MATEMATIČKI VESNIK
4(17)(32),1980

Radojko M. Sekuloski

JEDAN ITERATIVNI POSTUPAK ZA JEDNOVREMENO ODREDJIVANJE k FAKTORA POLINOMA

(Primljeno 16. maja 1980)*)

1. U ovom radu se proširuju rezultati izloženi u [3]. Naime, u [3] S.Prešić izlaže jedan iterativni postupak za jednovremeno odredjivanje svih faktora polinoma. Ovde izlažemo jedan iterativni postupak za jednovremeno odredjivanje k faktora (neobavezno svih) polinoma.

Za ideju kao i za niz korisnih sugestija zahvaljujem se dr S.Prešiću.

2. Neka je $P = x^n + p_{n-1}x^{n-1} + \dots + p_1x + p_o$ polinom na polju kompleksnih brojeva čiji su $(k+1)$ faktori polinomi:

$$A = x^a + \alpha_{a-1}x^{a-1} + \dots + \alpha_o$$

$$B = x^b + \beta_{b-1}x^{b-1} + \dots + \beta_o$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$S = x^s + \lambda_{s-1}x^{s-1} + \dots + \lambda_o$$

$$Q = x^q + \delta_{q-1}x^{q-1} + \dots + \delta_o$$

gde je $n = a+b+\dots+s+q$.

Polazeći od $A_o, B_o, \dots, S_o$ 1) nizove (A_m), (B_m), $\dots$, (S_m), (Q_m) i $(\overline{Q}_m)$ odredjujemo iz uslova:

$$(1)\qquad (A_{m+1}-A_m)B_m\dots S_m\overline{Q}_m + A_m(B_{m+1}-B_m)\dots S_m\overline{Q}_m + \dots + A_mB_m\dots(S_{m+1}-S_m)\overline{Q}_m +$$
$$+ A_mB_m\dots S_m(Q_{m+1}-\overline{Q}_m) + A_mB_m\dots S_m\overline{Q}_m = P,\quad m = 0,1,2,\dots$$

gde je $\overline{Q}_m$ količnik polinoma P i $A_mB_m\dots S_m$.

1) Polinomi A_o, $B_o, \dots, S_o$ istog su oblika redom sa polinomima $A, B, \dots, S$.

*) Saopšteno 17. novembra 1977.

Pri tome tačna je sledeća lema:

LEMA. Ako postoje $\lim\limits_{m\to\infty} A_m$, $\lim\limits_{m\to\infty} B_m, \ldots, \lim\limits_{m\to\infty} S_m$, tada

1°. Postoji $\lim\limits_{m\to\infty} \bar{Q}_m$;

2°. Postoji $\lim\limits_{m\to\infty} Q_m$;

3°. Važi jednakost $\lim\limits_{m\to\infty} A_m \lim\limits_{m\to\infty} B_m \ldots \lim\limits_{m\to\infty} S_m \lim\limits_{m\to\infty} Q_m = P$,

t.j. $\lim\limits_{m\to\infty} A_m$, $\lim\limits_{m\to\infty} B_m, \ldots, \lim\limits_{m\to\infty} S_m$ i $\lim\limits_{m\to\infty} Q_m$ su faktori polinoma P.

Dokaz. 1°. Na osnovu pretpostavke i definicije polinoma $\bar{Q}_m$ zaključujemo da postoji $\lim\limits_{m\to\infty} \bar{Q}_m$.

2°. Na osnovu pretpostavke i dokazanog u 1° po prelasku na lim iz uslova *(1)* dobijamo:

$$\lim_{m\to\infty} A_m \lim_{m\to\infty} B_m \ldots \lim_{m\to\infty} S_m \lim_{m\to\infty} Q_{m+1} = P,$$

odakle zaključujemo da postoji $\lim\limits_{m\to\infty} Q_m$ kao i da važi jednakost iz 3°. Odnosno da su $\lim\limits_{m\to\infty} A_m$, $\lim\limits_{m\to\infty} B_m, \ldots, \lim\limits_{m\to\infty} S_m$ i $\lim\limits_{m\to\infty} Q_m$ faktori polinoma P.

3°. Radi lakšeg izražavanja uvodimo sledeće vektorske oznake:

$$p \overset{\text{def}}{=} (\alpha_{a-1}, \ldots, \alpha_o, \beta_{b-1}, \ldots, \beta_o, \ldots, \lambda_{s-1}, \ldots, \lambda_o)$$

$$p(m) \overset{\text{def}}{=} (\alpha_{a-1}(m), \ldots, \alpha_o(m), \beta_{b-1}(m), \ldots, \beta_o(m), \ldots \lambda_{s-1}(m), \ldots, \lambda_j(m))$$

$m = 0, 1, 2, \ \ldots$.

U sledećoj teoremi dokazuje se da, pod odredjenim uslovima, nizovi (A_m), $(B_m), \ldots, (S_m)$ postoje i konvergiraju redom ka $A, B, \ \ldots \ , S$.

TEOREMA. Neka su polinomi $A, B, \ldots, S, Q$ po parovima uzajamno prosti i neka imaju samo proste korene, tada postoji okolina V vektora p takva da, ukoliko je $p(o) \in V$ onda nizovi $(A_m), (B_m), \ldots, (S_m)$ postoje i konvergiraju redom ka $A, B, \ldots, S$. Pri tome konvergencija je kvadratna.

Dokaz. Dokaz izvodimo u dva koraka.

Prvi korak. Uslov *(1)* zapisujemo u sledećem obliku:

$$A_{m+1}B_m \ldots S_m\bar{Q}_m + A_mB_{m+1} \ldots S_m\bar{Q}_m + \ldots + A_mB_m \ldots S_{m+1}\bar{Q}_m + A_mB_m \ldots S_mQ_{m+1} - kA_mB_m \ldots S_m\bar{Q}_m = P, \quad m = 0,1,2,\ldots \tag{2}$$

Svaki od uslova *(2)* predstavlja sistem od $n = a+b + \ldots + s+q$ linearnih jednačina sa isto toliko nepoznatih - nepoznati su koeficijenti približnih polinoma A_{m+1}, $B_{m+1}, \ldots, S_{m+1}$, Q_{m+1}. Svaki od tih sistema, pod izvesnim uslovima, se može svesti na ekvivalentan sistem diferencijskih jednačina oblika:

$$\left|\begin{array}{l}
\alpha_{a-1}(m+1) = F_{a-1}(p(m)) \\
\vdots \\
\alpha_o(m+1) = F_o(p(m)) \\
\beta_{b-1}(m+1) = G_{b-1}(p(m)) \\
\vdots \\
\beta_o(m+1) = G_o(p(m)) \\
\vdots \\
\lambda_{s-1}(m+1) = H_{s-1}(p(m)) \\
\vdots \\
\lambda_o(m+1) = H_o(p(m)) \\
\vdots \\
\delta_{q-1}(m+1) = T_{q-1}(p(m)) \\
\vdots \\
\delta_o(m+1) = T_o(p(m))
\end{array}\right. \tag{3}$$

gde su $F_{a-1}, \ldots, F_o$, $G_{b-1}, \ldots, G_o, \ldots, H_{s-1}, \ldots, H_o, T_{q-1}, \ldots, T_o$ izvesne racionalne funkcije, zbog toga što su uslovi *(2)* linearni po $\alpha_{a-1}(m+1), \ldots, \alpha_o(m+1)$, $\beta_{b-1}(m+1), \ldots, \beta_o(m+1), \ldots, \lambda_{s-1}(m+1), \ldots, \lambda_o(m+1), \ldots, \delta_{q-1}(m+1), \ldots, \delta_o(m+1)$.

Neka je $p(o) = p$, odnosno $A_o=A$, $B_o=B, \ldots, S_o=S$, tada je i $\bar{Q}_o = Q$, pa iz *(2)* za $m=0$ dobijamo:

$$A_1B \ldots SQ + AB_1 \ldots SQ + \ldots + AB \ldots S_1Q + AB \ldots SQ_1 - kAB \ldots SQ = P. \tag{4}$$

Pošto je $AB \ldots SQ + AB \ldots SQ + \ldots + AB \ldots SQ - kAB \ldots SQ = P$ zaključujemo da jednačina *(4)* ima bar jedno rešenje po A_1, B_1, ... ,S_1,Q_1 koje je jednako $A,B, \ldots ,S,Q$. Dokazujemo da je to i jedino rešenje. Polinomna jednakost *(4)* za $x=x_A$, gde je x_A bilo koji koren polinoma A, daje $\tilde{A}_1\tilde{B} \ldots \tilde{S}\tilde{Q} = 0$, odnosno $\tilde{A}_1 = 0$, gde $\sim$ znači vrednost odnosnog polinoma za $x = x_A$. Polinomi A i A_1 imaju sve zajedničke korene. Kako su to polinomi sa članom uz najveći stepen jednakim 1, to važi jednakost $A=A_1$. Slično $B=B_1,\ldots,S=S_1$, $Q=Q_1$.

Uslov *(4)* predstavlja sistem n linearnih jednačina čije su nepoznate koeficijenti polinoma $A_1,B_1,\ldots,S_1,Q_1$. Prema dokazanom, taj sistem ima jedinstveno rešenje, odakle sledi da je njegova determinanta različita od 0. Determinanta sistema je različita od 0 i u izvesnoj okolini vektora p. Odavde, takodje, sledi da postoji okolina V vektora p takva da ako je $p(m) \in V$ onda jednačina *(2)* ima jednoznačno rešenje $p(m+1)$ koje na osnovu prvih $n-q$ jednakosti *(3)* se može zapisati u obliku:

$$p(m+1) = F(p(m)), \quad m = 0,1,2,\ldots \tag{5}$$

gde je funkcija F definisana u okolini V.

Drugi korak. Dokažimo sada da i $p(m+1)$ ostaje u okolini V, kao i to da niz $p(m)$ konvergira ka p. Za tu svrhu potražimo parcijalne izvode po koordinatama prvog reda funkcije $F(r)$ kada je $r=p$. Diferenciranjem jednakosti *(2)* po α_A gde je α_A bilo koji koeficijent polinoma A_m dobijamo:

$$\frac{\partial A_{m+1}}{\partial \alpha_A} B_m \ldots S_m \bar{Q}_m + \frac{\partial A_m}{\partial \alpha_A} B_{m+1} \ldots S_m \bar{Q}_m + \ldots + \frac{\partial A_m}{\partial \alpha_A} B_m \ldots S_{m+1} \bar{Q}_m + \tag{6}$$

$$+ \frac{\partial A_m}{\partial \alpha_A} B_m \ldots S_m Q_{m+1} - k \frac{\partial A_m}{\partial \alpha_A} B_m \ldots S_m \bar{Q}_m = 0.$$

Neka je $A_m=A$, $B_m=B,\ldots,S_m=S$, tada je i $\bar{Q}_m=Q$. Takodje, tada je $A_{m+1}= =A$, $B_{m+1}=B,\ldots,S_{m+1}=S$ i $Q_{m+1}=Q$. Jednakost *(6)* za $x=x_A$, gde je x_A bilo koji koren polinoma A daje $\left(\frac{\partial A_{m+1}}{\partial \alpha_A}\right)_{x_A} = 0$. Znači polinom $\frac{\partial A_{m+1}}{\partial \alpha_A}$ ima a korena. On je nula polinom jer je njegov stepen jednak $a-1$. Slično dokazujemo da i polinomi $\frac{\partial B_{m+1}}{\partial \beta_B},\ldots,\frac{\partial S_{m+1}}{\partial \beta_S}$, gde je β_B bilo koji koeficijent polinoma B_m, a λ_S je bilo koji koeficijent polinoma S_m, su nula polinomi. Prema tome funkcija $F(r)$ ima za $r=p$ sve parcijalne izvode prvog reda jednake nuli. Na osnovu toga za funkciju $F(r)$ u okolini vektora p imamo sledeći Tajlorov razvoj:

$$F(r) = F(p) + O(\|r-p\|^2), \text{ odnosno}$$
$$\|F(r) - F(p)\| = \tilde{O}(\|r-p\|^2).$$

Pošto je p fiksni vektor za funkciju $F(r)$, $(p=F(p))$, to u okolini vektora p važi sledeća jednakost:

$$(7) \qquad \|F(r)-p\| = \tilde{O}(\|r-p\|^2).$$

Na osnovu izloženog i jednakosti (7) neposredno zaključujemo da postoji okolina V vektora p takva da niz $p(m)$ definisan jednakostima (2), (3), (5) postoji i da svi članovi toga niza pripadaju V ukoliko je $p(o) \in V$. Osim toga niz $p(m)$ konvergira ka p i ta je konvergencija kvadratna.

4. Sada izlažemo numerički postupak za izračunavanje polinoma A_{m+1}, $B_{m+1},\ldots,S_{m+1}$ polazeći od polinoma $A_o, B_o,\ldots,S_o$.

Iz izloženog u 3. zaključujemo da su polinomi A_m, $B_m,\ldots$, $S_m, \bar{Q}_m$ po parovima uzajamno prosti, pa primenom relacije kongruentnosti u skupu polinoma $C[X]$ iz jednakosti (1) dobijamo $k+1$ kongruencija [1], [2]:

$$(8) \qquad \begin{cases} (A_{m+1}-A_m)B_m \;\ldots\; S_m\bar{Q}_m \equiv P(\text{mod}A_m) \\ A_m(B_{m+1}-B_m) \;\ldots\; S_m\bar{Q}_m \equiv P(\text{mod}B_m) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ A_mB_m \;\ldots\; (S_{m+1}-S_m)\bar{Q}_m \equiv P(\text{mod}S_m) \\ A_mB_m \;\ldots\; S_m(Q_{m+1}-\bar{Q}_m) \equiv P(\text{mod}\bar{Q}_m). \end{cases}$$

Polinomi A_{m+1}, $B_{m+1},\ldots,S_{m+1}$ se mogu izračunati svaki iz odgovarajuće kongruencije (8) nezavisno od ostalih kongruencija i nezavisno od poslednje kongruencije.

Na osnovu toga i izloženog u 2. i 3. za izračunavanje polinoma A_{m+1}, $B_{m+1},\ldots,S_{m+1}$ se mogu koristiti prve k kongruencije iz (8). Time dobijamo jedan iterativni postupak za jednovremeno odredjivanje k faktora polinoma P.

Zavisno od izbora polinoma Q, broj faktora koji se mogu odrediti ovim postupkom je različit. Tako, ovim postupkom možemo odrediti jedan faktor, nekoliko (k) faktora, ili sve faktore polinoma P.

U slučaju kada su faktori $A,B,\dots,S$ linearni dobijamo iterativni postupak za jednovremeno odredjivanje k jednostrukih korena polinoma P.

Kako su polinomi $A_m,B_m,\dots,S_m,\bar{Q}_m$ po parovima uzajamno prosti važe jednakosti:

$$(9)\qquad \begin{cases} (B_m \dots S_m\bar{Q}_m, A_m) = 1 \\ (A_mC_m \dots S_m\bar{Q}_m, B_m)=1 \\ \dots\dots\dots\dots\dots\dots \\ (A_mB_m \dots L_m\bar{Q}_m, S_m)=1 \end{cases}$$

gde $(,)$ označuje najveći zajednički delitelj dvaju polinoma. Iz (9) sledi da postoje parovi polinoma U_{A_m}, V_{A_m}; U_{B_m}, V_{B_m};...; U_{S_m}, V_{S_m} tako da:

$$(10)\qquad \begin{cases} U_{A_m}(B_m \dots S_m\bar{Q}_m) + V_{A_m}\cdot A_m = 1 \\ U_{B_m}(A_mC_m\dots S_m\bar{Q}_m) + V_{B_m}\cdot B_m = 1 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ U_{S_m}(A_mB_m\dots L_m\bar{Q}_m) + V_{S_m}\cdot S_m = 1 \end{cases}$$

gde je step U_{A_m} < step A_m, step U_{B_m} < step B_m,..., step U_{S_m} < step S_m, step V_{A_m} < step $(B_m\dots S_m\bar{Q}_m)$, step V_{B_m} < step$(A_mC_m\dots S_m\bar{Q}_m)$, step V_{S_m} < step$(A_mB_m \dots L_m\bar{Q}_m)$.

Primenom relacije kongruentnosti u skupu polinoma $C[X]$ iz (10) dobijamo [1], [2]:

$$(11)\qquad \begin{cases} 1 \equiv [U_{A_m}(B_m \dots S_m\bar{Q}_m)] \pmod{A_m} \\ 1 \equiv [U_{B_m}(A_mC_m \dots S_m\bar{Q}_m)] \pmod{B_m} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ 1 \equiv [U_{S_m}(A_mB_m \dots L_m\bar{Q}_m)] \pmod{S_m}. \end{cases}$$

Koristeći neka svojstva pomenute relacije iz (8) i (11) dobijamo:

$$(A_{m+1}-A_m)B_m \dots S_m\bar{Q}_m \equiv P\,[U_{A_m}(B_m \dots S_m\bar{Q}_m)] \pmod{A_m}$$

$$(B_{m+1}-B_m)A_mC_m\dots S_m\bar{Q}_m \equiv P\,[U_{B_m}(A_mC_m\dots S_m\bar{Q}_m)] \pmod{B_m}$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$(S_{m+1}-S_m)A_mB_m\dots L_m\bar{Q}_m \equiv P[U_{S_m}(A_mB_m\dots L_m\bar{Q}_m)] \pmod{S_m}.$$

Odnosno:

$$(12)\quad \left|\begin{array}{l} A_{m+1}-A_m \equiv PU_{A_m} \pmod{A_m} \\ B_{m+1}-B_m \equiv PU_{B_m} \pmod{B_m} \\ \dots\dots\dots\dots\dots\dots \\ S_{m+1}-S_m \equiv PU_{S_m} \pmod{S_m} \end{array}\right.$$

odakle neposredno odredjujemo polinome $A_{m+1}, B_{m+1},\dots,S_{m+1}$. Polinomi $U_{A_m}, U_{B_m},\dots,U_{S_m}$ su definisani jednakostima *(10)*.

5. Navodimo i jedan primer.

Polinom $P = x^6+5x^5+11x^4+15x^3+14x^2+10x+4$ ima faktore x^2+1, x^2+3x+2 i x^2+2x+2. Za odredjivanje faktora x^2+1 i x^2+3x+2 iz kongruencija *(12)* koristimo dve kongruencije.

U "tablicama" koje navodimo u prvoj koloni nalazi se oznaka za red iteracije, dok u prvoj vrsti su početne vrednosti koeficijenata traženih polinoma. Simbol $E+n$, $n \in N$, znači da je broj koji neposredno stoji ispred njega pomnožen sa 10^n.

1	0	-1	0	4	3
	1	-0,3888869E+00	0,2222180E+00	0,3537034E+01	0,2537032E+01
	2	0,1452231E+01	0,5280300E+00	0,3219110E+01	0,2219113E+01
	3	0,1244375E+00	0,8986753E+00	0,3048939E+01	0,2048936E+01
	4	-0,1077604E-01	0,1008620E+01	0,3001615E+01	0,2001618E+01
	5	-0,1068115E-03	0,1000018E+01	0,3000006E+01	0,2000008E+01
	6	-0,2861023E-05	0,1000000E+01	0,3000000E+01	0,2000000E+01
	7	0,4768372E-06	0,1000000E+01	0,3000000E+01	0,2000000E+01
2	0	-1	2	4	1
	1	-0,6143666E+00	0,1274099E+01	0,3342154E+01	0,9848775E+00
	2	-0,2604442E+00	0,1029987E+01	0,2984268E+01	0,1157368E+01

	3	-0,6392671E-01	0,9936414E+00	0,2872181E+01	0,1482227E+01
	4	-0,5850792E-02	0,9996157E+00	0,2927794E+01	0,1824129E+01
	5	-0,9870530E-04	0,1000086E+01	0,2994592E+01	0,1989503E+01
	6	-0,2384186E-05	0,9999989E+00	0,2999999E+01	0,2000007E+01
3	0	1	-3	6	6
	1	0,1173214E+01	-0,2672062E+01	0,4499996E+01	0,3499983E+01
	2	0,1537124E+01	-0,2135164E+01	0,3370639E+01	0,2370628E+01
	3	-0,3087944E+01	0,3141580E+01	0,7583917E+01	0,6583877E+01
	4	-0,2478759E+01	0,2298435E+01	0,6016398E+01	0,5016340E+01
	5	-0,1804174E+01	0,1541544E+01	0,4932091E+01	0,3932053E+01
	6	-0,1169780E+01	0,1024839E+01	0,4172184E+01	0,3172155E+01
	7	-0,6265906E+00	0,7708026E+00	0,3639776E+01	0,2639749E+01
	8	-0,2145312E+00	0,7504259E+00	0,3282712E+01	0,2282694E+01
	9	0,1289844E-02	0,8896342E+00	0,3079591E+01	0,2079579E+01
	10	0,8854152E-02	0,9964505E+00	0,3007654E+01	0,2007651E+01
	11	-0,5912781E-04	0,1000009E+01	0,3000044E+01	0,2000054E+01
	12	-0,4767372E-06	0,1000000E+01	0,3000000E+01	0,2000000E+01
4	0	-1	-2	-3	-4
	1	-0,1110168E-01	-0,3168594E+01	-0,7496224E+00	-0,1464843E-02
	2	0,6914721E+00	-0,8218690E+00	-0,1057896E+01	-0,5019499E-01
	3	-0,1187859E+01	-0,3317934E+01	0,1913710E+01	-0,2077052E+00
	4	-0,5847455E-02	-0,1687134E+01	0,1860198E+01	-0,3093016E+00
	5	0,9532028E+00	-0,3220692E+00	0,1640682E+01	-0,7392047E+00
	6	-0,3732255E+01	-0,5901870E+01	0,6765080E+01	0,9568445E+01
	7	-0,2225525E+01	-0,4103371E+01	0,5788240E+01	0,7601083E+01
	8	-0,1134894E+01	-0,2009134E+01	0,4959218E+01	0,5934133E+01
	9	-0,3155429E+00	-0,1856229E+01	0,4265748E+01	0,4540246E+01
	10	0,3516011E+00	-0,1137470E+01	0,3655754E+01	0,3316115E+01
	11	0,1107720E+01	-0,6349991E+00	0,2922590E+01	0,1848511E+01
	12	0,1152591E+01	0,5048321E+00	0,2861336E+01	0,1720459E+01
	13	0,5089474E+00	0,1526817E+01	0,3557212E+01	0,3116052E+01
	14	0,3635719E+00	0,4725125E+00	0,3097130E+01	0,2194759E+01
	15	0,1707957E+00	0,1112212E+01	0,2975792E+01	0,1951449E+01
	16	0,3149271E-02	0,9480000E+00	0,3009514E+01	0,2019026E+01
	17	0,1128175E-02	0,9992271E+00	0,3000277E+01	0,2000549E+01
	18	-0,1192093E-05	0,1000000E+01	0,3000000E+01	0,2000000E+01

Л И Т Е Р А Т У Р А

[1] Бухштаб А.А., Теория чисел, Просвещение, Москва 1966.

[2] Обрешков Н., Висша алгебра, Наука и изкуство, София 1966.

[3] Прешић С.Б., Један итеративни поступак за факторизацију полинома, Мат. весн. 5(20) св. 2, 1968 (стр. 205-216).

[4] Прешић М.Д., Један итеративни поступак за једновремено одређивање реалних решења једначине на пољу реалних бројева, Мат. весн. 10 (25) св. 4, 1973.

[5] Секулоски Р.М., За методата на Прешиќ за факторизација на полиноми, Год. зборн. Мат. фак. 29(115-119) 1978.

METHODE D'ITERATION POUR DETERMINATION SIMULTANE DE FACTEURS k DES POLYNÔMES

Radojko Sekuloski

r é s u m é

En appliquant la relation de congruité dans l'équation *(1)* on obtient les congruités *(8)*.

Les polynômes $A_{m+1}, B_{m+1}, \ldots, S_{m+1}$ seront déterminés par les congruités *(8)*, chacun par la congruité adéquate et indépendamment des autres congruités et indépendamment de la congruité derniére.