## Лабораторна робота №3

**Тема:** Діофантові рівняння. Застосування конгруенції, їх властивостей та теорем Ейлера і Ферма.

**Ціль:** навчитись розвязувати Діофантові рівняння першого степеня, визначати остачу від ділення, розвязувати лінійні конгруенції та використовувати їх в прикладних задач цілочисельного розвязку.

**Теоретичні відомості**

Рівняння виду , де - многочлен декількох змінних з цілими коефіцієнтами для яких потрібно знайти цілі розв’язки, називають діофантовими рівняннями. Названі вони ім’ям грецького математика Діофанта, який жив у ІІІ столітті н.е. Його книга «Арифметика» містила 189 задач з цілими числами, для кожної з яких наводилося один або декілька розв’язків.

Розв’язати діофантове рівняння означає:

1. з’ясувати, чи має рівняння хоча б один ненульовий розв’язок в цілих числах;
2. якщо рівняння має розв’язок в цілих числах, то з’ясувати скінченна чи нескінченна множина його розв’язків;
3. знайти всі цілі розв’язки рівняння.

Лінійні діофантові рівняння виду навчились розв’язувати ще до Діофанта. Стародавні греки знали, що якщо це рівняння має один цілий розв’язок , то його буде задовольняти нескінченна множина пар  виду , де  - будь яке ціле число.

Математики Стародавньої Греції та Стародавньої Індії знали методи розв’язання деяких рівнянь другого степеня виду . Зокрема їм були відомі всі піфагорові трійки натуральних чисел , що задовольняють рівняння . Всі трійки взаємно простих піфагорових чисел стародавні математики знаходили за формулами ,  - натуральні числа причому .

Особливе місце серед діофантових рівнянь займає рівняння , де - натуральне число. Французький математик П’єр Ферма довів, що при  рівняння не має розв’язків в натуральних числах .

**Діофантові рівняння першого степеня**

Рівняння виду де  - числа, а - змінні, називають діофантовим рівнянням першого степеня з двома змінними. Для розв’язання рівняння застосовують наступні теореми.

*Теорема1.* Якщо  - взаємно прості числа, то для будь якого цілого , рівняння має хоча б один розв’язок в цілих числах.

*Теорема2.* Якщо мають спільний натуральний дільник , а ціле число  не ділиться на , то рівняння не має розв’язків в цілих числах.

*Теорема3.* Якщо взаємно прості числа, то рівняння  має нескінченну кількість розв’язків , які знаходять за формулами, де  - будь який цілий розв’язок даного рівняння, .

Частинний розв’язок  можна знайти підбором, для малих , а у випадку коли числа  великі, то користуємось наступною теоремою.

*Теорема4*. *НСД()* може бути записаний у вигляді , де  цілі числа.

 знаходимо за алгоритмом Евкліда.

***Означення 1***. *Цілі числа* і  *називають конгруентними за модулем*  *, де* — *ціле число, якщо їхня річниця*   *ділиться на* *.* Позначення:

**

Якщо і  не конгруентні за модулем *,* то пишуть

**

***Означення 2****. Цілі числа* і  *називають конгруентними ва модулем* *, де*  , *якщо еони при діленні на*  *дають однакові остачі.*

***Означення 3****. Цілі числа* і  *називають конгруентними за модулем* *, де* , *якщо існує таке ціле число , що .*

Означення 1, 2, 3 рівносильні.

**Основні властивості конгруенцій**

1°. Відношення конгруентності за даним модулем є бінарне відношення еквівалентності на множині цілих чисел. Класи еквівалентності називають **класами лишків за даним модулем**.

2°. Конгруенції за одним модулем можна почленно додавати, віднімати і множити.

3°. До обох частин конгруенції можна додати будь-яке ціле число (це дає змогу переносити будь-який доданок з однієї сторони в другу з протилежним знаком).

4°. До будь-якої частини конгруенції можна додати довільне ціле число, кратне модулю.

5°. Обидві частини конгруенції можна помножити на ціле число;

6°. Обидві частини конгруенції можна поділити на їхній спільний дільник, якщо він взаємно простий з модулем.

7°. Якщо у виразі 

усі коефіцієнти і числа замінити на конгруентні їм за модулем коефіцієнти і числа  відповідно, то вираз



буде конгруентний заданому за модулем *:*

.

8°. Обидві частини конгруенції і модуль можна множити на ціле число.

9°. Обидві частини конгруенції і модуль можна скорочувати на їхній спільний дільник.

10°. Якщо конгруенція має місце за кількома модулями, то вона має місце і за модулем, який дорівнює спільному найменшому кратному цих модулів.

11°. Якщо конгруенція має місце за модулем *,* то вона має місце за модулем *,* де — довільний дільник числа .

12°. Якщо одна частина конгруенції і модуль діляться на деяке число, то й друга частина конгруенції ділиться на те саме число.

13°. Якщо **, то *.*

**Теорема Ейлера**. *Якщо * і , то .

**Теорема Ферма (мала теорема Ферма).** *Якщо число  просте,*

* то* .

**Наслідок**. *Якщо  просте число,* — *будь-яке ціле число, то .*

***Методичні рекомендації до розв‘язування задач***

**Приклад 1**. Які з чисел 234, 634, 104 конгруентні числу 9 за модулем 25.

*Розв‘язання*. Віднімемо від даних чисел число 9. Дістанемо:

234 – 9= 225, 634 – 9=625, 104 – 9=95. Числа 225 і 625 діляться на 25, тому числа 234 і 634 конгруентні числу 9 за модулем 25, тобто

, .

**Приклад 2**. Довести, що .

*Розв‘язання*. Скористуємося другою властивістю конгруенцій за одним і тим самим модулем. Розглянемо почленно конгруенції

,,,,

Помножимо всі одержані конгруенції

.

Отже, .

**Приклад 3**. Знайти остачу від ділення  на .

*Розв‘язання*. Скористаємося властивостями конгруенцій за модулем . Нам треба знайти таке ціле невід‘ємне число , що  і . оскільки , то , тобто .

За властивостями  .

. (\*)

,  

. (\*\*)

, ,  .

 (⁂)

Виконаємо дії додавання та віднімання над конгруенціями (\*),(\*\*),(⁂).

(\*) – (\*\*) + (⁂),

  +  

.

Отже, число  при діленні на  дає остачу .

**Приклад 4. Розв’язати в цілих числах рівняння.** 

Так як *НСД(13,21)=1,* то дане рівняння має безліч розв’язків. Підбором встановлюємо частинний розв’язок .

Тоді загальний розв’язок має вигляд .

***Відповідь:*** .

**Приклад 5. Розв’язати в цілих числах рівняння.** ****

Так як *НСД(45;37)=1,* то рівняння має безліч розв’язків.

Щоб знайти  застосуємо алгоритм Евкліда:

. Отже . Запишемо алгоритм Евкліда в зворотньому напрямку (лінійне представлення):



Отже (14;17) частинний розв’язок рівняння **.**

Тоді тобто .

Отже всі розв’язки знайдемо за формулами .

***Відповідь:*** 

**Приклад 6. Розв’язати в цілих числах рівняння.** 

Знайдемо *НСД(2183;1961)=*для цього скористаємося алгоритмом Евкліда.

.

Отже, .

Запишемо алгоритм Евкліда в зворотньому напрямку:



Отже  - частинний розв’язок рівняння .

Тоді , тобто  частинний розв’язок рівняння .

Загальний розв’язок має вигляд: .

***Відповідь:*** .

**Приклад 7. Розв’язати конгруенцію.**

Нехай , нехай  чисельник передостаннього підхідного дробу  для числа  . Оскільки  нескоротний дріб, то . За властивостей підхідних дробів маємо .

Розглянемо приклад маємо таблицю, де , , , . Тоді ;

.

**Приклад 12 Розв’язати конгруенцію.** .

*Розв‘язання*. .

Розкладемо дріб  у ланцюговий дріб і знайдемо  та .

За алгоритмом Евкліді дістанемо

1993=501\***3**+490; n=0;

501=490\***1**+11; n=1;

490=11\***44**+6; n=2;

11=6\***1**+5; n=3;

6=5\***1**+1; n=4;

5=1\***5**+0; n=5;

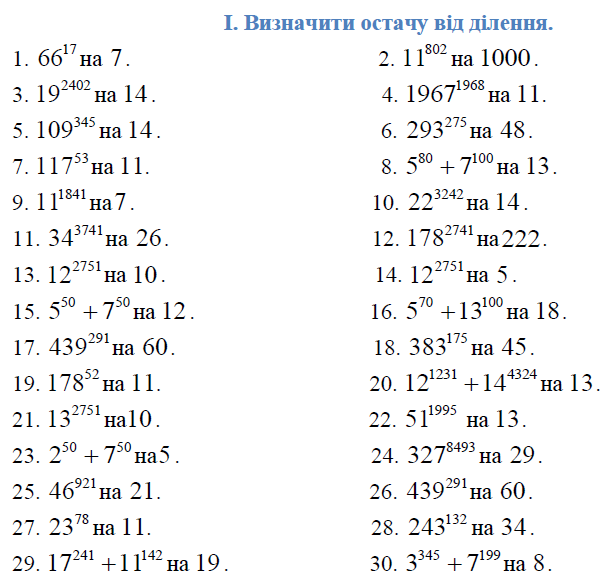
Отже, , .

Для обчислення , складемо таблицю

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| k | -1 | 0 | 1 | 2 | 3 | 4 | 5 |
| qk | ///////  + | **3** | **1** | **44** | **1** | **1** | **5** |
| Pk | 1 | \* |  |  |  |  |  |
| Qk | 0 | 1 |  |  |  |  |  |

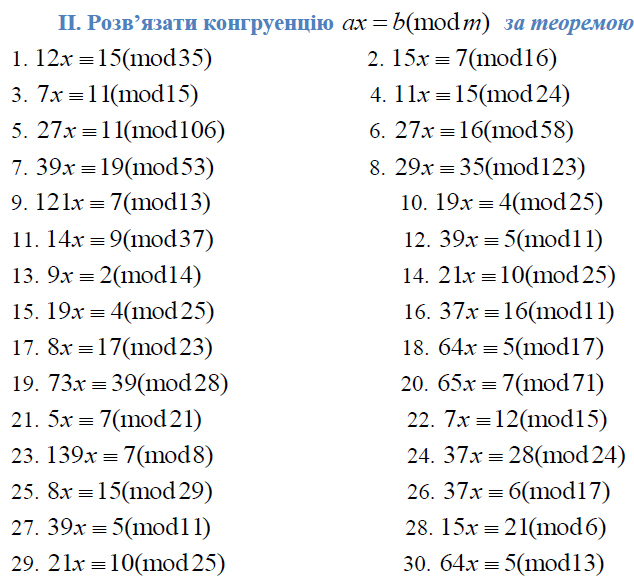
 Звідси .

*Відповідь*.



**Приклад. Варіант 30.**

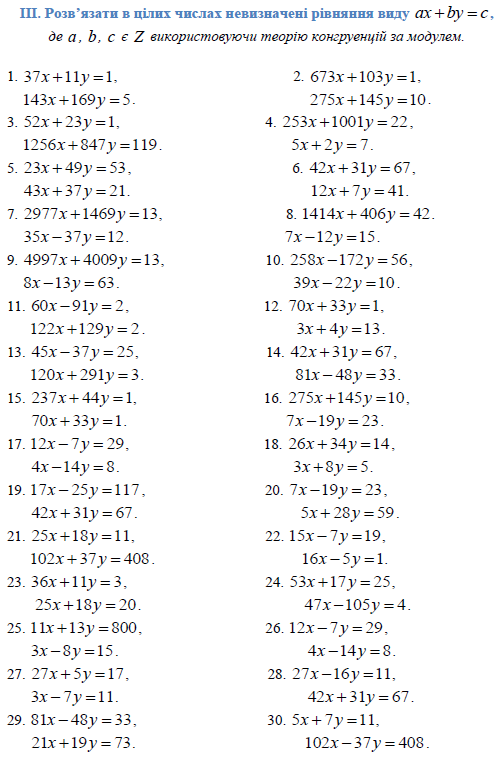
Остача від ділення на 8 дорівнює 2.



**Приклад. Варіант 30.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13=64\*0+13  64=13\*4+12  13=12\*1+1  12=1\*12+0 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | k | -1 | 0 | 1 | 2 | 3 | | qk | /////// | **0** | **4** | **1** | **12** | | Pk | 1 | **0** | 1 | 1 | 13 | | Qk | 0 | 1 | 4 | 5 | 64 | |

Перевірка:



**Приклад. Варіант 30.** 1) 5x+7y=11;

; **x=7t+5;**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| t | -2 | -1 | 0 | 1 | 2 | 3 |
| x | -9 | -2 | 5 | 12 | 19 | -9 |
| y | 8 | 3 | -2 | -7 | -12 | 8 |

Відповідь: (-9,8),(-2,3),(5,-2),(12,-7),(19,-12),(-9,8),…

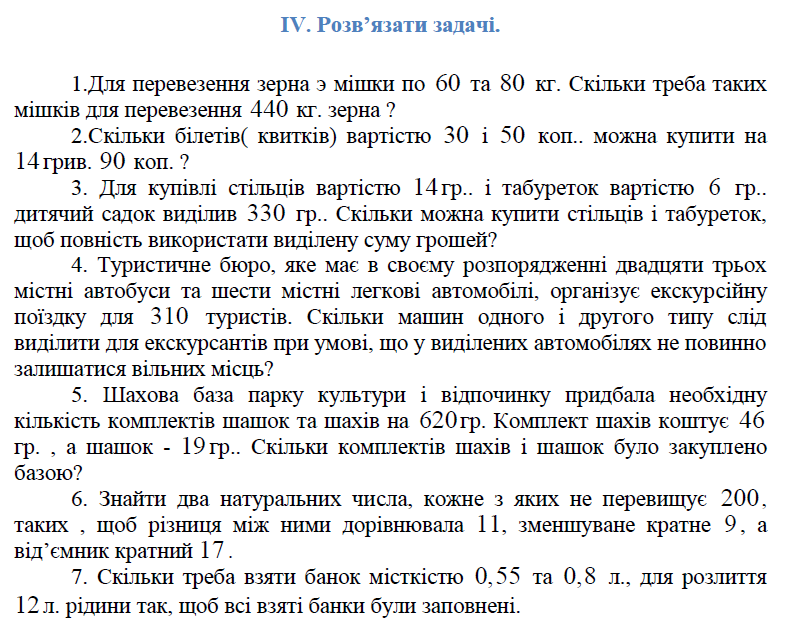
2) 102x-37y=408;

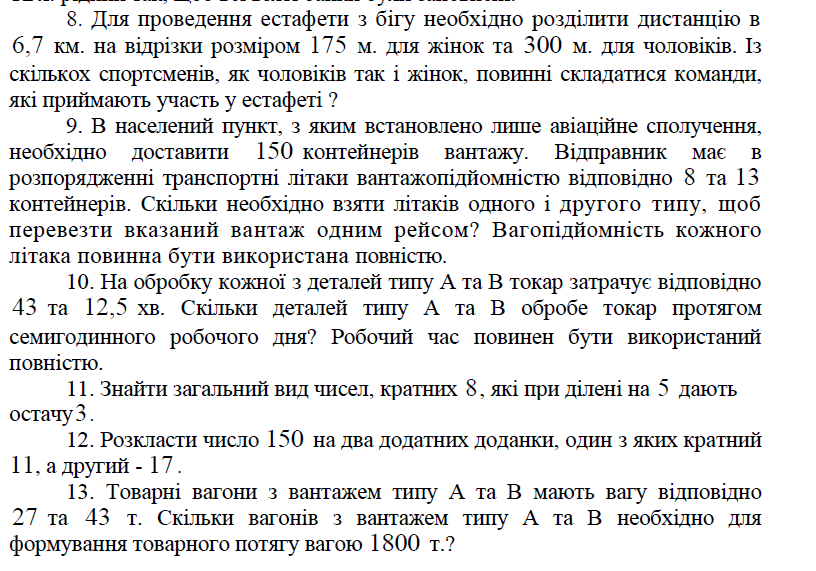
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37/28=[1;3,9]  37=28\***1**+9  28=9\***3**+1  9=1\***9**+0 | |  |  |  |  |  | | --- | --- | --- | --- | --- | | k | -1 | 0 | 1 | 2 | | qk | /////// | **1** | **3** | **9** | | Pk | 1 | **1** | 4 | 37 | | Qk | 0 | 1 | 3 | 28 | |

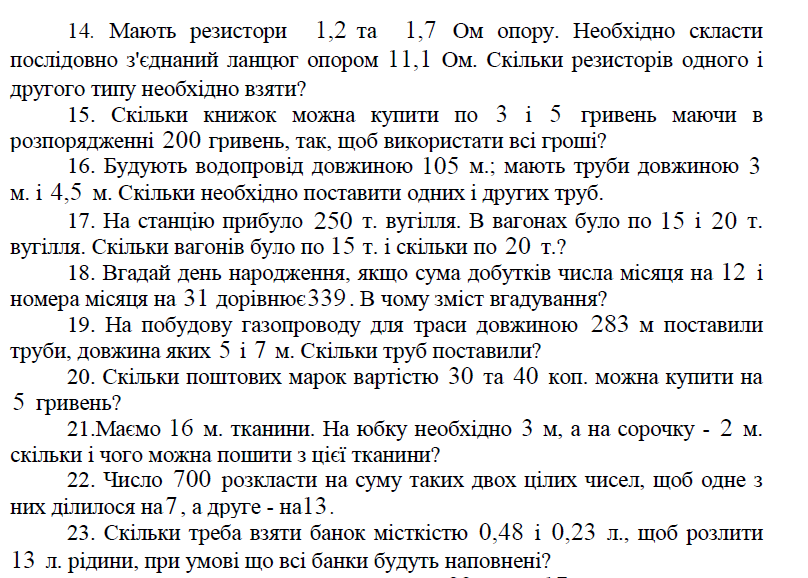
**x=37t+4;**

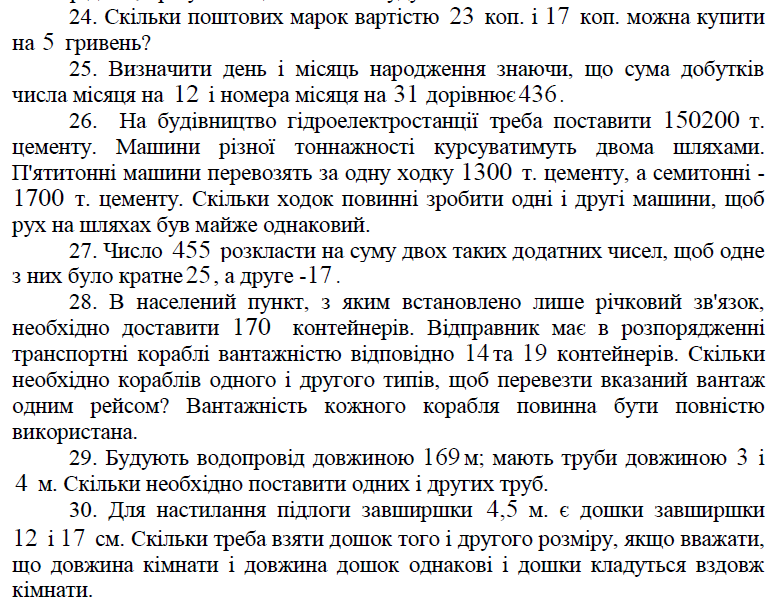
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| t | -2 | -1 | 0 | 1 | 2 | 3 |
| x | -70 | -33 | 4 | 41 | 78 | -70 |
| y | -204 | -102 | 0 | 102 | 204 | -204 |

Відповідь: (-70,-204),(-33,-102),(4,0),(41,102),(78,204),(-70,-204),….









**Приклад. Варіант 30.** 4.5m=450cm

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| t | -2 | -1 | 0 | 1 | 2 | 3 |
| x | -22 | -5 | 12 | 29 | 46 | 63 |
| y | 42 | 30 | 18 | 6 | -6 | -18 |

**Відповідь.** *Так як відємної кількості дошок неможе бути, тоді відповідь має міститися в додатніх розвязках (12,18) або (29,6).*