Generowanie wielomianów pierwotnych o współczynnikach z ciała skończonego

Andrzej Chmielowiec

12 marca 2012

Definicja 1 Powiemy, że wielomian $f \in GF(p)[X]$ jest nierozkładalny, jeżeli nie istnieje taki wielomian $g \in GF(p)[X]$ stopnia większego od 0, że $g \mid f$. $\square$

Definicja 2 Powiemy, że nierozkładalny wielomian $f \in GF(p)[X]$ jest pierwotny, jeżeli rząd elementu $X \bmod f$ wynosi $p^n - 1$, gdzie n jest stopniem f. $\square$

W dalszej części naszych rozważań będziemy przyjmowali, że $N = 2^n - 1$ i znany jest rozkład liczby N na czynniki pierwsze $N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.

Twierdzenie 1 Jeżeli $f \in GF(p)[X]$ jest wielomianem stopnia n, $N = p^n - 1 = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ i zachodzą następujące warunki

1. $\mathrm{NWD}(f, f') = 1$,
2. $X^N \equiv 1 \bmod f$,
3. $X^{N/p_i} \not\equiv 1 \bmod f$,
4. $\mathrm{NWD}(f, X^{N/p_i} - 1) = 1$,

to f jest wielomianem pierwotnym.

Dowód: Pierwszy warunek zapewnia, że wielomian f jest wielomianem bezkwadratowym. To znaczy takim, który nie jest podzielny przez kwadrat jakiegoś innego wielomianu. W celu udowodnienia tego faktu załóżmy, że $\mathrm{NWD}(f, f') = 1$ i istnieje taki wielomian $g \in GF(p)[X]$, że $g^2 \mid f$. W takim przypadku możemy zapisać $f = g^2 h$. Stosując wzory na pochodną iloczynu otrzymujemy $f' = (g^2 h)' = (g^2)' h + g^2 h' = 2gg'h + g^2 h' = g(2g'h + gh')$. Prowadzi to do sprzeczności, gdyż zarówno f, jak i f' są podzielne przez g. Otrzymana sprzeczność dowodzi słuszności postulowanej tezy, że wielomian f jest bezkwadratowy.

Zauważmy teraz, że warunki (2) i (3) gwarantują nam że rząd elementu X wynosi N pod warunkiem, że wielomian f jest nierozkładalny. W dalszej części

dowodu skupimy się więc na wykazaniu, że warunki (2)-(4) implikują nierozkładalność wielomianu f. Załóżmy przeciwnie, że pomimo spełnienia warunków (2)-(4) wielomian f jest podzielny przez nierozkładalny wielomian g, który ma stopień $m < n$. Skoro $g \mid f$, to istnieje taki wielomian h, że $f = gh$ i $g \nmid h$. Przy czym ostatnia zależność wynika z faktu, że wielomian f jest bezkwadratowy. Warunek (2) gwarantuje nam, że

$$f \mid X^N - 1.$$

Ponieważ $f = gh$, to również $g \mid X^N - 1$ i możemy zapisać

$$X^N \equiv 1 \bmod g.$$

Jeżeli przez d oznaczymy rząd $X \bmod g$, to możemy zapisać kongruencję

$$X^d \equiv 1 \bmod g.$$

Ponieważ $M = 2^m - 1$ jest rzędem grupy multiplikatywnej modulo g, to oczywiście $d \mid M$ i prawdziwa jest również kongruencja

$$X^M \equiv 1 \bmod g.$$

Ponieważ $m < n$, to $d \leq M < N$. Zatem d jest dzielnikiem właściwym liczby N. W związku z tym istnieje takie p_i, że $d \mid \frac{N}{p_i}$. Oznacza to, że

$$X^{N/p_i} \equiv 1 \bmod g.$$

To implikuje, że $g \mid (X^{N/p_i} - 1)$, a co za tym idzie $g \mid \mathrm{NWD}(f, X^{N/p_i} - 1)$. Ale to jest sprzeczne z warunkiem (4), który gwarantuje iż f jest względnie pierwsze z każdym wielomianem $X^{N/p_i} - 1$. Otrzymana sprzeczność dowodzi, że f nie może mieć dzielnika właściwego. Oznacza to, że f jest nierozkładalny, a warunki (2)-(3) gwarantują, że jest pierwotny. To kończy dowód. ■