Тема 3

https://github.com/v--/se2018

Полиноми на една променлива. Теорема за деление с остатък. Най-голям общ делител на полиноми - тъждество на Безу и алгоритъм на Евклид. Зависимост между корени и коефициенти на полиноми (формули на Виет).

Янис Василев

Оригинал: 15 юни 2019
Ревизия: 9c26f56 от 04 ноември 2024
За всеки случай проверете дали няма по-нова ревизия

1. Теория

Освен посочените в конспекта български книги на Сидеров и Чакърян, полезни са и ранната българска книга Обрешков, *Висша алгебра*, както и Генов, Миховски и Моллов, *Алгебра с теория на числата*. Някои твърдения и доказателства са заимствани от Knapp, *Basic Algebra* и Роячки, *Разписани лекции по висша алгебра*.

1.1. Анотация

Изложената анотацията е взета от *Конспект за ДИ за спец. статистика*.

1. Полином с коефициенти над поле.
2. Степен на полином.
3. Корени на полиноми.
4. Теорема за деление с остатък.
5. Схема на Хорнер.
6. Всеки идеал в $F[x]$ е главен.
7. Принцип за сравняване на коефициенти.
8. Определение на най-голям общ делител на два полинома.

9. Теорема за съществуване на най-голям общ делител на два полинома с коефициенти над поле.
10. Изразяване на НОД чрез полиномите (тъждество на Безу).
11. Алгоритъм на Евклид.
12. Формули на Виет.

1.2. Основни понятия

Нека F е фиксирано поле. За удобство ще означаваме с 0 и 1 съответно нулевият и единичният елемент на полето. Ще дефинираме полиноми като чисто алгебрични обекти вместо като функции. Причината за това е, че ако дефинираме полиноми като функции от вида[1]

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

тогава в общия случай една и съща функция може да се дефинира по няколко различни начина.

Например, в полето F_2 с два функциите x и x^2 съвпадат. Това ни пречи да говорим без двусмислица за „степен“, „старши член“, „коефициент“ на полином и подобни понятия.

Определение 1. Полином p на една променлива над F наричаме редица

$$p = (a_0, a_1, \ldots)$$

от елементи на F, наречени коефициенти, само краен брой от които са различни от 0. Ако всички елементи на редицата са нули, наричаме полинома нулев и също както нулевия елемент на полето го бележим с 0.

Степен $\deg(p)$ на полинома p наричаме най-големият индекс, съответстващ на ненулев коефициент. Формално,

$$\deg(p) := \max\Big\{k = 0, 1, \ldots \;\Big|\; a_k \neq 0\Big\}.$$

По конвенция оставяме степента $\deg(0)$ на нулевия полином да бъде неопределена (друг популярен вариант е да се положи $\deg(0)$ да бъде $-\infty$).

Старшият коефициент $\mathrm{LC}(p)$ на полинома p от степен n наричаме последната ненулева стойност в редицата от коефициенти и полагаме $\mathrm{LC}(p) := 0$.

Полинома p наричаме **унитарен**, ако $\mathrm{LC}(p) = 1$.

[1] Трябва да отбележим, че някои автори, сред които и Никола Обрешков в Обрешков, *Висша алгебра*, с. 1, предпочитат да означават с a_0 старшия коефициент, така че да имаме

$$p(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-2} x^2 + a_{n-1} x + a_n$$

Нека $p = (a_0, a_1, \ldots)$ и $q = (b_0, b_1, \ldots)$ са два полинома. Сума на p и q дефинираме покоординатно, т.е.

$$(p + q) = (a_0 + b_0, a_1 + b_1, \ldots),$$

а произведението им дефинираме като полинома $pq = (c_0, c_1, \ldots)$, където

$$c_k = \sum_{i+j=k} a_i b_j.$$

Забележка 2. Това произведение се обобщава почти без изменение за т. нар. „групови алгебри“ („group algebra/ring“), където в някои случаи се нарича „конволюция“. За справка в.ж. Rotman, *Advanced Modern Algebra*, пример B-1.1.

Сумата на ненулеви полиноми $p + q$ е полином, при това $p + q$ или е нулевият полином, или $\deg(p+q) \leq \max(\deg(p), \deg(q))$. Произведението на ненулеви полиноми е ненулев полином, при това $\deg(pq) = \deg p + \deg q$.

Полиноми със само един ненулев коефициент наричаме **мономи**.

Нека сега изберем символ, да речем X, с който ще означаваме монома $(0, 1, 0, 0, \ldots)$ (в забележка 3 ще дискутираме малко по-подробно ролята на X). Забелязваме, че от определението за умножение на полиноми, може да изразим коефициентите $c_0, c_1, \ldots$ на $X^2 = X \cdot X$ чрез коефициентите $a_0, a_1, \ldots$ на X като

$$\begin{aligned}
c_0 &= a_0 \cdot a_0 = 0 \\
c_1 &= a_0 \cdot a_1 + a_1 \cdot a_0 = 0 + 0 = 0 \\
c_2 &= a_0 \cdot a_2 + a_1 \cdot a_1 + a_2 \cdot a_0 = 0 + 1 + 0 = 1 \\
c_3 &= a_0 \cdot a_3 + a_1 \cdot a_2 + a_2 \cdot a_1 + a_0 \cdot a_3 = 0 + 0 + 0 + 0 = 0 \\
c_4 &= \cdots = 0 \\
c_5 &= \cdots = 0 \\
&\vdots
\end{aligned}$$

По индукция така получаваме, че

$$X^k = (\underbrace{0, \ldots, 0}_{k \text{ пъти}}, 1, 0, 0, \ldots).$$

За удобство полагаме $X^0 := 1$. Това ни позволява да записваме ненулевите полиноми $p = (a_0, a_1, \ldots)$ от степен $\deg(p) = n$ като линейна комбинация на мономи:

$$p(X) = \sum_{k=0}^{n} a_k X^k.$$

За променливата сме избрали главна буква, за да подчертаваме, че $p(X)$ не е функция. Бележим с $F[X]$ множеството на всички полиноми над F с променлива X.

Относно въведените операции $F[X]$ е комутативен пръстен с единица 1, тъй като

1. $F[X]$ наследява нулата си 0 и единицата си 1 от полето F.

2. Събирането на произволни полиноми наследява асоциативността и комутативността си директно от събирането в полето F.

3. Ако $p(X) = \sum_{k=0}^{n} a_k X^k$, то $-p(X) = \sum_{k=0}^{n} (-a_k) X^k$ е обратен на $p(X)$ относно събиране.

4. Произведението на ненулеви полиноми $p = (a_0, a_1, \ldots)$, $q = (b_0, b_1, \ldots)$ и $r = (c_0, c_1, \ldots)$ е асоциативно, тъй като

$$\sum_{k+m=n} \left(\sum_{i+j=k} a_i b_j \right) c_m = \sum_{i+j+m=n} a_i b_j c_m = \sum_{i+l=n} a_i \left(\sum_{j+m=l} b_j c_m \right),$$

   където всички индекси са неотрицателни цели числа.

5. Произведението на ненулеви полиноми наследява комутативността си и дистрибутивността си относно събирането директно от полето F.

Това ни позволява да разглеждаме F като подпръстен на $F[X]$ и да разглеждаме $F[X]$ като алгебра над полето F.

Нулевият полином и полиномите от степен 0 наричаме константи и чрез каноничната проекция $\pi : (a_0, 0, \ldots) \mapsto a_0$ ги отъждествяваме с първия им коефициент. Аналогично, каноничното влагане $\iota : a_0 \mapsto (a_0, 0, \ldots)$ влага F във $F[x]$.

Нека $(F \mapsto F)$ е пръстенът от функции над F с операция композиция. Дефинираме хомоморфизма

$$\Phi : F[X] \mapsto (F \mapsto F)$$
$$\Phi((a_0, a_1, \ldots, a_n, 0, 0, \ldots)) := \left(u \mapsto \sum_{k=0}^{n} a_k u^k \right),$$

който на всеки полином съпоставя **полиномиална функция**. Както споменахме по-горе, този хомоморфизъм в общия случай не е инективен. Когато имаме предвид функцията $x \mapsto \Phi(p)(x)$ вместо редицата от коефициенти p, ще пишем $p(x)$, като подобно означение ще използваме за стойността $p(u)$ на функцията $p(x)$ пресметната в точката u.

Забележка 3. В известен смисъл полиномите са синтактични обекти и от тази гледна точка X не е просто символ, защото играе ролята на променлива в смисъла на логиката и информатиката.

Формално това може да се изрази с твърдението, че пръстенът $F[X]$ е „свободната комутативна алгебра“ над F породена от X. Доказателство, както и съответните формализми, могат да бъдат намерени в Rotman, *Advanced Modern Algebra*, теорема 1-3.25.

Грубо казано, такава алгебра е пръстен, чиито елементи можем да умножаваме с елементите на F (по-точно е линейно пространство с комутативна билинейна операция, която превръща линейното пространство в пръстен). Прилагателното „свободна“ означава, че елементите на $F[X]$, т.е. полиномите над F с променлива X, са способни да опишат как взаимодействат елементите на всяка друга свободна комутативна алгебра над F породена от X.

1.3. Делимост на полиноми

Теорема 4 (Делене с остатък). *Нека са дадени полиномите*

$$p(X) = \sum_{k=0}^{n} a_k X^k \qquad \text{и} \qquad q(X) = \sum_{k=0}^{m} b_k X^k,$$

където $q(X) \neq 0$. *Тогава съществуват единствени полиноми* $s(X)$ *и* $r(X)$, *където* $r(X) = 0$ *или* $\deg(r) < m$, *такива че*

$$p = sq + r.$$

Доказателство.

Доказателство на единственост. Нека

$$p = sq + r = \hat{s}q + \hat{r}.$$

Тогава

$$0 = p - p = (s - \hat{s})q + (r - \hat{r})$$

и

$$(s - \hat{s})q = \hat{r} - r.$$

Тъй като $q \neq 0$, то $s - \hat{s} = 0$ тогава и само тогава, когато $\hat{r} - r = 0$. Ако сега допуснем, че $\hat{r} \neq r$ (и следователно $\hat{s} \neq s$), получаваме, че

$$\deg[(s - \hat{s})q] = \deg(s - \hat{s}) + m > m.$$

Но по условие имаме

$$\deg(\hat{r} - r) \leq \max(\deg \hat{r}, \deg r) < m.$$

Тъй като степента на полинома в двете страни на равенството трябва да бъде равна, получаваме противоречие от допускането, че $\hat{r} \neq r$. Следователно $r = \hat{r}$ и $s = \hat{s}$.

Доказателство на съществуване. Ако $n < m$, полагаме $s(X) \coloneqq 0$ и $r(X) \coloneqq p(X)$.

Остава случаят $n \geq m$. Ще докажем теоремата с индукция по n.

При $n = 0$ полагаме $s(X) \coloneqq b_0/a_0$ и $r(X) \coloneqq 0$. Да предположим, че теоремата е вярна за всички полиноми със степен по-малка от n и да положим

$$g(X) \coloneqq \frac{a_n}{b_m} X^{n-m} q(X).$$

Тъй като $\deg(p) = \deg(g)$ и $\mathrm{LC}(p) = \mathrm{LC}(g)$, то $\deg(p - g) < \deg(p) = n$ и индукционното предположение ни дава полиноми $\hat{s}$ и $\hat{r}$, такива че $p - g = \hat{s}q + \hat{r}$ и $\hat{r} = 0$ или $\deg(\hat{r}) < m$. Но ние имаме

$$p(X) = g(X) + \hat{s}(X)q(X) + \hat{r}(X) = \left(\frac{a_n}{b_m} X^{n-m} + \hat{s}(X)\right) q(X) + \hat{r}(X).$$

Полагаме

$$s(X) := \hat{s}(X) + \frac{a_n}{b_m} X^{n-m},$$
$$r(X) := \hat{r}(X).$$

Очевидно $\deg(r) = \deg(\hat{r}) < m$. С това и съществуването е доказано. □

Определение 5. Казваме, че полиномът $q \in F[X]$ **дели** $p \in F[X]$ и че p е **кратен** на q, ако съществува ненулев полином $s \in F[X]$, такъв че $p = sq$, т.е. ако алгоритъмът за делене с остатък дава нулев остатък.

Множеството от всички полиноми, кратни на q, образува идеал $\langle q \rangle$ на пръстена $F[X]$. Теорема 6 ни казва, че всеки идеал на $F[X]$ е от този вид.

Полиномът q дели p тогава и само тогава, когато p да принадлежи на идеала $\langle q \rangle$.

Теорема 6. *Всеки идеал в $F[X]$ е главен.*

Доказателство. Нулевият идеал $\langle 0 \rangle$ очевидно е главен. Нека I е ненулев идеал и нека $q \in I$ е полином от минимална за I степен. Ще докажем, че идеалът $\langle q \rangle$, породен от q, съвпада с I.

Нека първо $p \in \langle q \rangle$. Тогава съществува полином $s(X)$, за който $p = sq$. Но тъй като $q \in I$, то $p = sq \in I$. Тоест $\langle q \rangle \subseteq I$.

Нека сега $p \in I$. Теоремата за делене с остатък ни дава полиноми s и r с $r = 0$ или $\deg r < \deg q$, такива че $p = qs + r$. Но понеже I е затворен относно събиране, имаме $r = p - qs \in I$. Ако r е ненулев, то $\deg r < \deg q$, което противоречи на минималността на q. Значи $r = 0$ и $p = qs \in \langle q \rangle$. Тоест $I \subseteq \langle q \rangle$.

Доказахме, че $I = \langle q \rangle$. Понеже I беше произволен ненулев идеал, това означава, че всеки идеал на $F[X]$ е главен. □

1.4. Корени

Определение 7. Корен на полинома $p(X)$ наричаме всяка стойност $u \in F$, за която съответната функция се анулира, т.е. за която $p(u) = 0$.

Твърдение 8. *Полиномът $(X - u)$ дели ненулевия полином $p(X)$ тогава и само тогава, когато u е корен на p.*

Доказателство.

Доказателство на достатъчност. Ако $(X - u)$ дели $p(X)$, то $p(X) \in \langle X - u \rangle$. Тъй като u е корен на полинома $(X - u)$, той е корен и на всички полиноми от идеала $\langle X - u \rangle$ и значи u е корен на $p(X)$.

Доказателство на необходимост. Нека u е корен на $p(X)$.

Теорема 4 ни дава полиноми $q(X)$ и $r(X)$, където или $r(X) = 0$, или $\deg r < \deg b$, такива че

$$p(X) = (X - u)q(X) + r(X).$$

Да допуснем, че полиномът $r(X)$ е ненулев. Стойността на $p(X)$ в u е

$$0 = p(u) = (u - u)q(r) + r(u) = r(u),$$

следователно u е корен и на $r(X)$. Но $\deg r(X) < \deg(X - u) = 1$, тоест $r(X)$ е ненулев константен полином и $r(X)$ не може да има нули. Полученото противоречие доказва твърдението. □

Лема 9. *Ненулев полином от степен n има най-много n корена, броейки кратностите.*

Доказателство. Ще използваме индукция по степента n. В случая $n = 0$ имаме ненулев константен полином, а такъв полином не може да има корени, т.е. има най-много 0 корена.

Да допуснем, че твърдението е вярно за $n - 1$. Нека $p(X)$ е полином от степен n и нека u е негов корен. От твърдение 8 следва, че $X - u$ дели $p(X)$. Тогава съществува полином $q(X)$ от степен $n - 1$, такъв че

$$p(X) = (X - u)q(X).$$

Фиксираме елемент $t \in F$, различен от u и от корените на $q(X)$. Разглеждаме

$$p(t) = (t - u)q(t).$$

Имаме $(t - u) \neq 0$ и $q(t) \neq 0$. Понеже F няма делители на нулата, произведението $p(t)$ на ненулевите елемент $(t - u)$ и $q(t)$ също е ненулев елемент. Следователно единствените корени на $p(X)$ са u и корените на $q(X)$.

По индукционно предположение, $q(X)$ има най-много $n - 1$ корена, броейки кратностите. Следователно $p(X)$ има най много $(n - 1) + 1 = n$ корена. □

Теорема 10 (Принцип за сравняване на коефициентите)**.** *Нека $p(X)$ и $q(X)$ са полиноми от степен n над F и нека $u_0, \ldots, u_n$ са различни елементи на F (това изисква в полето има поне $n + 1$ елемента). Ако $p(u_i) = q(u_i)$ за всички $i = 0, \ldots, n$, то полиномите p и q съвпадат.*

Доказателство. Разликата $r(X) \coloneqq p(X) - q(X)$ е полином от степен най-много n, който има $n + 1$ корена — стойностите $u_0, u_1 \ldots, u_n$. Според лема 9, това не е възможно за ненулев полином. Тоест $r = 0$ и $p(X) = q(X)$. □

1.5. Схема на Хорнер

Забележка 11. Има определени разногласия относно кое именно е „правилото на Хорнер“.

Самият Уилиам Хорнер в Horner, „XXI. A new method of solving numerical equations of all orders, by continuous approximation“ описва метод за търсене на корени. Методът му в контекста на трансформиране на уравнения е описан в Обрешков, *Висша алгебра*, §III.V.2 като „правило на Хорнер“.

От друга страна Доналд Кнут (чиято терминология е широко разпространена сред информатиците) в Knuth, *The Art of Computer Programming*, с. 486 нарича „Horner's rule“ („правилото на Хорнер“) представянето

$$p(X) = \sum_{k=0}^{n} a_k X^k = a_0 + X(a_1 + \cdots + X(a_{n-1} + Xa_n) + \cdots), \tag{1}$$

разгледано от гледна точка на изчислителната сложност — то изисква n умножения и n събирания, докато директното пресмятане на $p(u)$ изисква $n(n+1)/2$ умножения и n събирания.

Както ще видим, (1) като правило за пресмятане на стойностите на полином наистина е обосновано от рекурсията (2), която обаче е само част от метода на Хорнер.

Нека сега разделим полинома

$$p(X) = \sum_{k=0}^{n} a_k X^k,$$

на $X - u$:

$$p(X) = (X - u)q(X) + r(X).$$

Нека означим с $b_0, b_1, \ldots, b_{n-1}$ коефициентите на $q(X)$. Според теорема 4 остатъкът $r(X)$ е константа. Ще бележим тази константа с b_{-1}. Тогава за неотрицателни цели k имаме

$$a_k = b_{k-1} - ub_k$$

и съответно

$$b_{k-1} = a_k + ub_k.$$

Това води до следната рекурсия:

$$b_{-1} = a_0 + ub_0 = a_0 + u(a_1 + ub_1) = a_0 + u(a_1 + u(a_2 + b_2)) = \cdots = \sum_{k=0}^{n} a_k u^n = p(u), \tag{2}$$

която при ръчно смятане е прието да се записва в табличен вид:

$$\begin{array}{c|cccccc} & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ u & b_{n-1} & b_{n-2} & \cdots & b_0 & b_{-1} \end{array}$$

Например, за $p(X) = X^3 + 6$ и $u = -2$ таблицата има вида

$$\begin{array}{c|cccc} & 1 & 0 & 0 & 6 \\ -2 & 1 & \underbrace{0 + (-2) \cdot 1}_{-2} & \underbrace{0 + (-2) \cdot (-2)}_{4} & \underbrace{6 + (-2) \cdot 4}_{-2} \end{array}$$

Освен че така намираме стойността $p(-2)$, ние получаваме и коефициентите на частното и остатъка на $p(X)$ разделено на $X + 2$:

$$p(X) = (X + 2)(X^2 - 2X + 4) - 2.$$

Нещо повече, посредством последователно делене можем да намерим и резултата от субституцията на X с $X+2$:

	1	0	0	6
-2	1	-2	4	-2
-2	1	-4	12	
-2	1	-6		
-2	1			

Така получаваме

$$p(X+2) = (X+2)^3 - 6(X+2)^2 + 12(X+2) - 2.$$

1.6. Най-голям общ делител на полиноми

Определение 12. Нека фиксираме два полинома p и q над полето F. Казваме, че d е **най-голям общ делител** (НОД) на p и q, ако d дели p и q и ако всеки общ делител на p и q дели d.

Тъй като всички НОД на p и q се различават по умножение с ненулева константа, за определеност въвеждаме означението $\gcd(p,q)$ за унитарния НОД.

Казваме, че полиномите p и q са **взаимно прости**, ако $\gcd(p,q) = 1$.

Оставяме НОД на два нулеви полинома да бъде неопределен.

Теорема 13. *За всеки два полинома p и q над F съществува единствен с точност до умножение с ненулева константа най-малък общ делител.*

Доказателство. От теорема 6 следва, че идеалът $I = \langle p \rangle + \langle q \rangle$ е главен, т.е. съществува унитарен полином $d \in I$, който го поражда.

Тогава d е общ делител на p и q. Но $d \in I$, следователно съществуват полиноми u и v, такива че

$$up + vq = d.$$

Тъй като $\langle g \rangle$ съдържа p и q за всеки общ делител g, имаме $d = up + vq \in \langle g \rangle$, т.е. g дели d. Ако $\deg g = \deg d$, то те се различават с ненулева константа.

Тогава d е най-голям общ делител на p и q. □

Като част от горното доказателство ние доказахме и следната

Теорема 14 (Тъждество на Безу)**.** *За всеки два полинома p и q над поле съществуват полиноми u и v, такива че*

$$up + vq = \gcd(p,q).$$

Ако $p = 0$ и $q \neq 0$, имаме $\gcd(p,q) = p$ (и обратно). За ненулеви полиноми имаме явен алгоритъм за намиране на НОД.

Теорема 15 (Алгоритъм на Евклид). *Нека p и q са ненулеви полиноми над поле F. Полагаме*

$$f_{-1} \coloneqq p \qquad \text{и} \qquad f_0 \coloneqq q.$$

Алгоритъм на Евклид (k-та стъпка; $k \geq 1$): Деленето с остатък ни дава полиноми g_k и f_k, такива че $f_{k-2} = f_{k-1}g_k + f_k$.

1. *Ако $f_k = 0$, то f_{k-1} е НОД на p и q и алгоритъмът приключва.*
2. *Ако $f_k \neq 0$ и $\deg f_k < \deg f_{k-1}$, преминаваме към стъпка $k+1$.*

Твърдим, алгоритъмът приключва след краен брой стъпки и че резултатът му е НОД на p и q.

Доказателство. Броят стъпки е ограничен от степените на p и q тъй като на стъпка $k \geq 1$, ако f_k още не е 0, то $\deg f_k < \deg f_{k-1}$ (възможно е обаче $\deg f_0 > \deg f_{-1}$).

Нека $m \geq 1$ е последният индекс за който $f_m \neq 0$. С индукция по $i = 0, \dots, m+1$ ще докажем, че f_m дели f_{m-i}:

- Очевидно f_m дели f_m.
- Тъй като $f_{m-1} = g_m f_m + f_{m+1}$ и по построение $f_{m+1} = 0$, оттук следва, че f_m дели f_{m-1}.
- Нека допуснем, че f_m дели $f_{m-(k-1)}$ и $f_{m-(k-2)}$. Тогава

$$f_{m-k} = g_{m-k+1}f_{m-k+1} + f_{m-k+2} = f_m\Big(g_{m-k+1}\frac{f_{m-k+1}}{f_m} + \frac{f_{m-k+2}}{f_m}\Big).$$

Така доказахме, че f_m дели $p = f_{-1}$ и $q = f_0$.

Нека сега d е произволен общ делител на p и q. Тогава

$$f_1 = p - qg_1 = d\Big(\frac{p}{d} - g_1\frac{q}{d}\Big),$$

следователно d дели f_1. Със същото разсъждение и с индукция по $i = 1, \dots, m$ стигаме до извода, че d дели f_i, в частност g дели f_m. Следователно f_m е НОД на p и q □

1.7. Формули на Виет

Теорема 16 (Формули на Виет). *Нека над полето F е зададен унитарен полином*

$$p(X) = \sum_{k=0}^{n} a_k X^k$$

с положителна степен и нека всичките му корени $u_1, \dots, u_n$ (с евентуални повторения) са от F.

Тогава за $k = 1, \dots, n$ имаме следната връзка между коефициентите и корените на p:

$$a_{n-k} = a_n \cdot (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} u_{i_1} \dots u_{i_k}.$$

Доказателство. След като всички корени на p са във F, то p се разлага на линейни множители над $F[X]$, т.е.

$$p(X) = a_n(X - u_1) \cdots (X - u_n). \tag{3}$$

Ще докажем теоремата с индукция по $n = \deg p$. Базовият случай $n = 1$ е тривиален, тъй като тогава $p(X) = (X - u_1)$ и $a_0 = -u_1$.

Нека теоремата е вярна за всички полиноми от степен $n - 1$. Ще докажем теоремата за полинома (3).

Индукционното предположение е изпълнено за

$$q(X) \coloneqq (X - u_1) \cdots (X - u_{n-1}).$$

Нека означим коефициентите на $q(X)$ с $b_0, \ldots, b_{n-1}$. От правилото на Хорнер, за всички коефициенти на $p(X)$ имаме

$$a_k = b_{k-1} - u_n b_k,$$

където $b_{-1} = 0$.

Тогава от индукционното предположение за $k = 0 = (n - 1) - (n - 1)$ имаме

$$a_{n-n} = a_0 = b_{-1} - u_n b_0 = u_n \prod_{k=0}^{n-1} u_k = \prod_{k=0}^{n} u_k$$

и, при $0 < k < n$, от индукционното предположение за k и за $k + 1$ имаме

$$\begin{aligned}
a_{n-k} &= b_{n-k-1} - u_n b_{n-k} = \\
&= b_{(n-1)-k} - u_n b_{(n-1)-(k-1)} = \\
&= a_n \cdot (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n-1} u_{i_1} \ldots u_{i_k} - u_n \cdot a_n \cdot (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_{k-1} \le n-1} u_{i_1} \ldots u_{i_{k-1}} = \\
&= a_n \cdot (-1)^k \left(\sum_{1 \le i_1 < \cdots < i_k \le n-1} u_{i_1} \ldots u_{i_k} + \sum_{1 \le i_1 < \cdots < i_{k-1} \le n-1} u_{i_1} \ldots u_{i_{k-1}} u_n \right) = \\
&= a_n \cdot (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} u_{i_1} \ldots u_{i_k}.
\end{aligned}$$

□

2. Примерни задачи

Условията на представените задачи са взети от Каспарян, *Примерни задачи за полиноми за спец. КН*.

2.1. Анотация

1. Намиране на НОД на два полинома - алгоритъм на Евклид, тъждество на Безу
2. Прилагане на формулите на Виет за полином с числови коефициенти

2.2. Най-голям общ делител на полиноми

Задача 1.

1. *Да се намери най-големият общ делител $d(X)$ на полиномите*

$$f(X) \coloneqq X^3 + X^2 + X + 1,$$
$$g(X) \coloneqq X^2 - X + 2.$$

2. *Да се намерят полиноми $u(X)$ и $v(X)$, за които е изпълнено тъждеството на Безу*

$$d(X) = f(X)u(X) + g(X)v(X).$$

Решение.

1. Делим $f(X)$ на $g(X)$:

$$\begin{array}{r|l} & X+2, \\ \hline X^3 + X^2 + X + 1 & \\ -X^3 + X^2 - 2X & \\ \hline 2X^2 - X + 1 & \\ -2X^2 + 2X - 4 & \\ \hline X - 3 & \end{array}$$

Делим $g(X)$ на $f_1(X) \coloneqq X - 3$:

$$\begin{array}{r|l} & X+2, \\ \hline X^2 - X + 2 & \\ -X^2 + 3X & \\ \hline 2X + 2 & \\ -2X + 6 & \\ \hline 8 & \end{array}$$

Полиномът $f_2(X) \coloneqq 8$ дели $f_1(X)$, следователно $d(X) = f_2(X) = \gcd(f, g) = 8$ и $f(X)$ и $g(X)$ са взаимно прости.

2. Изразяваме остатъците от деленето при алгоритъма на Евклид:

$$\begin{aligned} f_1(X) &= f(X) - (X+2)g(X), \\ d(X) &= g(X) - (X+2)f_1(X) = \\ &= g(X) - (X+2)[f(X) - (X+2)g(X)] = \\ &= (X+2)f(X) + [(X+2)^2 + 1]g(X) = \\ &= \boxed{(X+2)f(X) + (X^2 + 4X + 5)g(X)}. \end{aligned}$$

□

2.3. Формули на Виет

Задача 2. *За кои стойности на параметъра $p \in \mathbb{R}$ корените $u_1, \dots, u_4$ на полинома*

$$f(X) = X^4 - 8X^3 + 22X^2 + pX + 16$$

изпълняват равенството $u_1 + u_2 + u_3 = u_4$?

Решение. Заместваме $u_4 = u_1 + u_2 + u_3$ във формулите на Виет:

$$\begin{aligned} 8 &= (u_1 + u_2 + u_3) + u_4 = 2u_4 = 8 \\ &\implies u_4 = 4, \end{aligned}$$

$$\begin{aligned} 22 &= u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4 = \\ &= u_1u_2 + u_1u_3 + u_2u_3 + (u_1 + u_2 + u_3)u_4 \\ &\implies u_1u_2 + u_1u_3 + u_2u_3 = 6, \end{aligned}$$

$$\begin{aligned} -p &= u_1u_2u_3 + u_1u_2u_4 + u_1u_3u_4 + u_2u_3u_4 = \\ &= u_1u_2u_3 + (u_1u_2 + u_1u_3 + u_2u_3)u_4 \\ &\implies u_1u_2u_3 = -p - 24, \end{aligned}$$

$$\begin{aligned} 16 &= (u_1u_2u_3)u_4 \\ &\implies (-p - 24)4 = 16 \implies p = -28. \end{aligned}$$

□

3. Литература

Horner, William George. „XXI. A new method of solving numerical equations of all orders, by continuous approximation“. Англ. В: *Philosophical Transactions of the Royal Society of London* 109 (31 дек. 1819), с. 308—335. ISSN: 0261-0523. DOI: 10.1098/rstl.1819.0023.

Knapp, Anthony. *Basic Algebra*. Англ. Digital Second Edition. 2016. URL: http://www.math.stonybrook.edu/~aknapp/.

Knuth, Donald. *The Art of Computer Programming. Seminumerical Algorithms*. Англ. 3-е изд. Т. 2. Addison-Wesley, 1997. ISBN: 978-0-201-89684-8.

Rotman, Joseph J. *Advanced Modern Algebra*. Англ. Т. 1. Graduate Studies in Mathematics 165. American Mathematical Society, 30 ноем. 2015. ISBN: 978-1-4704-1554-9.

Генов, Георги, Стоил Миховски и Тодор Моллов. *Алгебра с теория на числата*. Наука и изкуство, 1991.

Каспарян, Азнив. *Примерни задачи за полиноми за спец. КН*. 2015. URL: https://my.pcloud.com/publink/show?code=kZEsNWZ85cYym2f0jh9ryV05aw254DQvlUV#folder=31576956 (дата на посещ. 14.06.2019).

Конспект за ДИ за спец. статистика. 2018. URL: https://intranet.fmi.uni-sofia.bg/index.php/s/KOTdUnmqbrnd0sX (дата на посещ. 24.03.2019).
Обрешков, Никола. *Висша алгебра*. 5-е изд. Наука и изкуство, 1962.
Роячки, Александър. *Разписани лекции по висша алгебра*. 2013. URL: https://debian.fmi.uni-sofia.bg/study/materials/va/lectures/ (дата на посещ. 04.07.2019).