Задача 1

Постройте явное поле $\mathbb{F}_8$ и составьте для него таблицы сложения и умножения.

Отметим тот факт, что поле $\mathbb{F}_8 \simeq \mathbb{F}_2[x]/x^3 \simeq$ остаткам при деление на $x^3 + x^2 + 1$, то есть многочлены степени не более чем 2 над полем 2. По данному отображению легко строим таблицу сложения и умножения:

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

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

Задача 2

Реализуем поле $\mathbb{F}_9$ в виде $\mathbb{Z}_3[x]/(x^2+1)$. Перечислите в этой реализации все элементы данного поля, являющиеся пораждающими циклической группы $\mathbb{F}_9^\times$.

Для начала построим таблицу умножения:

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

Отметим, что порядок пораждающих элементов равен 8, откуда получаем ответ:
$x+1, x+2, 2x+1, 2x+2$

Задача 3

Проверьте, что многочлен x^2+1 и y^2-y-1 непреводимы над $\mathbb{Z}_3$, и установите явно изоморфизм между $\mathbb{Z}_3[x]/(x^2+1)$ и $\mathbb{Z}_3[y]/(y^2-y-1)$.

$x^2+1=\{1,2\}$ над $\mathbb{Z}_3 \Rightarrow$ корней нет. $y^2-y-1=y^2+2y+2=(y+1)^2+1=\{1,2\}$, так же без корней.

Построим таблицу умножения в $\mathbb{Z}_3[y]/(y^2-y-1)$:

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

Для корректного определения изоморфизма, нам достаточно указать, куда переходит 1 и x. Учитываю порядки элементов получаем:

$$\varphi(1)=1 \qquad \varphi(x)=y+1$$