Домашняя работа 3. Громов А.А.

Задание 1. Квадратичные вычеты по модулю p (3 балла)

Пусть p - это нечетное простое целое число. Докажите следующие теоремы:

1. В группе $\mathbb{Z}_{\mathbb{p}}^{*}$ существует ровно $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов:
   $|Qp| = \overline{|Qp|} = \frac{p-1}{2}$
   Так как $x^2 \equiv (p-x)^2 mod(p)$. Т.е. квадратичных вычетов не более чем $\frac{p-1}{2}$. Покажем, что среди чисел $1^2, 2^2 \ldots, (\frac{p-1}{2})^2$ нет сравнимых по модулю p. Пусть $x^2 \equiv y^2 mod(p)$. Тогда $(x-y)(x+y)|p$ что невозможно, так как $x \neq y$ и $x+y<p$.

2. Каждый квадратичный вычет $a \in \mathbb{Z}_p^*$ имеет ровно 2 корня по модулю p.
   Так как $x^2 \equiv a(mod(p))$, то x может быть как положительным $+x$ так и отрицательным $-x$, т.е два квадратных корня по модулю p

Задание 2. Символ Лежандра — Якоби — Кронекера (3 балла)

1. (1 балл) Найдите символ Лежандра — Якоби — Кронекера:
   1. $(\frac{8}{13}) = (\frac{2^3}{13}) = (\frac{2}{13}) = (-1)^{\frac{p^2-1}{8}} = -1$
   2. $(\frac{9}{13}) = (\frac{3}{13})(\frac{3}{13}) = (-1)^{(\frac{13-1}{2})(\frac{3-1}{2})} = 1$
   3. $(\frac{14}{21}) = (\frac{14}{3}) \times (\frac{14}{7}) = 0$
   4. $(\frac{15}{21}) = (\frac{15}{3}) \times (\frac{15}{7}) = 0$
   5. $(\frac{100}{100}) = (\frac{100}{2})^2 \times (\frac{100}{5})^2 = 0$
   6. $(\frac{290}{431}) = (\frac{2}{431}) \times (\frac{5}{431}) \times (\frac{29}{431}) = (-1)^{(\frac{431-1}{2})(\frac{5-1}{2})} \times (-1)^{(\frac{431-1}{2})(\frac{29-1}{2})} \times (-1)^{\frac{431^2-1}{8}} = 1$
2. (2 балла) Символ Лежандра — Якоби — Кронекера $(\frac{a}{n}) = 1$ не гарантирует того что a будет квадратичным вычетом по модулю n.
   a. Для каждого элемента a in Z_n^*, где n = 5・7 = 35, найдите является ли он квадратичным вычетом или невычетом.
   $1^2 = 1mod(35)$ - вычет
   Вычеты: 0, 1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30
   Невычеты: 2, 3, 5, 6, 7, 8, 10, 12, 13, 17, 18, 19, 20, 22, 23, 24, 26, 27, 28, 31, 32, 33, 34

```
p = int(input("Введите количество числе в группе, число должно быть просты
a = []
```

```
for i in range(0, p):
    a.append((i**2)%p)
print(f"full: {a}")
print(f"Вычеты: {set(a)}")
b = [a for a in range(p)]
print(f"Невычеты: {set(b)-set(a)}")
```

b, c. Для каждого элемента a in Z_{35}^{*}, Найдите символы Лежандра $(\frac{a}{5})$ и $(\frac{a}{7})$, а также - Найдите Символ Лежандра — Якоби — Кронекера $(\frac{a}{35})$

a	$\frac{a}{5}$	$\frac{a}{7}$	$\frac{a}{35}$
1	1	1	1
2	-1	1	-1
3	-1	-1	1
4	1	1	1
5	0	-1	0
6	1	-1	-1
7	-1	0	0
8	-1	1	-1
9	1	1	1
10	0	-1	0
11	1	1	1
12	-1	-1	1
13	-1	-1	1
14	1	0	0
15	0	1	0
16	1	1	1
17	-1	-1	1
18	-1	1	-1
19	1	-1	-1
20	0	-1	0
21	1	0	0
22	-1	1	-1
23	-1	1	-1

a	$\frac{a}{5}$	$\frac{a}{7}$	$\frac{a}{35}$
24	1	-1	-1
25	0	1	0
26	1	-1	-1
27	-1	-1	1
28	-1	0	0
29	1	1	1
30	0	1	0
31	1	-1	-1
32	-1	1	-1
33	-1	-1	1
34	1	-1	-1
35	0	0	0

d. Найдите элементы которые не являются квадратичными вычетами, но имеют символ Лежандра — Якоби — Кронекера равный 1.
Символы: 3, 12, 13, 17, 27, 33

Задание 3. Криптосистема Гольдвассер — Микали (4 балла)

output:

```
['0', '1', '0', '1', '0', '1', '0', '0']
['0', '1', '1', '1', '0', '1', '0', '1']
['0', '1', '1', '1', '0', '0', '1', '0']
['0', '1', '1', '0', '1', '0', '0', '1']
['0', '1', '1', '0', '1', '1', '1', '0']
['0', '1', '1', '0', '0', '1', '1', '1']
['T', 'u', 'r', 'i', 'n', 'g']
```

Код:

```
c = [218, 34, 194, 164, 220, 50, 237, 77,
    68, 151, 135, 21, 101, 167, 196, 98,
    196, 219, 89, 241, 16, 134, 240, 43,
    36, 193, 37, 17, 184, 61, 81, 41,
    81, 148, 18, 172, 193, 37, 203, 233,
    244, 145, 18, 1, 121, 46, 18, 193]
p = 13
```

```
q = 19
g = [i for i in range(p)]
v = [i**2%p for i in g]
nev = set(g)-set(v)
res = []
bit = []
j = 1
for i in c:
    if i%p in v:
        bit.append('0')
    else:
        bit.append('1')
    if j%8 == 0:
        print(bit)
        res.append(chr(int(''.join(bit), 2)))
        bit = []
    j+=1

print(res)
```

Задание 4. Тесты простоты: Ферма и Соловея-Штрассена (6 баллов)

Тест простотыт Ферма

```
from random import *

n = int(input("введите число: "))
k = int(input("Количество тестов: "))
isPrime = True
if n % 2 == 0:
    print("Составное")
    exit(0)
for i in range(k):
    a = randint(1, n-1)
    if (a**(n-1))%n != 1:
        isPrime = False

if isPrime:
    print("Простое")
else:
    print("Составное")
```

1. 2455921
   output:

```
введите число: 2455921
Количество тестов: 10
Составное
```

Остальные задания слишком долго считать на python(на скрине прошло больше 60 минут, а так и не посчиталось):

Тест Соловея-Штрассена

```
from random import *
import math

def jacobi(a, n):
    a = a % n
    res = 1
```

```
    while (a != 0):
        while (a % 2 == 0):
            a = a // 2
            tarr = [3, 5]
            if ((n % 8) in tarr):
                res *= -1
        a, n = n, a
        if (a % 4 == n % 4 == 3):
            res *= -1
        a = a % n
    if (n == 1):
        return res
    return 0

n = int(input("введите число: "))
k = int(input("Количество тестов: "))
isPrime = True
if n == 2:
    print("Прсотое")
    exit(0)

if n % 2 == 0:
    print("Составное")
    exit(0)

for i in range(k):
    a = randint(1, n-1)
    if math.gcd(a,n) > 1:
        isPrime = False
        break
    s = pow(a,(n-1)//2, n)
    j = jacobi(a,n)
    m = (n+j)%n
    if s != m:
        isPrime = False
        break

if isPrime:
    print("Простое")
else:
    print("Составное")
```

1. 2455921
   output:

```
введите число: 2455921
Количество тестов: 10
Составное
```

2. 134899510405807901072383429627628720821425287778688627092802 7
   output:

```
введите число: 134899510405807901072383429627628720821425287778688627092802
Количество тестов: 100
Простое
```

3. 3220808895729190650533318829462672153492607799896814316239090605 4
   269771332195153578543417
   output:

```
введите число: 322080889572919065053331882946267215349260779989681431623909
Количество тестов: 100
Составное
```

4. 1873521835488216910116034832063351754450588181648586633193917382049
   683634480683605082812594241877158908865359535527849183634834114 92
   06598146682089072399770417002736809905920110596285867969468281189 2
   53753266702516831877840048790039143707155242781379638905777628244 5
   773043473465166488167430004446908766934755 49
   output:

```
введите число: 187352183548821691011603483206335175445058818164858663319391
Количество тестов: 100
Составное
```

5. 411482053694408436626203894097575331763736396159120829209725307798
   091953819317408863704725757666061847735945600515243416861922837875
   630632076871634802128134649341322136729331485528591019303696377030
   3210522096348335431652569264398955304660387881195949480680964846 0
   55881685507395352086629186591845883418798567 7

```
введите число: 411482053694408436626203894097575331763736396159120829209727
Количество тестов: 100
Составное
```

Задание 5. Операции над полиномами (4 балла, $\frac{1}{2}$ за каждое)

1. Сложение. Для полиномов
   $f(x) = x^{10} + x^9 + x^5 + x^3 + 1$
   $g(x) = x^8 + x^4 + x^3 + x + 1$
   Найти $f(x) + g(x)$.
   $f(x) + g(x) = x^{10} + x^9 + x^8 + x^5 + x^4 + x$

2. Вычитание. Для полиномов
   $f(x) = x^{10} + x^9 + x^5 + x^3 + 1$
   $g(x) = x^8 + x^4 + x^3 + x + 1$
   Найти $f(x) - g(x)$.
   $f(x) - g(x) = x^{10} + x^9 + x^8 + x^5 + x^4 + x$

3. Умножение. Для полиномов
   $f(x) = x^{10} + x^9 + x^5 + x^3 + 1$
   $g(x) = x^8 + x^4 + x^3 + x + 1$
   Найти $f(x)g(x)$.
   $f(x)g(x) = (x^{10} + x^9 + x^5 + x^3 + 1)(x^8 + x^4 + x^3 + x + 1) =$
   $x^{18} + x^{14} + x^{13} + x^{11} + x^{10} + x^{17} + x^{13} + x^{12} + x^{10} + x^9 +$
   $x^{13} + x^9 + x^8 + x^6 + x^5 + x^{11} + x^7 + x^6 + x^4 + x^3 + x^8 + x^4 + x^3 + x + 1 =$
   $x^{18} + x^{17} + x^{14} + x^{13} + x^{12} + x^5 + x + 1$

4. Деление с остатком. Для полиномов
   $f(x) = x^{10} + x^9 + x^5 + x^3 + 1$
   $g(x) = x^8 + x^4 + x^3 + x + 1$
   Найти частное $q(x)$ и остаток $r(x)$ для $f(x)/g(x)$.

$x^{10} + x^9 + x^5 + x^3 + 1$	$x^8 + x^4 + x^3 + x + 1$
$x^{10} + x^6 + x^5 + x^3 + x^2$	$\overline{x^2 + x}$ - $g(x)$
$\overline{x^9 + x^6 + x^2 + 1}$	
$x^9 + x^5 + x^4 + x^2 + x$	
$\overline{x^6 + x^5 + x^4 + x + 1}$ - $r(x)$	

5. Факторизация. Разложите на множители: $f(x) = x^3 + 1$
   $f(x) = x^3 + 1 = (x + 1)(x^2 + x + 1)$

6. Умножение по модулю полинома.Для полиномов
   $f(x) = x^2 + x + 1$
   $g(x) = x^3 + 1$
   $h(x) = x^4 + x + 1$

Найти $f(x)g(x)mod(h(x))$.

$f(x) \cdot g(x) = (x^2 + x + 1)(x^3 + 1) = x^5 + x^2 + x^4 + x + x^3 + 1$

$x^5 + x^2 + x^4 + x + x^3 + 1$	$x^4 + x + 1$
$x^5 + x^2 + x$	$\overline{x + 1}$
$\overline{x^4 + x^3 + 1}$	
$x^4 + x + 1$	
$\overline{x^3 + x}$ - $f(x)g(x)mod(h(x))$	

7. GCD. Для полиномов
   $f(x) = x^5 + x^4 + 1$
   $g(x) = x^5 + x^2 + x + 1$
   Найти $gcd(f(x), g(x))$ (используя алгоритм Евклида для полиномов).

$x^5 + x^4 + 1$	$x^5 + x^2 + x + 1$
$x^5 + x^2 + x + 1$	$\overline{1}$
$\overline{x^4 + x^2 + x}$	

$x^5 + x^2 + x + 1$	$x^4 + x^2 + x$
$x^5 + x^3 + x^2$	$\overline{x}$
$\overline{x^3 + x + 1}$ - $gcd(f(x), g(x))$	

Задание 7. Построение $GF(p^m)$ (3 балла)

Найдите все элементы поля Галуа $GF(2^4)$ с примитивным полиномом $p(x) = x^4 + x^3 + 1$.

$\text{Элемент}^{\text{Степень}}$	1	ε	ε^2	ε^3	полином
ε^0	1	0	0	0	1
ε^1	0	1	0	0	x
ε^2	1	1	0	0	$x + 1$
ε^3	0	0	1	0	x^2
ε^4	1	0	1	0	$x^2 + 1$
ε^5	0	1	1	0	$x^2 + x$
ε^6	1	1	1	0	$x^2 + x + 1$
ε^7	0	0	0	1	x^3

$Элемент^{Степень}$	1	ε	ε^2	ε^3	**полином**
ε^8	1	0	0	1	x^3+1
ε^9	0	1	0	1	x^3+x
ε^{10}	1	1	0	1	x^3+x+1
ε^{11}	0	0	1	1	x^3+x^2
ε^{12}	1	0	1	1	x^3+x^2+1
ε^{13}	0	1	1	1	x^3+x^2+x
ε^{14}	1	1	1	1	x^3+x^2+x+1
ε^{15}	1	0	0	0	1