Контрольні питання. Необхідний мінімум.

1. Скінченні поля.
2. Група. Кільце. Поле.
3. Існування і єдиність скінченних полів.
4. Критерій підполя.
5. Циклічна група $\mathbb{F}_q^*$ поля $\mathbb{F}_q$. Примітивний елемент поля $\mathbb{F}_q$.
6. Побудова поля з p^n елементів (p —просте, $n \in \mathbb{N}$).
7. Лінійні шифри.
8. Обчислення в кільці $\mathbb{Z}_n$.
9. Алгоритм Евкліда знаходження найбільшого спільного дільника.
10. Шифрсистеми.
11. Шифрсистема RSA.
12. Проективні криві та площини.
13. Криві над скінченними полями.
14. Нормальна форма Вейєрштраса.
15. Група точок еліптичної кривої.

Елементарні задачі.

1. З'ясуйте, які з груп будуть циклічними: $\mathbb{Z}_8^*$, $\mathbb{Z}_{16}^*$, $\mathbb{Z}_9^*$, $\mathbb{Z}_{27}^*$? Для циклічних груп вкажіть які-небудь твірні елементи.
2. Знайдіть всі примітивні елементи полів $\mathbb{F}_7$, $\mathbb{F}_{19}$, $\mathbb{F}_9$, $\mathbb{F}_{16}$.
3. Знайдіть деякий примітивний елемент α поля $\mathbb{F}_{32}$ і для кожного елемента $\beta \in \mathbb{F}_{32}^*$ знайдіть найменше невід'ємне число n, для якого $\beta = \alpha^n$.
4. Покажіть, що факторкільце $F = \mathbb{Z}_3/(x^2 + x + 1)$ є полем. Знайдіть всі твірні елементи мультиплікативної групи F^* цього поля. Для одного з твірних побудуйте таблицю додавання 1.
5. Доведіть незвідність над $\mathbb{F}_2$ многочлена $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Побудуйте таблиці додавання і множення для простого розширення $\mathbb{F}_2(\Theta)$, де Θ — корінь многочлена $f(x)$.
6. Нехай $\alpha \in \mathbb{F}_8$ — корінь незвідного многочлена $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Знайдіть базис поля $\mathbb{F}_8$ над полем $\mathbb{F}_2$. Запишіть елементи поля $\mathbb{F}_8$ у вигляді лінійних комбінацій базисних елементів над полем $\mathbb{F}_2$.
7. Нехай перетворення $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ задане формулою $f(x) = 17x+15$. Знайдіть таке перетворення $g : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, що $f \circ g = \mathrm{id}$.
8. Нехай $P_1 = (-2, 3)$ та $P_2 = (-1, 4)$ — точки кубічної кривої $y^2 = x^3 + 17$. Знайдіть точки $2P_1$ та $P_1 + P_2$.
9. Нехай $y^2 = x^3 + x + 1$ — крива над полем $\mathbb{F}_5$. **Знайдіть раціональні точки на цій прямій. (Або так: Знайдіть групу $C(\mathbb{F}_5)$ раціональних точок цієї кривої).** Для точки $P = (0, 1)$ обчисліть $2P$, $3P$.