙1431 – 893017∙1607 = 1002850∙1431 – (2898717 – 1002850∙2)∙1607 = 1002850∙4645 – 2898717∙1607 = (58977190 – 2898717∙20)∙4645 – 2898717∙1607 = 58977190∙4645 – 2898717∙94507 = 58977190∙4645 – (61875907 – 58977190)∙94507 = 58977190∙99152 – 61875907∙94507 = (244604911 – 61875907∙3)∙99152 – 61875907∙94507 = 244604911∙99152 – 61875907∙391963 = 244604911∙(99152) + 61875907∙(-391963) = 31

a = 244604911, u = 99152  
b = 61875907, v = -391963

**Задание №4**

Найти остаток от деления данного числа на простое.

Найти остаток от деления на 17.

**2001 = 17∙117 + 6; 2001 ≡ 6 mod 17**

**φ (17) = 17(1 - 1/17) = 16; 616 ≡ 1 mod 17; 1995 = 16∙124 + 11 => 61995 = 616∙124 + 11 = (616)124 ∙ 611 ≡ 362797056 mod 17; 362797056 = 21341003∙17 + 5 => 362797056 ≡ 5 mod 17**

**Ответ: r(20011995)17 = 5**

**Вывод: я повторил математику. А также алгоритмы Эйлера и Евклида здорово помогают найти НОД чисел. А с помощью малой теоремы Ферма и формулы Эйлера можно найти остаток от деления больших чисел.**