НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ім. ІВАНА ФРАНКА

ТЕХНІЧНИЙ КОЛЕДЖ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"

МАТЕРІАЛИ

XX Міжвузівської науково-практичної конференції

"Методичні проблеми викладання математики у вищих навчальних закладах"

ЛЬВІВ – 2017

Відповідальні за випуск:

к.пед.н. Васіна Людмила Степанівна **(Технічний коледж НУ "Львівська політехніка")**

к.ф.-м.н. Мохонько Валентина Дмитрівна **(Технічний коледж НУ "Львівська політехніка")**

Терехов Віктор Володимирович **(Технічний коледж НУ "Львівська політехніка")**

Матеріали XX Міжвузівської науково-практичної конференції "Методичні проблеми викладання математики у вищих навчальних закладах" / **"Українські технології", Методичні проблеми.: – Львів, 2017. – 105 с.**

ISBN 966-666-068-7

До збірника увійшли матеріали XX Міжвузівської науково-практичної конференції "Методичні проблеми викладання математики у вищих навчальних закладах", яка проходила 22 лютого 2017 року у Технічному коледжі Національного університету "Львівська політехніка".

ISBN 966-666-068-7

Точка O — центр зовні вписаного кола; ON, OK і OM— його радіуси, проведені в точку дотику. Тому $ON \perp AB, OK \perp BC$ і $OM \perp AC$. Точки N, K і M сполучаємо з вершиною S. Тоді $SN \perp AB, SM \perp AC, SK \perp BC$ (теорема про три перпендикуляри),

$\angle SNO = \angle SMO = \angle SKO = 45°. S_{ABC} = 540$ см^2.

Тоді

$$SO = r_{BC} = \frac{S}{p-a} = \frac{540}{54-39} = 36 \text{ (см)} \qquad V = \frac{1}{3} \cdot 540 \cdot 36 = 6480 \text{ см}^3.$$

3) Вершина піраміди проектується в центр зовні вписанного кола *(рис. 3)*, яке дотикається до основи AC і продовжень двох бічних сторін AB і BC.

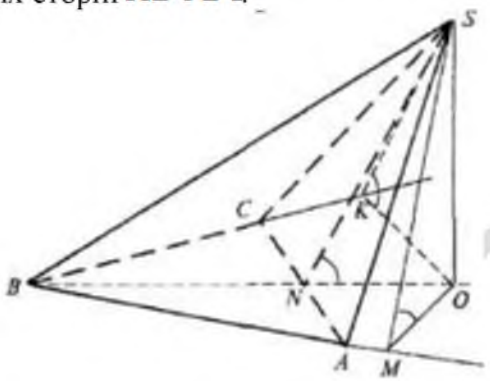

Рис. 3

Розв'язування аналогічне випадку 2):

$$SO = r_{AC} = \frac{S}{p-AC} = \frac{540}{54-30} = \frac{45}{2} \text{ (см)} \qquad V = \frac{1}{3} \cdot 540 \cdot \frac{45}{2} = 4050 \text{ см}^3.$$

СКІНЧЕНІ ПОЛЯ ТА ЇХ ПОБУДОВА

М.Ф. Стасюк, к.ф.-м.н., Р.М. Тацій, д.ф.-м.н.,
Львівський державний університет безпеки життєдіяльності

Теорія скінчених полів має широке застосування в криптографії. Відомо [1, 2], що є багато криптологічних протоколів і криптосистем, що базуються на застосуванні скінчених полів. Сюди відносяться схеми Ель-Гамаля, Advanced Encryption Standard, схема Шнорра, алгоритм Чаума, криптосистема XTR та ряд інших.

Дослідження многочленів над скінченими полями привели до створення коду БЧХ, частинним випадком якого є широко відомий код Ріда-Соломона,що має широке застосування.

В багатьох підручниках з алгебри [3] добре описані скінчені елементарні поля F_p характеристики $p > 0$ (p – просте ціле число), що складаються з p елементів . Такі поля можна інтерпретувати, як поля лишків за модулем p.

Складніше будувати скінчені поля, що складаються з p^n елементів. Конструкція таких полів базується на наступних твердженнях, які є наслідком цілого комплексу теорем алгебраїчної теорії скінчених полів [3, 4] .

1. Довільне скінчене поле має характеристику $p > 0$ і складається з p^n елементів.

2. Якщо $f(x)$ – незвідний многочлен $n-$го степеня, коефіцієнти якого належать полю F_p, а $\alpha-$його корінь, то $F_{p^n}=F_p(\alpha)-$ це лінійний простір розмірності n над полем F_p з базою $1,\alpha,\alpha^2,...,\alpha^{n-1}$, тобто

$$F_{p^n}=\left\{a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{n-1}\alpha^{n-1},\quad f(\alpha)=0\right\},\quad a_i\in F_p,\quad i=\overline{0,n-1}. \qquad (1)$$

3. Якщо $K-$ скінчене поле, що складається з p^n елементів, то його мультиплікативна група K^* – циклічна і породжена деяким елементом ξ, який називається *примітивним елементом* поля K, тобто $K^*=\left\{1,\xi,\xi^2,...,\xi^{p^n-1}\right\},\quad \xi^{p^n}=1.$

Число l примітивних коренів поля K визначене рівністю

$$l=\varphi\left(p^n-1\right), \qquad (2)$$

де $\varphi(x)-$ функція Ейлера.

На основі цих тверджень побудуємо конкретні скінчені поля, які використовуються в криптології.

Приклади побудови деяких скінчених полів

Приклад 1. *Побудувати поле* $F_9=F_{3^2}$.

Згідно твердження 2 для побудови поля F_9 потрібно знайти незвідний над F_3 многочлен $f(x)$ 2-го степеня. Таким многочленом є, наприклад, многочлен $f(x)=x^2+1$. Нехай $u-$ його корінь. Тоді за формулою (1) маємо

$$F_9=F_3(u)=\left\{a_0+a_1u,\quad a_0,a_1\in F_3,\quad u^2=2\right\}=\left\{0,1,2,u,2u,1+u,1+2u,2+u,2+2u\right\}.$$

Можна перевірити, що одним із примітивних елементів поля є $\xi=1+u$. Дійсно

$$\xi^0=1,\quad \xi^1=1+u,\quad \xi^2=1+2u+u^2=2u,$$

$$\xi^3=2u(1+u)=2u+2u^2=2u+1,\quad \xi^4=4u^2=2,\quad \xi^5=2(u+1)=2u+2,$$

$$\xi^6=2(u+1)^2=\mathrm{u},\quad \xi^7=u(u+1)=2+u.$$

Таким чином, степенями ξ вичерпані всі ненульові елементи поля F_9.

Зауважимо, що поле F_9 має чотири примітивні елементи, бо за формулою (2) $l=\varphi(8)=4$. Цими елементами є: $\xi=\xi_1=1+u,\quad \xi_2=1-u=1+2u,\quad \xi_3=2+u,\quad \xi_4=2-u=2+2u.$

Приклад 2. *Побудувати поле* $F_{16}=F_{2^4}$..

Використаємо незвідний многочлен 4-го степеня $f(x)=x^4+x+1$ над полем F_2 Нехай $\alpha-$ його корінь. Тоді за формулою (1), маємо

$$F_{16}=F_2(\alpha)=\left\{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3,\quad \alpha^4+\alpha+1=0\right\}=\left\{0,1,\alpha,1+\alpha,\alpha^2,1+\alpha^2,\alpha+\alpha^2,\right\}\cup$$

$$\cup\left\{1+\alpha+\alpha^2,\alpha^3,1+\alpha^3,1+\alpha+\alpha^3,\alpha^2+\alpha^3,1+\alpha^2+\alpha^3,\alpha+\alpha^2+\alpha^3,\alpha+\alpha^3,1+\alpha+\alpha^2+\alpha^3\right\}.$$

Легко перевірити, що один з примітивних елементів поля F_{16} – це $\xi=\alpha$. Іншими примітивними елементами поля є: $\alpha^2,1+\alpha,1+\alpha^2,1+\alpha+\alpha^3,\alpha+\alpha^2+\alpha^3,1+\alpha^2+\alpha^3,1+\alpha^3,$ оскільки за формулою (2) $l=\varphi(15)=8$.

Приклад 3. *Побудувати поле* $F_{49}=F_{7^2}$. Поле F_{7^2} є лінійним простором розмірності 2 над полем F_7. Побудуємо це поле, використавши незвідний многочлен 2-го степеня над полем F_7 – $P(X)=X^2+1$. Нехай $X-$ корінь многочлена $P(X)=X^2+1$. Тоді за формулою (1) отримаємо

$$F_{7^2}=\left\{a_0+a_1X,\quad a_0,a_1\in F_7,\quad X^2+1=0\right\}.$$

Можна переконатись, що мультиплікативна група поля F_{7^2} – циклічна група порядку 48 з примітивним елементом, наприклад, $\xi = 2X+1$. Дійсно,

$\xi^2 = 4X+4,\ \xi^3 = 5X+3,\ \xi^4 = 4X,\ \xi^5 = 4X+6,\ \xi^6 = 2X+5,\ \xi^7 = 5X+1\ \ \xi^8 = 5,$

$\xi^9 = 3X+5,\ \xi^{10} = 6X+6,\ \xi^{11} = 4X+1,\ \xi^{12} = 6X, \xi^{13} = 6X+2, \xi^{14} = 3X+4, \xi^{15} = 4X+5,$

$\xi^{16} = 4,\ \xi^{17} = X+4,\ \xi^{18} = 2X+2,\ \xi^{19} = 6X+5, \xi^{20} = 2X, \xi^{21} = 2X+3,\ \ \xi^{22} = X+6,$

$\xi^{23} = 6X+4,\ \xi^{24} = 6,\ \xi^{25} = 5X+6,\ \xi^{26} = 3X+3, \xi^{27} = 2X+4,\ \xi^{28} = 3X,$

$\xi^{29} = 3X+1,\ \xi^{30} = 5X+2,\ \xi^{31} = 2X+6,\ \xi^{32} = 2,\ \xi^{33} = 4X+2, \xi^{34} = X+1, \xi^{35} = 3X+6,$

$\xi^{36} = X,\ \xi^{37} = X+5,\ \xi^{38} = 4X+3,\ \xi^{39} = 3X+2,\ \xi^{40} = 3,\ \xi^{41} = 6X+3,\ \xi^{42} = 5X+5,$

$\xi^{43} = X+2,\ \xi^{44} = 5X,\ \xi^{45} = 5X+4,\ \xi^{46} = 6X+1,\ \xi^{47} = X+3,\ \xi^{48} = 1.$

Таким чином, ми перебрали всі 48 елементів мультиплікативної групи поля $F_{49} = F_{7^2}$, тобто побудували це поле.

Зауважимо, що в полі F_{7^2} існує за формулою (2) $l = \varphi(48) = 16$ примітивних елементів.

Список використаних джерел

1. Ю.С.Харин Математические основы криптологии / Ю.С.Харин, В.И. Берник, Г.В.Матвеев Учебн. Пособие – Мн. БГУ, 1999. – 319 с.
2. О.В.Вербіцький Вступ до криптології / О.В.Вербіцький. –Львів.: ВНТЛ, 1998. –246с.
3. А.И. Кострикин Введение в алгебру / А.И. Кострикин – М.:Наука.1977. – 492 с.
4. Я.В. Радыно Элементы алгебры для студентов-аналитиков / Я.В. Радыно, А.Я. Радыно, Е.М. Радыно –Гродно.: ГрГУ им. Я. Купалы, 2013. – 196 с.

Через паралельне проектування від геометрії площини до геометрії простору

Б.С. Кравець, викладач-методист,
Дрогобицький коледж нафти і газу

Вивчення теми стереометрії «Прямі і площини в просторі» викликає у більшості студентів затруднення. Вони полягають в тому, що крім виконання алгебраїчних дій і обчислень треба ще володіти просторовою уявою і просторовим мисленням.

Опираючись на власний досвід, хочу поділитись ним як можна покращити ефективність вивчання цієї теми, а в деяких випадках алгоритмізувати, а отже покращити вивчення всієї стереометрії.

Ключове полягає в тому, щоб на самих початках навчити студентів роботи те, що їм в подальшому доведеться робити чи не на кожному занятті, а саме. – як це не банально звучить, - розв'язувати прямокутні трикутники, але використовуючи їх образи при паралельному проектуванні. Але цьому повинне передувати повторення і відтворення основних понять з планіметрії.

А саме:

1) Означення медіани, бісектриси і висоти в трикутнику, їх властивості в рівносторонньому і рівнобічному трикутниках.
2) Висоти і медіани в прямокутному трикутнику.
3) Площа трикутника, трикутника рівностороннього і прямокутного.
4) Знаходження центрів і радіусів вписаного і описаного кіл для довільного трикутника і для прямокутного зокрема.
5) Означення синуса, косинуса, тангенса і котангенса гострого кута в прямокутному трикутнику.
6) Розв'язання прямокутного трикутника за гіпотенузою і гострим кутом та за катетом і гострим кутом.