Алгебра
Домашнее задание
В.Мозговой

31 декабря 2021 г.

1 Задачи

1.1 1 Диофантовы уравнения

1)
Рассмотрим $ax + by = k$, разделим все, если возможно(иначе корней нет), на $\gcd(a, b)$,
Получим $\frac{a}{\gcd(a,b)}x + \frac{b}{\gcd(a,b)}y = \frac{k}{\gcd(a,b)} \ = \ a_0x + b_0y = k_0$, теперь $\gcd(a_0, b_0) = 1$
По алгоритму евклида найдем 1 пару $a_1, \ b_1$ при которой равенство выполнено, тогда все решения можно записать как:

$$\begin{cases} x_n \ = \ a_1 + n \cdot \frac{a}{\gcd(a,b)} \ = \ a_1 + n \cdot a_0 \\ y_n \ = \ b_1 - n \cdot \frac{b}{\gcd(a,b)} \ = \ b_1 - n \cdot b_0 \end{cases} \qquad n \in \mathbb{Z}$$

$$\text{gcd(a,b)} \ = \ \text{НОД(a,b)} \ = \ \text{(a,b)}$$

2)
Рассмотрим $ax + by + cz = k$. Если $k \mod \gcd(a, b, c) = 0$, то у уравнения есть решения, иначе их нет.
Пусть $p = \gcd(a, b)$, и $a^\star = \frac{a}{p} \quad b^\star = \frac{b}{p}$
Тогда решим уравнение $a^\star u + b^\star v = c$ – его решения u_0 и v_0 (по (1) пункту)
z_0 и t_0 – решения $cz + pt = d$ (по (1) пункту)
x_0 и y_0 – решения $a^\star x + b^\star y = t_0$ (по (1) пункту)
Тогда решения системы это:

$$\begin{cases} x \ = \ x_0 + b^\star k - u_0 m \\ y \ = \ y_0 - a^\star k - v_0 m \\ z \ = \ z_0 + pm \end{cases}$$

$$k, m \in \mathbb{Z}$$

1.2 2

Докажем что все конечные поля одинакового порядка изоморфны
Рассмотрим поля A и B порядка p^n. Пусть $a \in A$ и $b \in B$ – примитивные элементы полей. Ненулевых элементов в A и B ровно $p^n - 1$.
У многочлена $x^{p^n - 1} - 1$ ровно $p^n - 1$ ненулевых корней. Все эти корни различны и лежат как в A, так и в B. Тогда, так как порядки полей совпадают, то некий $\alpha \in A$ перешел в $\beta \in B$. И тогда $\alpha^k = \beta$, а это отоношение задает изоморфизм полей.
2:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

4:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	0	1
$x+1$	0	$x+1$	1	0

8:

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

$\times$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

3:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

9:

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x+1$	$2x$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

$\times$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

5:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

7:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

1.3 3

Приводимые в $\mathbb{F}_3$ приводимы и в $\mathbb{F}_9$.
В $\mathbb{F}_3$ неприводимые это x^2+1; x^2+x+2; x^2+2x+2
В $\mathbb{F}_9$ $y^2+1=0$; y^2+y+2 имеет корень $(x+1)$; y^2+2y+2 имеет корень $(x+2)$.

1.4 4

Покажем, что в $F_{16} = F[y]/(y^2 + y\overline{(x+1)} + 1)$ есть корни.
Заметим, что если любое уравнение можно свести к $x^2+x+c=0$ или $x^2+c=0$. Докажем это: пусть уравнение вида $ax^2+bx+c=0$ (считаем a не нулевым), тогда оно эквивалентно уравнению $x^2+\frac{b}{a}x+\frac{c}{a}$. Сделаем замену переменных: $z \cdot \frac{b}{a} = x$. Тогда уравнение эквивалентно $z^2+z+\frac{c \cdot a^2}{b^2}=0$ с заменой корней (при $b \neq 0$, иначе эквивалентно уравнению вида $x^2+c=0$). Заметим, что $x^2+x+c=0$ имеют корни в $F16$:

$$\begin{aligned} &x^2+x=0 && x=0; \quad x=1 \\ &x^2+x+1=0 && x=\overline{x}; \quad x=\overline{x+1} \end{aligned}$$

Примечание:
$(y\cdot\overline{x}+\alpha)^2 = y^2\cdot\overline{x+1}+\alpha^2 = y\cdot\overline{x}+\overline{x+1}+\alpha^2$, поэтому решение двух оставшихся уравнений сводится к двум первым: $(y\cdot\overline{x}+\alpha)^2+(y\cdot\overline{x}+\alpha)+c = \alpha^2+\alpha+\overline{x+1}+c$

$$\begin{aligned} &x^2+x+\overline{x}=0 && x=y\cdot\overline{x}+\overline{x}; \quad x=y\cdot\overline{x}+\overline{x+1} \\ &x^2+x+\overline{x+1}=0 && x=y\cdot\overline{x}; \qquad x=y\cdot\overline{x}+1 \end{aligned}$$

Покажем, что у уравнений вида $x^2+c=0$ есть решения:
$0\cdot 0=0$, откуда $x^2+0=0$ имеет корень.
$1\cdot 1=1$, откуда $x^2+1=0$ имеет корень.
$\overline{x}\cdot\overline{x}=\overline{x+1}$, откуда $x^2+\overline{x+1}=0$ имеет корень.
$\overline{x+1}\cdot\overline{x+1}=\overline{x}$, откуда $x^2+\overline{x}=0$ имеет корень.

1.5 5

Рассмотрим группу обратимых для $n=12$ $\quad\mathbb{Z}/12\mathbb{Z}$, это $\{1,\ 5,\ 7,\ 11\}$.
Заметим, что $5\cdot 5=25=1,\ 7\cdot 7=49=1,\ 11\cdot 11=-1\cdot -1=1$, откуда следует, что эта группа не циклична.

1.6 6

Докажем, что существует первообразный корень в Z/pZ.
(1) **Теорема Ферма**: $\alpha^{p-1}=1$ при $\alpha\neq 0$. Доказательство:
Рассмотрим всевозможные произведения α на другие элемента поля. Так как это поле, значит в нём нет делителей 0, откуда не может быть такого, что $\alpha\cdot x=\alpha\cdot y$ при $x\neq y$, поэтому всевозможные произведения различны. Откуда следует, что $\alpha\cdot 2\alpha\cdot\ldots\cdot(p-1)\alpha=(p-1)!\ \Leftrightarrow\ a^{p-1}(p-1)!=(p-1)!\ \Leftrightarrow\ a^{p-1}=1$ $((p-1)!\neq 0)$.

(2) **Лемма**: $n=\sum\phi(i)$, где i пробегает по всем делителям n (Здесь мы работаем в натуральных числах).
Доказательство:
Будем говорить, что $\alpha\in[1,n]$ принадлежит множеству M_i (где i – делитель n), если $\frac{\alpha}{\frac{n}{i}}$ целое, меньше i и взаимнопросто с i. Нетрудно видеть, что каждое α может принадлежать не более 1 множеству, так как то, что $\alpha\in M_{i_1}\ \Leftrightarrow\ (\alpha,\ n)=\frac{n}{i_1}$. Также видно, что любое α принадлежит хоть какому то множеству.
Теперь заметим, что в каждом множестве M_i ровно $\phi(i)$ элементов, так как таких $\alpha:\ \frac{\alpha}{n/i}\in Z$ - i $(\frac{n}{i},\ \frac{2n}{i},\ \ldots,\ \frac{in}{i})$, при этом среди чисел в промежутке $[1,i]$ взаимнопростых $\phi(i)$. Откуда следует то, что и требовалось доказать.

(3) **Замечание**: элементов порядка k либо 0, либо $\phi(k)$. Доказательство:
Предположим есть хотя бы 1. (элемент g) Тогда элементы вида $g,\ g^2,\ g^3,\ \ldots,\ g^k$ различны и являются корнями уравнения $x^k-1=0$, откуда следует, что других корней нет, при этом если $\alpha\in[1,k]$ не взаимнопросто с k (пусть $(\alpha,k)=y$), то порядок у $g^\alpha=\frac{k}{y}$, что не равно k. Поэтому элементов порядка k ровно $\phi(k)$.

Следствие **(1)**, **(2)** и **(3)**:
Заметим, что если k - не делитель $p-1$, то чисел порядка k - ноль, так как порядок не может быть больше чем $p-1$ (иначе среди чисел $g,\ g^2,\ \ldots,\ g^i$ найдутся 2 одинаковых, тогда разделим одно на другое и получим, что порядок меньше, чем предполагался – противоречие), при этом любое число в степени $p-1$ равно 1.
Теперь рассмотрим все k, которые делят $p-1$. Заметим, что для всякого k количество чисел порядка k не

больше чем $\phi(k)$, при этом сумма всех $\phi(i)$, где i делит $p-1$, равна $p-1$, то есть ($\sum_{i \mid p-1} \phi(i) = p-1$), и всякое ненулевой элемент принадлежит хоть какому то порядку, откуда следует, что для всякого k количество чисел порядка k ровно $\phi(k)$.

Откуда есть элементы порядка $p-1$, что и требовалось доказать.

Пусть первообразный корень это g, и $g^{p-1} = 1 + pk$. Рассмотрим числа вида $(g+pt)^{p-1} \quad \forall t \in Z$. Тогда $(g+pt)^{p-1} = 1+p\cdot(k+(p-1)g^{p-2}\cdot t+p\cdot X)$. Заметим, что существует такое t_1, что $k+(p-1)g^{p-2}\cdot t_1+p\cdot X = 1 \pmod{\mathbb{Z}/p^{n-1}\mathbb{Z}}$, так как существует обратное у $(p-1)\cdot g^{p-2}$ (назовем его t_0). Рассмотрим $t_1 = t_0\cdot(1-k-p\cdot X)$, заметим, что $1+p$ принадлежит показателю вида p^{α}, так как $g+pt_1$ принадлежит показателю вида $p^{\beta}\cdot(p-1)$, так как все возможные непустые показатели являются делителями $p^{n-1}\cdot(p-1)$, при этом $(g+pt_1)^{p-1} \neq 1$.

Рассмотрим $(1+p)^{p^{\alpha}} = 1 + p^{\alpha+1}\cdot(1+p\cdot Y) = 1 + p^{\alpha+1}\cdot u_{\alpha}$, где u_{α} взаимнопросто с p. Предположим, что $(1+p)^{p^{\alpha}} = 1$, тогда $p^{\alpha+1} = 0$, откуда $\alpha+1 = n$, поэтому $1+p$ принадлежит показателю p^{n-1}, следовательно $g+pt_1$ принадлежит показателю $p^{n-1}\cdot(p-1)$, и тогда $g+pt_1$ – первообразный корень.