Филиппова Анастасия

Домашнее задание 7

(1) **Предложите алгоритм.**

Будем решать данную систему методом последовательных подстановок: решаем систему, подставляя $x = r_1 + a_1 y, y \in \mathbb{Z}$ во второе уравнение. Получаем, $r_1 + a_1 y \equiv r_2 \ mod \ a_2$, получим $y = z + a_2 h$,, где $h \in \mathbb{Z}$. Получаем, $x = r_1 + a_1(z + a_2 h)$. Подставляем полученное значение в следующее уравнение, и так далее. Продолжаем, пока не дойдем до последнего уравнения. Так как все переходы равносильные, алгоритм корректен. Следовательно , получаем верный ответ: $x = t \ mod$ НОК$(a_1, a_2, ..., a_n)$. Если же на каком-то шаге уравнение не будет иметь решений, то система будет не совместна.

(2) (a) **Найдите все целые числа n такие, что n дает остаток 7 при делении на 9, остаток 3 при делении на 4 и остаток 16 при делении на 17.**

Решим систему сравнений:

$$\begin{cases} x & \equiv 7 \pmod 9 \\ x & \equiv 3 \pmod 4 \\ x & \equiv 17 \pmod{17}, \end{cases}$$

Будем искать x в виде: $x = x_1 + 4x_2 + 36x_3$ (по алгориму Гарнера).

$x_1 \equiv 3 \ mod \ 4 \to x_1 = 3$.

$3 + 4x_2 \equiv 7 \ mod \ 9 \Leftrightarrow 4x_2 \equiv 4 \ mod \ 9 \Leftrightarrow x_2 \equiv 4 \cdot 7 \equiv 1 \ mod \ 9 \Rightarrow x_2 = 1$.

$7 + 36x_3 \equiv 16 \ mod \ 17 \Leftrightarrow 36x_3 \equiv 9 \ mod \ 17 \Leftrightarrow 2x_3 \equiv 9 \ mod \ 17 \Leftrightarrow x_3 \equiv 9 \cdot 9 \equiv 81 \equiv 13 \Rightarrow x = 3 + 4 + 36 \cdot 13 = 475$

Ответ:457.

(b) **Найдите все целые числа n такие, что n дает остаток 35 при делении на 49, остаток 27 при делении на 50 и остаток 49 при делении на 56.**

Решим систему сравнений, по алгоритму, описанному в 1-ой задаче:

$$\begin{cases} \text{x} & \equiv 35 \pmod{49} \\ \text{x} & \equiv 27 \pmod{50} \\ \text{x} & \equiv 49 \pmod{56}, \end{cases}$$

$x = 35 + 49y, y \in Z$

$35 + 49y \equiv 27 \ mod \ 50$

$-1y \equiv -8 \equiv 41 \ mod \ 50$

$y \equiv -8 \cdot 49 \equiv 8 \ mod \ 50 \Rightarrow y = 8 + 50z$

$x = 35 + 49(8 + 50z) = 427 + 2450z$

Подставим в 3 сравнение: $427 + 2450z \equiv 49 \ mod \ 56 \Rightarrow 42y \equiv 14 \ mod \ 56 \Rightarrow 3z \equiv 1 \ mod \ 4 \Rightarrow z \equiv 3 \ mod \ 4$

Следовательно, $y = 3 + 4c$, тогда $x = 427 + 2450 \cdot 3 + 9800c \Rightarrow x = 7777$

Ответ: 7777.

(3) **Существует ли элемент, обратный к x, в кольце $\mathbb{R}[x]/(x^4+1)$?**

Да: $-x^3 \in \mathbb{R}[x]/(x^4+1), (-x^3) \cdot (x) = -x^4 = 1$ в $\mathbb{R}[x]/(x^4+1)$.

(4) **Решите уравнение $x^3 f(x) = 1 + x$ в кольце $\mathbb{Q}[x]/(x^4+1)$.**

$x^4 + 1$ - неприводим в кольце многочленов с коэффиентами из $\mathbb{Q} \Rightarrow \mathbb{Q}[x]/(x^4+1)$ - поле, то есть евклидово кольцо, то есть есть аналог алгоритма Евклида:

$x^3 f(x) + g(x)(x^4+1) = 1 + x$

$(x^3, x^4+1) = (1, x^3) = 1, 1|(1+x) \Rightarrow$ решения есть.

$x^3 f'(x) + (x^4+1)g'(x) = 1$

$f'(x) = -x, g'(x) = 1 \Rightarrow f(x) = -x^2 - x + ax^3 + bx^2 + cx + d$, где $a, b, c, d \in \mathbb{Q}$

(5) **Являются ли неприводимыми многочлены:**

(a) $x^2 - 3x + 11 \in \mathbb{F}_{37}[x]$

Посмотрим на дискрименант : $D = 9 - 44 = -35 = 2, 2^{\frac{37-1}{2}} = 2^{18} = 262144 = -1 \Rightarrow 2$ - квадратичный не вычет по модулю 37, следовательно, дискрименант не является квадратом, то есть корней у этого многочлена в поле нет, а для многочлена степени меньшей либо равной 3 это эквивалентно неприводимости.

Ответ: неприводим.

(b) $x^3 - x + 2 \in \mathbb{F}_5[x]$

$0 : 0 - 0 + 2 = 2;$

$1 : 1 - 1 + 2 = 2;$

$2 : 8 - 2 + 2 = 3;$

$3 : 27 - 3 + 2 = 1;$

$4 : 64 - 4 + 2 = 2 \Rightarrow$корней нет, то есть неприводим.

Ответ: неприводим.

(c) $x^4 + 1 \in \mathbb{F}_{11}[x]$

Пусть многочлен имеет корни, тогда $\exists x \hookrightarrow (x^2)^2 = -1 \Rightarrow$ -1 - квадратичный вычет по модулю 11, но $(-1)^{\frac{11-1}{2}} = (-1)^5 = -1 \ mod \ 5 \Rightarrow$ получили противоречие. То есть у многочлена не корней.

Посмотрим, может ли он раскладываться в произведение неприводимых второй степени:

$(x^4 + 1) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + x^3(c + a) + x^2(d + b + ac) + x(ad + bc) + bd$; получаем систему сравнений:

$$\begin{cases} a & \equiv -c \pmod{11} \\ d + b + ac & \equiv 0 \pmod{11} \\ ad + bc & \equiv 0 \pmod{11}, \\ bd & \equiv 1 \pmod{11}, \end{cases} \Rightarrow \begin{cases} a & \equiv -c \pmod{11} \\ d + b + ac & \equiv 0 \pmod{11} \\ c(b - d) & \equiv 0 \pmod{11}, \\ bd & \equiv 1 \pmod{11}, \end{cases}$$

Рассмотрим 2 варианта:

1) $c \equiv 0 \ mod \ 11 \Rightarrow b \equiv -d \ mod \ 11 \Rightarrow b^2 \equiv -1 \ mod \ 11 \Rightarrow$ получили противоречие, так как ранее доказали, что -1 не является квадратичным вычетом по модулю 11.

2) $b = d \Rightarrow \begin{cases} a & \equiv -c \pmod{11} \\ a^2 & \equiv 2b \pmod{11} \\ b^2 & \equiv 1 \pmod{11}, \end{cases}$

Первый случай: $b = -1$, тогда $a^2 = -2 = 9 \Rightarrow a = -3, c = 3$, получаем:

$(x^4 + 1) = (x^2 - 3x - 1)(x^2 + 3x - 1)$,но полученные многочлены приводимы: $D = 9 - 4 = 5, 5^5 \equiv 3125 \equiv 1 \ mod \ 11 \Rightarrow$ имеют корни.

Второй случай: $b = 1$, тогда $a^2 = 2$, но $2^{\frac{11-1}{2}} \equiv 32 \equiv -1 \ mod \ 11 \Rightarrow$ не является квадратичным вычетов по модулю 11. Получаем, что такого разложение на неприводимые не существует, следовательно, многочлен $(x^4 + 1)$ неприводим.

Ответ: неприводим. $d)$ $x^6 + 1 \in \mathbb{F}_{17}[x]$

Имеет корень 4: $4^6 + 1 \equiv 4097 \equiv 0 \ mod \ 11$, следовательно, приводим.

Ответ: приводим.

(6) **В зависимости от размера поля**

(a) **Чему равна сумма всех элементов конечного поля?** Если поле состоит из 2 элементов, то ,очевидно, 1.

Если больше, чем из 2 элементов, то, так как $\mathbb{F}^*$ - циклическая, пусть a - порождающий, $\mathbb{F}^* = (a^0, a^1 ... a^{p^n - 2})$, по формуле суммы геометрической прогрессии:$S = a^0(a^{p^n - 1} - 1)/(a - 1)$, а так как $a^{p^n - 1} - 1 = 0 \Rightarrow S = 0$.

(b) **Чему равно произведение всех ненулевых элементов конечного поля?**

Если поле состоит из 2 элементов, очевидно, 1.

Если поле содержит больше 2 элементов: в поле все элементы без нуля имеют обратные, то есть элементы разбиваются на пары, причем, для всех элементов кроме -1 и 1 эти элементы не совпадают. $\forall \ a \neq -1, a \neq 1 \hookrightarrow a \cdot a^{-1} = 1 \Rightarrow$ произведение равно -1.

(7) **Постройте изоморфизм между полями** $GF(7)[x]/(x^2 + x - 1)$ **и** $GF(7)[x]/(x^2 + 1)$**.**

Надо найти образ 1 и образ x. $\varphi(1) = 1$, так как это нейтральный элемент по умножению.

Пусть $\varphi(x) = ax + b$. В первом поле $x^2 = -x + 1$, во втором $x^2 = -1$

$\varphi(x^2) = a^2x^2 + 2ax + b^2 = 6a^2 + 2ax + b^2 = -ax - b + 1$

$$\begin{cases} a(2b + 1) & \equiv 0 \pmod{7} \\ 6a^2 + b^2 & \equiv -b + 1 \pmod{7} \end{cases}$$

$a \neq 0 \ mod\ 7 \Rightarrow 2b+1 \equiv 0 \Rightarrow b \equiv 3 \ mod\ 7$
$6a^2 \equiv -11 \ mod\ 7$
$a^2 \equiv 11 \equiv 4 \ mod\ 7 \Rightarrow a = 2$ или $a = -2$. Получаем, $\varphi(x) = 2x+3$ или $\varphi(x) = -2x+3$.
Проверим сохранение операций: $ax+b, cx+d$ - какие-то элементы поля $GF(7)[x]/(x^2+x-1)$
$\varphi(ax+b+cx+d) = 2(a+c)x+3(a+c)+b+d = 2ax+3a+b+2cx+3c+d = \varphi(ax+b)+\varphi(cx+d)$
$\varphi((ax+b)(cx+d)) = \varphi(acx^2+(ad+bc)x+db) = \varphi(x(bc+ad-ac)+ac+bd) = (2x+3)(dc+ad-ac)+ac+bd = -2ac-2acx+2bcx+2adx+3ad+3bc+bd = 4acx^2+6acx+2cbx+6acx+2ac+3bc+2adx+3ad+bd = (2ax+3a+b)(2cx+3c+d) = \varphi(ax+b)\varphi(cx+d)$. Операции сохраняются.

(8) **Постройте подгруппу размера 56 в S_8**
Рассмотрим автоморфизм $\varphi : x \to ax+b$, $a \neq 0$, так как в этом случае не было бы взаимооднозначного соответствия, то есть это был бы не автоморфизм. Следовательно, a может принимать 7 значений, b - 8 значений, следовательно, так как автоморфизм однозначно задается образом x - всего возможно 56 линейных автоморфизмов. Каждый автоморфизм переводит один элемент поля в другой, то есть кажды элемент является перестановкой. Линейные автоморфизмы образуют группу, следовательно построенное множество из 56 перестановок будет образовывать подгруппу.

(9) (a) **Докажите, что любой автоморфизм – это некоторая степень автоморфизма Фробениуса.**
(b) **Сколько элементов F^k переводит в себя?**
Пусть автоморфизм $F^k : a \hookrightarrow a^{p^k}$, для всех элементов, которые данный автоморфизм оставляет на месте будет верно:$a = a^{p^k}$, также $a = (a^{p^k})^{p^k} = a^{p^k p^k} = a^{p^{2k}}$,(легко проверить, что элементы, остающиеся на месте без 0 образуют группу по умножению), то есть верно следующее:$a = a^{p^{kx}}$, где $x \in \mathbb{Z}$. Обознаим $(k,n) = d$, уравнение $kx = yn + d$ - имеет решения. $a = a^{p^{kx}} = a^{p^{xn+d}} = (a^{p^{xn}})^{p^d}$, а так как $\forall\ a \in \mathbb{F}_{p^n} \hookrightarrow a = a^{p^n}$, получаем: $a = a^{p^d} \Rightarrow$ автоморфизм F^k оставляет на месте элементы под поле $\mathbb{F}_{p^d}$, где $d = (n,k)$.
(c) **Сколько существует вложений $\mathbb{F}_{p^n}$ в $\mathbb{F}_{p^{kn}}$**
Перефразируем задачу: необходимо найти количество инъективных гомоморфизмов данных полей. То есть вложение G устанавливает изофорфизм между $\mathbb{F}_{p^n}$ и $G(\mathbb{F}_{p^n}$, необходимо найти количество таких вложений. Полю $\mathbb{F}_{p^n}$ ставится в соответсвие изоморфное ему подполе в поле $F_{p^{nk}}$.
Рассмотрим автоморфизмы в поле $\mathbb{F}_{p^n}$, каждый из них задает биекцию, то есть взаимооднозначное соответствие. Автоморфизмы образуют группу, мощность которой n, следовательно, так как любое вложение $\mathbb{F}_{p^n}$ в $\mathbb{F}_{p^{nk}}$ задает автоморфизм, следовательно таких вложений n.

(10) **Является ли неприводимым над полем $\mathbb{F}_3$ из 3 элементов многочлен $x^9 - x^3 + 1$?**
Предположим, что многочлен неприводим, тогда $\mathbb{F}_3/(x^9-x^3+1)$ - поле. $(x^3-x+1) \in \mathbb{F}_3/(x^9-x^3+1)$. $(x^3-x+1)^3 = (x^9+(1-x)^3) = (x^9+1-x^3) = 0 \Rightarrow$ в поле есть делители нуля, что противоречит определению поля. Получаем, что (x^9-x^3+1) неприводим.

(11) **Сколько решений имеет уравнение $x^{22} - x^7 = 1$ в поле из 9 элементов?**
Автоморфизм Фробениуса: $F : x \hookrightarrow x^3$, применим автоморфизм Фробениуса:$(x^{66}-x^{21}-1), x^8 = 1 \Rightarrow x^2-x^5-1$, снова применим автоморфизм Фробениуса:$x^6-x^{15}-1 = 0 \Leftrightarrow 1/x^2-1/x-1 = 0 \Leftrightarrow 1-x-x^2 = 0$ - данный многочлен имеет столько же корней сколько и $x^{22}-x^7-1$.Следовательно у него не более 2-х корней. Построем поля в явном виде: $\mathbb{F}_9 \widetilde{=} \mathbb{F}_3[x]/(x^2+1)$ (многочлен x^2+1 неприводим над $\mathbb{F}_3$, так как не имеет корней).
$x+1 : [x+1]+[x+1]^2-1 = [x]+[1]+[x^2+1]+[2x]-1 = 0 \Rightarrow$корень.
$2x+1 : [2x+1]+[2x+]^2-1 = [2x]+[1]+[x]-[1] = 0 \Rightarrow$ корень.
Следовательно, уравнение имеет 2 кореня.
Ответ: 2.

(12) **Порядок элемента a в поле $\mathbb{F}_{25}$ равен 8. Является ли многочлен $-x^2+ax+a+a^2$ неприводимым?**
Многочлен 2-ой степени неприводим, тогда и только тогда, когда не имеет корней. Посмотрим, имеет ли данный многочлен корни: $-x^2+ax+a+a^2 = 0$
$-x^2+6ax-9a^2+a = 0$ (берем коэффиценты по модулю 5, поэтому можем так делать)
$-(x-3a)^2+a = 0$
$a = (x-3a)^2 \Rightarrow$ если x - корень многочлена, то а является квадратом какого-то элемента из поля. Но $ord(a) = 18, |F^*| = 24$, если $a = b^2$, тогда существует такой элемент поля b, что $(b^2)^8 = 1 \Rightarrow b^{16} = 1 \Rightarrow$ это элементы порядка $1,8$ или 4(так как искомый порядок делит 16 и делит 24).
1 не подходит, так как это порядок нейтрального элемента по умножению, то есть $1 : a = 1 \Rightarrow -x^2+x+1+1 = -x^2+x+2$ - приводим, так как имеет корень 2.
4: $a = b^2, a^2 = 1$, но порядок а равен 8, противоречие.
$8 : a = b^2 \Rightarrow a^4 = 1$, снова получаем противоречие определению порядка элемента.
Следовательно, многочлен неприводим.
Ответ: неприводим.