Критерии оценивания домашнего задания 1.

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Правила игры: сначала каждое решение оценивалось в условных баллах (уб). За полностью правильное решение ставилось 2 уб, в исключительных случаях — 3 уб (за особо оригинальное решение). За частично правильные решения ставились оценки в 0,5 уб, 1 уб и 1,5 уб в зависимости от характера и степени недочётов (см. ниже критерии по конкретным задачам). Затем все уб по каждой задаче складывались, чтобы вычислить рыночную стоимость задачи. Для вычисления итоговой оценки за домашнее задание оценка (в уб) за каждую задачу умножалась на нормировочный коэффициент в соответствии с рыночной стоимостью задачи.

Пример 1. Все сданные решения задачи 1 суммарно набрали 91 уб. Рыночная стоимость задачи минимальна — 2 балла. Поэтому нормировочный коэффициент в этом случае равен 1.

Пример 2. Все сданные решения задачи 2 суммарно набрали 5 уб. Рыночная стоимость задачи максимальна — 4 балла. Поэтому нормировочный коэффициент в этом случае равен 2.

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

- $1,5$ Не вполне понятно объяснение, почему построенное в решении "новое простое число" имеет вид $4k+1$. Например, используется утверждение малой теоремы Ферма без каких-либо пояснений (слова "по МТФ" считались достаточным пояснением).
- $0,5$ Совершенно непонятно (или отсутствует) объяснение, почему построенное в решении "новое простое число" имеет вид $4k+1$.

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

- $0,5$ Разобраны частные случаи (степени $n = 1, 2$ и 3) и намечена общая идея, но в её реализации имеется ошибка уже при $n = 4$.
- $0,5$ Сформулирована теорема о существовании поля из 2^n элементов, но не объясняется, почему из наличия такого поля следует существование неприводимого многочлена степени n.

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.

- 1 Формулируется теорема из лекции (без доказательства), из неё выводится утверждение задачи.

0,5 Формулируется теорема из лекции (без доказательства), из неё выводится утверждение задачи, сопровождаемое неверным утверждением “Кольцо $\mathbb{Z}[x]$ евклидово”.

0 Рассуждения опираются на неверные утверждения, такие как “Кольцо $\mathbb{Z}[x]$ евклидово” или “В кольце $\mathbb{Z}[x]$ можно делить многочлены с остатком”.

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

1 Приводится два разных разложения одного и того же числа на множители, но не доказывается, что множители неприводимы.

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.

1,5 Утверждение доказано в одну сторону (более простую), и приведены рассуждения, которые несложно довести до полного доказательства в другую сторону. Например, доказано, что некоторое кратное числа p представляется в виде суммы двух квадратов.

0,5 Утверждение доказано в одну сторону (более простую), в другую сторону приводится лишь ссылка на теорему Ферма–Эйлера без каких-либо самостоятельных рассуждений.

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

3 В процессе решения передоказывается малая теорема Ферма (для основания 10) путём изящных манипуляций с десятичными дробями.

1 В процессе решения неявно используется малая теорема Ферма (для основания 10) без какой-либо ссылки на неё (аббревиатура “МТФ” засчитывались за ссылку).

Задача 11. Какие целые простые числа p представляются в виде

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

для некоторых целых x и y?

1,5 Утверждение доказано в обе стороны, но опечатки в записи существенно затрудняют понимание.

0,5 Утверждение доказано в одну сторону (более простую).

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.

1 В процессе решения неявно используется малая теорема Ферма без какой-либо ссылки на неё (аббревиатура “МТФ” засчитывались за ссылку).

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:

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

1 Используется, что порядок мултипликативной группы кольца $\mathbb{Z}[i]/(p)$ равен p^2-1, но не объясняется, почему все ненулевые элементы этого кольца обратимы.

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

0.5 Доказано только, что $IJ \subset I \cap J$. Обратное включение не доказано.

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.

3 Из доказательства дополнительно следует, что каждый ненулевой элемент обратен по умножению некоторой своей степени.

0.5 Доказано только, что в поле 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.

1 Верный ответ, решение полностью отсутствует (в качестве решения засчитывались краткие комментарии, такие как “по КТО”, “разложим на простые”, “$\mathbb{Z}/p\mathbb{Z}$ — поле при простом p”).

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

0 Неверный ответ и неверное решение.

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

$$p = 3276913299326670954996198819083446141317764296799294253979828853 3$$

$$q = 3490529510847650949147849619903898133417764638493387843990820577,$$

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.

1,5 Опечатка в ответе (в слове “squeamish”) при верном решении.

0,5 Только ответ без внятных объяснения, что именно было посчитано на компьютере, и какова математическая составляющая компьютерных вычислений.