Домашняя работа 2. Громов А.А.

Задание 1. Повторение - мать учения (2 балла, $\frac{1}{3}$ каждый)

1. A = {Blue, Yellow, Red, White, Green}
2. A = {2, 4, 6, 8, 10, 12}, B = {3, 6, 9, 12}
   1. $A \cup B = \{2, 3, 4, 6, 8, 9, 10, 12\}$
   2. $A \cap B = \{6, 12\}$
   3. $A \setminus B = \{2, 4, 8, 10\}$
   4. $B \setminus A = \{3, 9\}$
   5. $A \times B = \{(2,3), (2,6), (2,9), (2,12), (4,3), (4,6), (4,9), (4,12),$
      $(6,3), (6,6), (6,9)(6,12), (8,3), (8,6), (8,9), (8,12),$
      $(10,3), (10,6), (10,9), (10,12), (12,3), (12,6), (12,9), (12,12)\}$
3. Найти:
   1. $\mathbb{Z}_7^* = \{x \in \mathbb{Z}_7 | gcd(x, 7) = 1\} = \{1, 2, 3, 4, 5, 6\}$
   2. $\mathbb{Z}_8^* = \{x \in \mathbb{Z}_8 | gcd(x, 8) = 1\} = \{1, 3, 5, 7\}$
4. Пусть множество $n\mathbb{Z} = \{nx | x \in \mathbb{Z}\}$. Найдите:
   1. $2\mathbb{Z} = \{2x | x \in \mathbb{Z}\}\{0, \pm 2, \pm 4 \ldots\}$
   2. $3\mathbb{Z} = \{3x | x \in \mathbb{Z}\}\{0, \pm 3, \pm 6 \ldots\}$
   3. $3\mathbb{Z} \cap 2\mathbb{Z} = \{3x | x \in 2\mathbb{Z}\}\{0, \pm 6, \pm 12 \ldots\}$
   4. $3\mathbb{Z} \setminus 2\mathbb{Z} = \{3x | x \in \mathbb{Z}; x \notin 2\mathbb{Z}\}\{0, \pm 3. \pm 9, \pm 15\}$
5. $\{0,1\}^3 = \{0,1\} \times \{0,1\} \times \{0,1\} = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1),$
   $(1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$
6. 2^X = $\{\varnothing\}, 1, 2, 3, 1, 2, 1, 3, 2, 3, 1, 2, 3$

Задание 2. Группа или не группа? (2 балла, $\frac{1}{4}$ за каждый)

1. $\langle \mathbb{N}, + \rangle$
   Отсутвует нейтральный элемент: $(a + e) = (e + a) \neq a$
   Не группа
2. $\langle \mathbb{Z}, + \rangle$
   (a+b)+c=a+(b+c)
   Наличие нейтрального элемента: $(a + e) = (e + a) = a$ при $e = 0$
   $(a + (-a)) = (-a) + a = 0$
   Группа
3. $\langle \mathbb{Q}, * \rangle$
   Отсутствует обратный элемент для нуля. $0 * 0^{-1} = \varnothing$
   Не группа

4. $\langle \mathbb{Z}_{12}^*, * \rangle$, где $\mathbb{Z}_{12}^* = \{x \in \mathbb{Z}_{12}^* | gcd(x, 12) = 1\}$ и $*$ - это умножение по модулю 12.
$(a * b) * c(mod12) = a * (b * c)(mod12)$
Наличие нейтрального элемента: $e = 1$, т.к. $a * 1 = a$
Обратный элемент есть: $6 * 6^{-1} = 1$
Группа
5. $\langle B_n, \vee \rangle$, где $B_n = \{0, 1\}^n$ — множество всех бинарных строк длинны n и $\vee$ — побитовая операция ИЛИ.
$(a \vee b) \vee c = a \vee (b \vee c)$
Наличие нейтрального элемента: $e = 0$
Отсутствует обратный элемент
Не группа
6. $\langle B_n, \oplus \rangle$, где $B_n = \{0, 1\}^n$ — множество всех бинарных строк длинны n и $\oplus$ — побитовая операция XOR.
$(a \oplus b) \oplus c = a \oplus (b \oplus c)$
Наличие нейтрального элемента: при $e = 0$ $(0 \oplus 0 = 0, 1 \oplus 0 = 1)$
Наличие обратного элемента: $0 \oplus 1 = 1$
Группа
7. $\langle \mathbb{F}, + \rangle$, где $\mathbb{F}$ — множество всех функций: $\mathbb{Z} \to \mathbb{Z}$ и $(f + g)(x) = f(x) + g(x)$.
Ассоциативность: $(a + b)(x) = a(x) + b(x) = b(x) + a(x) = (b + a)(x)$
Наличие нейтрального элемента: $f = 0$ $(f + 0)(x) = f(x) + 0(x) = f$
Наличие обратного элемента: $(f + (-f))(x) = f(x) – f(x) = 0 = e$
Группа
8. $\langle \mathbb{F}, \circ \rangle$, где $\mathbb{F}$ — множество всех функций: $\mathbb{Z} \to \mathbb{Z}$ и $(f \circ g)(x) = f(g(x))$.
$f(x) = x^2 + x^3, g(x) = 3x - 2 => (f \circ g)(x) \neq (g \circ f)(x)$,
т.к. $(3x - 2)^2 + (3x - 2)^3 \neq 3(x^2 + x^3) - 2$
Не группа

Задание 3. Уникальность обратного (1 балл)

Докажите, что в группе G для любого элемента a ∊ G существует единственный обратный:
$\forall a \in G : \exists! a^{-1} : aa^{-1} = a^{-1}a = e$
Доказательство:
Пусть $a * a' = e$ или $a' * a = e$, => $a^{-1} * (a * a') = a^{-1}$, то есть $(a^{-1} * a) * a' = a^{-1} => e * a' = a^{-1}$, получается что $a' = a^{-1}$
Аналогичным образом можно из $a'a = e$ вывести $a' = a^{-1}$.
Для данного a существует единственный элемент a', удовлетворяющий равенству $a * a' = e$ или равенству $a' * a = e$, а именно элемент a^{-1} . Возьмем элемент a^{-1}.
Элемент a удовлетворяет равенству $a^{-1} * a = e$, т.е. является для элемента a^{-1} обратным элементом => $(a^{-1})^{-1} = a$

Задание 5. Использование теории чисел в теории групп (2 балла)

1. Докажите, что $\langle a \rangle$ - это подгруппа группы G. Каков порядок данной подгруппы?
   Содержит произведение любых двух элементов:
   $\forall a^n, a^m \in \langle a \rangle \subseteq G : a^n * a^m = a^m * a^n = a^{n+m} \in \langle a \rangle$
   Содержит единичный элемент: $a^0 = 1 \in \langle a \rangle$
   Содержит обратный элемент:$\exists a \in \langle a \rangle : a^n * a^{-n} = 1$
2. Докажите, что ⟨a⟩ — это абелева группа
   $a^n * a^m = a^m * a^n = a^{n+m} = a^{m+n}$
3. Докажите, что $a^m = e \iff m \vdots n$
   Из определения: Порядок элемента группы $g \in G$ — это наименьшее $n \in N$ такое, что $g^n = e \Rightarrow g^n = g^m \Rightarrow m \vdots n$.
4. Докажите, что $a^k = a^l \iff k \equiv l(mod(n))$
   $l(mod(n)) = k$, $k = l - k * n$
5. Докажите, что $ord(a^k) = \frac{n}{gcd(n,k)}$
   $gcd(n, k) = d$
   $(a^k)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e \Rightarrow ord(a^k) \leq \frac{n}{d}$
   $(a^d)^{\frac{n}{d}} = a^n = e \Rightarrow ord(a^d) \leq \frac{n}{d}$
   $0 < i < \frac{n}{d} \Rightarrow di < n$, $(a^d)^i = a^{di} \neq e \Rightarrow ord(a^d) = \frac{n}{d}$
   $ord(a^k) = ord(\langle a^k \rangle) = ord(\langle a^d \rangle) = ord(a^d) = \frac{n}{d} = \frac{n}{gcd(n,k)}$

Задание 6. Теорема Лагранжа (1 баллов)

1. Докажите, что если $g \in H$, тогда $gH = H$
   Если $x \in gH$, то для некоторого $h \in H$ имеем $x = gh$, а так как $g \in H$ и множество Н замкнуто относительно умножения группы $\mathcal{G}$, то $x \in H$. Обратно, если $x \in H$, то $x = gg^{-1}x = gh$, где $h = g^{-1}x \in H$. Поэтому $x \in gH$. Окончательно получим $H = gH$
   .

Задание 7. Изоморфизм (2 балла)

Даны 2 группы:

- $\langle \mathbb{R}, + \rangle$ - все действительные числа по сложению
- $\langle \mathbb{R}_{>0}, \cdot \rangle$ - положительные действительные числа по умножению
  Найти:
  Изоморфизм f между ними и его обратный f^{-1}
  Решение:
  $f : R \to R_{>0}$
  $f(a + b) = f(a) * f(b)$
  $f(0) = 1$
  $\Downarrow$
  $e(exp) : e^{a+b} = e^a * e^b \Rightarrow f(x) = e^x$
  Так как f - экспонента ($f(x) = e^x$), то f^{-1} - натуральный логарифм
  $(ln(x) = f^{-1}(x))$

Задание 9. Рубашка и пиджак (2 балла)

1. Докажите, что $(ab)^{-1} = b^{-1}a^{-1}$
   $(ab)(b^{-1}a^{-1}) = 1$, $(abb^{-1}) * a^{-1} = a * 1 * a^{-1} = 1 \Rightarrow 1 = 1$
2. На основании (1) найдите $(a_1 * a_2 * \dots * a_k)^{-1}$. Докажите вашу правоту, используя метод математической индукции.
   База индукции:
   $k = 2$: $(a_1 * a_2)^{-1} = a_2^{-1} * a_1^{-1}$ - доказанов в (1)
   Индкутивный переход:
   $n = k$: $(a_1 * a_2 * \dots * a_n)^{-1}$
   $(a_1 * a_2 * \dots * a_{n-1} * a_n) * (a_n^{-1} * a_{n-1}^{-1} * \dots * a_2^{-1} * a_1^{-1}) = 1$, так как
   $(a_1 * a_2 * \dots * a_{n-1} * a_n * a_n^{-1}) * a_{n-1}^{-1} * \dots * a_2^{-1} * a_1^{-1} =$
   $(a_1 * a_2 * \dots * a_{n-1} * a_{n-1}^{-1}) * a_{n-2}^{-1} * \dots * a_2^{-1} * a_1^{-1} = 1$

Задание 10. Генератор подгруппы (5 балла)

```
import math

def isPrime(a):
    _a=a
    for i in range(2,int(a**0.5)+1):
        if a%i==0:
            print("Число должно быть простым")
            _a = getnum()
            break
    return _a

def getnum():
    a = isPrime(int(input(f"Простое число: ")))
    return a

def sansara(p,n):
    while len(p) < n:
        a = getnum()
        if (a not in p):
            p.append(a)
        else:
            print("Число должно быть уникальным")
            sansara(p,n)
    return p

def main():
    q = isPrime(int(input("Введите q: ")))
    p = []
    n = int(input("Количество простых уникальных чисел: "))
    p = sansara(p, n)
```

```python
    if q!=2*math.prod(p)+1:
        exit("q не совпадает с введенными p")

    z=[i for i in range(2,q)]
    for i in range(len(p)):
        for j in range(len(z)):
            if pow(z[j],p[i],q)==1:
                print(f"При ord(a{i+1})=p{i+1}, a = {z[j]}, p{i+1}={p[i]}")
                break

if __name__ == "__main__":
    main()
```

```
input:
  q = 211
  n = 3
  p1 = 3
  p2 = 5
  p3 = 7
output:
  При ord(a1)=p1, a = 14, p1=3
  При ord(a2)=p2, a = 55, p2=5
  При ord(a3)=p3, a = 58, p3=7
```