LUNDS UNIVERSITET

Matematikcentrum
Matematik NF

Polynompotenser

Kjell Elfström

Med ett konstant polynom skall vi mena ett polynom, som antingen är nollpolynomet, eller vars gradtal är noll. Läsaren förutsätts känna till att polynomringen $\mathbf{Z}[x]$ är ett integritetsområde med entydig primfaktorisering och att $\mathbf{Q}[x]$ är en euklidisk ring. Om f och g är relativt prima polynom i $\mathbf{Z}[x]$, så följer det av detta, att det finns h och k i $\mathbf{Z}[x]$ och $c \neq 0$ i $\mathbf{Z}$, sådana att $hf + kg = c$.

Definition 1 Låt $f \in \mathbf{Z}[x]$ och $p \in \mathbf{Z}$. Vi säger, att p delar f, och skriver $p \parallel f$, om det finns ett $a \in \mathbf{Z}$, sådant att $p \mid f(a)$.

Lemma 1 Låt f vara ett icke-konstant polynom i $\mathbf{Z}[x]$. Då finns det oändligt många primtal p, sådana att $p \parallel f$.

Bevis Eftersom f inte är konstant, antar f värden andra än 0 och ± 1. Det följer, att det finns minst ett primtal p, sådant att $p \parallel f$. Antag att de olika primtalen $p_1, p_2, \ldots, p_m$ delar f. Låt a och b vara heltal, sådana att $f(a) = b \neq 0$. Då är polynomet

$$g(x) = \frac{1}{b} f(a + bp_1 \cdots p_m x) \in \mathbf{Z}[x]$$

icke-konstant. Det gäller vidare, att $g(c) \equiv 1 \pmod{p_1 \cdots p_m}$ för varje $c \in \mathbf{Z}$. Det måste därför finnas ytterligare ett primtal p förutom primtalen $p_1, p_2, \ldots, p_m$, sådant att $p \parallel g$. Eftersom då också $p \parallel f$, visar detta påståendet. ■

Lemma 2 Låt f och g vara relativt prima polynom i $\mathbf{Z}[x]$, och antag, att f inte är konstant. Då finns det ett primtal p och ett heltal a, sådana att $p \mid f(a)$ och $p \nmid g(a)$.

Bevis Eftersom f och g är relativt prima, finns det polynom h och k i $\mathbf{Z}[x]$ och ett heltal $c \neq 0$, sådana att $hf + kg = c$. Det finns enligt lemma 1 oändligt många primtal p, sådana att $p \parallel f$. Eftersom bara ändligt många av dessa delar c, finns det ett primtal p, sådant att $p \parallel f$ och $p \nmid c$. Till detta primtal p finns det ett heltal a, sådant att $p \mid f(a)$, och eftersom $p \nmid c$, så kan inte p dela $g(a)$. ■

Lemma 3 Låt f och g vara relativt prima polynom i $\mathbf{Z}[x]$, och antag, att f är irreducibelt och inte konstant. Då finns det ett primtal p och ett heltal a, sådana att $p \mid f(a)$, $p^2 \nmid f(a)$ och $p \nmid g(a)$.

Bevis Eftersom f är irreducibelt och inte konstant, så är f och derivatan f' relativt prima. Det följer, att f och $h = f'g$ är relativt prima. Det finns därför enligt lemma 2 ett primtal p och ett heltal c, sådana att $p \mid f(c)$ och $p \nmid h(c)$. Det gäller då också, att $p \mid f(c+p)$ och $p \nmid h(c+p)$. Eftersom $p^2 \mid (f(c+p) - f(c) - pf'(c))$, kan inte p^2 dela både $f(c)$ och $f(c+p)$. Om $p^2 \mid f(c+p)$, så kan vi välja $a = c$, och annars $a = c + p$. ■

Sats 1 Låt $f \in \mathbf{Z}[x]$ och $n \in \mathbf{Z}_+$, och antag, att det till varje heltal a finns ett heltal b, sådant att $f(a) = b^n$. Då finns det ett polynom $g \in \mathbf{Z}[x]$, sådant att $f = g^n$.

Bevis Om $n = 1$ eller f är konstant, så är påståendet trivialt. Vi kan därför antaga, att $n \geq 2$ och att f inte är konstant. Eftersom man har entydig faktorisering i $\mathbf{Z}[x]$, så är

$$f = \varepsilon f_1^{n_1} \cdots f_m^{n_m},$$

där $\varepsilon = \pm 1$, $m \geq 1$, $n_i > 0$, $i = 1, \ldots, m$ och $f_1, \ldots, f_m$ är icke-associerade irreducibla polynom i $\mathbf{Z}[x]$ med positiva högstagradskoefficienter. Välj nu heltal q_i och r_i, $i = 1, \ldots, m$, sådana att $n_i = nq_i + r_i$ och $0 \leq r_i < n$. Vi kan då skriva

$$f = \varepsilon g^n f_1^{r_1} \cdots f_m^{r_m},$$

där $g = f_1^{q_1} \cdots f_m^{q_m}$.

Antag, att $r_i > 0$ för något i. Om polynomet $f_1^{r_1} \cdots f_m^{r_m}$ är konstant, kan vi, eftersom f inte är konstant, välja ett heltal a, sådant att $f(a) \neq 0$. Vi får, att antalet förekomster av primtalet $p = f_i$ i faktoriseringen av $f(a)$ inte är delbart med n, vilket motsäger förutsättningarna.

Om polynomet $f_1^{r_1} \cdots f_m^{r_m}$ inte är konstant, kan vi efter eventuell omnumrering antaga att $r_1 > 0$ och att f_1 inte är konstant. Sätt $h = f_2^{r_2} \cdots f_m^{r_m}$, där produkten skall tolkas som 1, om $m = 1$. Enligt lemma 3 finns det ett primtal p och ett heltal a, sådana att $p \mid f_1(a)$, $p^2 \nmid f_1(a)$ och $p \nmid h(a)$. Att detta strider mot förutsättningarna inser man på samma sätt som i det förra stycket.

Därför är $f = \varepsilon g^n$. Eftersom f inte är konstant, finns det ett heltal a, sådant att $f(a) \neq 0$. Det finns enligt förutsättningarna ett heltal b, sådant att $f(a) = b^n = \varepsilon(g(a))^n$, och det följer, att $\varepsilon = (b/g(a))^n$. Detta visar, att $f = (bg/g(a))^n$. ■