Контрольная работа. Вариант III

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Фамилия и имя студента:

Задача	1	2	3	Итог
Оценка				

Продолжительность контрольной — 80 минут. Каждый пункт оценивается в 2 балла. Если хотя бы в одном решении будет обнаружен плагиат, то все баллы за все решения будут аннулированы.

Задача 1. Шифр RSA использует открытый ключ из модуля 143 и экспоненты 7, а также следующее соответствие между буквами и цифрами:

$$\text{И} = 1,\ \text{Н} = 2,\ \text{Е} = 3,\ \text{А} = 4,\ \text{О} = 5,\ \text{Т} = 6,\ \text{Л} = 7,\ \text{Р} = 8,\ \text{С} = 9,\ \text{В} = 0.$$

Сообщение перевели в цифры, разбили на блоки по две цифры (получилось два блока) и зашифровали. Получилось 47 82. Расшифруйте сообщение.

Задача 2. Разложите многочлен $x^{15} - 1$ на неприводимые множители над
(а) $\mathbb{Q}$; (б) $\mathbb{R}$; (в) $\mathbb{C}$.

Достаточно объяснить, как находить неприводимые множители, и найти их степени (не требуется явно выписывать коэффициенты неприводимых множителей).

Задача 3. Можно ли представить факторкольцо $\mathbb{Z}[\omega]/(6)$ в виде прямой суммы полей? (Через ω обозначается комплексное число $e^{\frac{2\pi i}{3}}$.)