Математичка гимназија

Матурски рад
из математике

Циклотомични полиноми

Ученик
Марко Трајковић, IVд

Ментор
Вукашин Брковић

Београд, *30.05.2025.*

Садржај

1

Увод

Циклотомични полиноми представљају посебну класу полинома чији су корени примитивни корени јединице. Њих је прве посматрао Гаус још почетком 19. века када је доказивао који се правилни многоуглови могу конструисати лењиром и шестаром. Ови полиноми имају значајну примену у различитим пољима математике, од теорије бројева, апстрактне алгебре, теорије Галоа, па до геометрије.

Циљ овог рада је да покаже њихову дефиницију, основна својсвта и места на којима се примењују.

Овом приликом желео бих да искажем искрену захвалност свом ментору, Вукашину Брковићу, на стручним саветима и стрпљењу током рада на овом матурском раду. Такође, желео бих да се захвалим и свим осталим професорима са којима сам сарађивао све ове године.

2

Уводни појмови и дефиниције

2.1 Мебијусова функција

Дефиниција 2.1 (Мебијусова функција)**.** Нека је n природан број и нека је $\prod_{k=1}^{r} p_k^{f_k}$ његова факторизација на просте чиниоце. Тада функцију дефинисану као

$$\mu(n) = \begin{cases} (-1)^r & \text{ако је } f_k = 1 \text{ за свако } k, \\ 0 & \text{у супротном.} \end{cases}$$

зовемо Мебијусова функција.

Можемо приметити да је $\mu(n) = 0$ ако и само ако је n дељиво квадратом природног броја већег од 1. Додатно, лако се примети да је Мебијусова функција мултипликативна, односно, важи $\mu(nm) = \mu(n)\mu(m)$ за свака 2 узајамно проста природна броја n и m.

Теорема 2.1. Нека је n природан број. Тада важи:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{када је } n = 1, \\ 0 & \text{иначе.} \end{cases}$$

Доказ. Тврђење очигледно важи за $n = 1$. За $n > 1$ уведимо ознаку $\mathrm{rad}(n)$ која означава производ свих простих делилаца броја n. Приметимо да уколико за неко d важи $d \mid n$ и $d \nmid \mathrm{rad}(n)$ онда мора бити $\mu(d) = 0$. Додатно, нека број n има r различитих простих делилаца. Посматрајмо делиоце $\mathrm{rad}(n)$ који имају тачно k простих фактора. Њих има $\binom{r}{k}$ и за сваки је $\mu(d) = (-1)^k$.

$$\sum_{d|n} \mu(d) = \sum_{d|rad(n)} \mu(d) = \sum_{k=0}^{r} (-1)^k \binom{r}{k} = (1-1)^r = 0.$$

□

Ово тврђење је само по себи веома битно и помоћи ће нам при доказивању следећих теорема.

Теорема 2.2 (Мебијусова инверзна формула)**.** Нека су $f, F : \mathbb{N} \to \mathbb{R}$ функције такве да важи:

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

Тада је:

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Доказ. Тврђење ћемо показати прегруписавањем сума и применом претходне теореме:

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \sum_{g|\frac{n}{d}} f(g)\right) = \sum_{g|n} \left(f(g) \sum_{d|\frac{n}{g}} \mu(d)\right) = f(n)$$

□

Теорема 2.3. Нека су $f, F : \mathbb{N} \to \mathbb{R}$ функције такве да важи:

$$F(n) = \prod_{d|n} f(d).$$

Тада је:

$$f(n) = \prod_{d|n} F(d)^{\mu\left(\frac{n}{d}\right)}.$$

Доказ. Довољно је применити претходну теорему на функције $\ln(f(x))$ и $\ln(F(x))$. □

Пример 1. Иначе је познато, а касније у раду и доказано, да важи $n = \sum_{d|n} \varphi(d)$. Сада, на основу теореме 2.2 можемо извести и формулу за $\varphi(n)$:

$$\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d.$$

2.2 Примитивни корени јединице

Дефиниција 2.2. Нека је n природан број. За број $\zeta \in \mathbb{C}$ кажемо да је n-ти корен јединице уколико задовољава $\zeta^n = 1$.

Иначе је познато да има тачно n n-тих корена јединице и да су то бројеви облика $\zeta^k = e^{\frac{2i\pi k}{n}}$ за $k = 1, 2, .., n$.

Дефиниција 2.3. Нека је ζ n-ти корен јединице. Поретком броја ζ, у ознаци $\mathrm{ord}(\zeta)$, називамо најмањи природни број k за који важи $\zeta^k = 1$.

Лема 1. Нека је ζ n-ти корен јединице. Нека за неки природан број k важи $\zeta^k = 1$. Онда $\mathrm{ord}(\zeta) \mid k$. Специјално, $\mathrm{ord}(\zeta)|n$.

Доказ. Нека је $d = \mathrm{ord}(\zeta)$. Онда број k можемо да запишемо као $k = qd + r$ где је $0 \leq r < d$. Приметимо да важи $1 = \zeta^k = (\zeta^d)^q\zeta^r = \zeta^r$. Пошто је $\zeta^r = 1$ и $r < d$, то по дефиницији поретка мора важити $r = 0$ што значи да $d \mid k$. □

Дефиниција 2.4. Нека је ζ n-ти корен јединице за неки природан број n. Уколико важи $ord(\zeta) = n$, тада за број ζ кажемо да је **примитивни n-ти корен јединице**.

Лема 2. Нека су n и k природни бројеви, а ζ примитивни n-ти корен јединице. Онда је ζ^k примитивни n-ти корен јединице ако и само ако су n и k узајамно прости природни бројеви.

Доказ. Нека је $(n, k) = 1$. Ако је $d = \mathrm{ord}(\zeta^k)$, онда је $\zeta^{kd} = 1$. По леми 1 $n \mid kd$, а како је $(n, k) = 1$, то мора да важи $n \mid d$. Још важи и $(\zeta^k)^n = (\zeta^n)^k = 1$ па је $d = n$, тј. ζ^k је примитивни n-ти корен јединице. У супротном, уколико је $(n, k) = g > 1$, онда важи $(\zeta^k)^{\frac{n}{g}} = (\zeta^n)^{\frac{k}{g}} = 1$. Како је $\frac{n}{g} < n$, то ζ^k не може бити примитивни n-ти корен. □

Последица. Из претходне леме можемо закључити да имамо тачно $\varphi(n)$ примитивних n-тих корена јединице и да су то сви бројеви облика $e^{\frac{2i\pi k}{n}}$ када је $(n, k) = 1$.

Теорема 2.4. Сума свих примитивних n-тих корена јединице једнака је $\mu(n)$.

Доказ. Трансформишимо суму користећи теорему 2.1:

$$\sum_{(n,k)=1} \zeta^k = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d)\zeta^k = \sum_{d|n} \mu(d) \sum_{k=1}^{n/d} \zeta^{kd} = \mu(n).$$

Приметимо да је $\sum_{k=1}^{n/d} \zeta^{kd} = \frac{1-1}{\zeta^d-1} = 0$ сем у тривијалном случају када је $d = n$, односно, једини члан који преостаје у суми горе управо јесте $\mu(n)$. □

Теорема 2.5. Нека је n природан број већи од 2. Онда је производ примитивних n-тих корена јединице једнак 1.

Доказ. Приметимо да кад је $n > 2$ примитивних n-тих корена јединице има паран број и можемо их упарити: $\zeta^k\zeta^{n-k} = 1$. □

2.3 О полиномима

Теорема 2.6 (Гаусова лема)**.** Нека су $g(x)$ и $h(x)$ монични полиноми са рационалним коефицијентима. Уколико је $f(x) = g(x)h(x)$ полином са целобројним коефицијентима, онда су такође и $g(x)$ и $h(x)$ полиноми са целобројним коефицијентима.

Доказ. Нека су u и v најмањи природни бројеви тако да важи $ug(x), vh(x) \in \mathbb{Z}[x]$. Треба показати да је $uv = 1$. Претпоставимо супротно, да постоји просто p тако да $p \mid uv$. Нека је $ug(x) = b_k x^k + ... + b_0$, $vh(x) = c_m x^m + ... + c_0$ и $uvf(x) = a_n x^n + ... + a_0$. Нека су i и j најмањи бројеви такви да $p \nmid b_i$ и $p \nmid c_j$. Они морају постојати због минималности u и v. Посматрајмо:

$$a_{i+j} = b_i c_j + (b_{i-1}c_{j+1} + ...) + (b_{i+1}c_{j-1} + ...).$$

Како p дели израз са леве стране и чланове у заградама, то можемо закључити да $p \mid b_i c_j$ што је у супротности са претпоставком. □

Под пољем $\mathbb{P}$ сматраћемо неко од поља $\mathbb{R}$, $\mathbb{Q}$ или $\mathbb{Z}_p$.

Теорема 2.7. Нека је полином $P(x) \in \mathbb{P}[x]$. Тада постоји неконстантни полином $m(x)$ такав да $m(x)^2 \mid P(x)$ акко важи $(P(x), P'(x)) \neq 1$. Под $P'(x)$ подразумевамо први извод по x полинома $P(x)$.

Доказ. Покажимо прво једну лему:

Лема. Нерастављиви неконстантни полином над пољем $\mathbb{P}$ не може имати извод једнак 0.

Доказ. Тврђење једино није тривијално за поље $\mathbb{Z}_p$. Пошто је извод полинома једнак 0, он мора бити облика $p(x) = \sum a_k x^{kp}$, али тада важи $p(x) = \left(\sum a_k x^k\right)^p$ што је у супротности са претпоставком да је наш полином нерастављив. □

Вратимо се сад доказивању теореме. Уколико $m(x)^2 \mid P(x)$ онда је $P'(x) = (m(x)^2 Q(x))' = m(x)^2 Q'(x) + 2m(x)m'(x)Q(x)$ па је свакако $(P(x), P'(x)) > 1$. Што се тиче другог смера, претпоставимо да је $Q(x)$ неки нерастављиви фактор $(P(x), P'(x))$. Онда $Q(x) \mid P'(x) = (Q(x)r(x))' = Q'(x)r(x) + Q(x)r'(x)$. Како је $degQ' < degQ$ и по леми $Q'(x) \neq 0$ то мора да важи $Q(x) \mid r(x)$ тј. $Q(x)^2 \mid P(x)$. □

Теорема 2.8. Нека је p прост број. Претпоставимо да постоји природан број a и полином $f \in \mathbb{Z}[x]$, такав да важи:

$$x^n - 1 = (x - a)^2 f(x) \pmod{p}.$$

Онда $p \mid n$.

Доказ. Приметимо $p \nmid a$. Уведимо смену $y = x - a$. Израз горе постаје $(y+a)^n - 1 - y^2 f(y+a) = 0 \pmod{p}$. Посматрајмо коефицијент уз y. Како он мора бити 0, $p \mid na^{n-1}$ тј. $p \mid n$. □

3

Циклотомични полиноми и основна својства

Дефиниција 3.1. За природан број n дефинишемо n-ти циколотомични полином као моничан полином чији су корени примитивни n-ти корени јединице:

$$\Phi_n = \prod_{\substack{ord(\zeta)=n \\ \zeta^n=1}} (x-\zeta) = \prod_{\substack{1\leq k\leq n \\ (k,n)=1}} (x - e^{\frac{2i\pi k}{n}}).$$

Како имамо тачно $\varphi(n)$ примитивних n-тих корена јединице, то је степен полинома $\Phi_n(x)$ једнак $\varphi(n)$.

Теорема 3.1. За сваки природан број n важи:

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

Доказ. Корени $x^n - 1$ су сви n-ти корени јединице. Нека је ζ један од њих и нека је $ord(\zeta) = d$, притом $d|n$. Тада је ζ примитивни d-ти корен јединице па је и нула полинома $\Phi_d(x)$, односно нула полинома са десне стране једнакости. За произвољну нулу полинома са десне важи $ord(\zeta)|n$, те је она нула и полинома са леве стране. Како су оба полинома монична и имају све једнаке нуле, то су и они сами једнаки. □

Последица. За природан број n важи $n = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$.

Пример 2. $x^9 - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x) = (x-1)(x^2+x+1)(x^6+x^3+1)$

Пример 3. $x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$

$\Phi_1(x) = x - 1$	$\Phi_6(x) = x^2 - x + 1$
$\Phi_2(x) = x + 1$	$\Phi_7(x) = x^6+x^5+x^4+x^3+x^2+x+1$
$\Phi_3(x) = x^2 + x + 1$	$\Phi_8(x) = x^4 + 1$
$\Phi_4(x) = x^2 + 1$	$\Phi_9(x) = x^6 + x^3 + 1$
$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$	$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$

Табела 3.1: Првих 10 циклотомичних полинома

Примећујемо да сви горе наведени полиноми имају коефицијенте који су цели бројеви. Испоставља се да сви циклотомични полиноми имају целобројне коефицијенте и о томе сведочи следећа теорема.

Теорема 3.2. Нека је n природан број. Полином $\Phi_n(x)$ има све целобројне коефицијенте, односно $\Phi_n(x) \in \mathbb{Z}[x]$.

Доказ. Докажимо тврђење индукцијом по n. За $n = 1$ је $\Phi_1(x) = x - 1$ па тврђење очигледно важи. Претпоставимо да оно важи за све бројеве мање од n. По теореми 3.1:

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

Како је $x^n - 1 \in \mathbb{Z}[x]$ и по индуктивној хипотези такође важи $\prod_{\substack{d|n \\ d<n}} \Phi_d(x) \in \mathbb{Z}[x]$, то по Гаусовој леми следи $\Phi_n(x) \in \mathbb{Z}[x]$. □

Теорема 3.3. Нека је n природан број. Онда је:

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

Доказ. Тврђење следи директно из теорема 2.3 и 3.1. □

Овакав запис који омогућава израчунавање циклотомичних полинома имаће различите примене у наставку.

Сада ћемо видети пар идентитета и примера који нам могу помоћи при израчунавању циклотомичних полинома у неким специјалним случајевима.

Теорема 3.4. Нека је n природан број и $n = \prod_{k=1}^{r} p_k^{f_k}$ његова проста факторизација. Ако је $m = \prod_{k=1}^{r} p_k^{g_k}$ број за који важи $1 \leq g_k \leq f_k$, односно $\mathrm{rad}(n)|m$, тада важи:

$$\Phi_n(x) = \Phi_m(x^{n/m}).$$

Доказ. Посматрајмо број d такав да $d \mid n$ и $d \nmid m$. Тада број d мора бити дељив квадратом неког природног броја па је $\mu(d) = 0$, односно $(x^{\frac{n}{d}} - 1)^{\mu(d)} = 1$.

$$\begin{aligned}\Phi_n(x) = \prod_{d|n}(x^{\frac{n}{d}} - 1)^{\mu(d)} &= \left(\prod_{\substack{d|m\\ d|n}}(x^{\frac{n}{d}} - 1)^{\mu(d)}\right)\left(\prod_{\substack{d|n\\ d\nmid m}}(x^{\frac{n}{d}} - 1)^{\mu(d)}\right)\\ &= \prod_{d|m}(x^{\frac{n}{d}} - 1)^{\mu(d)}\\ &= \prod_{d|m}\left((x^{\frac{n}{m}})^{\frac{m}{d}} - 1\right)^{\mu(d)}\\ &= \Phi_m(x^{n/m}).\end{aligned}$$

□

Последица. Специјално, ако је n природан и p прост такав да $p \mid n$, онда је $\Phi_{np}(x) = \Phi_n(x^p)$.

Теорема 3.5. Нека су a и n узајамно прости природни бројеви. Онда важи:

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

Доказ. Степен полинома са десне стране је $\sum_{d|a}\varphi(nd) = \varphi(n)\sum_{d|a}\varphi(d) = a\varphi(n)$, што је управо и степен полинома са леве стране. Како су оба полинома монична, довољно је показати да су им све нуле једнаке.

Корени полинома са леве стране су a-ти корени примитивних n-тих корена јединице. Нека је ζ примитивни na-ти корен јединице. Тада су корени полинома са леве стране облика ζ^k и $(k, n) = 1$. Постатрајмо $g = (k, a)$. Онда је $\zeta^k = (\zeta^g)^{\frac{k}{g}}$ примитивни $\frac{an}{g}$-ти корен јединице, односно корен $\Phi_{n\frac{a}{g}}(x)$. Тако смо показали да су све нуле левог полинома истовремено и нуле десног. □

Последица. Ако је n природан број и p прост и важи $p \nmid n$, онда је $\Phi_n(x)\Phi_{np}(x) = \Phi_n(x^p)$.

Последица. Ако су n и k природни бројеви и p прост и важи $p \nmid n$, онда је $\Phi_n(x^{p^{k-1}})\Phi_{np^k}(x) = \Phi_n(x^{p^k})$.

Теорема 3.6. Нека је q непаран природан број већи од 1. Онда је:

$$\Phi_{2q}(x) = \Phi_q(-x).$$

Доказ. Користимо неке основне особине Мебијусове функције:

$$\begin{aligned}
\Phi_{2q}(x) &= \prod_{d|2q}(x^d-1)^{\mu(\frac{2q}{d})} \\
&= \prod_{d|q}(x^d-1)^{\mu(\frac{2q}{d})}(x^{2d}-1)^{\mu(\frac{2q}{2d})} \\
&= \prod_{d|q}(x^d-1)^{-\mu(\frac{q}{d})}(x^d-1)^{\mu(\frac{q}{d})}(x^d+1)^{\mu(\frac{q}{d})} \\
&= \prod_{d|q}(x^d+1)^{\mu(\frac{q}{d})} \\
&= (-1)^{\sum_{d|q}\mu(d)}\prod_{d|q}\left((-x)^d-1\right)^{\mu(\frac{q}{d})} = \Phi_q(-x).
\end{aligned}$$

□

Последица. Нека је n непаран природан број. Број ζ је примитивни n-ти корен јединице ако и само ако је $-\zeta$ примитивни $2n$-ти корен јединице.

Ови идентитети нам могу помоћи приликом израчунавања циклотомичних полинома.

Сада ћемо видети пар примера неких специфичних и лако израчунљивих циклотомичних полинома.

Пример 4. Нека су n и m природни бројеви, а p непаран прост број. Онда важи:

1. $\Phi_p(x) = 1 + x + x^2 + ... + x^{p-1}$;
2. $\Phi_{2p}(x) = 1 - x + x^2 - ... + x^{p-1}$;
3. $\Phi_{2^m}(x) = x^{2^{m-1}} + 1$;
4. $\Phi_{p^m}(x) = \sum_{k=0}^{p-1} x^{kp^{m-1}}$;
5. $\Phi_{2^m p^n}(x) = \sum_{k=0}^{p-1}(-1)^k x^{k2^{m-1}p^{n-1}}$.

Погледајмо Табелу 1. Можемо приметити да су сви полиноми сем првог симетрични. Испоставља се да то тврђење важи и за све остале.

Теорема 3.7. Нека је n природан број већи од 1. Тада је циклотомични полином $\Phi_n(x)$ симетричан, тј. важи $\Phi_n(x) = x^{\varphi(n)}\Phi\left(\frac{1}{x}\right)$.

Доказ. Циклотомични полиноми имају све реалне коефицијенте па можемо приметити да уколико је ζ његов корен, онда то мора бити и $\bar{\zeta} = \frac{1}{\zeta}$. Доказ ћемо спровести користећи то тврђење, теорему 2.5 и мало рачуна.

$$\begin{aligned}
\Phi_n(x) &= \prod (x - \zeta_k) \\
&= x^{\varphi(n)} \prod \left(1 - \frac{\zeta_k}{x}\right) \\
&= x^{\varphi(n)} \prod (-\zeta_k) \prod \left(\frac{1}{x} - \frac{1}{\zeta_k}\right) \\
&= x^{\varphi(n)} \Phi_n \left(\frac{1}{x}\right).
\end{aligned}$$

□

4

Нерастављивост циклотомичних полинома

Нерастављивост циклотомичних полинома представља један од фундаменталних закључака у вези са истим. Он је доказиван много пута, од стране различитих математичара, у различитим степенима општости и коришћењем различитих метода. Овде ћемо размотрити пар приступа том проблему.

Теорема 4.1. Нека је p прост број. Онда је $\Phi_p(x)$ нерастављив у $\mathbb{Q}[x]$.

Овим проблемом се први бавио Гаус још у његовом делу *Disquisitiones Arithmeticae* (1801) [6]. На њега је наишао приликом доказивања познатог резултата да је правилан 17-тоугао, општије n-тоугао где је n Фермаов прост број, могуће конструисати лењиром и шестаром. Доказ тог тврђења се заснивао на нерастављивости $\Phi_n(x)$. Он даље креће да разматра овакве полиноме за све просте бројеве.

Напомена. До краја овог дела ћемо са p означавати просте бројеве.

Доказ (Гаус). Претпоставимо супротно, да је $\Phi_p(x) = f(x)g(x)$ за неке полиноме $f(x)$ и $g(x)$ са целобројним коефицијентима. Нека је $f(x) = (x-\zeta_1)...(x-\zeta_d)$. Дефинишимо $f_k(x) = (x-\zeta_1^k)...(x-\zeta_d^k)$. Сви коефицијенти $f_k(x)$ су симетричне функције по коренима $f(x)$ па по фундаменталној теореми о симетричним полиномима и они морају бити целобројни пошто сви основни симетрични полиноми (коефицијенти $f(x)$) узимају целобројне вредности. Још имамо и да су $f_k(x)$ монични и да немају реалних нула, па су у свим вредностима позитивни. Лако се види:

$$\Phi_p(x)^d = f_1(x)f_2(x)...f_{p-1}(x),$$

односно кад убацимо $x = 1$:

$$p^d = f_1(1)f_2(1)...f_{p-1}(1).$$

Како је $d < p-1$ и $f_k(1) \in \mathbb{Z}^+$, то за неких g од њих мора важити $f_k(1) = 1$. Онда је:

$$\sum_{k=1}^{p-1} f_k(1) \equiv g \not\equiv 0 \pmod{p}.$$

Са друге стране користећи $f_p(1) = 0$ имамо:

$$\begin{aligned}\sum_{k=1}^{p-1} f_k(1) &= \sum_{k=1}^{p} f_k(1) = \sum_{k=1}^{p}\sum_{i=0}^{d}(-1)^i s_i(\zeta_1^k, ..., \zeta_d^k) \\ &= \sum_{i=0}^{d}(-1)^i \sum_{k=1}^{p} s_i(\zeta_1^k, ..., \zeta_d^k) \equiv 0 \pmod{p},\end{aligned}$$

пошто је: $\sum_{k=1}^{p} s_i(\zeta_1^k, ..., \zeta_d^k) = \sum_{k=1}^{p}(\zeta^{kx_{j1}} + ... + \zeta^{kx_{jy}}) \equiv 0 \pmod{p}$, што је у супротности са претходном тврдњом.

□

После Гауса, на овом пољу није било пуно напретка све до четрдесетих година 19. века. Кронекер 1845. [8] проналази ,по некима, мало једноставније решење од Гаусовог служећи се сличним методама. Као основ, оно користи следећу лему.

Лема. Нека је $f(x)$ произвољан полином са целобројним коефицијентима. Нека је ζ примитивни p-ти корен јединице. Онда је $f(\zeta)f(\zeta^2)...f(\zeta^{p-1})$ цео број и $f(\zeta)f(\zeta^2)...f(\zeta^{p-1}) \equiv f(1)^{p-1} \pmod{\text{p}}$.

Доказ. Нека је $e(x)$ полином дефинисан као $e(x) = f(x)f(x^2)...f(x^{p-1})$. Приметимо да је $e(\zeta)$ израз симетричан по $\zeta, \zeta^2, ..., \zeta^{p-1}$, па по фундаменталној теореми о симетричним полиномима следи да је $e(\zeta)$ полином са целобројним коефицијентима по основним симетричним полиномима. Како сви основни симетрични полиноми по $\zeta, \zeta^2, ..., \zeta^{p-1}$ имају целобројне вредности (± 1), то и сама вредност $e(x)$ мора бити целобројна.
Сада посматрајмо израз:

$$S = \sum_{k=0}^{p-1} e(\zeta^k) = f(1)^{p-1} + (p-1)f(\zeta)f(\zeta^2)...f(\zeta^{p-1}).$$

Са друге стране запишимо $e(x)$ као $e(x) = \sum A_k x^k$. Онда је:

$$S = \sum A_k \left(1 + \zeta^k + \zeta^{2k} + ... + \zeta^{(p-1)k}\right) = pA_0 \equiv 0 \pmod{\text{p}}.$$

Одатле директно следи тврђење леме. □

Доказ (Кронекер). Кронекер завршава доказ користећи наведену лему. Претпоставимо да је полином $\Phi_p(x)$ растављив. Онда га можемо записати као $\Phi_p(x) = f(x)g(x)$ где су f и g полиноми са целобројним коефицијентима по Гаусовој леми. Како је $\Phi_p(1) = p = f(1)g(1)$, одатле, без умањења општости можемо претпоставити $f(1) = \pm 1$. За неки примитивни корен важи $f(\zeta) = 0$ па је онда $f(\zeta)f(\zeta^2)...f(\zeta^{p-1}) = 0$, што је у супротности са претходно наведеном лемом. □

Француски математичар Сере 1850. [15] године доказује уопштење Кронекерове леме која важи и за примитивне p^k-те коренове јединице и самим тим успева да докаже и нерастављивост циклотомичних полинома редова p^k.

У слично време, 1846. немачки математичар Шонеман избацује рад о полиномима са целобројним коефицијентима у којем представља крајње једноставан критеријум када је полином нерастављив. Он омогућава још једноставнији доказ у случају простих бројева. [14]

Лема (Шонеман)**.** Нека је $f(x)$ полином степена k. Претпоставимо да за неки прост број p, цео број a и полином $g(x)$ са целобројним коефицијентима такав да $p \nmid g(a)$ важи:

$$f(x) = (x-a)^k + pg(x).$$

Онда је полином $f(x)$ нерастављив (mod p).

Касније, 1850. године Ајзенштајн [4] објављује рад у коме доказује свој познати критеријум. Сада ћемо видети доказ самог критеријума као и још један доказ нерастављивости.

Лема (Ајзенштајн)**.** Нека је $f(x) = a_n x^n + ... + a_0$ полином са целобројним коефицијентима. Претпоставимо да p дели сваки од коефицијената $a_0, a_1, ..., a_{n-1}$, не дели a_n и p^2 не дели a_0. Онда је $f(x)$ нерастављив у $\mathbb{Z}[x]$.

Доказ. Претпоставимо супротно, да је $f(x) = g(x)h(x)$ за неке полиноме са целобројним коефицијентима $g(x) = b_m x^m + ... + b_0$ и $h(x) = c_k x^k + ... + c_0$. Сада посматрајмо најмање i и j такве да $p \nmid b_i$ и $p \nmid c_j$. Онда је:

$$a_{i+j} = b_i c_j + (b_{i-1}c_{j+1} + ...) + (b_{i+1}c_{j-1} + ...).$$

Додатно, приметимо да $p^2 \nmid b_0 c_0$ па мора да важи $i = 0$ или $j = 0$, односно $i + j < n$. Сада имамо да p дели сваки од чланова у заградама као и a_{i+j}, па мора да дели и $b_i c_j$, што је у супротности са претпоставком. □

Доказ (Ајзенштајн). Није могуће применити Ајзенштајнов критеријум директно на $\Phi_p(x)$. Уместо тога погледајмо како изгледа $\Phi_p(x+1)$:

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + x^{p-1}\binom{p}{1} + ... + x\binom{p}{p-2} + \binom{p}{p-1}.$$

Дати полином испуњава услове критеријума па можемо закључити да је $\Phi_p(x)$ нерастављив у $\mathbb{Z}[x]$, а самим тим и у $\mathbb{Q}[x]$ по Гаусовој леми. □

Испоставља се да су Шонеманов и Ајзенштајнов критеријум еквивалентни. Ајзенштајнов критеријум је данас далеко познатији од Шонемановог упркос томе што је Шонеманов старији.

Сада ћемо се позабавити општим случајем.

Теорема 4.2. Нека је n произвољан природан број. Онда је $\Phi_n(x)$ нерастављив над $\mathbb{Q}[x]$.

Први да покаже ово тврђење био је Кронекер 1854. [9] године. Његов доказ је елементаран али крајње компликован и дуг па га нећемо показати овде. Заснива се на индукцији по простим факторима броја n и знатно се разликује од било ког другог приступа овом проблему.

Сви остали докази, сем Ландауовог (1929) [10], заснивају се на показивању да уколико је $f(x)$ нерастављиви фактор $\Phi_n(x)$, ζ његов корен и p прост број који не дели n, онда је и ζ^p корен $f(x)$. Ландау показује да то мора важити, не само за p, него и за све k узајамно просте с n. Сада ћемо показати Дедекиндов доказ.

Доказ (Дедекинд). Нека је $f(x)$ неки нерастављиви фактор $\Phi_n(x)$ и нека је ζ такво да је $f(\zeta) = 0$ и $f(\zeta^p) \neq 0$ за неки прост број p који не дели n. По Гаусовој леми $f(x) = (x - \zeta_1)...(x - \zeta_k)$ има све целобројне коефицијенте. Сада посматрајмо полином $f_p(x) = (x - \zeta_1^p)...(x - \zeta_k^p)$. Још у Гаусовом доказу смо показали да овакав полином има целобројне коефицијенте, а сада имамо и $f(x) \equiv f_p(x) \pmod{p}$.
Полином $f_p(x)$ је такође нерастављив. У супротном би $f_p(x)$ имао неки нерастављив фактор $h(x)$. Тада би $h_q(\zeta^{pq}) = h_q(\zeta) = 0$ за неки природан број q такав да је $pq \equiv 1 \pmod{n}$ што је у супротности с нерастављивошћу $f(x)$.

Како су $f(x)$ и $f_p(x)$ различити нерастављиви полиноми и $f(\zeta) = f_p(\zeta^p) = 0$, то $f(x)f_p(x) \mid x^n - 1$.

Сада се пребацимо у поље $\mathbb{Z}_p$: У том пољу важи $f(x) = f_p(x)$, па $f(x)^2 \mid x^n - 1$ што је супротно теореми 2.7, пошто је $(x^n - 1, nx^{n-1}) = 1$. □

Показали смо да су циклотомични полиноми нерастављиви над $\mathbb{Q}[x]$. Шта је случај са другим пољима? Над $\mathbb{R}[x]$ и $\mathbb{C}[x]$ они су тривијално растављиви на квадратне и линеарне полиноме. У $\mathbb{Z}_p[x]$ ствари су мало другачије. О томе најбоље сведочи следећа теорема коју ћемо навести без доказа.

Теорема 4.3. Нека је n природан број и p прост такав да је $(n, p) = 1$. Нека је $d = \mathrm{ord}_p(n)$ (поредак броја по простом модулу). Онда је $\Phi_n(x)$ производ $\frac{\varphi(n)}{d}$ нерастављивих полинома степена тачно d у $\mathbb{Z}_p[x]$.

Последица. Нека је n природан број и p прост такав да је $(n, p) = 1$. Онда је $\Phi_n(x)$ нерастављив над $\mathbb{Z}_p[x]$ ако и само ако је $\mathrm{ord}_p(n) = \varphi(n)$, односно ако и само ако је n примитивни корен по модулу p.

5

Веза циклотомичних полинома и поретка броја по простом модулу

Лема 3. Нека је n природан број и $d < n$ неки његов делилац. Ако је p прост број такав да дели и $\Phi_n(x)$ и $\Phi_d(x)$ за неко целобројно x, онда $p \mid n$.

Доказ. По теореми 3.1 је $x^n - 1$ дељиво и са $\Phi_n(x)$ и са $\Phi_d(x)$. Када се пребацимо у $\mathbb{Z}_p$, то значи да $x^n - 1$ има двоструку нулу, па по теореми 2.8 $p \mid n$. □

Последица. Нека су m, n природни бројеви, p прост такав да $p \nmid mn$ и a произвољан цео број. Тада $p \nmid (\Phi_n(a), \Phi_m(a))$.

Лема 4. Нека су m, n природни бројеви и p прост такав да $p \nmid mn$. Онда у $\mathbb{Z}_p$ важи $(\Phi_n(x), \Phi_m(x)) = 1$.

Доказ. Претпоставимо супротно, $(\Phi_n(x), \Phi_m(x)) = f(x) > 1$. Како $\Phi_n(x)\Phi_m(x) \mid x^{mn} - 1$, то $f(x)^2 \mid x^{nm} - 1$, па по теореми 2.8 $p \mid mn$ што је у супротности с тврђењем леме. □

Дефиниција 5.1. Нека је a цео број, а p прост. Поретком броја a по простом модулу p, у ознаци $\mathrm{ord}_p(a)$, називамо најмањи природан број k за који важи $a^k \equiv 1 \pmod{p}$.

Слично као код корена јединице, овде опет важи да уколико је $a^k \equiv 1 \pmod{p}$ онда $\mathrm{ord}_p(a) | k$. Специјално, $\mathrm{ord}_p(a) | p - 1$.

Сада ћемо навести пар битнијих теорема и њихове доказе.

Теорема 5.1. Нека је p прост број. Тада за све природне бројеве n који нису дељиви са p и целе бројеве a важи да $p \mid \Phi_n(a)$ акко је $\mathrm{ord}_p(a) = n$.

Доказ. Доказ ћемо спровести индукцијом по n. За $n = 1$ тврђење очигледно важи. Претпоставимо да тврђење важи за све $k < n$.

Претпоставимо да за неко a важи $p \mid \Phi_n(a)$. Онда је $a^n \equiv 1 \pmod{p}$. Претпоставимо супротно, да је $\mathrm{ord}_p(a) = k < n$ и $k \mid n$. Онда по индуктивној хипотези имамо $\Phi_k(a) = 0$, па по леми 3 имамо да $p \mid n$ што је супротно услову из теореме.

Нека је $\mathrm{ord}_p(a) = n$. Онда је $0 \equiv a^n - 1 = \prod_{k|n} \Phi_k(a)$ па $p|\Phi_k(a)$ за неко k које дели n. То k мора бити управо n јер у супротном имамо то да $p \mid a^k - 1$ што је супротно претпоставци да је поредак броја a једнак n.

Тако смо доказали оба смера теореме. □

Теорема 5.2. Нека је n природан и a цео број. Тада за сваки прост делилац p броја $\Phi_n(a)$ важи или $p \equiv 1 \pmod{n}$ или $p \mid n$.

Доказ. Имамо да $p \mid \Phi_n(a)$ па $p \mid a^n - 1$, тј. $a^n \equiv 1 \pmod{p}$. Нека је $k = \mathrm{ord}_p(a)$. Онда $k \mid n$. Сада имамо 2 опције:

1. $k = n$: Из Мале Фермаове теореме имамо да је $a^{p-1} \equiv 1 \pmod{p}$. Сада $n \mid p - 1$, односно $p \equiv 1 \pmod{n}$.

2. $k < n$: Онда имамо:
$$p \mid a^k - 1 = \prod_{d|k} \Phi_d(a),$$
па $p \mid \Phi_d(a)$ за неко d које дели k а самим тим и n. Тада, уз чињеницу да $p \mid \Phi_n(a)$, по леми 3 имамо да $p \mid n$.

□

Теорема 5.3. Нека су a и b природни бројеви, $a \neq b$. Уколико за неко цело x важи
$$(\Phi_a(x), \Phi_b(x)) > 1,$$
онда су и $\frac{a}{b}$ и $(\Phi_a(x), \Phi_b(x))$ целобројни степени неког истог простог броја p.

Доказ. Нека је p прост број који дели и $\Phi_a(x)$ и $\Phi_b(x)$. Показаћемо да уколико је $a = p^\alpha A$ и $b = p^\beta B$, где је $(p, A) = (p, B) = 1$, онда важи $A = B$.

Покажимо да $p \mid \Phi_a(x)$. Уколико је $\alpha = 0$ онда смо готови јер $p \mid \Phi_a(x) = \Phi_A(x)$. У супротном, имамо да из теореме 3.5 важи:
$$0 \equiv \Phi_a(x) \equiv \Phi_a(x)\Phi_A(x^{p^\alpha - 1}) = \Phi_A(x^{p^\alpha}) \pmod{p},$$
па $p \mid \Phi_A(x^{p^\alpha})$. Међутим, по Малој Фермаовој теореми имамо да је $x^{p^\alpha} \equiv x \pmod{p}$, па је:
$$0 \equiv \Phi_A(x^{p^\alpha}) \equiv \Phi_A(x) \pmod{p}.$$
Аналогно, $p \mid \Phi_b(x)$.

Нека је $g = (A, B)$. Пошто $p \mid \Phi_A(x) \mid x^A - 1$ и $p \mid \Phi_B(x) \mid x^B - 1$, то $p \mid (x^A - 1, x^B - 1)$, тј. $p \mid x^g - 1 = \prod_{d|g} \Phi_d(x)$.

Сада постоји неко $d|t|A$ такво да $p \mid \Phi_d(x)$. Како $p \nmid A$, то је, по леми 3, могуће само уколико је $d = t = A$. Аналогно се добија да мора важити и $t = B$, одакле следи да је $A = B$ што је и требало показати.

Што се тиче другог дела теореме, довољно је да претпоставимо да $(\Phi_a(x), \Phi_b(x))$ има неки други прости делилац. Аналогно би важило да је сада a/b степен тог другог простог броја што није могуће. □

6

Неке примене циклотомичних полинома

Циклотомичне полиноме је проучавао још Гаус почетком 19. века. Њихову нерастављивост користио је да покаже који се правилни многоуглови могу конструисати лењиром и шестаром. То је била једна од првих веза апстрактне алгебре са геометријом. Сама нерастављивост циклотомичних полинома представља јако битан резулат у теорији поља и теорији Галоа. Циклотомична проширења поља $\mathbb{Q}$ су имали кључне улоге у апстрактној алгебри и теорији бројева због њихове везе са Великом Фермаовом теоремом.

Још један од познатијих примера циклотомичних полинома у алгебри јесте доказ Ведербурнове теореме. Она тврди како је свако коначно тело уједно и поље.

У претходној глави видели смо нешто мало о вези циклотомичних полинома и поретка бројева по простом модулу. Та тврђења, уз остала, их чине врло подобним за коришћење у задацима из теорије бројева. У наредном делу ћемо приказати доказ једне теореме познате међу такмичарима као и примере задатака у којима се могу искористити циклотомични полиноми.

6.1 Жигмондијева теорема

Теорема 6.1 (Жигмондијева теорема)**.** Нека су a и n природни бројеви већи од 1. Тада постоји прост делилац броја $a^n - 1$ такав да не дели $a^j - 1$ за све $0 < j < n$ осим у случајевима:

1. $n = 2,\ a = 2^s - 1,$ где је $s \geq 2,$
2. $n = 6,\ a = 2.$

Ово тврђење је еквивалентно томе да за све природне $a, n > 1$ можемо наћи прост број p такав да је $\mathrm{ord}_p(a) = n$ сем у наведеним случајевима.

Лема 5. Нека су $a, n > 1$ природни бројеви. Нека сви прости делиоци броја $\Phi_n(a)$ деле и број n. Онда је $\Phi_n(a)$ прост број који дели n или је $n = 2$.

Доказ. Посматрајмо прост делилац p броја $\Phi_n(a)$. Нека је $k = \mathrm{ord}_p(a)$.

Сада на основу теореме 5.1 имамо да $p \mid \Phi_k(a)$, па по теореми 5.3 следи да је $\frac{n}{k} = p^t$ за неки природан t.

Даље је $x^n - 1 = \Phi_n(x)Q(x)$ за неки полином $Q(x)$. Приметимо да $(x^{n/p} - 1) \mid Q(x)$, пошто ни један корен $x^{n/p} - 1$ није примитивни n-ти корен јединице.

Претпоставимо да је p непаран прост број. Пошто $(a^{n/p} - 1)\Phi_n(a) \mid (a^n - 1)$, то по познатој Леми о подизању степена (видети [11]) највећи степен броја p који дели n може бити највише 1. Како $p \mid \Phi_n(x)$, то је тај степен тачно 1.

Претпоставимо супротно, нека постоји и неки други прост број q који дели $\Phi_n(x)$. Онда применом истих аргумената као и горе добијамо:

$$n = p^x \mathrm{ord}_p(a) = q^y \mathrm{ord}_q(a).$$

Из тога имамо да $p \mid \mathrm{ord}_q(a)$ и $q \mid \mathrm{ord}_p(a)$. Додавајући то на чињеницу да $\mathrm{ord}_p(a) \mid p - 1$ и $\mathrm{ord}_q(a) \mid q - 1$, добијамо да $p \mid q - 1$ и $q \mid p - 1$ што је немогуће.

Остао нам је још случај када је $\Phi_n(a)$ степен двојке. Тада је $\mathrm{ord}_2(a) = 1$ па је слично као раније и n степен двојке. Сада је $\Phi_{2^x}(a) = a^{2^{x-1}} + 1 \equiv 2 \pmod 4$. То није могуће за $n > 2$, па смо готови. □

Лема 6. Нека су $a, n > 1$ природни бројеви. Нека је $n = p^k r$ где је p прост који не дели r. Тада имамо $\Phi_n(a) > (b^{p-2}(b-1))^{\varphi(r)}$ где је $b = a^{p^{k-1}}$.

Доказ. На основу последице теореме 3.5 имамо:

$$\Phi_n(x) = \frac{\Phi_r(b^p)}{\Phi_r(b)}.$$

Сада можемо приметити:

$$\Phi_r(b^p) = \prod(b^p - \zeta_k) = \prod |b^p - \zeta_k| \geq |b^p - 1|^{\varphi(r)}$$

Аналогно:

$$\Phi_r(b) = \prod(b - \zeta_k) = \prod |b - \zeta_k| \leq |b + 1|^{\varphi(r)}$$

Из ове две неједнакости имамо да је:

$$\Phi_n(a) \geq \left(\frac{b^p - 1}{b + 1}\right)^{\varphi(r)}$$

То у комбинацији са $b^p - 1 > b^{p-2}(b^2 - 1)$ даје тражену неједнакост. □

Докажимо сада Жигмондијеву теорему.

Доказ. Лако се види да теорема не важи у специјалним случајевима. За $n = 2$ теорема тривијално важи. Сада претпоставимо да је $n > 2$. Претпоставимо супротно, да не постоји такав прост q. Ако постоји прости делилац броја $\Phi_n(a)$ који не дели n онда смо готови по теореми 5.1. У супротном по леми 5 имамо да је $\Phi_n(a) = p$ за неко просто p које дели n.

Нека је $n = p^k r$, $(p, r) = 1$. Онда по леми 6 имамо:

$$\Phi_n(a) = p > (b^{p-2}(b-1))^{\varphi(r)},$$

где је $b = a^{p^{k-1}}$. За $p \geq 5$ ово тврђење очигледно не важи. Остаје још да проверимо шта је када је $p = 3$. Онда је због неједнакости $a = 2$ и $n = 3$ или $n = 6$. Први случај се лако проверава, а други смо навели као изузетак. Покрили смо све случајеве па је доказ завршен. □

Жигмондијева теорема је вероватно познатија у својој општијој варијанти. Наводимо је без доказа.

Теорема 6.2 (Жигмондијева теорема (ген.))**.** Нека су a и b природни бројеви такви да је $a > b > 0$ и n природан број већи од 1. Тада број $a^n - b^n$ има прост делилац који не дели $a^j - b^j$ за све $0 < j < n$ осим у случајевима:

1. $n = 2$, $a + b = 2^s$, где је $s \geq 2$ и
2. $n = 6$, $a = 2$, $b = 1$.

6.2 Примена у неким задацима

Задатак 1 (Специјалан случај Дирихлеове теореме)**.** Нека је n природан број. Тада постоји бесконачно много простих бројева p, таквих да је $p \equiv 1 \pmod{n}$.

Решење. За $n = 1$ и $n = 2$ тврђење очигледно важи. Нека је $n > 2$. Претпоставимо супротно, да постоји коначно много простих бројева који задовољавају услове задатка. Нека је x производ таквих простих бројева. Посматрајмо $\Phi_n(nx)$:

$$\Phi_n(nx) \geq (nx-1)^{\varphi(n)} \geq 2.$$

Сада посматрајмо прост број p који дели $\Phi_n(nx)$. Онда $p \mid (nx)^n - 1$ па $p \nmid nx$. По теореми 5.2 је $p \equiv 1 \pmod{n}$, што је супротно претпоставци да је x производ свих таквих бројева. □

Задатак 2. За које природне бројеве n се полином:

$$p(x) = 1 + x^n + x^{2n}$$

може записати као производ два полинома са целобројним коефицијентима (степена ≥ 1)?

Решење. Приметимо:

$$p(x) = \frac{x^{3n}-1}{x^n-1} = \frac{\prod_{d|3n}\Phi_d(x)}{\prod_{d|n}\Phi_d(x)} = \prod_{\substack{d|3n \\ d\nmid n}}\Phi_d(x).$$

Сада ако је $n = 3^k$ за неки природан k, онда је $p(x) = \Phi_{3^{k+1}}(x)$, па је $p(x)$ нерастављив. У супротном, претпоставимо да је $n = m \cdot 3^k,\ (m,3) = 1$. Онда полиноми $\Phi_{m3^{k+1}}$ и $\Phi_{3^{k+1}}$ оба деле $p(x)$ па смо готови. Одговор су сви природни бројеви n који нису степен броја 3. □

Задатак 3 (Предлог за ИМО 2006)**.** Нађи сва целобројна решења једначине:

$$\frac{x^7-1}{x-1} = y^5 - 1.$$

Решење. Приметимо да је та једначина еквивалентна са једначином $\Phi_7(x) = (y-1)\Phi_5(y)$. Сваки прост делилац p броја $y-1$ дели и $\Phi_7(x)$ па је по теореми 5.2 или $p = 7$ или $p \equiv 1 \pmod 7$. Одатле се добија $y - 1 \equiv 0 \pmod 7$ или $y - 1 \equiv 1 \pmod 7$. Сада разликујемо 2 случаја:

1. $y \equiv 1 \pmod 7$, онда је $\Phi_5(y) \equiv 5 \not\equiv 0, 1 \pmod 7$,
2. $y \equiv 2 \pmod 7$, онда је $\Phi_5(y) \equiv 3 \not\equiv 0, 1 \pmod 7$.

Дакле, једначина нема целобројних решења. □

Задатак 4. Нека је n природан број. Доказати да се број $2^{2^n} + 2^{2^{n-1}} + 1$ може представити као производ бар n (не нужно различитих) простих бројева.

Решење. По теореми 3.5 имамо:

$$2^{2^n} + 2^{2^{n-1}} + 1 = \Phi_3(2^{2^{n-1}}) = \prod_{d|2^{n-1}}\Phi_{3d}(2)$$

Како је $\Phi_{3d}(2) > 1$ то наш број већ има бар n простих делилаца.
Покажимо сада јаче тврђење, да су сви ови прости различити.
Довољно је да су свака два $\Phi_{3d}(2)$ узајамно проста што је управо директна последице теореме 5.3. □

Задатак 5 (ИМО 2003)**.** Нека је p прост број. Доказати да постоји прост број q такав да $q \nmid n^p - p$ за сваки природан број n.

Решење. Приметимо да уколико $q \mid n^p - p$, тада је $1 \equiv n^{q-1} \equiv p^{\frac{q-1}{p}}$. Сада је довољно да покажемо да постоји прост број q такав да је поредак броја p по модулу q једнак p (онда $p \mid q-1$) и да $p^2 \nmid q-1$.

Нека је q прост делилац броја $\Phi_p(p)$. Онда је по теореми 5.1 $\mathrm{ord}_q(p) = p$. Тада очигледно $p \mid q-1$. Претпоставимо да за овакво q важи $p^2 \mid q-1$. То уз чињеницу да $q \nmid p-1$ повлачи да је $1+p+...+p^{p-1} \equiv 1 \pmod{p^2}$ што није тачно. Одатле следи тврђење задатка. □

Задатак 6 (Предлог за ИМО 2002)**.** Нека су $p_1, p_2, ...p_n$ различити прости бројеви већи од 3. Доказати да број $2^{p_1p_2...p_n}+1$ има бар 4^n делилаца.

Решење. Поново, доказаћемо јаче тврђење, да дати број има бар $2^{2^{n-1}}$ делилаца.

Довољно је показати да број $2^{p_1p_2...p_n}+1$ има бар 2^{n-1} различитих узајамно простих делилаца. Приметимо да важи:

$$\begin{aligned}(2^{p_1p_2...p_n}-1)(2^{p_1p_2...p_n}+1) = 2^{2p_1p_2...p_n}-1 &= \prod_{d \mid 2p_1p_2...p_n} \Phi_d(2) \\ &= \left(\prod_{d \mid p_1p_2...p_n} \Phi_d(2)\right)\left(\prod_{d \mid p_1p_2...p_n} \Phi_{2d}(2)\right) \\ &= (2^{p_1p_2...p_n}-1) \prod_{d \mid p_1p_2...p_n} \Phi_{2d}(2).\end{aligned}$$

Одатле је:

$$2^{p_1p_2...p_n}+1 = \prod_{d \mid p_1p_2...p_n} \Phi_{2d}(2).$$

Посматрајмо делиоце d броја $p_1p_2...p_n$ који имају паран број простих делилаца. Њих има 2^{n-1}. По теореми 5.3, за свака два од њих је $(\Phi_{d_1}(2), \Phi_{d_2}(2)) = 1$ па смо готови. □

7

О коефицијентима циклотомичних полинома

На крају ћемо се мало позабавити коефицијентима циклотомичних полинома. Навешћемо нека занимљива тврђења у вези са њима. Раније смо показали једно јако битно тврђење, да су сви коефицијенти циклотомичних полинома цели бројеви. Такође смо показали и да су симетрични.

Покажимо за почетак једно тврђење о збиру коефицијената:

Теорема 7.1. Нека је n природан број. Онда је:

$$\Phi_n(x) = \begin{cases} p, \text{ ако је } n = p^k \text{ за неки прост } p \text{ и природан } k \\ 1, \text{ у супротном} \end{cases}$$

Доказ. Због теореме 3.4 можемо претпоставити да ниједан квадрат неког простог броја не дели n. Сада, уколико је $n = p$ прост, имамо $\Phi_n(x) = x^{p-1} + ... + 1$ па је $\Phi_n(1) = p$. У супротном, нека је p прост делилац броја n. Тада по последици теореме 3.5 имамо да је $\Phi_n(1) = \frac{\Phi_{n/p}(1^p)}{\Phi_{n/p}(1)} = 1$. □

Бацимо поново поглед на табелу 1. Поред тога што су сви коефицијенти целобројни, можемо још приметити и да сви припадају скупу $\{-1, 0, 1\}$. Да ли је то случај и за све остале? На први поглед изгледа као да јесте, али се испоставља да није. Први који не задовољава то тврђење је чак $\Phi_{105}(x)$ који има -2 као коефицијент. Иако број 105 изгледа мало насумично, испоставља се да то није случајност. Број 105 је први природан број који има 3 различита непарна проста делиоца. Мало више о овоме говоре наредних пар тврђења.

Лема 7. Нека су p и q неки различити прости бројеви. Тада важи:

$$(x^{pq} - 1)\Phi_{pq}(x) = (x - 1)\Phi_p(x^q)\Phi_q(x^p).$$

Доказ. По теореми 3.2 имамо следећа 3 идентитета:

$$x^{pq}-1=(x^p)^q-1=\Phi_q(x^p)\Phi_1(x^p)=\Phi_q(x^p)\Phi_p(x)\Phi_1(x)$$
$$x^{pq}-1=(x^q)^p-1=\Phi_p(x^q)\Phi_1(x^q)=\Phi_p(x^q)\Phi_q(x)\Phi_1(x)$$
$$x^{pq}-1=\Phi_{pq}(x)\Phi_p(x)\Phi_q(x)\Phi_1(x)$$

Тражени идентитет се добија када се производ прва два подели трећим. □

Лема 8. Нека су p и q неки различити прости бројеви. Онда су коефицијенти $P(x)=\Phi_p(x^q)\Phi_q(x^p)$ елементи скупа $\{0,1\}$.

Доказ. Знамо да је:

$$\Phi_p(x^q)\Phi_q(x^p)=\left(1+x^q+...+x^{(p-1)q}\right)\left(1+x^p+...+x^{(q-1)p}\right)=\sum_{\substack{0\le m<q\\0\le n<p}}x^{mp+nq}.$$

Сада је довољно показати да сваки члан суме има различити степен. Претпоставимо супротно, нека постоје n,m,n',m' такви да важи $mp+nq=m'p+n'q$. Онда је $p(m-m')=q(n'-n)$, па пошто су p и q различити прости, мора бити $p\mid n'-n$ и $q\mid m-m'$ што није могуће због ограничења сем када је $n=n'$ и $m=m'$. □

Теорема 7.2. Нека су p и q неки различити прости бројеви. Онда су коефицијенти $\Phi_{pq}(x)$ елементи скупа $\{-1,0,1\}$.

Доказ. По леми 5 имамо да важи:

$$(x^{pq}-1)\Phi_{pq}(x)=(x-1)\Phi_p(x^q)\Phi_q(x^p).$$

Како је $pq>\varphi(pq)$, можемо приметити да су сви степени $x^{pq}\Phi_{pq}(x)$ већи од степена $\Phi_{pq}(x)$ па је скуп коефицијената $(x^{pq}-1)\Phi_{pq}(x)$ исти као скуп коефицијената $\Phi_{pq}(x)$.

Сада је довољно показати да сви коефицијенти десне стране припадају скупу $\{-1,0,1\}$. По леми 6 знамо да су коефицијенти $x\Phi_p(x^q)\Phi_q(x^p)$ у $\{0,1\}$, као и да су коефицијенти $-\Phi_p(x^q)\Phi_q(x^p)$ у $\{-1,0\}$. Онда можемо закључити да су коефицијенти збира та два полинома у $\{-1,0,1\}$, што је и требало показати. □

Теорема 7.3. Нека је n произвољан непаран број с највише 2 непарна проста делиоца. Онда су његови коефицијенти елементи скупа $\{-1,0,1\}$

Доказ. У зависности од броја n разликујемо 4 различита случаја:

1. $n=p$ за прост p: Готови смо.

2. $n=pq$ за просте p,q: Готови смо по претходној теореми.

3. $n = 2pq$ за непарне просте p, q: По теореми 3.6 важи $\Phi_{2pq}(x) = \Phi_{pq}(-x)$ па се можемо позвати на претходни случај.

4. иначе: По теореми 3.4 се можемо опет позвати на претходни случај пошто је $\Phi_n(x) = \Phi_{2pq}(x^{\frac{n}{2pq}})$.

Тиме смо доказали тврђење теореме. □

Будимо пажљиви јер обрнуто не важи. На пример, $\Phi_{231}(x)$ има све коефицијенте $\{-1, 0, 1\}$ иако је $231 = 3 \times 7 \times 11$.

Сада када смо видели ово, природно се намеће следеће питање: Који све то бројеви могу бити њихови коефицијенти? Испоставља се да то могу бити сви цели бројеви.

У последњих 10-15 година, коефицијенти циклотомичних полинома су постали активно поље академског истраживања. Дошло се до разних закључака. Они углавном описују асимптоматско понашање коефицијената или неке неједнакости које их укључују. У овом раду се нажалост нисмо дотакли тог поља али препоручујем радозналима да погледају [13].

За крај рада ћу представити један леп доказ да се сваки цео број појављује као коефицијент циклотомичног полинома.

Теорема 7.4. Сваки цео број се појављује као коефицијент неког циклотомичног полинома.

Доказ. Показаћемо ово тврђење давањем конструкције за сваки цео број. Пре тога докажимо једну лему која ће нам бити потребна.

Лема. Нека је t прозвољан природан број већи од 2. Онда постоји t простих бројева $p_1 < p_2 < ... < p_t$ таквих да је $p_1 + p_2 > p_t$.

Доказ. Претпоставимо супротно, нека је t такво да ово тврђење не важи. Онда за било којих t простих $p_1 < p_2 < ... < p_t$ имамо да важи $p_1 + p_2 < p_t$. Одатле важи и $2p_1 < p_t$. Сада за сваки природан број k између бројева 2^{k-1} и 2^k мора бити мање од t простих бројева јер би у супротном било $2p_1 > 2 \cdot 2^{k-1} = 2^k > p_t$. Онда је $\pi(2^k) < kt$ што је у супротности са теоремом о простим бројевима. □

Сада се вратимо на доказ теореме. Нека је t неки непаран прост број већи од 1. Онда по леми постоје прости бројеви $p_1 < p_2 < ... < p_t$ такви да је $p_1 + p_2 > p_t$.

Рецимо да је $p = p_t$ и $n = p_1 p_2 ... p_t$. Посматрајмо полином $\Phi_n(x)$. Посматраћемо га mod x^{p+1} односно само последњих $p + 1$ коефицијената.

$$\begin{aligned}\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu\left(\frac{n}{d}\right)} &\equiv \frac{1}{x-1}\prod_{k=1}^{t}(x^{p_k} - 1) \pmod{x^{p+1}} \\ &\equiv (1 + x + ... + x^{p-1})(x^{p_1} - 1)...(x^{p_{t-1}} - 1) \pmod{x^{p+1}} \\ &\equiv (1 + x + ... + x^{p-1})(1 - x^{p_1} - ... - x^{p_{t-1}}) \pmod{x^{p+1}}\end{aligned}$$

Посматрајмо коефицијенте уз x^p и x^{p-2}. Они су редом $1-t$ и $2-t$. Сада како се t креће по непарним природним бројевима већим од 2 добијамо да коефицијент циклотомичног полинома може бити било који негативан цео број. Сада посматрајмо $\Phi_{2n}(x)$. По теореми 3.6 је $\Phi_{2n}(x) = \Phi_n(-x)$. Како су $p-1$ и $p-2$ непарни, то ће коефицијенти на њиховим местима у овим полиномима бити супротног знака па добијамо и класу полинома у којима се јавља сваки позитиван цео број. Пример полинома у којем се 0 јавља као коефицијент је $\Phi_4(x)$. Тиме смо завршили доказ. □

Литература

[1] M ans Edvardsson, Ida Grimheden, Arvid Kristoffersson, Jiachen Mi, and Emil Sandberg. Cyclotomic polynomials, 2023.

[2] Vukašin Brković. Ciklotomični polinomi, 2013.

[3] Gary Brookfield. The coefficients of cyclotomic polynomials. *Mathematical Magazine*, 89(3):179–188, 2016.

[4] F. G. M. Eisenstein. Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt. *Journal für die reine und angewandte Mathematik*, 39:160–179, 1850.

[5] Yves Gallot. Cyclotomic polynomials and prime numbers, 2001.

[6] Gauss. *Disquisitiones Arithmeticae*. 1801.

[7] Yimin Ge. Elementary properties of cyclotomic polynomials, 2008.

[8] Leopold Kronecker. Beweis, dass für jede Primzahl p die Gleichung $1+x+\cdots+x^{p-1}=0$ irreduzibel ist. *Journal für die reine und angewandte Mathematik*, 29:280, 1845.

[9] Leopold Kronecker. Mémoire sur les facteurs irréductibles de l'expression x^n-1. *Journal de Mathématiques Pures et Appliquées*, 19:177–192, 1854.

[10] Edmund Landau. Über die irreduzibilität der kreisteilungsgleichung. *Mathematische Zeitschrift*, 29:462–476, 1929.

[11] Amir Hossein Parvardi. Lifting the exponent lemma (lte), 2011.

[12] Brett Porter. Cyclotomic polynomials, 2015.

[13] Carlo Sanna. A survey on coefficients of cyclotomic polynomials. *Expositiones Mathematicae*, 40(3):469–494, 2022.

[14] Theodor Schönemann. Von denjenigen moduln, welche potenzen von primzahlen sind. *Journal für die reine und angewandte Mathematik*, 32:93–105, 1846.

[15] Joseph-Alfred Serret. Sur une question de théorie des nombres. *Journal de Mathématiques Pures et Appliquées*, 15:296–302, 1850.

[16] Lawrence Sun. Cyclotomic polynomials in olympiad number theory, 2013.

[17] Ravindranathan Thangadurai. On the coefficients of cyclotomic polynomials, 2000. In: Cyclotomic Fields and Related Topics, Bhaskaracharya Pratishthana, Pune, pp. 311–322.

[18] Steven H. Weintraub. Several proofs of the irreducibility of the cyclotomic polynomials, 2005.

[19] Steven H. Weintraub. The irreducibility of the cyclotomic polynomials. In Jr. John W. Dawson, editor, *Why Prove It Again? Alternative Proofs in Mathematical Practice*, pages 149–170. 2015.