Фундаментальная и компьютерная алгебра

Вопросы к экзамену

1. Определение поля и примеры полей.
2. Характеристика поля. Теорема о том, что характеристика простое число.
3. Алгебраическое расширение. Теорема о структуре простого алгебраического расширения, как фактор кольца.
4. Простое поле. Простое поле нулевой характеристики.(Поле рациональных чисел).
5. Простое поле Галуа. Теорема о существовании.(Кольцо вычетов).
6. Теорема о существовании поля $GF(p^n)$.
7. Структура подполей поля Галуа.
8. Теорема описания неприводимых многочленов над полем Галуа.
9. Теорема о существовании примитивного элемента в полях Галуа.
10. Алгоритм нахождения примитивного элемента.
11. Решение уравнений в конечных полях. Логарифм Якоби. Пример.
12. Функция Эйлера. Группа обратимых элементов кольца вычетов $\mathbb{Z}_n$.
13. Алгебраические расширения полей любой характеристики. Алгебраические числа.
14. Норма и след элементов поля Галуа.
15. Примитивные элементы колец вычетов порядка p^n и $2p^n$. Идея доказательства и примеры.
16. Линейные регистры сдвига с обратной связью.
17. Длина периода. Матричная запись.
18. Решение линейного уравнения в кольце вычетов.
19. Решение системы линейных уравнений по разным модулям.
20. Алгоритм шифрования RSA. Пример вычислений.
21. Алгоритм шифрования AES. нахождение обратных элементов в поле $GF(2^8)$. Преобразование, нелинейная замена.
22. Алгоритм AES - замена столбцов.

3. Структура простого алгебраического расширения

Пусть P - поле, α - алгебраический элемент. По определению алгебраического элемента,
$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_n$
корнем которого он является.
Так как такой многочлен не единственный, а нам нужна определенность. Разложим $f(x)$ на неприводимые множители, тогда α - будет корнем одного из них. На самом деле, единственный будет такой многочлен и его

называют минимальным. Пусть напротив таких многочленов 2: $g_1(x)g_2(x)$ т.к они неприводимы, найдем $(g_1, g_2) = 1$. По следствию из алгоритма Евклида $\exists h_1, h_2$ так что $h_1g_1 + h_2g_2 = 1$
$h_1(\alpha)g_1(\alpha) + h_2(\alpha)g_2(\alpha) = 1 \Rightarrow 0 + 0 = 1$ (противоречие)
Минимальное поле, которое содержит α и называется $P(\alpha)$ простым алгебраическим расширением.
Как устроено это поле $P(\alpha)$?
1. Абстрактное строение:
Рассмотрим идеал, порождаемый многочленом $f(x)$, то есть
$I = ug(f(x)) = e(x)|e(x) = f(x)h(x), h(x) \in P[x]$
Рассмотрим фактор кольцо $P[x]/ug(x)$ (из теоремы о построении поля разложения) многочлен $f(x)$ имеет хотя бы один корень и пусть это будет α
2. Символьное описание простого расширения:
$p(\alpha) = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}|b_j \in P$ - это поле является векторным пространством размерности n над полем P. Базис $(1, \alpha, ..., \alpha^{n-1}), f(\alpha) = 0$
$\alpha^n = -a_{n-1}\alpha^{n-1} - ... - a_n$ - это соотношение задает умножение в поле.

Теорема
Простое алгебраическое расширение $P(\alpha)$ изоморфно
$P[x]/ug(f(x))P(\alpha) = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}|b_j \in P$

Обобщение
$\alpha_1, \alpha_2, ..., \alpha_k$
$P(\alpha_1, \alpha_2, ..., \alpha_k)$
$(P(\alpha_1))(\alpha_2))(\alpha_3)$ - алгебраическое расширение $P(\alpha_1, \alpha_2, ..., \alpha_k)$ строится индуктивно.
Если поле непроизвольное, а поле рациональных чисел, то алгебраические расширения называются алгебраическими числами.
Вся теория полей родилась из алгебраических чисел.

5. Структура полей Галуа

Определение
Поле Галуа - это любое конечное поле.

Так как конечное поле имеет ненулевую характеристику, то у поля Галуа характеристика P - простое число.

Теорема
$\mathbb{Z}_p = 0, 1, ..., p - 1 = GF(p)$ - единственное простое поле, то есть не содержит подполей.

Доказательство

Так как любое подполе содержит единицу по умножению.
$\{1, 1+1, 1+1+1...\} = \mathbb{Z}_p$

6. Теорема о существовании простого поля Галуа

Теорема

Для любого простого числа p и натурального числа n существует поле, содержащее p^n элементов.

$x^{p^n} - x$ - по теореме о поле разложения, разлагается на множители.

Доказательство

Пусть $\alpha, \beta \in F$ - корни этого многочлена, то есть
$\alpha^{p^n} - \alpha = 0$
$\beta^{p^n} - \beta = 0$
1. Проверим, что $\alpha + \beta$ - корень
$(\alpha + \beta)^{p^n} - (\alpha + \beta)$ так как характеристика поля = p, $p\alpha = 0$
То по Биному Ньютона:
$\alpha^{p^n} + \beta^{p^n} - (\alpha + \beta)$ - действительно корень.
$\alpha\beta$ - тоже корень.
$(\alpha\beta)^{p^n} - \alpha\beta$ 2. $\alpha^{p^n}\beta^{p^n} - \alpha\beta$ - корень.
3. $-\alpha$
4.$-\alpha^{-1}$

Таким образом поле $GF(p^n)$ $\exists n$ состоящий из корней многочлена $x^p - x$.

7. Структура подполей поля Галуа

Теорема о структуре подполей

$GF(p^n)GF(p^m)$ - поля Галуа.
Тогда, $GF(p^n) \geq GF(p^m) \Rightarrow m|n$(делит)

То есть структура подполей определяется структурой делителей числа n.

Доказательство

Пусть $GF(p^n) \leq GF(p^m)$, где $GF(p^n) = PGF(p^m) = F$
Так как P подполе F, то - векторное пространство над полем P. Пусть размерность этого пространства K.
$| F | = | P |^k$

$p^n = (p^m)^k$
$n = mk$
Пусть $m \mid n$, тогда $\frac{x^{p^n}-x}{x^{p^m}-x}$, по формуле геометрической прогрессии. Значит поле разложение нижнего многочлена содержится в поле разложения верхнего многочлена. Является подполем, а поле разложением $GF(p^n)$ по 2 - ой теореме.

8. Неприводимые многочлены в полях Галуа

Теорема

Пусть $f(x)$ неприводимый многочлен над полем $GF(p)$.
α - корень $GF(p^n)$(n - степень). Тогда $\alpha, \alpha^p, ..., \alpha^{p^{n-1}}$ - различные корни многочлена $f(x)$. Если в поле Галуа добавить один корень, то многочлен разлагается на простые множители.

Доказательство

$0 = f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0, a \in GF(p)$
По условию дано, что $0 = f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0$. Чтобы доказать теорему, нужно проверить, что возведение в степень p ост-ет корень корнем.
Заметим, что $a_i \in GF(p)\ \forall\ i\ {a_i}^p = a_i(*)$.
Заметим в многочлене α на α^p, получим
$(\alpha^p)^n + a_{n-1}(\alpha^p)^{n-1} + ... + a_0 \neq$ исп-ся рав(*) и
$(\alpha^p)^n + a_{n-1}(\alpha^p)^{n-1} + ... + a_0 = (\alpha^n)^p + {a_{n-1}}^p(\alpha^{n-1})^p + ... + {a_0}^p$,
так как характеристика = p, то есть $p\alpha = 0$, то по фомруле Бинома запишем так.
$(\alpha^n)^p + {a_{n-1}}^p(\alpha^{n-1})^p + ... + {a_0}^p = (\alpha^n + a_{n-1}\alpha^{n-1} + a_0)^p = f(\alpha)^p = 0^p = 0.$

Задание №1.1

Это работа с примитивным элементом в поле.
Нахождение примитивного элемента p(простое число) в поле $GF(p)$.
Так как p = 467, то в поле $GF(467)$ и количество примитивных элементов равно 232(по функции Эйлера).

```
gap> p := Random(Primes);
467
gap> l := Factors(p - 1);
[ 2, 233 ]
gap> list := [];
[  ]
gap> for i in [1 .. p-1] do
> g := 1^i mod p;
> Add(list, g);
> od;
gap> list;
[ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 ]
```

Рис. 1: Непримитивный элемент

```
gap> list := [];
[  ]
gap> for i in [1 .. p-1] do
> g := 2^i mod p;
> Add(list, g);
> od;
gap> list;
[ 2, 4, 8, 16, 32, 64, 128, 256, 45, 90, 180, 360, 253, 39, 78, 156, 312, 157, 314, 161, 322, 177, 354, 241, 15, 30,
  60, 120, 240, 13, 26, 52, 104, 208, 416, 365, 263, 59, 118, 236, 5, 10, 20, 40, 80, 160, 320, 173, 346, 225, 450,
  433, 399, 331, 195, 390, 313, 159, 318, 169, 338, 209, 418, 369, 271, 75, 150, 300, 133, 266, 65, 130, 260, 53,
  106, 212, 424, 381, 295, 123, 246, 25, 50, 100, 200, 400, 333, 199, 398, 329, 191, 382, 297, 127, 254, 41, 82, 164,
  328, 189, 378, 289, 111, 222, 444, 421, 375, 283, 99, 198, 396, 325, 183, 366, 265, 63, 126, 252, 37, 74, 148, 296,
  125, 250, 33, 66, 132, 264, 61, 122, 244, 21, 42, 84, 168, 336, 205, 410, 353, 239, 11, 22, 44, 88, 176, 352, 237,
  7, 14, 28, 56, 112, 224, 448, 429, 391, 315, 163, 326, 185, 370, 273, 79, 158, 316, 165, 330, 193, 386, 305, 143,
  286, 105, 210, 420, 373, 279, 91, 182, 364, 261, 55, 110, 220, 440, 413, 359, 251, 35, 70, 140, 280, 93, 186, 372,
  277, 87, 174, 348, 229, 458, 449, 431, 395, 323, 179, 358, 249, 31, 62, 124, 248, 29, 58, 116, 232, 464, 461, 455,
  443, 419, 371, 275, 83, 166, 332, 197, 394, 321, 175, 350, 233, 466, 465, 463, 459, 451, 435, 403, 339, 211, 422,
  377, 287, 107, 214, 428, 389, 311, 155, 310, 153, 306, 145, 290, 113, 226, 452, 437, 407, 347, 227, 454, 441, 415,
  363, 259, 51, 102, 204, 408, 349, 231, 462, 457, 447, 427, 387, 307, 147, 294, 121, 242, 17, 34, 68, 136, 272, 77,
  154, 308, 149, 298, 129, 258, 49, 98, 196, 392, 317, 167, 334, 201, 402, 337, 207, 414, 361, 255, 43, 86, 172, 344,
  221, 442, 417, 367, 267, 67, 134, 268, 69, 138, 276, 85, 170, 340, 213, 426, 385, 303, 139, 278, 89, 178, 356, 245,
  23, 46, 92, 184, 368, 269, 71, 142, 284, 101, 202, 404, 341, 215, 430, 393, 319, 171, 342, 217, 434, 401, 335, 203,
  406, 345, 223, 446, 425, 383, 299, 131, 262, 57, 114, 228, 456, 445, 423, 379, 291, 115, 230, 460, 453, 439, 411,
  355, 243, 19, 38, 76, 152, 304, 141, 282, 97, 194, 388, 309, 151, 302, 137, 274, 81, 162, 324, 181, 362, 257, 47,
  94, 188, 376, 285, 103, 206, 412, 357, 247, 27, 54, 108, 216, 432, 397, 327, 187, 374, 281, 95, 190, 380, 293, 119,
  238, 9, 18, 36, 72, 144, 288, 109, 218, 436, 405, 343, 219, 438, 409, 351, 235, 3, 6, 12, 24, 48, 96, 192, 384,
  301, 135, 270, 73, 146, 292, 117, 234, 1 ]
```

Рис. 2: Примитивный элемент

```
gap> list := [];
[  ]
gap> for i in [1 .. p-1] do
> g := 3^i mod p;
> Add(list, g);
> od;
gap> list;
[ 3, 9, 27, 81, 243, 262, 319, 23, 69, 207, 154, 462, 452, 422, 332, 62, 186, 91, 273, 352, 122, 366, 164, 25, 75,
  225, 208, 157, 4, 12, 36, 108, 324, 38, 114, 342, 92, 276, 361, 149, 447, 407, 287, 394, 248, 277, 364, 158, 7, 21,
  63, 189, 100, 300, 433, 365, 161, 16, 48, 144, 432, 362, 152, 456, 434, 368, 170, 43, 129, 387, 227, 214, 175, 58,
  174, 55, 165, 28, 84, 252, 289, 400, 266, 331, 59, 177, 64, 192, 109, 327, 47, 141, 423, 335, 71, 213, 172, 49,
  147, 441, 389, 233, 232, 229, 220, 193, 112, 336, 74, 222, 199, 130, 390, 236, 241, 256, 301, 436, 374, 188, 97,
  291, 406, 284, 385, 221, 196, 121, 363, 155, 465, 461, 449, 413, 305, 448, 410, 296, 421, 329, 53, 159, 10, 30, 90,
  270, 343, 95, 285, 388, 230, 223, 202, 139, 417, 317, 17, 51, 153, 459, 443, 395, 251, 286, 391, 239, 250, 283,
  382, 212, 169, 40, 120, 360, 146, 438, 380, 206, 151, 453, 425, 341, 89, 267, 334, 68, 204, 145, 435, 371, 179, 70,
  210, 163, 22, 66, 198, 127, 381, 209, 160, 13, 39, 117, 351, 119, 357, 137, 411, 299, 430, 356, 134, 402, 272, 349,
  113, 339, 83, 249, 280, 373, 185, 88, 264, 325, 41, 123, 369, 173, 52, 156, 1, 3, 9, 27, 81, 243, 262, 319, 23, 69,
  207, 154, 462, 452, 422, 332, 62, 186, 91, 273, 352, 122, 366, 164, 25, 75, 225, 208, 157, 4, 12, 36, 108, 324, 38,
  114, 342, 92, 276, 361, 149, 447, 407, 287, 394, 248, 277, 364, 158, 7, 21, 63, 189, 100, 300, 433, 365, 161, 16,
  48, 144, 432, 362, 152, 456, 434, 368, 170, 43, 129, 387, 227, 214, 175, 58, 174, 55, 165, 28, 84, 252, 289, 400,
  266, 331, 59, 177, 64, 192, 109, 327, 47, 141, 423, 335, 71, 213, 172, 49, 147, 441, 389, 233, 232, 229, 220, 193,
  112, 336, 74, 222, 199, 130, 390, 236, 241, 256, 301, 436, 374, 188, 97, 291, 406, 284, 385, 221, 196, 121, 363,
  155, 465, 461, 449, 413, 305, 448, 410, 296, 421, 329, 53, 159, 10, 30, 90, 270, 343, 95, 285, 388, 230, 223, 202,
  139, 417, 317, 17, 51, 153, 459, 443, 395, 251, 286, 391, 239, 250, 283, 382, 212, 169, 40, 120, 360, 146, 438,
  380, 206, 151, 453, 425, 341, 89, 267, 334, 68, 204, 145, 435, 371, 179, 70, 210, 163, 22, 66, 198, 127, 381, 209,
  160, 13, 39, 117, 351, 119, 357, 137, 411, 299, 430, 356, 134, 402, 272, 349, 113, 339, 83, 249, 280, 373, 185, 88,
  264, 325, 41, 123, 369, 173, 52, 156, 1 ]
```

Рис. 3: Непримитивный элемент

```
gap> list:= [];
[  ]
gap> for i in [1 .. p-1] do
> g := 4^i mod p;
> Add(list, g);
> od;
gap> list;
[ 4, 16, 64, 256, 90, 360, 39, 156, 157, 161, 177, 241, 30, 120, 13, 52, 208, 365, 59, 236, 10, 40, 160, 173, 225,
  433, 331, 390, 159, 169, 209, 369, 75, 300, 266, 130, 53, 212, 381, 123, 25, 100, 400, 199, 329, 382, 127, 41, 164,
  189, 289, 222, 421, 283, 198, 325, 366, 63, 252, 74, 296, 250, 66, 264, 122, 21, 84, 336, 410, 239, 22, 88, 352, 7,
  28, 112, 448, 391, 163, 185, 273, 158, 165, 193, 305, 286, 210, 373, 91, 364, 55, 220, 413, 251, 70, 280, 186, 277,
  174, 229, 449, 395, 179, 249, 62, 248, 58, 232, 461, 443, 371, 83, 332, 394, 175, 233, 465, 459, 435, 339, 422,
  287, 214, 389, 155, 153, 145, 113, 452, 407, 227, 441, 363, 51, 204, 349, 462, 447, 387, 147, 121, 17, 68, 272,
  154, 149, 129, 49, 196, 317, 334, 402, 207, 361, 43, 172, 221, 417, 267, 134, 69, 276, 170, 213, 385, 139, 89, 356,
  23, 92, 368, 71, 284, 202, 341, 430, 319, 342, 434, 335, 406, 223, 425, 299, 262, 114, 456, 423, 291, 230, 453,
  411, 243, 38, 152, 141, 97, 388, 151, 137, 81, 324, 362, 47, 188, 285, 206, 357, 27, 108, 432, 327, 374, 95, 380,
  119, 9, 36, 144, 109, 436, 343, 438, 351, 3, 12, 48, 192, 301, 270, 146, 117, 1, 4, 16, 64, 256, 90, 360, 39, 156,
  157, 161, 177, 241, 30, 120, 13, 52, 208, 365, 59, 236, 10, 40, 160, 173, 225, 433, 331, 390, 159, 169, 209, 369,
  75, 300, 266, 130, 53, 212, 381, 123, 25, 100, 400, 199, 329, 382, 127, 41, 164, 189, 289, 222, 421, 283, 198, 325,
  366, 63, 252, 74, 296, 250, 66, 264, 122, 21, 84, 336, 410, 239, 22, 88, 352, 7, 28, 112, 448, 391, 163, 185, 273,
  158, 165, 193, 305, 286, 210, 373, 91, 364, 55, 220, 413, 251, 70, 280, 186, 277, 174, 229, 449, 395, 179, 249, 62,
  248, 58, 232, 461, 443, 371, 83, 332, 394, 175, 233, 465, 459, 435, 339, 422, 287, 214, 389, 155, 153, 145, 113,
  452, 407, 227, 441, 363, 51, 204, 349, 462, 447, 387, 147, 121, 17, 68, 272, 154, 149, 129, 49, 196, 317, 334, 402,
  207, 361, 43, 172, 221, 417, 267, 134, 69, 276, 170, 213, 385, 139, 89, 356, 23, 92, 368, 71, 284, 202, 341, 430,
  319, 342, 434, 335, 406, 223, 425, 299, 262, 114, 456, 423, 291, 230, 453, 411, 243, 38, 152, 141, 97, 388, 151,
  137, 81, 324, 362, 47, 188, 285, 206, 357, 27, 108, 432, 327, 374, 95, 380, 119, 9, 36, 144, 109, 436, 343, 438,
  351, 3, 12, 48, 192, 301, 270, 146, 117, 1 ]
```

Рис. 4: Непримитивный элемент

```
gap> list := [];
[  ]
gap> for i in [1 .. p-1] do
> g := 5^i mod p;
> Add(list, g);
> od;
gap> list;
[ 5, 25, 125, 158, 323, 214, 136, 213, 131, 188, 6, 30, 150, 283, 14, 70, 350, 349, 344, 319, 194, 36, 180, 433, 297,
  84, 420, 232, 226, 196, 46, 230, 216, 146, 263, 381, 37, 185, 458, 422, 242, 276, 446, 362, 409, 177, 418, 222,
  176, 413, 197, 51, 255, 341, 304, 119, 128, 173, 398, 122, 143, 248, 306, 129, 178, 423, 247, 301, 104, 53, 265,
  391, 87, 435, 307, 134, 203, 81, 405, 157, 318, 189, 11, 55, 275, 441, 337, 284, 19, 95, 8, 40, 200, 66, 330, 249,
  311, 154, 303, 114, 103, 48, 240, 266, 396, 112, 93, 465, 457, 417, 217, 151, 288, 39, 195, 41, 205, 91, 455, 407,
  167, 368, 439, 327, 234, 236, 246, 296, 79, 395, 107, 68, 340, 299, 94, 3, 15, 75, 375, 7, 35, 175, 408, 172, 393,
  97, 18, 90, 450, 382, 42, 210, 116, 113, 98, 23, 115, 108, 73, 365, 424, 252, 326, 229, 211, 121, 138, 223, 181,
  438, 322, 209, 111, 88, 440, 332, 259, 361, 404, 152, 293, 64, 320, 199, 61, 305, 124, 153, 298, 89, 445, 357, 384,
  52, 260, 366, 429, 277, 451, 387, 67, 335, 274, 436, 312, 159, 328, 239, 261, 371, 454, 402, 142, 243, 281, 4, 20,
  100, 33, 165, 358, 389, 77, 385, 57, 285, 24, 120, 133, 198, 56, 280, 466, 462, 442, 342, 309, 144, 253, 331, 254,
  336, 279, 461, 437, 317, 184, 453, 397, 117, 118, 123, 148, 273, 431, 287, 34, 170, 383, 47, 235, 241, 271, 421,
  237, 251, 321, 204, 86, 430, 282, 9, 45, 225, 191, 21, 105, 58, 290, 49, 245, 291, 54, 270, 416, 212, 126, 163,
  348, 339, 294, 69, 345, 324, 219, 161, 338, 289, 44, 220, 166, 363, 414, 202, 76, 380, 32, 160, 333, 264, 386, 62,
  310, 149, 278, 456, 412, 192, 26, 130, 183, 448, 372, 459, 427, 267, 401, 137, 218, 156, 313, 164, 353, 364, 419,
  227, 201, 71, 355, 374, 2, 10, 50, 250, 316, 179, 428, 272, 426, 262, 376, 12, 60, 300, 99, 28, 140, 233, 231, 221,
  171, 388, 72, 360, 399, 127, 168, 373, 464, 452, 392, 92, 460, 432, 292, 59, 295, 74, 370, 449, 377, 17, 85, 425,
  257, 351, 354, 369, 444, 352, 359, 394, 102, 43, 215, 141, 238, 256, 346, 329, 244, 286, 29, 145, 258, 356, 379,
  27, 135, 208, 106, 63, 315, 174, 403, 147, 268, 406, 162, 343, 314, 169, 378, 22, 110, 83, 415, 207, 101, 38, 190,
  16, 80, 400, 132, 193, 31, 155, 308, 139, 228, 206, 96, 13, 65, 325, 224, 186, 463, 447, 367, 434, 302, 109, 78,
  390, 82, 410, 182, 443, 347, 334, 269, 411, 187, 1 ]
```

Рис. 5: Примитивный элемент

```
gap> list := [];
[  ]
gap> for i in [1 .. p-1] do
> g := 6^i mod p;
> Add(list, g);
> od;
gap> list;
[ 6, 36, 216, 362, 304, 423, 203, 284, 303, 417, 167, 68, 408, 113, 211, 332, 124, 277, 261, 165, 56, 336, 148, 421,
  191, 212, 338, 160, 26, 156, 2, 12, 72, 432, 257, 141, 379, 406, 101, 139, 367, 334, 136, 349, 226, 422, 197, 248,
  87, 55, 330, 112, 205, 296, 375, 382, 424, 209, 320, 52, 312, 4, 24, 144, 397, 47, 282, 291, 345, 202, 278, 267,
  201, 272, 231, 452, 377, 394, 29, 174, 110, 193, 224, 410, 125, 283, 297, 381, 418, 173, 104, 157, 8, 48, 288, 327,
  94, 97, 115, 223, 404, 89, 67, 402, 77, 462, 437, 287, 321, 58, 348, 220, 386, 448, 353, 250, 99, 127, 295, 369,
  346, 208, 314, 16, 96, 109, 187, 188, 194, 230, 446, 341, 178, 134, 337, 154, 457, 407, 107, 175, 116, 229, 440,
  305, 429, 239, 33, 198, 254, 123, 271, 225, 416, 161, 32, 192, 218, 374, 376, 388, 460, 425, 215, 356, 268, 207,
  308, 447, 347, 214, 350, 232, 458, 413, 143, 391, 11, 66, 396, 41, 246, 75, 450, 365, 322, 64, 384, 436, 281, 285,
  309, 453, 383, 430, 245, 69, 414, 149, 427, 227, 428, 233, 464, 449, 359, 286, 315, 22, 132, 325, 82, 25, 150, 433,
  263, 177, 128, 301, 405, 95, 103, 151, 439, 299, 393, 23, 138, 361, 298, 387, 454, 389, 466, 461, 431, 251, 105,
  163, 44, 264, 183, 164, 50, 300, 399, 59, 354, 256, 135, 343, 190, 206, 302, 411, 131, 319, 46, 276, 255, 129, 307,
  441, 311, 465, 455, 395, 35, 210, 326, 88, 61, 366, 328, 100, 133, 331, 118, 241, 45, 270, 219, 380, 412, 137, 355,
  262, 171, 92, 85, 43, 258, 147, 415, 155, 463, 443, 323, 70, 420, 185, 176, 122, 265, 189, 200, 266, 195, 236, 15,
  90, 73, 438, 293, 357, 274, 243, 57, 342, 184, 170, 86, 49, 294, 363, 310, 459, 419, 179, 140, 373, 370, 352, 244,
  63, 378, 400, 65, 390, 5, 30, 180, 146, 409, 119, 247, 81, 19, 114, 217, 368, 340, 172, 98, 121, 259, 153, 451,
  371, 358, 280, 279, 273, 237, 21, 126, 289, 333, 130, 313, 10, 60, 360, 292, 351, 238, 27, 162, 38, 228, 434, 269,
  213, 344, 196, 242, 51, 306, 435, 275, 249, 93, 91, 79, 7, 42, 252, 111, 199, 260, 159, 20, 120, 253, 117, 235, 9,
  54, 324, 76, 456, 401, 71, 426, 221, 392, 17, 102, 145, 403, 83, 31, 186, 182, 158, 14, 84, 37, 222, 398, 53, 318,
  40, 240, 39, 234, 3, 18, 108, 181, 152, 445, 335, 142, 385, 442, 317, 34, 204, 290, 339, 166, 62, 372, 364, 316,
  28, 168, 74, 444, 329, 106, 169, 80, 13, 78, 1 ]
```

Рис. 6: Примитивный элемент

```
gap> list := [];
[ ]
gap> for i in [1 .. p-1] do
> g := 7^i mod p;
> Add(list, g);
> od;
gap> list;
[ 7, 49, 343, 66, 462, 432, 222, 153, 137, 25, 175, 291, 169, 249, 342, 59, 413, 89, 156, 158, 172, 270, 22, 154,
  144, 74, 51, 357, 164, 214, 97, 212, 83, 114, 331, 449, 341, 52, 364, 213, 90, 163, 207, 48, 336, 17, 119, 366,
  227, 188, 382, 339, 38, 266, 461, 425, 173, 277, 71, 30, 210, 69, 16, 112, 317, 351, 122, 387, 374, 283, 113, 324,
  400, 465, 453, 369, 248, 335, 10, 70, 23, 161, 193, 417, 117, 352, 129, 436, 250, 349, 108, 289, 155, 151, 123,
  394, 423, 159, 179, 319, 365, 220, 139, 39, 273, 43, 301, 239, 272, 36, 252, 363, 206, 41, 287, 141, 53, 371, 262,
  433, 229, 202, 13, 91, 170, 256, 391, 402, 12, 84, 121, 380, 325, 407, 47, 329, 435, 243, 300, 232, 223, 160, 186,
  368, 241, 286, 134, 4, 28, 196, 438, 264, 447, 327, 421, 145, 81, 100, 233, 230, 209, 62, 434, 236, 251, 356, 157,
  165, 221, 146, 88, 149, 109, 296, 204, 27, 189, 389, 388, 381, 332, 456, 390, 395, 430, 208, 55, 385, 360, 185,
  361, 192, 410, 68, 9, 63, 441, 285, 127, 422, 152, 130, 443, 299, 225, 174, 284, 120, 373, 276, 64, 448, 334, 3,
  21, 147, 95, 198, 452, 362, 199, 459, 411, 75, 58, 406, 40, 280, 92, 177, 305, 267, 1, 7, 49, 343, 66, 462, 432,
  222, 153, 137, 25, 175, 291, 169, 249, 342, 59, 413, 89, 156, 158, 172, 270, 22, 154, 144, 74, 51, 357, 164, 214,
  97, 212, 83, 114, 331, 449, 341, 52, 364, 213, 90, 163, 207, 48, 336, 17, 119, 366, 227, 188, 382, 339, 38, 266,
  461, 425, 173, 277, 71, 30, 210, 69, 16, 112, 317, 351, 122, 387, 374, 283, 113, 324, 400, 465, 453, 369, 248, 335,
  10, 70, 23, 161, 193, 417, 117, 352, 129, 436, 250, 349, 108, 289, 155, 151, 123, 394, 423, 159, 179, 319, 365,
  220, 139, 39, 273, 43, 301, 239, 272, 36, 252, 363, 206, 41, 287, 141, 53, 371, 262, 433, 229, 202, 13, 91, 170,
  256, 391, 402, 12, 84, 121, 380, 325, 407, 47, 329, 435, 243, 300, 232, 223, 160, 186, 368, 241, 286, 134, 4, 28,
  196, 438, 264, 447, 327, 421, 145, 81, 100, 233, 230, 209, 62, 434, 236, 251, 356, 157, 165, 221, 146, 88, 149,
  109, 296, 204, 27, 189, 389, 388, 381, 332, 456, 390, 395, 430, 208, 55, 385, 360, 185, 361, 192, 410, 68, 9, 63,
  441, 285, 127, 422, 152, 130, 443, 299, 225, 174, 284, 120, 373, 276, 64, 448, 334, 3, 21, 147, 95, 198, 452, 362,
  199, 459, 411, 75, 58, 406, 40, 280, 92, 177, 305, 267, 1 ]
```

Рис. 7: Непримитивный элемент

```
gap> for i in [1 .. p-1] do
> g := 8^i mod p;
> Add(list, g);
> od;
gap> list;
[ 8, 64, 45, 360, 78, 157, 322, 241, 60, 13, 104, 365, 118, 10, 80, 173, 450, 331, 313, 169, 418, 75, 133, 130, 106,
  381, 246, 100, 333, 329, 297, 41, 328, 289, 444, 283, 396, 366, 126, 74, 125, 66, 61, 21, 168, 410, 11, 88, 237,
  28, 224, 391, 326, 273, 316, 193, 143, 210, 279, 364, 110, 413, 35, 280, 372, 174, 458, 395, 358, 62, 29, 232, 455,
  371, 166, 394, 350, 465, 451, 339, 377, 214, 311, 153, 290, 452, 347, 441, 259, 204, 231, 447, 307, 121, 34, 272,
  308, 129, 98, 317, 201, 207, 255, 172, 442, 267, 268, 276, 340, 385, 278, 356, 46, 368, 142, 202, 215, 319, 217,
  335, 345, 425, 131, 114, 445, 291, 460, 411, 19, 152, 282, 388, 302, 81, 181, 47, 376, 206, 247, 108, 397, 374,
  190, 119, 18, 144, 218, 343, 409, 3, 24, 192, 135, 146, 234, 4, 32, 256, 180, 39, 312, 161, 354, 30, 240, 52, 416,
  59, 5, 40, 320, 225, 399, 390, 318, 209, 271, 300, 65, 53, 424, 123, 50, 400, 398, 382, 254, 164, 378, 222, 375,
  198, 183, 63, 37, 296, 33, 264, 244, 84, 205, 239, 44, 352, 14, 112, 429, 163, 370, 158, 330, 305, 105, 373, 182,
  55, 440, 251, 140, 186, 87, 229, 431, 179, 31, 248, 116, 461, 419, 83, 197, 175, 466, 459, 403, 422, 107, 389, 310,
  145, 226, 407, 454, 363, 102, 349, 457, 387, 294, 17, 136, 154, 298, 49, 392, 334, 337, 361, 86, 221, 367, 134,
  138, 170, 426, 139, 178, 23, 184, 71, 101, 341, 393, 342, 401, 406, 446, 299, 57, 456, 379, 230, 439, 243, 76, 141,
  194, 151, 274, 324, 257, 188, 103, 357, 54, 432, 187, 95, 293, 9, 72, 109, 405, 438, 235, 12, 96, 301, 73, 117, 2,
  16, 128, 90, 253, 156, 314, 177, 15, 120, 26, 208, 263, 236, 20, 160, 346, 433, 195, 159, 338, 369, 150, 266, 260,
  212, 295, 25, 200, 199, 191, 127, 82, 189, 111, 421, 99, 325, 265, 252, 148, 250, 132, 122, 42, 336, 353, 22, 176,
  7, 56, 448, 315, 185, 79, 165, 386, 286, 420, 91, 261, 220, 359, 70, 93, 277, 348, 449, 323, 249, 124, 58, 464,
  443, 275, 332, 321, 233, 463, 435, 211, 287, 428, 155, 306, 113, 437, 227, 415, 51, 408, 462, 427, 147, 242, 68,
  77, 149, 258, 196, 167, 402, 414, 43, 344, 417, 67, 69, 85, 213, 303, 89, 245, 92, 269, 284, 404, 430, 171, 434,
  203, 223, 383, 262, 228, 423, 115, 453, 355, 38, 304, 97, 309, 137, 162, 362, 94, 285, 412, 27, 216, 327, 281, 380,
  238, 36, 288, 436, 219, 351, 6, 48, 384, 270, 292, 1 ]
```

Рис. 8: Примитивный элемент

```
gap> for i in [1 .. p-1] do
> g := 9^i mod p;
> Add(list, g);
> od;
gap> list;
[ 9, 81, 262, 23, 207, 462, 422, 62, 91, 352, 366, 25, 225, 157, 12, 108, 38, 342, 276, 149, 407, 394, 277, 158, 21,
  189, 300, 365, 16, 144, 362, 456, 368, 43, 387, 214, 58, 55, 28, 252, 400, 331, 177, 192, 327, 141, 335, 213, 49,
  441, 233, 229, 193, 336, 222, 130, 236, 256, 436, 188, 291, 284, 221, 121, 155, 461, 413, 448, 296, 329, 159, 30,
  270, 95, 388, 223, 139, 317, 51, 459, 395, 286, 239, 283, 212, 40, 360, 438, 206, 453, 341, 267, 68, 145, 371, 70,
  163, 66, 127, 209, 13, 117, 119, 137, 299, 356, 402, 349, 339, 249, 373, 88, 325, 123, 173, 156, 3, 27, 243, 319,
  69, 154, 452, 332, 186, 273, 122, 164, 75, 208, 4, 36, 324, 114, 92, 361, 447, 287, 248, 364, 7, 63, 100, 433, 161,
  48, 432, 152, 434, 170, 129, 227, 175, 174, 165, 84, 289, 266, 59, 64, 109, 47, 423, 71, 172, 147, 389, 232, 220,
  112, 74, 199, 390, 241, 301, 374, 97, 406, 385, 196, 363, 465, 449, 305, 410, 421, 53, 10, 90, 343, 285, 230, 202,
  417, 17, 153, 443, 251, 391, 250, 382, 169, 120, 146, 380, 151, 425, 89, 334, 204, 435, 179, 210, 22, 198, 381,
  160, 39, 351, 357, 411, 430, 134, 272, 113, 83, 280, 185, 264, 41, 369, 52, 1, 9, 81, 262, 23, 207, 462, 422, 62,
  91, 352, 366, 25, 225, 157, 12, 108, 38, 342, 276, 149, 407, 394, 277, 158, 21, 189, 300, 365, 16, 144, 362, 456,
  368, 43, 387, 214, 58, 55, 28, 252, 400, 331, 177, 192, 327, 141, 335, 213, 49, 441, 233, 229, 193, 336, 222, 130,
  236, 256, 436, 188, 291, 284, 221, 121, 155, 461, 413, 448, 296, 329, 159, 30, 270, 95, 388, 223, 139, 317, 51,
  459, 395, 286, 239, 283, 212, 40, 360, 438, 206, 453, 341, 267, 68, 145, 371, 70, 163, 66, 127, 209, 13, 117, 119,
  137, 299, 356, 402, 349, 339, 249, 373, 88, 325, 123, 173, 156, 3, 27, 243, 319, 69, 154, 452, 332, 186, 273, 122,
  164, 75, 208, 4, 36, 324, 114, 92, 361, 447, 287, 248, 364, 7, 63, 100, 433, 161, 48, 432, 152, 434, 170, 129, 227,
  175, 174, 165, 84, 289, 266, 59, 64, 109, 47, 423, 71, 172, 147, 389, 232, 220, 112, 74, 199, 390, 241, 301, 374,
  97, 406, 385, 196, 363, 465, 449, 305, 410, 421, 53, 10, 90, 343, 285, 230, 202, 417, 17, 153, 443, 251, 391, 250,
  382, 169, 120, 146, 380, 151, 425, 89, 334, 204, 435, 179, 210, 22, 198, 381, 160, 39, 351, 357, 411, 430, 134,
  272, 113, 83, 280, 185, 264, 41, 369, 52, 1 ]
```

Рис. 9: Непримитивный элемент

```
gap> list := [];
[ ]
gap> for i in [1 .. p-1] do
> g := 10^i mod p;
> Add(list, g);
> od;
gap> list;
[ 10, 100, 66, 193, 62, 153, 129, 356, 291, 108, 146, 59, 123, 296, 158, 179, 389, 154, 139, 456, 357, 301, 208, 212,
  252, 185, 449, 287, 68, 213, 262, 285, 48, 13, 130, 366, 391, 174, 339, 121, 276, 425, 47, 3, 30, 300, 198, 112,
  186, 459, 387, 134, 406, 324, 438, 177, 369, 421, 7, 70, 233, 462, 417, 434, 137, 436, 157, 169, 289, 88, 413, 394,
  204, 172, 319, 388, 144, 39, 390, 164, 239, 55, 83, 363, 361, 341, 141, 9, 90, 433, 127, 336, 91, 443, 227, 402,
  284, 38, 380, 64, 173, 329, 21, 210, 232, 452, 317, 368, 411, 374, 4, 40, 400, 264, 305, 248, 145, 49, 23, 230,
  432, 117, 236, 25, 250, 165, 249, 155, 149, 89, 423, 27, 270, 365, 381, 74, 273, 395, 214, 272, 385, 114, 206, 192,
  52, 53, 63, 163, 229, 422, 17, 170, 299, 188, 12, 120, 266, 325, 448, 277, 435, 147, 69, 223, 362, 351, 241, 75,
  283, 28, 280, 465, 447, 267, 335, 81, 343, 161, 209, 222, 352, 251, 175, 349, 221, 342, 151, 109, 156, 159, 189,
  22, 220, 332, 51, 43, 430, 97, 36, 360, 331, 41, 410, 364, 371, 441, 207, 202, 152, 119, 256, 225, 382, 84, 373,
  461, 407, 334, 71, 243, 95, 16, 160, 199, 122, 286, 58, 113, 196, 92, 453, 327, 1, 10, 100, 66, 193, 62, 153, 129,
  356, 291, 108, 146, 59, 123, 296, 158, 179, 389, 154, 139, 456, 357, 301, 208, 212, 252, 185, 449, 287, 68, 213,
  262, 285, 48, 13, 130, 366, 391, 174, 339, 121, 276, 425, 47, 3, 30, 300, 198, 112, 186, 459, 387, 134, 406, 324,
  438, 177, 369, 421, 7, 70, 233, 462, 417, 434, 137, 436, 157, 169, 289, 88, 413, 394, 204, 172, 319, 388, 144, 39,
  390, 164, 239, 55, 83, 363, 361, 341, 141, 9, 90, 433, 127, 336, 91, 443, 227, 402, 284, 38, 380, 64, 173, 329, 21,
  210, 232, 452, 317, 368, 411, 374, 4, 40, 400, 264, 305, 248, 145, 49, 23, 230, 432, 117, 236, 25, 250, 165, 249,
  155, 149, 89, 423, 27, 270, 365, 381, 74, 273, 395, 214, 272, 385, 114, 206, 192, 52, 53, 63, 163, 229, 422, 17,
  170, 299, 188, 12, 120, 266, 325, 448, 277, 435, 147, 69, 223, 362, 351, 241, 75, 283, 28, 280, 465, 447, 267, 335,
  81, 343, 161, 209, 222, 352, 251, 175, 349, 221, 342, 151, 109, 156, 159, 189, 22, 220, 332, 51, 43, 430, 97, 36,
  360, 331, 41, 410, 364, 371, 441, 207, 202, 152, 119, 256, 225, 382, 84, 373, 461, 407, 334, 71, 243, 95, 16, 160,
  199, 122, 286, 58, 113, 196, 92, 453, 327, 1 ]
gap>
```

Рис. 10: Непримитивный элемент

Задание №1.2

Решить систему уравнений по модулю p в поле $GF(p)$.
$p = 467$ - было выбранно рандомно в предыдущем заданиии. Следовательно решить систему уравнений по модулю $GF(467)$.

$$\begin{cases} 354x + 17y + 160z = 3 \\ 56x + 130y + 6z = 249 \\ 43x + 9y + 322z = 5 \end{cases}$$

```
 ┌─────┐  GAP 4.8.8, 20-Aug-2017, build of 2017-08-20 19:05:21 (GMTDT)
 │ GAP │  https://www.gap-system.org
 └─────┘  Architecture: i686-pc-cygwin-gcc-default32
 Libs used:  gmp, readline
 Loading the library and packages ...
 Components: trans 1.0, prim 2.1, small* 1.0, id* 1.0
 Packages:   AClib 1.2, Alnuth 3.0.0, AtlasRep 1.5.1, AutPGrp 1.8, Browse 1.8.7, CRISP 1.4.4, Cryst 4.1.12,
             CrystCat 1.1.6, CTblLib 1.2.2, FactInt 1.5.4, FGA 1.3.1, GAPDoc 1.6, IO 4.4.6, IRREDSOL 1.4,
             LAGUNA 3.7.0, Polenta 1.3.7, Polycyclic 2.11, RadiRoot 2.7, ResClasses 4.6.0, Sophus 1.23, SpinSym 1.5,
             TomLib 1.2.6, Utils 0.46
 Try '??help' for help. See also '?copyright', '?cite' and '?authors'
gap> p := 467;
467
gap> m := [ [354, 17, 160, 3],
>           [56,  130,6,   249],
>           [43,  9,   322, 5] ];
[ [ 354, 17, 160, 3 ], [ 56, 130, 6, 249 ], [ 43, 9, 322, 5 ] ]
gap> Display(m);
[ [  354,   17,  160,    3 ],
  [   56,  130,    6,  249 ],
  [   43,    9,  322,    5 ] ]
gap> m[3] := (m[3]*222 mod p - m[2]) mod p;
[ 150, 0, 27, 394 ]
gap> Display(m);
[ [  354,   17,  160,    3 ],
  [   56,  130,    6,  249 ],
  [  150,    0,   27,  394 ] ]
gap> m[2] := (m[2]*453 mod p - m[3]) mod p;
[ 0, 48, 356, 323 ]
gap> Display(m);
[ [  354,   17,  160,    3 ],
  [    0,   48,  356,  323 ],
  [  150,    0,   27,  394 ] ]
gap> m[1] := (m[1]*305 mod p - m[2]) mod p;
[ 93, 0, 343, 125 ]
gap> Display(m);
[ [   93,    0,  343,  125 ],
  [    0,   48,  356,  323 ],
  [  150,    0,   27,  394 ] ]
```

Рис. 11: Объявление матрицы

```
gap> m[1] := m[1]*231 mod p;
[ 1, 0, 310, 388 ]
gap> m[3] := (m[3] - m[1]*150 mod p) mod p;
[ 0, 0, 227, 102 ]
gap> Display(m);
[ [   1,    0,  310,  388 ],
  [   0,   48,  356,  323 ],
  [   0,    0,  227,  102 ] ]
gap> m[2] := m[2]*360 mod p;
[ 0, 1, 202, 464 ]
gap> Display(m);
[ [   1,    0,  310,  388 ],
  [   0,    1,  202,  464 ],
  [   0,    0,  227,  102 ] ]
gap> m[3] := m[3]*395 mod p;
[ 0, 0, 1, 128 ]
gap> Display(m);
[ [   1,    0,  310,  388 ],
  [   0,    1,  202,  464 ],
  [   0,    0,    1,  128 ] ]
```

Рис. 12: Приведение к единичной матрице

```
gap> Display(m);
[ [   1,    0,  310,  388 ],
  [   0,    1,  202,  464 ],
  [   0,    0,    1,  128 ] ]
gap> m[2] := (m[2] - m[3]*202 mod p) mod p;
[ 0, 1, 0, 293 ]
gap> m[1] := (m[1] - m[3]*310 mod p) mod p;
[ 1, 0, 0, 403 ]
gap> Display(m);
[ [   1,    0,    0,  403 ],
  [   0,    1,    0,  293 ],
  [   0,    0,    1,  128 ] ]
gap> (354*403 mod p + 17*293 mod p + 160*128 mod p) mod p;
3
gap> (56*403 mod p + 130*293 mod p + 6*128 mod p) mod p;
249
gap> (43*403 mod p + 9*293 mod p + 128*322 mod p) mod p;
5
gap>
```

Рис. 13: Продолжение. Проверка.

Задание №1.3

Найти обратимый элемент по модулю $GF(p)$.
$p = 467 \Rightarrow GF(467)$

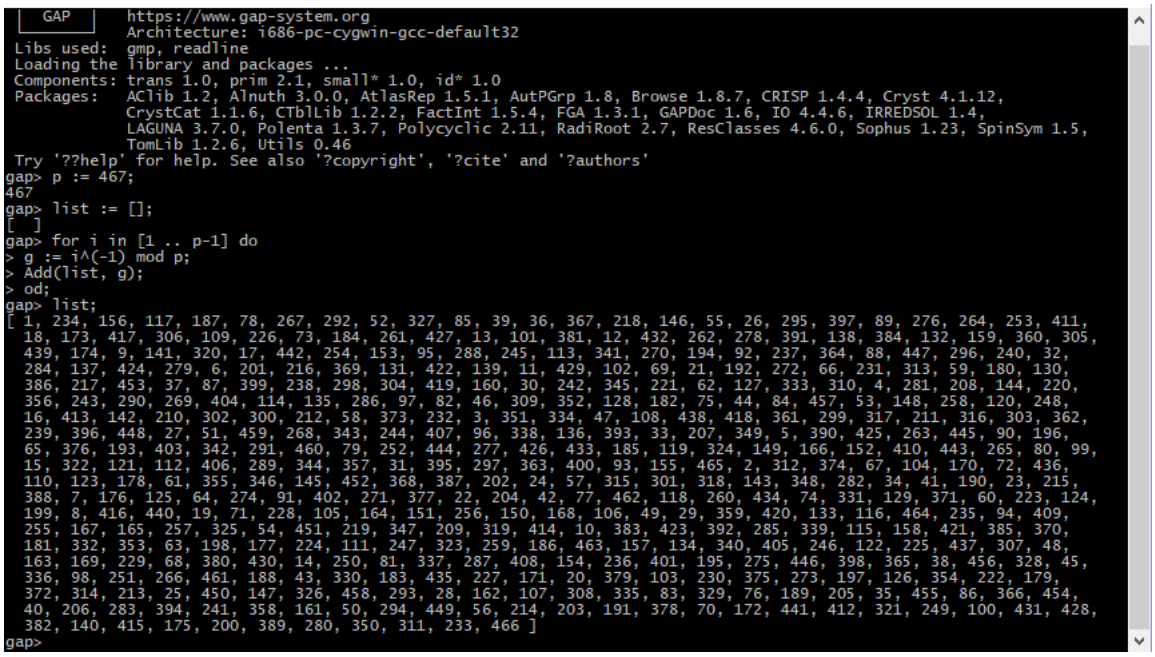

Рис. 14: Список из всех обратимых элементов

Задание №1.4

Решить квадратное уравнение по модулю $GF(p)$.

$24x^2 - 365x + 1506 = 0$

1. Написать программу, которая вычисляет квадраты всех элементов поля $GF(p)$

```
 GAP      https://www.gap-system.org
          Architecture: i686-pc-cygwin-gcc-default32
 Libs used:  gmp, readline
 Loading the library and packages ...
 Components: trans 1.0, prim 2.1, small* 1.0, id* 1.0
 Packages:   AClib 1.2, Alnuth 3.0.0, AtlasRep 1.5.1, AutPGrp 1.8, Browse 1.8.7, CRISP 1.4.4, Cryst 4.1.12,
             CrystCat 1.1.6, CTblLib 1.2.2, FactInt 1.5.4, FGA 1.3.1, GAPDoc 1.6, IO 4.4.6, IRREDSOL 1.4,
             LAGUNA 3.7.0, Polenta 1.3.7, Polycyclic 2.11, RadiRoot 2.7, ResClasses 4.6.0, Sophus 1.23, SpinSym 1.5,
             TomLib 1.2.6, Utils 0.46
 Try '??help' for help. See also '?copyright', '?cite' and '?authors'
gap> p := 467;
467
gap> list := [];
[ ]
gap> for i in [1 .. p-1] do
> g := i^(-1) mod p;
> Add(list, g);
> od;
gap> list;
[ 1, 234, 156, 117, 187, 78, 267, 292, 52, 327, 85, 39, 36, 367, 218, 146, 55, 26, 295, 397, 89, 276, 264, 253, 411,
  18, 173, 417, 306, 109, 226, 73, 184, 261, 427, 13, 101, 381, 12, 432, 262, 278, 391, 138, 384, 132, 159, 360, 305,
  439, 174, 9, 141, 320, 17, 442, 254, 153, 95, 288, 245, 113, 341, 270, 194, 92, 237, 364, 88, 447, 296, 240, 32,
  284, 137, 424, 279, 6, 201, 216, 369, 131, 422, 139, 11, 429, 102, 69, 21, 192, 272, 66, 231, 313, 59, 180, 130,
  386, 217, 453, 37, 87, 399, 238, 298, 304, 419, 160, 30, 242, 345, 221, 62, 127, 333, 310, 4, 281, 208, 144, 220,
  356, 243, 290, 269, 404, 114, 135, 286, 97, 82, 46, 309, 352, 128, 182, 75, 44, 84, 457, 53, 148, 258, 120, 248,
  16, 413, 142, 210, 302, 300, 212, 58, 373, 232, 3, 351, 334, 47, 108, 438, 418, 361, 299, 317, 211, 316, 303, 362,
  239, 396, 448, 27, 51, 459, 268, 343, 244, 407, 96, 338, 136, 393, 33, 207, 349, 5, 390, 425, 263, 445, 90, 196,
  65, 376, 193, 403, 342, 291, 460, 79, 252, 444, 277, 426, 433, 185, 119, 324, 149, 166, 152, 410, 443, 265, 80, 99,
  15, 322, 121, 112, 406, 289, 344, 357, 31, 395, 297, 363, 400, 93, 155, 465, 2, 312, 374, 67, 104, 170, 72, 436,
  110, 123, 178, 61, 355, 346, 145, 452, 368, 387, 202, 24, 57, 315, 301, 318, 143, 348, 282, 34, 41, 190, 23, 215,
  388, 7, 176, 125, 64, 274, 91, 402, 271, 377, 22, 204, 42, 77, 462, 118, 260, 434, 74, 331, 129, 371, 60, 223, 124,
  199, 8, 416, 440, 19, 71, 228, 105, 164, 151, 256, 150, 168, 106, 49, 29, 359, 420, 133, 116, 464, 235, 94, 409,
  255, 167, 165, 257, 325, 54, 451, 219, 347, 209, 319, 414, 10, 383, 423, 392, 285, 339, 115, 158, 421, 385, 370,
  181, 332, 353, 63, 198, 177, 224, 111, 247, 323, 259, 186, 463, 157, 134, 340, 405, 246, 122, 225, 437, 307, 48,
  163, 169, 229, 68, 380, 430, 14, 250, 81, 337, 287, 408, 154, 236, 401, 195, 275, 446, 398, 365, 38, 456, 328, 45,
  336, 98, 251, 266, 461, 188, 43, 330, 183, 435, 227, 171, 20, 379, 103, 230, 375, 273, 197, 126, 354, 222, 179,
  372, 314, 213, 25, 450, 147, 326, 458, 293, 28, 162, 107, 308, 335, 83, 329, 76, 189, 205, 35, 455, 86, 366, 454,
  40, 206, 283, 394, 241, 358, 161, 50, 294, 449, 56, 214, 203, 191, 378, 70, 172, 441, 412, 321, 249, 100, 431, 428,
  382, 140, 415, 175, 200, 389, 280, 350, 311, 233, 466 ]
gap>
```

Рис. 15: Квадраты всех элементов $GF(467)$

2. Написать программу, которая вычисляет степени примитивного элемента поля $GF(p)$ и выяснить какой степенью является дискриминант.

```
gap> for i in [1 .. p-1] do
> g := 2^i mod p;
> if g = 324 then
> t := i;
> fi;
> od;
gap> t;
404
gap>
```

Рис. 16: Примитивный элемент 2 в поле $GF(467)$

```
gap> D := ((-365)^2 - 4*24*1506) mod p;
324
gap> x1 := ((365 + 18)*(24*2)^(-1)) mod p;
115
gap> x2 := ((365 - 18)*(24*2)^(-1)) mod p;
231
```

Рис. 17: Решение квадратного уравнения в поле $GF(467)$

Задание №1.5

ФИО
$\alpha = 9$ - количество букв фамилии(Присяжнюк).

$\beta = 4$ - количество букв имени(Анна).
$\gamma = 13$ - количество букв в отчестве(Александровна).

```
gap> p := 467;
467
gap> 9^(4 + 13) mod p;
38
gap>
```

Рис. 18: $\alpha^{\beta+\gamma} \bmod 467$

Задание №2.1

Зашифровать свое имя по алгоритму RSA
Анна - 014140 = 14140
$p = 152, q = 98 \Rightarrow n = p * q = 14896$
$\phi(n) = (p-1)(q-1) = n - p - q + 1 = 14896 - 152 - 98 + 1 = 14647$
$e = 839$ - взаимопростое число с $\phi(n)$
$(e, n) = (839, 14896)$ - открытый ключ

```
gap> 14140^839 mod 14896;
5488
gap>
```

Рис. 19: Зашифрованное число

Задание №2.2

Найти 16 - ти значное простое число

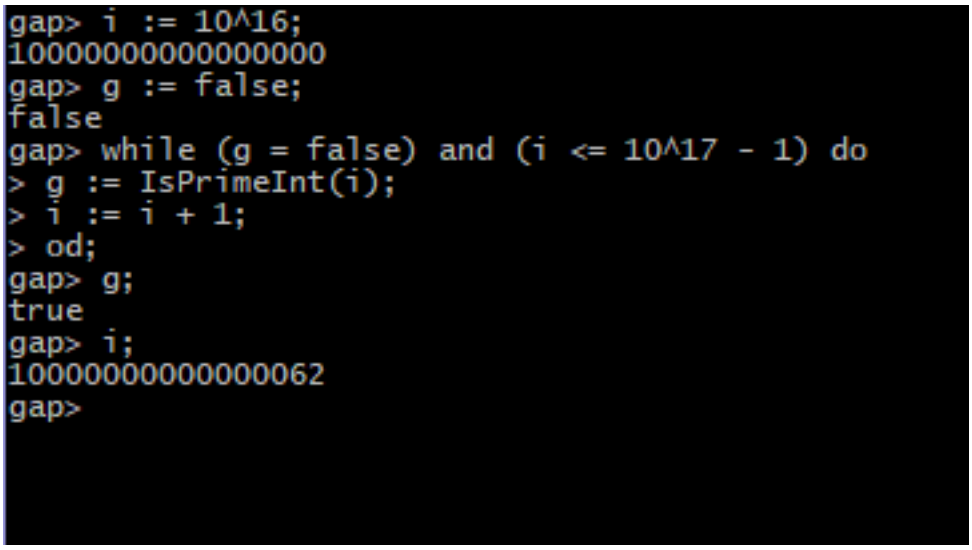

Рис. 20: 16 - ти значное простое число i

Задание №3