Типи задач

1. Прості задачі на доведення
2. З'ясувати, чи буде групою… (Завдання 1)
3. Скласти таблицю Келі групи(Завдання 2)
4. Знайти порядок елемента групи(Завдання 3)
5. У циклічній групі порядку n знайти всі елементи порядку k (Завдання 5)
6. Чи буде відображення гомоморфізмом? Чи буде воно ізоморфізмом? (Завдання 6)
7. З'ясувати, чи буде кільцем…(Завдання 7)
8. Знайти обернений елемент для елемента a у кільці/полі (Завдання 8)
9. Обчислити символ Якобі
10. Розв'язати рівняння у полі раціональних чисел (Завдання 9)
11. Розв'язати систему рівнянь у кільці/полі (Завдання 9)
12. Визначити кратність кореня для многочлена. Знайти значення многочлена f(x) і його похідних у точці (Завдання 12)
13. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел: а) за допомогою схеми Горнера; б) методом невизначених коефіцієнтів (Завдання 13)
14. Знайти всі раціональні корені многочлена (Завдання 15)
15. Відокремити дійсні корені многочлена (Завдання 16)
16. Знайти обернену матрицю у кільці/полі
17. Обчислити символ Лежандра/Якобі
18. Обчислити дискретний квадратний корінь за допомогою алгоритму Чіполи
19. Знайти всі генератори мультиплікативної групи поля
20. Знайти обернений многочлен у розширенні поля
21. Знайти круговий многочлен (Теорема 3.27, Лідл)
22. Знайти частковий розклад добутку незвідних многочленів через кругові (Теорема 3.31, Лідл)
23. Знайти порядок многочлена $f(x)$ у розширенні поля (мінімальне n таке що $(f(x))^n = 1$)
24. Обчислити суму двох точок P+Q на еліптичній кривій. Обчислити подвоювання точки P+P на еліптичній кривій
25. Проілюструвати передачу шифротексту за допомогою схеми Діффі-Геллмана (Приклад 232, AlgStructCrypto)
26. Проілюструвати передачу шифротексту за допомогою схеми RSA (Приклад 235, AlgStructCrypto)
27. Проілюструвати передачу шифротексту за допомогою схеми Ель-Гамаля (Приклад 238, AlgStructCrypto)