Домашнее задание

1. Найдите остаток от деления:

а) 3^{102} на 101, б) 7^{120} на 143, в) $2007^{2008^{2009}}$ на 11.

а) по м.т. Ферма $3^{100} \equiv 1 \pmod{101}$, тогда $3^{102} \equiv 9 \pmod{101}$.

б) По т. Эйлера: $7^{\varphi(143)} \equiv 1 \pmod{143}$, $\varphi(143) = 120$.

в) $2007^{2008^{2009}} \equiv 5^{2008^{2009}} \pmod{11}$. По м.т. Ферма $5^{10} \equiv 1 \pmod{11}$. Найдем $2008^{2009} \pmod{10} = 8^{2009} \pmod{10}$. Осталось выяснить, на какую цифру оканчивается число 8^{2009}. Выпишем последние цифры степеней 8: $8,4,2,6,8,4,2,6,\ldots$. Видим, что период равен 4. Так как $2009 \pmod 4 = 1$, число 8^{2009} оканчивается на 8. Находим $5^8 \pmod{11} = 4$.

2. Докажите, что кольцо $\mathbb{Z}_n$ не содержит подполей.

Пусть $A \subset \mathbb{Z}_n$ — подкольцо в $\mathbb{Z}_n$, тогда оно содержит единицу и замкнуто относительно сложения. Но порядок единицы по сложению равен n. Следовательно, складывая единички, мы перечислим все элементы $\mathbb{Z}_n$.

3. Может ли кольцо $\mathbb{Z}_m \times \mathbb{Z}_n$ содержать подполе?

Да, при $m = n = p$, где p—простое. Например, $\mathbb{Z}_3 \times \mathbb{Z}_3$ содержит подполе, изоморфное $\mathbb{Z}_3$: $\{(0,0),(1,1),(2,2)\}$. При $m \neq n$ ответ: нет. Пусть $m < n$, тогда если существует подполе, то оно содержит единицу: $(1,1)$, сложив ее с собой m раз получим, что в поле появится элемент $(0,m)$, который является делителем нуля. Противоречие.

4. Докажите, что кольцо $\mathbb{Z}_{12}$ не изоморфно кольцу $\mathbb{Z}_2 \times \mathbb{Z}_6$.

Порядок еденицы по сложению в $\mathbb{Z}_{12}$ равен 12, а в $\mathbb{Z}_2 \times \mathbb{Z}_6$: 6.

5. Найдите элемент максимального порядка в кольце $\mathbb{Z}_{56}$.

Разложим $\mathbb{Z}_{56}$ в произведение колец и найдем максимальный порядок: $\mathbb{Z}_{56} \cong \mathbb{Z}_7 \times \mathbb{Z}_8$. Максимальные порядки в кольцах $\mathbb{Z}_7$ и $\mathbb{Z}_8$ равны 6 и 2 соответственно. Максимальный порядок в $\mathbb{Z}_{56}$ равен НОК$(6,2) = 6$.

Перебором находим, что ответ: 3.

6. Изоморфны ли группы $\mathbb{Z}_{10}^*$ и $\mathbb{Z}_{12}^*$?

Нет, в группе $\mathbb{Z}_{10}^*$ элемент 3 имеет порядок 4, а в группе $\mathbb{Z}_{12}^*$ элементов порядка 4 нет.

7. Разложите на множители многочлен x^4+2 в кольце $\mathbb{Z}_3$.

$x^4+2=x^4-1=(x-1)(x+1)(x^2+1)$

8. Разложите на множители многочлен $x^7+x^6+4x^5+x^2+x+4$ в кольце $\mathbb{Z}_5$.

$x^7+x^6+4x^5+x^2+x+4=x^5(x^2+x+4)+x^2+x+4=(x^2+x+4)(x^5+1)=(x^2-4x+4)(x+1)^5=(x-2)^2(x+1)^5$. Тут мы воспользовались любопытным фактом: в поле $\mathbb{Z}_p$ (p — простое) выполняется равенство $(a+b)^p=a^p+b^p$. Докажите его в следующей домашней работе.