Домашнее задание 1. Арифметика

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Правила игры: нужно записать решения пяти задач на Ваш выбор из тех, которые получилось решить. За каждое верное решение Вы получите 2 балла или больше. Стоимость каждой задачи будет вычисляться, исходя из общего количества правильных решений (чем больше студентов решит задачу, тем меньше её стоимость). За особо оригинальные решения можно получить дополнительные баллы. При обнаружении плагиата хотя бы в одном решении, баллы за всю работу будут аннулированы.

Через R обозначается коммутативное кольцо с единицей.

Задача 1. Докажите, что простых целых чисел вида $4k+1$ бесконечно много.

Задача 2. Докажите, что над $\mathbb{F}_2$ существует неприводимый многочлен любой ненулевой степени.

Задача 3. Обозначим через I_m количество неприводимых многочленов степени m над $\mathbb{F}_2$. Докажите тождество

$$1-2z=\prod_{m=1}^{\infty}(1-z^m)^{I_m}.$$

(Одним из элементов доказательства должно быть объяснение, в каком смысле нужно понимать бесконечное произведение в правой части.)

Задача 4. Сформулируйте и докажите основную теорему арифметики в кольце $\mathbb{Z}[\sqrt{-2}]$.

Задача 5. Докажите, что кольцо многочленов $\mathbb{Z}[x]$ факториально.

Задача 6. Докажите, что кольцо $\mathbb{Z}[\sqrt{-5}]$ не факториально.

Задача 7. Докажите, что кольцо $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ факториально.

Задача 8. Предъявите какую-нибудь норму в кольце формальных степенных рядов $\mathbb{Q}[[x]]$, относительно которой это кольцо является евклидовым (в частности, нужно показать, что можно делить с остатком один ряд на другой).

Задача 9. Докажите, что простое натуральное число p представляется в виде суммы двух квадратов тогда и только тогда, когда -1 является квадратичным вычетом по модулю p.

Задача 10. Пусть p — простое целое число. Докажите, что длина периода в разложении рационального числа $\frac{1}{p}$ в десятичную дробь делит $p-1$.

Задача 11. Какие целые простые числа p представляются в виде

$$p=x^2+5y^2$$

для некоторых целых x и y?

Задача 12. Пусть p и q — различные простые натуральные числа. Докажите, что сравнение

$$p^x+q^y\equiv 1 \pmod{pq}$$

разрешимо в натуральных числах.

Задача 13. Пусть p — простое целое число не представимое в виде суммы двух квадратов. Докажите, что для любого целого гауссова числа $a+bi$, взаимно простого с p, справедливо следующее обобщение малой теоремы Ферма:

$$(a+bi)^{p^2-1} \equiv 1 \pmod{p}.$$

Задача 14. Пусть I, $J \subset R$ — два взаимно простых идеала. Докажите, что $IJ = I \cap J$.

Задача 15. Докажите, что идеал $P \subset R$ прост тогда и только тогда, когда в факторкольце R/P нет делителей нуля.

Задача 16. Докажите, что конечное коммутативное кольцо с единицей является полем тогда и только тогда, когда в нём нет делителей нуля.

Задача 17. Докажите, что конечномерная коммутативная алгебра с единицей является полем тогда и только тогда, когда в ней нет делителей нуля.

Задача 18. Представьте кольцо вычетов $\mathbb{Z}/30\mathbb{Z}$ в виде прямой суммы полей.

Задача 19. Можно ли представить факторкольцо $\mathbb{Z}[i]/(30)$ в виде прямой суммы полей?

Задача 20 (Конкурс RSA-129)**.** В 1977 году Ривест, Шамир и Адлеман объявили такой конкурс. Текстовое сообщение было зашифровано заменой A на 01, B на 02 и т.д. Пробел между словами зашифровали как 00. Затем полученное из текста число зашифровали с помощью 129-значного модуля $n = pq$, где

$$p = 32769132993266709549961988190834461413177642967992942539798288533$$

$$q = 34905295108476509491478496199038981334177646384933878439908205 77,$$

и открытой экспоненты 9007. Зашифрованное сообщение выглядит так:

9686 9613 7546 2206 1477 1409 2225 4355

8829 0575 9991 1245 7431 9874 6951 2093

0816 2982 2514 5708 3569 3147 6622 8839

8962 8013 3919 9055 1829 9451 5781 5154

Найдите исходное текстовое сообщение.