МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №2

“Тема №2”

з дисципліни «Математичні основи криптології»

Виконав:

Студент групи 6.04.125.010.21.2

факультету Інформаційних технологій

спеціальності 125

П.І.П. Бойко В.В.

Перевірив:

Чугай А.М.

Харків – 2022

1. Які з таких відносин є істинними, а які — хибними?

5|26 3|123 27†127 15†21 23|96 8|5

5|26 26 = 5 \* 5 + 1 – твердження хибне

3|123 123 = 41 \* 3 – твердження не хибне

27†127 127 = 4 \* 27 + 19 – твердження не хбне

15†21 21 = 1 \* 15 + 6 – твердження не хибне

23|96 96 = 4 \* 23 – твердження не хибне

8|5 5 = 1 \* 8 + (-3) – твердження хибне

2. Використовуючи алгоритм Евкліда, знайдіть найбільший спільний дільник наступних пар цілих чисел:

88 і 220 (220, 88) => (88, 44) => (44, 0) НОД = 44

* 1. 300 і 42 (300, 42) => (42, 6) => (6, 0) НОД = 6
  2. 24 і 320 (320, 24) => (24, 8) => (8, 0) НОД = 8
  3. 401 і 700 (700, 401) => (401, 299) => (299, 102) => (102, 95) => (95, 7) => (7, 4) => (4, 3) => (3, 1) => (1, 0) НОД = 1

3. Розв'яжіть такі приклади: o ДаноНОД (a, b) = 24, знайдітьНОД (a, b, 16)

* 1. Дано НОД (a, b, c) = 12, знайдіть НОД (a, b, c, 16)
  2. (16, 12) => (12, 4) => (4, 0)
  3. НОД = 4
  4. Знайдіть НОД (200, 180, і 450)
  5. (200, 180) => (180, 20) => (20, 0)
  6. (450, 20) => (20, 10) => (10, 0)

1. НОД = 10
   1. Знайдіть НОД (200, 180450610)
   2. (180450610, 200) = (200, 10) => (10, 0)
   3. НОД = 10

4. Припустимо, що n- Невід'ємне ціле число.

Знайдіть НОД (3 n + 1,2 n +1).

* 1. Використовуючи результат частиниа, знайдіть НОД (301, 201) і НОД (121, 81)

5. Використовуючи розширений алгоритм Евкліда, знайдіть найбільший спільний дільник наступних пар та значення s і t:

4 і 7 (7, 4) => (4, 3) => (3, 1) => (1, 0) 1 s = -1 t = 2

* 1. 291 і 42 (291, 42) => (42, 39) => (39, 3) => (3, 0) 3 s = -1 t = 7
  2. 84 і 320 (320, 84) => (84, 68) => (68, 16) => (16, 4) => (4, 0) 4 s = 5 t = -19
  3. 400 і 60 (400, 60) => (60, 40) => (40, 20) => (20, 0) 20 s = -1 t = 7

6. Знайдіть результати наступних операцій:

22 mod 7 = 1

* 1. 140 mod 10 = 0
  2. -78 mod 13 = 0
  3. 0 mod 15 = 0

7. Виконайте такі операції, спочатку використовуючи наступне скорочення:

(273 + 147) mod 10 = 0

* 1. (4223 + 17323) mod 10 = 6
  2. (148 + 14432) mod 12 = 0
  3. (2467+461) mod 12 = 0

8. Знайдіть приватне та загальні рішення наступних лінійних діофантових рівнянь:

25x + 10y = 15

приватне(x0=3, y0=-6) загальне(x=3+2n, y=-6 - 5n)

* 1. 19x + 13y = 20

приватне(x0=40, y0=60) загальне(x=-40+13n, y=60-19n)

* 1. 14x + 21y = 77
  2. приватне(x0=-11, y0=11) загальне(x=-11 + 3n, y=11-2n
  3. 40x +16y = 88

приватне(x0=11, y0=22) загальне(x=11+2n, y=22-5n)

9. Покажіть, що немає жодного рішення наступних лінійних діофантових рівнянь:

15x + 12y = 13 (Рішення немає бо 13 не ділиться на 3)

* 1. 18x + 30y = 20 (Рішення немає бо 20 не ділиться на 6)
  2. 15x + 25y = 69 (Рішення немає бо 69 не ділиться на 5)
  3. 40x +30y = 98 (Рішення немає бо 98 не ділиться на 10)

10. Поштове відділення продає марки лише за15центів та за39центів. Знайдіть число марок, які має купити клієнт, щоб сплатити пересилання пакета вартістю2,70 $. Знайдіть кілька рішень.

(0.15, 2.7) (2.7, 0.15) => (0.15, 0) = 0.15

1. 2.7 = 0.15 \* 18
2. 0,39 \* 5 = 1,95  
   2,7 – 1,95 = 0.75  
   5 \* 0.15 = 0.75