MATERIAŁY NA XXXII KONFERENCJĘ SZKOLENIOWĄ Z GEOMETRII ANALITYCZNEJ I ALGEBRAICZNEJ ZESPOLONEJ

2011 **Łódź** **str. 61**

ALGORYTM EUKLIDESA I UKŁADY RÓWNAŃ WEDŁUG LABATIE

Arkadiusz Płoski (Kielce)

Wstęp

Celem tego opracowania jest przypomnienie twierdzenia Labatie z 1832 roku. Twierdzenie i jego dowód opracowałem na podstawie kursu algebry wyższej Serreta [4], str. 198–208 który miał kilkanaście wydań we Francji aż do lat dwudziestych minionego wieku. Niestety nie udało mi się odnaleźć oryginalnego artykułu Labatie ani informacji o tym autorze.

W całym opracowaniu rozważamy wielomiany o współczynnikach w ustalonym ciele $\mathbb{K}$. Gdy $W = W(x, y) \in \mathbb{K}[x, y]$ to symbolem $\deg_y W$ oznaczamy stopień wielomianu W względem zmiennej y. Niezerowy wielomian W nazywamy y-prymitywnym gdy jest on prymitywny jako wielomian pierścienia $\mathbb{K}[x][y]$ to znaczy gdy największy wspólny podzielnik jego współczynników przy potęgach zmiennej y jest równy 1. Jeżeli $V, W \in \mathbb{K}[x, y]$ spełniają warunek $0 < \deg_y V \leq \deg_y W$ to istnieją wielomiany Q (iloraz) i R (reszta) oraz niezerowy wielomian $u = u(x) \in \mathbb{K}[x]$ takie, że $uW = QV + R$ oraz $\deg_y R < \deg_y V$. Największy wspólny dzielnik wielomianów V, W może być wyznaczony za pomocą algorytmu Euklidesa [1], Rozdział XVI. Ostatnio Hilmar i Smyth [2] podali bardzo prosty dowód twierdzenia Bezouta dla rzutowych krzywych płaskich używając jako głównego narzędzia euklidesowego dzielenia z resztą.

1 Algorytm Euklidesa

Niech V_1, $V_2 \in \mathbb{K}[x,y]$ będą wielomianami spełniającymi warunki:
1) $0 < \deg_y V_2 \leq \deg_y V_1$,
2) V_1, V_2 są względnie pierwsze,
3) V_1, V_2 są y-prymitywne.

Stosując wielokrotnie dzielenie z resztą otrzymujemy ciąg y-prymitywnych wielomianów V_3, ..., V_{n+1} malejących y-stopni: $0 < \deg_y V_{n+1} < \ldots < \deg_y V_3 < \deg_y V_2$ powiązanych równościami

$$\begin{aligned} u_1V_1 &= Q_1V_2 + v_1V_3, \\ u_2V_2 &= Q_2V_3 + v_2V_4, \\ &\vdots \\ u_{n-1}V_{n-1} &= Q_{n-1}V_n + v_{n-1}V_{n+1}, \\ u_nV_n &= Q_nV_{n+1} + v_n \end{aligned}$$

gdzie $u_1,\ldots, u_n$, $v_1,\ldots, v_n$ są niezerowymi wielomianami pierścienia $\mathbb{K}[x]$. Przyjmijmy $V_{n+2} = 1$ i podane wyżej równości zapiszmy w formie

$$(1)_\mu \qquad u_\mu V_\mu = Q_\mu V_{\mu+1} + v_\mu V_{\mu+2} \quad \text{dla } \mu = 1,\ldots,n.$$

Powyższe oznaczenia i założenia obowiązują w całym artykule.

2 Twierdzenie Labatie

Definiujemy $d_0 = 1$, $d_1 = \mathrm{NWP}(u_1, v_1)$, $d_2 = \mathrm{NWP}(\frac{u_1}{d_1}u_2, v_2)$; ogólnie $d_\mu = \mathrm{NWP}(\frac{u_1\cdots u_{\mu-1}}{d_1\cdots d_{\mu-1}}u_\mu, v_\mu)$ dla $\mu = 2,\ldots, n$. Łatwo sprawdzić, że $\frac{u_1\cdots u_{\mu-1}}{d_1\cdots d_{\mu-1}} \in \mathbb{K}[x]$ a więc definicja ciągu $d_0,\ldots, d_\mu$ jest poprawna.

Dla dowolnych V, $W \in \mathbb{K}[x,y]$ oznaczmy $\{V = W = 0\} = \{\, P \in \mathbb{K}^2 : V(P) = W(P) = 0 \,\}$.

Twierdzenie 2.1 (Labatie 1832) *Przy wprowadzonych wyżej oznaczeniach i założeniach*

$$\{V_1 = V_2 = 0\} = \bigcup_{\mu=1}^{n} \{V_{\mu+1} = \frac{v_\mu}{d_\mu} = 0\}.$$

Dowód powyższego twierdzenia podajemy w trzecim rozdziale tego artykułu. Twierdzenie Labatie pokazuje, że układ równań $V_1(x,y) = 0$, $V_2(x,y) = 0$ jest równoważny alternatywie układów ,,trójkątnych"

$$V_{\mu+1}(x,y) = 0,\ \frac{v_\mu}{d_\mu}(x) = 0 \qquad (\mu = 1,\ldots,n).$$

Tego typu twierdzenia odkryto stosunkowo niedawno dla przypadku równań wielomianowych o dowolnej liczbie niewiadomych, por. [3] i literatura tam cytowana.

3 Dowód twierdzenia Labatie

Oznaczmy $w_\mu = \frac{u_1 \cdots u_\mu}{d_1 \cdots d_\mu}$. Zatem $w_\mu \in \mathbb{K}[x]$ oraz wielomiany w_μ i $\frac{v_\mu}{d_\mu}$ są względnie pierwsze.

Lemat 3.1 *Istnieją ciągi wielomianów $G_0,\ldots, G_n$ oraz $H_0,\ldots, H_n$ pierścienia $\mathbb{K}[x,y]$ takie, że*

$$(2)_\mu \qquad w_{\mu-1}V_1 = G_{\mu-1}V_\mu + G_{\mu-2}V_{\mu+1}\frac{v_{\mu-1}}{d_{\mu-1}},$$

$$(3)_\mu \qquad w_{\mu-1}V_2 = H_{\mu-1}V_\mu + H_{\mu-2}V_{\mu+1}\frac{v_{\mu-1}}{d_{\mu-1}}$$

dla $\mu = 2,\ldots, n+1$.

Dowód (indukcja względem μ)**.** Udowodnimy najpierw pierwszą tożsamość. Z równości $u_1V_1 = Q_1V_2 + v_1V_3$ wynika, że $d_1 = \mathrm{NWP}(u_1, v_1)$ dzieli iloczyn Q_1V_2 a więc dzieli wielomian Q_1 bo V_2 jest wielomianem prymitywnym. Przyjmując $G_0 = 1$, $G_1 = \frac{Q_1}{d_1}$ dostajemy $w_1V_1 = G_1V_2 + G_0V_3\frac{v_1}{d_1}$ to znaczy tożsamość (2) dla $\mu = 2$. Załóżmy teraz, że $2 \le \mu < n+1$ i że dla pewnych wielomianów $G_{\mu-1}$ oraz $G_{\mu-2}$ zachodzi $(2)_\mu$. Po pomnożeniu tożsamości $(2)_\mu$ przez wielomian u_μ dostajemy

$$w_{\mu-1}u_\mu V_1 = u_\mu G_{\mu-1}V_\mu + u_\mu G_{\mu-2}V_{\mu+1}\frac{v_{\mu-1}}{d_{\mu-1}}.$$

Do powyższej tożsamości podstawmy $u_\mu V_\mu = Q_\mu V_{\mu+1} + u_\mu V_{\mu+2}$. Po prostych przeróbkach otrzymujemy:

$$w_{\mu-1}u_\mu V_1 = \Big(G_{\mu-1}Q_\mu + u_\mu G_{\mu-2}\frac{v_{\mu-1}}{d_{\mu-1}}\Big)V_{\mu+1} + G_{\mu-1}v_\mu V_{\mu+2}$$

Ponieważ $d_\mu = \mathrm{NWP}(w_{\mu-1}u_\mu, v_\mu)$ zaś wielomian $V_{\mu+1}$ jest prymitywny więc $G_\mu := \frac{G_{\mu-1}Q_\mu}{d_\mu} + G_{\mu-2}\frac{u_\mu v_{\mu-1}}{d_\mu d_{\mu-1}}$ jest wielomianem i mamy

$$w_\mu V_\mu = G_\mu V_{\mu+1} + G_{\mu-1}V_{\mu+2}\frac{v_\mu}{d_\mu}$$

to znaczy tożsamość $(2)_{\mu+1}$. To dowodzi pierwszej tożsamości lematu.

Dla dowodu drugiej tożsamości zauważmy, że

$$w_1V_2 = H_1V_2 + H_0V_3\frac{v_1}{d_1}$$

jeśli przyjmiemy $H_0 = 0$ oraz $H_1 = \frac{v_1}{d_1}$. To dowodzi (3) dla $\mu = 2$. Dowód tożsamości $(3)_\mu$ dla dowolnego μ przebiega jak dowód $(2)_\mu$: wystarczy zastąpić G_μ przez H_μ. ■

Uwaga 3.2 *Wielomiany G_μ są określone wzorami $G_0 = 1$, $G_1 = \frac{Q_1}{d_1}$, $G_\mu = \frac{G_{\mu-1}Q_\mu}{d_\mu} + \frac{G_{\mu-2}u_\mu v_{\mu-1}}{d_{\mu-1}d_\mu}$ natomiast wielomiany H_μ wzorami $H_0 = 0$, $H_1 = \frac{u_1}{d_1}$ oraz $H_\mu = \frac{H_{\mu-1}Q_\mu}{d_\mu} + \frac{H_{\mu-2}u_\mu v_{\mu-1}}{d_{\mu-1}d_\mu}$.*

Lemat 3.3 *Przy oznaczeniach poprzedniego lematu zachodzą tożsamości*

$$(4)_\mu \qquad (-1)^\mu \frac{v_1 \cdots v_{\mu-1}}{d_1 \cdots d_{\mu-1}} V_{\mu+1} = H_{\mu-1}V_1 - G_{\mu-1}V_2 \qquad \text{dla } \mu = 2, \ldots, n+1.$$

Dowód. Oznaczmy $D_\mu = G_\mu H_{\mu-1} - G_{\mu-1}H_\mu$ dla $\mu = 2, \ldots, n$. Potraktujmy układ $(2)_\mu$, $(3)_\mu$ jako układ równań liniowych o niewiadomych V_μ, $V_{\mu+1}\frac{v_{\mu-1}}{d_{\mu-1}}$. Wyznacznikiem układu jest $D_{\mu-1}$, stosując wzory Cramera dostajemy

$$\begin{aligned} D_{\mu-1}V_\mu &= w_{\mu-1}(H_{\mu-2}V_1 - G_{\mu-2}V_2), \\ D_{\mu-1}V_{\mu+1}\frac{v_{\mu-1}}{d_{\mu-1}} &= -w_{\mu-1}(H_{\mu-1}V_1 - G_{\mu-1}V_2). \end{aligned}$$

W pierwszej formule po zastąpieniu μ poprzez $\mu+1$ otrzymamy

$$D_\mu V_{\mu+1} = w_\mu(H_{\mu-1}V_1 - G_{\mu-1}V_2) \tag{5}$$

Natomiast mnożąc drugą formułę przez $\frac{u_\mu}{d_\mu}$ otrzymamy

$$D_{\mu-1}V_{\mu+1}\frac{v_{\mu-1}}{d_{\mu-1}}\frac{u_\mu}{d_\mu} = -w_\mu(H_{\mu-1}V_1 - G_{\mu-2}V_2) \tag{6}$$

Porównując stronami (5) i (6) i skracając przez $V_{\mu+1}$ mamy $D_\mu = -\frac{v_{\mu-1}u_\mu}{d_{\mu-1}d_\mu}D_{\mu-1}$. Ponadto $D_1 = G_1H_0 - G_0H_1 = -\frac{u_1}{d_1}$ a więc przez łatwą indukcję dostajemy

$$D_\mu = (-1)^\mu w_\mu \frac{v_1 \cdots v_{\mu-1}}{d_1 \cdots d_{\mu-1}}.$$

Wstawiając obliczony wyżej wyznacznik do tożsamości (5) otrzymujemy tożsamość (4). ■

Możemy teraz podać dowód twierdzenia Labatie.

Dowód. Ustalmy $P \in \mathbb{K}^2$. Jeżeli $V_\mu(P) = \frac{v_{\mu-1}}{d_{\mu-1}}(P) = 0$ dla pewnego $\mu \in \{2, \ldots, n+1\}$ to z Lematu 3.1 wynika, że $V_1(P) = V_2(P) = 0$ bo $w_{\mu-1}(P) \neq 0$ gdyż $w_{\mu-1}$, $\frac{v_{\mu-1}}{d_{\mu-1}}$ są względnie pierwsze.

Załóżmy teraz, że $V_1(P) = V_2(P) = 0$. Z formuły $(4)_{n+1}$ lematu 3.3 otrzymujemy $\frac{v_1 \cdots v_n}{d_1 \cdots d_n}(P) = 0$ a więc chociaż jeden z wielomianów $\frac{v_1}{d_1}, \ldots, \frac{v_n}{d_n}$ zeruje się w punkcie P. Jeżeli $\frac{v_1}{d_1}(P) = 0$ to $P \in \{V_2 = \frac{v_1}{d_1} = 0\}$.

Jeżeli najmniejszy wskaźnik μ dla którego $\frac{v_\mu}{d_\mu}(P) = 0$ jest większy od 1 to z formuły $(4)_\mu$ wynika, że $V_{\mu+1}(P) = 0$ bo $\frac{v_1 \cdots v_{\mu-1}}{d_1 \cdots d_{\mu-1}}(P) \neq 0$ ze względu na wybór μ. To dowodzi twierdzenia. ■

Pytanie. Niech $i_P(V,W)$ będzie krotnością pary wielomianów V, W w punkcie $P \in \mathbb{K}^2$ zdefiniowaną jako kowymiar ideału $(V,W)\mathcal{O}_P$ w pierścieniu lokalnym $\mathcal{O}_P$ punktu P. Czy prawdą jest, że przy założeniach Twierdzenia 2.1 mamy

$$i_P(V_1,V_2) = \sum_{\mu=1}^{n} i_P\Big(V_{\mu+1}, \frac{v_\mu}{d_\mu}\Big)?$$

Literatura

[1] H. Bôcher, Introduction to Higher Algebra. New York 1907 (reprinted 1947).

[2] J. Hilmar, Ch. Smyth, *Euclid Meets Bézout: Intersecting Algebraic Plane Curves with the Euclidean Algorithm,* The Amer. Math. Monthly, vol 117, Number 3, March 2010, pp. 250–260.

[3] M. Kalkbreuner, *A Generalized Euclidean Algorithm for Computing Triangular Representation of Algebraic Varieties,* J. Symbolic Computation (1993) 15, 143–167.

[4] J. A. Serret, Cours D'Algèbre Supérieure. Paris

Politechnika Świętokrzyska
Katedra Matematyki
Al. Tysiąclecia Państwa Polskiego 7
25-314 Kielce

Euclidean algorithm and polynomial equations after Labatie

Summary. We recall Labatie's effective method of solving polynomial equations with two unknowns by using the Euclidean algorithm.

Łódź, 10 – 14 stycznia 2011 r.