פולינומים ציקלוטומים הגדרות וטענות

הגדרה: נגיד ששורש יחידה מסדר n הוא פרימיטיבי אם אינו שורש יחידה מסדר קטן יותר.

הגדרה: הפולינום הציקלוטומי ה-n הוא פולינום מתוקן ששורשיו הם שורשי יחידה פרימיטיביים מסדר n. מסמנים את הפולינום ב-$\Phi_n(x)$, כלומר

$$\Phi_n(x) = \prod_{\gcd(n,i)=1, i<n} (x - \omega^i)$$

כאשר ω הוא שורש יחידה פרימיטיבי מסדר n.

טענה חשובות:

1. $$\prod_{d|n} \Phi_d(x) = x^n - 1$$

2. המקדמים של $\Phi_n(x)$ שלמים.

3. עבור n שלם ו-p ראשוני, אם $p|n$ אז $\Phi_{np}(x) = \Phi_n(x^p)$.
אם $p \nmid n$ אז

$$\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}.$$

מסקנה, אם m, n זרים אז:

$$\Phi_n(x^m) = \prod_{d|m} \Phi_{nd}(x).$$

4. לכל n, a שלמים ו-p ראשוני, אם $p|\Phi_n(a)$ אז $p|n$ או ש-$p \equiv 1 \ mod \ n$.

5. $\Phi_n(x)$ אי-פריק מעל השלמים.