Циклотомични полиноми и примитивни корени

Лука Милићевић
децембар 2012.
lukavert@gmail.com

Комплексни примитивни корени

Дефиниција 1. За дати комплексан број x, најмањи природан број n такав да $x^n = 1$ важи (уколико такво n постоји), називамо поретком броја x и обележавамо са $r(x)$. Уколико је поредак броја x једнак n, кажемо да је x примитивни n-ти корен јединице.

Пример 2. (РММ 2010) За дати коначан скуп простих бројева P, обележимо са $m(P)$ највећи могући број узастопних природних бројева таквих да је сваки дељив неким елементом из P.
(i) Доказати да $m(P) \geq |P|$ и да једнакост важи ако и само ако $\min P > |P|$.
(ii) Доказати да $m(P) < (|P| + 1)(2^{|P|} - 1)$.

Циклотомични полиноми

Дефиниција 3. Нека је n природан број, а ζ n-ти примитивни корен јединице. Тада је n-ти циклотомични полином дат као $\Phi_n(X) = \prod(X - \zeta^j)$ где j узима вредности између 1 и n, које су узајамно просте са n.

Лема 4. Када је x цео број са $|x| > 1$ и n природан број већи од 1, тада је $\Phi_n(x) > 1$ осим за $n = 2, x = -2$.

Лема 5. Нека је n природан број. Тада је $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Дефиниција 6. Мебијусова функција је пресликавање $\mu : \mathbb{N} \to \{-1, 0, 1\}$ задато са $\mu(n) = 0$ уколико је n дељив квадратом различитим од 1, иначе $\mu(n) = (-1)^k$ где је k број простих делилаца броја n.

Теорема 7. Нека је n природан број. Тада је $\sum_{d|n} \mu(d)$ једнако 1 за $n = 1$, иначе је 0.

Теорема 8. Нека су $f, F : \mathbb{N} \to \mathbb{N}$ две функције које задовољавају $F(n) = \sum_{d|n} f(d)$ за свако n. Тада важи

$$f(n) = \sum_{d|n} \mu(d) F(n/d)$$

такође за свако n.

Последица 9. За сваки природан број n имамо $\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}$.

Лема 10. За сваки природан број n полином $\Phi_n(X)$ има целобројне коефицијенте.

Лема 11. За природан број n и прост број p

$$\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & p|n \\ \Phi_n(X^p)/\Phi_n(X) & p \not| n \end{cases}$$

важи.

Лема 12. Ако $X^n - 1$ има дупли корен по модулу p тада $p|n$.

Последица 13. Ако $d|n$, $d < n$ и x је цео број, тада сваки заједнички прост делилац $\Phi_n(x), \Phi_d(x)$ дели и n.

Теорема 14. Нека је n природан број, x цео, а p прост. Тада из $p|\Phi_n(x)$ следи да p дели n или $p \equiv 1 \pmod{n}$.

Последица 15. Нека је p прост, а x цео број. Тада је сваки прост делилац q израза $1+x+x^2+\cdots+x^{p-1}$ или $q = p$ или $q \equiv 1 \pmod{p}$.

Лема 16. За природне бројеве a и b и цео број x важи $(x^a - 1, x^b - 1) = x^{(a,b)} - 1$.

Теорема 17. Нека су a и b природни бројеви, и нека $\Phi_a(x), \Phi_b(x)$ имају заједнички прост делилац p за неки цео број x. Тада је b/a степен броја p.

Пример 18. Нека је n природан број. Тада постоји бесконачно много простих бројева конгруентних са 1 по модулу n.

Пример 19. (Тежа верзија ИМО 2002 SL) Нека су $p_1, p_2, \ldots, p_n$ различити прости бројеви већи од 3. Показати да $2^{p_1 p_2 \cdots p_n} + 1$ има бар $2^{2^{n-1}}$ различитих делилаца.

Пример 20. (ИМО 2006 SL) Наћи целобројна решења једначине $\frac{x^7-1}{x-1} = y^5 - 1$.

Примитивни корени по простом модулу

Дефиниција 21. Нека је n природан број већи од 1, и нека је a цео број. Најмањи природан број m (уколико постоји) такав да $a^m = 1 \pmod{n}$називамо поретком a по модулу n и обележавамо са $r_n(a)$. Уколико је $r_n(a) = \phi(n)$, кажемо да је a примитивни корен по модулу n.

Теорема 22. Уколико је n облика p^α или $2p^\alpha$ или једнак 4, где је p непаран прост број, постоји примитивни корен по модулу n.

Пример 23. Нека је n природан број. Тада постоји бесконачно много простих бројева p, таквих да међу $1, 2, \ldots, n$ нема примитвних корена по модулу p.

Пример 24. За сваки непаран прост број p постоји природан број $g < p$ такав да је g примитивни корен по модулу p^n за свако $n \geq 1$.

Пример 25. За прост број p наћи суму (по модулу p) свих примитивних корена по модулу p.

Пример 26. Нека је дат непаран прост број p. Наћи све функције $f : \mathbb{Z} \to \mathbb{Z}$ такве да за све целе бројеве m и n важи:
(i) Ако је $m \equiv n \pmod{p}$ тада $f(m) = f(n)$, (ii) $f(mn) = f(m)f(n)$.

Пример 27. (Кина 2012) Нека је $n \geq 2$ цео број. За функцију $f : \mathbb{Z} \to [n]$ кажемо да је *добра* уколико за све k у $[n-1]$ постоји цео број $j(k)$ такав да за све целе бројеве m важи

$$f(m + j(k)) \equiv f(m + k) - f(m) \pmod{n+1}.$$

Колико има *добрих* функција?

Пример 28. Нека је k природан број и $n = 2^k + 1$. Показати да је n прост број ако и само ако је следећи услов задовољен:
Постоји пермутација $a_1, a_2, \ldots, a_{n-1}$ скупа $[n-1]$ и низ целих бројева $g_1, g_2, \ldots, g_{n-1}$ таквих да n дели $g_i^{a_i} - a_{i+1}$ за све i у $[n-1]$, где је $a_n = a_1$.