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: 91d5bc9 от 09 юни 2021
За всеки случай проверете дали няма по-нова ревизия

1. Теория

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

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

тогава в общия случай една и съща функция може да се дефинира по няколко различни начина. Например, в полето F_2 с два елемента, имаме равенството

$$x^2 = x, x \in \{0, 1\},$$

тоест $x \mapsto x^2$ и $x \mapsto x$ съвпадат като функции.

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

$$p = (a_0, a_1, ...)$$

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-малкия индекс, след който всички елементи на редицата са 0. Формално,

$$\deg(p) := \min\left\{k \in \{0, 1, ...\} \;\middle|\; a_{k+m} = 0 \text{ за всички } m = 1, 2, ...\right\}.$$

По конвенция оставяме степента $\deg(0)$ на нулевия полином да бъде неопределена, макар и горната дефиниция да ни дава $\deg(0) = 0$.

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 $\mathrm{LC}(p) = 1$.

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

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

а произведението им дефинираме като полинома $pq = (c_0, c_1, ...)$, където:

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

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 $(0, 1, 0, 0, ...)$. Забелязваме, че от определението за умножение на полиноми, може да изразим коефициентите $c_0, c_1, ...$ на $X^2 = X \cdot X$ чрез коефициентите $a_0, a_1, ...$ 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

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

За удобство полагаме $X^0 := 1$. Това ни позволява да записваме ненулевите полиноми $p = (a_0, a_1, ...)$ 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 със свободна 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 $p = (a_0, a_1, ...)$, $q = (b_0, b_1, ...)$ и $r = (c_0, c_1, ...)$ 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 $\pi : (a_0, 0, ...) \mapsto a_0$ ги отъждествяваме с първия им коефициент. Аналогично, каноничното влагане $\iota : a_0 \mapsto (a_0, 0, ...)$ влага F във $F[x]$.

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

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

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.

1.3. Делимост на полиноми

Теорема 2 (Делене с остатък)**.** *Нека са дадени ненулевите полиноми* $p(X) = \sum_{k=0}^{n} a_k X^k$ *и* $q(X) = \sum_{k=0}^{m} b_k X^k$*, където* $q(X) \neq 0$*. Тогава съществуват единствени полиноми* s *и* r*, където* $r = 0$ *или* $\deg(r) < m$*, такива че*

$$p = sq + r.$$

Доказателство. Първо ще докажем единствеността. 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 $s - \hat{s} = 0 \iff \hat{r} - r = 0$. 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 $\deg(\hat{r} - r) \leq \max(\deg \hat{r}, \deg r) < m$. 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 $s = \hat{s}$.

Сега ще докажем съществуване. Ако $n < m$, полагаме $s(X) := 0$ и $r(X) := p(X)$. Нека $n \geq m$. Ще докажем теоремата с индукция по n. Случаят $n = 0$ е тривиален, тъй като тогава полагаме $s(X) := \frac{b_0}{a_0}$ и $r(X) := 0$. Да предположим, че теоремата е вярна за всички полиноми с $\deg < n$ и да означим $g(X) := \frac{a_n}{b_m} X^{n-m} q(X)$.

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 $s(X) := \hat{s}(X) + \frac{a_n}{b_m}X^{n-m}$ и $r(X) := \hat{r}(X)$. Очевидно $\deg(r) = \deg(\hat{r}) < m$. С това и съществуването е доказано. □

Определение 3. 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 4 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 $\langle q \rangle \lhd F[X]$.

Теорема 4. *Всеки идеал в $F[X]$ е главен.*

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

Нека първо $p \in \langle q \rangle$. Тъй като идеалът $\langle q \rangle$ е устойчив относно умножение, то съществува полином $s \in F[X]$, 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. □

Определение 5. 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 6. *Полиномът $(X - u)$ дели ненулевия полином $p(X) \in F[X]$ 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 2 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. □

Твърдение 7. *За всеки полином $p(X) \in F[X]$ и за всеки скалар $u \in F$ съществува полином $q(X)$ със степен $\deg q < \deg p$, за който $p(X) = (X - u)q(X) + p(u)$.*

Доказателство. Тъй като u непременно е корен на $p(X) - p(u)$, по твърдение 6 полиномът $(X - u)$ дели $p(X) - p(u)$. Следователно съществува полином $q(X)$ със степен $\deg q < \deg p$, такъв че $p(X) - p(u) = (X - u)q(X)$. □

Твърдение 8. *Схемата (или правилото) на Хорнер за пресмятане на стойността на ненулевия полином p в дадена точка се дължи на следното представяне на $p(X)$:*

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

Доказателство. Формално правилото се основава на следното наблюдение:

Нека $u \in F$. Искаме да пресметнем $p(u)$. От твърдение 7 знаем, че съществува $q(X)$, така че

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

Ако $q(X)$ има представяне $\sum_{k=0}^{n-1} b_k X^k$, то

$$p(X) = (X - u) \sum_{k=0}^{n-1} b_k X^k + p(u),$$

$$\sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{n-1} b_k X^{k+1} - u \sum_{k=0}^{n-1} b_k X^k + p(u),$$

$$0 = (p(u) - u b_0 - a_0) + \sum_{k=1}^{n-1} (b_{k-1} - u b_k - a_k) X^k + (b_{n-1} - a_n) X^n$$

Като приравним коефициентите пред съответните едночлени, получаваме следната рекурентна зависимост за коефициентите $b_k, k = 0, \ldots, n - 1$:

$$\begin{cases} p(u) & = u b_0 + a_0 \\ b_{k-1} & = a_k + u b_k, k = 1, \ldots, n - 1 \\ b_{n-1} & = a_n. \end{cases}$$

Правилото на Хорнер изисква само n умножения и n събирания, докато директното пресмятане на $p(u)$ изисква $\frac{n(n+1)}{2}$ умножения и n събирания. □

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 корени.

Да допуснем, че твърдението е вярно за $1, \dots, n-1$. Нека $p \in F[X]$ е полином от степен n и нека r е негов корен. От твърдение 6 следва, че съществува полином $q(X)$ от степен $n-1$, такъв че

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

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

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

Имаме $(t - r) \neq 0$ и $q(t) \neq 0$. Понеже F няма делители на нулата, произведението $p(t)$ на ненулевите елемент $(t - r)$ и $q(t)$ също е ненулев елемент. Следователно единствените корени на $p(X)$ са r 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 и q са полиноми от степен n и нека $u_0, \dots, u_n \in F$ са различни скалари (това изисква в полето има поне $n+1$ елемента). Ако е изпълнено $p(u_i) = q(u_i), i = 0, \dots, n$, то полиномите p и q съвпадат.*

Доказателство. Дефинираме полинома $r := p - q$. Това е полином от степен най-много n, който има $n+1$ корена: стойностите $u_0, u_1, \dots, u_n$. Според лема 9, това не е възможно за ненулев полином. Тоест $r = 0$ и $p = q$. □

1.4. Най-голям общ делител на полиноми

Определение 11. Казваме, че един полином $d \in F[X]$ е **най-голям общ делител** (НОД) на $p \in F[X]$ и $q \in F[X]$ и пишем $d = \gcd(p, q)$, 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, ако не е казано иначе, за определеност взимаме $\gcd(p, q)$ да бъде унитарен.

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

Оставяме НОД на два нулеви полинома да бъде неопределен.

Теорема 12. *За всеки два полинома $p, q \in F[X]$ съществува единствен с точност до умножение с ненулева константа* $\gcd(p, q)$.

Доказателство. От теорема 4 следва, че идеалът $I = \langle p \rangle + \langle q \rangle \lhd F[x]$ 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 $u, v \in F[X]$, такива че $up + vq = d$.

Тогава за всеки общ делител g на p и q имаме $p, q \in \langle g \rangle$ и следователно $d = up + vq \in \langle g \rangle$, 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 13 (Тъждество на Безу)**.** *За всеки два полинома $p, q \in F[X]$ съществуват полиноми u и v, такива че $up + vq = \gcd(p, q)$.*

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

Теорема 14 (Алгоритъм на Евклид)**.** *Нека p и q са произволни ненулеви полиноми. Полагаме*

$$f_{-1} := p \qquad\qquad f_0 := q.$$

Алгоритъм на Евклид (k-та стъпка): Делението с остатък ни дава полиноми s и r, такива че $f_{k-2} = p_{k-1}s + r$.

1. *Ако $r = 0$, алгоритъмът приключва.*
2. *Ако $r \neq 0$ и $\deg r < \deg f_{k-1}$, полагаме $f_k := r$ и алгоритъмът преминава към стъпка $k + 1$.*

Твърдим, че така построената редица е крайна с дължина m, при това $\gcd(p, q) = f_m$.

Доказателство. Тъй като построяваме редица със строго намаляващи степени (с евентуално изключение $\deg f_{-1} < \deg f_0$), тази редица непременно е крайна. Нека m е дължината ѝ.

С индукция по $i = 2, \ldots, m+1$ ще докажем, че f_m дели f_{m-i}. Разглеждаме базовия случай $i = 2$:

1. $f_{m-1} = f_m s$ за някой полином s и значи f_m дели f_{m-1}.
2. $f_{m-2} = f_{m-1}t + f_m = f_m(st + 1)$ за някой полином t и значи f_m дели и f_{m-2}.

Сега допускаме, че f_m дели f_{m-j} за $j < i$. Но $f_{m-i} = f_{m-(i-1)}s + f_{m-(i-2)}$ за някой полином s и по индукционно предположение f_m дели $f_{m-(i-1)}$ и $f_{m-(i-2)}$, следователно f_m дели и f_{m-i}.

В частност, доказахме, че, f_m дели p и q.

Нека сега g е произволен общ делител на p и q, т.е. съществуват полиноми h_1 и h_2, така че $p = gh_1$ и $q = gh_2$. Тогава за някой полином s е изпълнено

$$f_1 = p - qs = gh_1 - gh_2 s = g(h_1 - h_2 s),$$

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

1.5. Формули на Виет

Теорема 15 (Формули на Виет)**.** *Нека е даден унитарен неконстантен полином $p(X) = \sum_{k=0}^{n} a_k X^k \in F[X]$ и нека всичките му корени $u_1, \dots, u_n$ (с евентуални повторения) са от F.*

Тогава $a_n = 1$ и за $k = 0, \dots, n-1$ имаме следната връзка между коефициентите и корените на полинома p:

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

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

$$p(x) = (X - u_1) \cdots (X - u_n).$$

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

Нека теоремата е вярна за всички полиноми от степен n и $p = (X - u_1) \cdots (X - u_{n+1})$. Полагаме

$$q(X) := (X - u_1) \cdots (X - u_n).$$

Нека коефициентите на q са $q = (b_0, \dots, b_n)$.

Индукционното предположение е изпълнено за $q(X)$ и освен това имаме връзката

$$\begin{aligned}
(X - u_{n+1}) q(X) &= (X - u_{n+1}) \sum_{k=0}^{n} b_k X^k = \\
&= \sum_{k=1}^{n+1} b_{k-1} X^k + \sum_{k=0}^{n} (-u_{n+1}) b_k X^k = \\
&= (-u_{n+1}) b_0 + \sum_{k=1}^{n} (b_{k-1} - u_{n+1} b_k) X^k + b_n X^{n+1} = \\
&= \sum_{k=0}^{n+1} a_k X^k = p(X).
\end{aligned}$$

Като приравним коефициентите пред съответните едночлени, получаваме

$$a_0 = (-u_{n+1})b_0 = (-u_{n+1})(-1)^n \sum_{1\le i_1<\cdots<i_n\le n} u_{i_1}\dots u_n = (-1)^{n+1}u_1\dots u_{n+1} =$$
$$= (-1)^n \sum_{1\le i_1<\cdots<i_n<i_{n+1}\le n+1} u_{i_1}\dots u_{n+1},$$

$$a_{n+1-k} = b_{n-k} - u_{n+1}b_{n+1-k} =$$
$$= (-1)^k \sum_{1\le i_1<\cdots<i_k\le n} u_{i_1}\dots u_{i_k} - u_{n+1}(-1)^{k-1} \sum_{1\le i_1<\cdots<i_{k-1}\le n} u_{i_1}\dots u_{i_{k-1}} =$$
$$= (-1)^k\left(\sum_{1\le i_1<\cdots<i_k\le n} u_{i_1}\dots u_{i_k} + u_{n+1}\sum_{1\le i_1<\cdots<i_{k-1}\le n} u_{i_1}\dots u_{i_{k-1}}\right) =$$
$$= (-1)^k \sum_{1\le i_1<\cdots<i_{k-1}\le n} u_{i_1}\dots u_{i_{k-1}}\left(\sum_{i_k=i_{k-1}+1}^{n} u_{i_k} + u_{n+1}\right) =$$
$$= (-1)^k \sum_{1\le i_1<\cdots<i_k\le n+1} u_{i_1}\dots u_{i_k},$$

$$a_{n+1} = b_n = 1.$$

□

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*

$$f(X) := X^3 + X^2 + X + 1,$$
$$g(X) := X^2 - X + 2.$$

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 $g(X)$:

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

Делим $g(X)$ на $f_1(X) := X - 3$:

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

Полиномът $f_2(X) := 8$ 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 $p \in \mathbb{R}$ кореният $u_1, \ldots, u_4$ 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

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

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).

Роячки, Александър. *Разписани лекции по висша алгебра*. 2013. URL: https://debian.fmi.uni-sofia.bg/study/materials/la/lectures/ (дата на посещ. 04.07.2019).