UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Uroš Kovač

Posplošitev malega Fermatovega izreka

Delo diplomskega seminarja

Mentor: doc. dr. Primož Moravec

Ljubljana, 2012

Kazalo

Posplošitev malega Fermatovega izreka

Povzetek

Temeljni kamen mojega diplomskega seminarja je mali Fermatov izrek, ki pravi, da za vsako praštevilo p in vsako celo število a velja kongruenca $a^p \equiv a \pmod{p}$. Predstavljena je pot do malega Fermatovega izreka in povezanih rezultatov preko teorije grup. Izrek namreč lahko posplošimo na druga naravna števila, ne samo praštevila. Naš glavni izrek bo tako posplošitev malega Fermatovega izreka s pomočjo Möbiusove funkcije μ.

Spoznali bomo še Eulerjevo funkcijo φ, Möbiusovo inverzno formulo, se srečali z delovanji grup ter s tem povezanim štetjem orbit in fiksnih točk. Potrebovali bomo tudi kratek skok k polinomom in n-tim korenom enote v $\mathbb{C}$.

Generalization of Fermat's Little Theorem

Abstract

This thesis revolves around Fermat's Little Theorem which states that $a^p \equiv a \pmod{p}$ for any integer a and prime number p. I present a path to Fermat's Little Theorem and related results via group theory. The theorem can be generalized for all positive integers, not only prime numbers. Our main theorem will thus be a generalization of Fermat's Little Theorem with the aid of the Möbius function μ.

We will get to know Euler's function φ, Möbius inversion, group actions and related orbit counting and fixed point counting. We will also need a short trip to polynomials and roots of unity in $\mathbb{C}$.

Math. Subj. Class. (2010): 20A05, 11A07, 11A25

Ključne besede: končne grupe, kongruence, aritmetične funkcije

Keywords: finite groups, congruences, arithmetic functions

1. Od malega Fermatovega izreka do posplošitev

Francoski matematik Pierre de Fermat je svoj izrek, pozneje imenovan mali Fermatov, odkril okrog leta 1636. Prvi naj bi ga dokazal Gottfried Wilhelm Leibniz skoraj petdeset let pozneje. Izrek je dobil ime mali Fermatov izrek leta 1913 v knjigi Zahlentheorie nemškega matematika Kurta Hensla.

V nadaljevanju se bomo osredotočili na glavno posplošitev, ki jo bomo dokazali s pomočjo tehnike, ki še ni zelo razširjena. Potrebovali bomo posplošitev štetja orbit s pomočjo Cauchy-Frobeniusove leme, grupo n-tih korenov enote in povezavo med koreni enote ter Möbiusovo funkcijo.

Za začetek uvedemo pojem kongruenc.

$$a \equiv b \pmod{n} \iff n|a-b,$$

beremo a je kongruentno b po modulu n.

1.1. **Mali Fermatov izrek.**

Izrek 1.1 (Mali Fermatov izrek)**.** *Naj bo p praštevilo. Za vsako celo število a velja:*

$$a^p \equiv a \pmod{p}.$$

Naredili bomo dva dokaza, prvega s pomočjo indukcije, drugega pa z najosnovnejšim znanjem iz teorije grup.

Za dokaz z matematično indukcijo potrebujemo naslednjo lemo:

Lema 1.2. *Za poljubni celi števili a in b ter vsako praštevilo p velja:*

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

Dokaz. Uporabimo dobro znani binomski izrek:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}$$

Binomski koeficient $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$ je celo število. V števcu je za $i > 0$ večkratnik praštevila p, v imenovalcu pa p za $0 < i < p$ ne nastopa. Torej je $\binom{p}{i}$ deljivo s p za $0 < i < p$. Naša lema sledi. □

Prvi dokaz izreka 1.1. Za $a = 1$ dobimo $1^p \equiv 1 \pmod{p}$, kar očitno drži. Naredimo indukcijski korak: $k \to k+1$.
Naj izrek velja za $a = k$. Za $a = k+1$ s pomočje zgornje leme dobimo

$$(k+1)^p \equiv k^p + 1 \pmod{p}.$$

Upoštevamo še indukcijsko predpostavko $k^p \equiv k \pmod{p}$ in imamo želen rezultat

$$(k+1)^p \equiv k+1 \pmod{p}.$$

□

Opomba 1.3. Izrek je dokazan za pozitivna cela števila, argument za vsa cela števila pride v nadaljevanju.

Dokažimo še pomočjo teorije grup.

Drugi dokaz izreka 1.1. Množica $G = \{1, 2, 3, \ldots, p-1\}$ tvori grupo za množenje kongruenčnih razredov ostankov po modulu p. Asociativnost je očitna, saj je navadno množenje števil asociativno, enota je število 1. Edina stvar, ki ni trivialna, je obstoj inverza. Za poljuben b iz G velja, da je tuj proti p. V tem primeru vemo, da obstajata celi števili x in y, da velja $bx + py = 1$. Sledi $bx \equiv 1 \pmod{p}$. To pomeni, da ima vsak element iz G inverz za množenje po modulu p (tudi x ima ostanek pri deljenju, ki pripada množici G, ta ostanek je inverz za b). G je končna grupa, zato lahko govorimo o redu elementa a. Označimo ga s k. Torej $a^k \equiv 1 \pmod{p}$. Po temeljnem Lagrangevem izreku v teoriji grup vemo, da k deli $|G|$, tj. k deli $p-1$. Lahko zapišemo $p - 1 = km$ za neko celo število m. Potem velja:

$$a^p = a^{p-1}a = a^{km}a = (a^k)^m a \equiv 1^m a = 1a = a,$$

torej res $a^p \equiv a \pmod{p}$ za vsako celo število a. □

1.2. **Eulerjev izrek.** Prvi izrek, ki posploši mali Fermatov izrek, je Eulerjev izrek. Najprej povejmo, kaj je Eulerjeva funkcija φ in kaj popoln ter reduciran sistem ostankov.

Definicija 1.4. *Eulerjeva funkcija* $\varphi(n)$ prešteje naravna števila, ki so manjša od n in hkrati tuja proti n.

Primer 1.5. $\varphi(9) = 6$, saj so števila $1, 2, 4, 5, 7, 8$ tuja proti 9.
$\varphi(p) = p - 1$, kjer je p praštevilo, saj so števila $1, 2, \ldots, p-1$ očitno tuja proti p.

Definicija 1.6. *Popoln sistem ostankov* pri deljenju z n tvori množica števil $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

Vsako celo število da pri deljenju z n ostanek, ki je element popolnega sistema ostankov pri deljenju z n. Lahko je videti, da ta množica tvori abelovo grupo za seštevanje po modulu n.

Definicija 1.7. *Reduciran sistem ostankov* pri deljenju z n pa je podmnožica popolnega sistema ostankov pri deljenju z n in vsebuje tiste elemente popolnega sistema, ki so tuji proti n, $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : D(a, n) = 1\}$.

Reduciran sistem tvori abelovo grupo za množenje po modulu n. 0 ne pripada reduciranemu sistemu, saj privzamemo, da je največji skupni delitelj števil 0 in n; $D(0, n) = n$. Število elementov reduciranega sistema ostankov pri deljenju z n je torej enako $\varphi(n)$.

Trditev 1.8. *Imamo popoln sistem ostankov po modulu n ($\{0, 1, \ldots, n-1\}$) in reduciran sistem ostankov pri deljenju z n ($\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : D(a, n) = 1\}$). Naj bo b poljubno celo število, ki je tuje proti n, tj. $D(b, n) = 1$. Potem velja*

(1) $\{0, b, 2b, \ldots, (n-1)b\}$ *je popoln sistem ostankov po modulu n.*
(2) *Če z $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ označimo reduciran sistem ostankov pri deljenju z n, potem je tudi $\{br_1, br_2, \ldots, br_{\varphi(n)}\}$ reduciran sistem ostankov pri deljenju z n.*

Dokaz. Obe trditvi je lahko pokazati:

(1) Preverimo le, da so vsi elementi predstavniki različnih kongruenčnih razredov. Če je $bk \equiv bl \pmod{n}$, $k, l \in \mathbb{Z}_m$, potem $b(k-l) \equiv 0 \pmod{n}$, torej n deli $b(k-l)$. Števili b in n pa sta tuji, zato n deli $k - l$, se pravi $k \equiv l \pmod{n}$ in seveda $k = l$.

(2) Po (1) vemo, da so br_i sami različni elementi po modulu n. Pokažemo še, da so tuji proti n. Vemo $D(b,n) = 1$ in $D(r_i,n) = 1$, potem pa je tudi $D(br_i,n) = 1$. □

Izrek 1.9 (Eulerjev izrek)**.** *Naj bo $n \in \mathbb{N}$, $a \in \mathbb{Z}$ in $D(a,n) = 1$. Tedaj je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dokaz. Vemo že, da tvori $\mathbb{Z}_n^* = \{c_1, c_2, \ldots, c_{\varphi(n)}\}$ isto množico ostankov kot množica $\{ac_1, ac_2, \ldots, ac_{\varphi(n)}\}$, le da so permutirani. Sklepamo, da sta produkta $\prod_{j=1}^{\varphi(n)} c_j$ in $\prod_{j=1}^{\varphi(n)} ac_j$ enaka po modulu n:

$$\prod_{j=1}^{\varphi(n)} c_j \equiv \prod_{j=1}^{\varphi(n)} ac_j \pmod{n}.$$

Torej

$$\prod_{j=1}^{\varphi(n)} c_j \equiv a^{\varphi(n)} \prod_{j=1}^{\varphi(n)} c_j \pmod{n}.$$

Kongruenco lahko krajšamo, saj so vsi c_j tuji proti n (✿). Res dobimo

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

□

(✿): $ac \equiv bc \pmod{n} \iff n|ac - bc$, tj. $n|c(a-b)$. Če sta c in n tuji, potem $n|a-b$, torej $a \equiv b \pmod{n}$.

Primer 1.10. Za $a = -4$, $n = 12$ dobimo $(-4)^{\varphi(12)} \equiv 1 \pmod{12}$, $\varphi(12) = |\{1,5,7,11\}| = 4$. Ampak $(-4)^4 = 256 \not\equiv 1 \pmod{12}$, saj $256 = 12 \cdot 21 + 4$. Vidimo, da izrek ne velja za števila, ki si niso tuja, namreč $D(-4,12) \neq 1$.
Sedaj za a namesto -4 vzamemo -5, $D(-5,12) = 1$. Imamo $(-5)^{\varphi(12)} \equiv 1 \pmod{12}$ in to res drži, saj $(-5)^4 = 625 = 12 \cdot 52 + 1$.

Zakaj je Eulerjev izrek posplošitev malega Fermatovega izreka? Za praštevilo p vemo, da je $\varphi(p) = p - 1$. Po Eulerjevem izreku za celo število a, ki je tuje proti p, velja $a^{\varphi(p)} \equiv 1 \pmod{p}$, oziroma $a^{p-1} \equiv 1 \pmod{p}$, kar je ravno različica malega Fermatovega izreka, ki velja za cela števila a, ki so tuja proti p. V primeru, ko a in p nista tuja, zlahka ugotovimo, da mora p deliti a, torej p deli tudi a^p in velja $a^p \equiv a \pmod{p}$ za vsa cela števila a.

Mali Fermatov in Eulerjev izrek nam prideta zelo prav, ko se ubadamo s problemom deljivosti števil in kongruencami.

Primer 1.11. Pokažimo, da ima število $17^{1092 \cdot 1093}$ pri deljenju s številoma 1093 in1093^2 ostanek 1. Število 1093 je praštevilo, saj ni deljivo z nobenim praštevilom, ki je manjše od $\sqrt{1093} \doteq 33,1$. Po malem Fermatovem izreku je

$$(17^{1092})^{1093} \equiv 17^{1092} \pmod{1093}.$$

Po Eulerjevem izreku pa je

$$17^{\varphi(1093)} = 17^{1092} \equiv 1 \pmod{1093}.$$

Torej je tudi

$$(17^{1092})^{1093} \equiv 1 \pmod{1093}.$$

Naprej lahko zapišemo

$$(17^{1092})^{1093} = (1093b+1)^{1093}$$

za neko naravno število b. Razpišemo:

$$\begin{aligned}(1093b+1)^{1093} &= (1093b)^{1093} + \binom{1093}{1}(1093b)^{1092} + \cdots + \binom{1093}{1092}1093b + 1 \\ &= 1093^2 \cdot c + 1\end{aligned}$$

za neko naravno število c. Torej ima število $17^{1092\cdot 1093}$ res ostanek 1 pri deljenju s številoma 1093 in 1093^2.

1.3. **Glavni izrek.**

Definicija 1.12. Möbiusova funkcija μ je definirana za vsa naravna števila in zasede vrednosti v množici $\{-1, 0, 1\}$.

$$\mu(n) = \begin{cases} (-1)^k; & n = p_1 \cdot p_2 \cdots p_k \\ 0 \quad\;\; ; & p^2 \mid n \end{cases}$$

Primer 1.13. Za izračun Möbiusove funkcije potrebujemo praštevilski razcep naravnega števila.

- $\mu(42) = \mu(2 \cdot 3 \cdot 7) = (-1)^3 = -1$
- $\mu(60) = \mu(2^2 \cdot 3 \cdot 5) = 0$
- $\mu(858) = \mu(2 \cdot 3 \cdot 11 \cdot 13) = (-1)^4 = 1$
- Če p praštevilo, je $\mu(p) = (-1)^1 = -1$.

Izrek 1.14 (Glavni izrek)**.** *Naj bo a poljubno celo število, za vsako naravno število n velja:*

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) a^d \equiv 0 \pmod{n},$$

kjer je μ Möbiusova funkcija.

Primer, ko je a praštevilo, je poznal že Gauss; njegov dokaz je bil objavljen posmrtno leta 1863. Kdaj naj bi bil izrek najprej zapisan v obliki, ki jo poznamo danes, ni znano. Šele okrog leta 1880 se je prvič pojavil dokaz celotnega izreka. V letih 1880-1883 so bili namreč objavljeni štirje neodvisni dokazi, in sicer Kantorjev, Weyrov, Lucasov in Pelletov. Pozneje se je pojavilo še več različnih dokazov.

Če v izreku vzamemo $n = p$ praštevilo, dobimo

$$\sum_{d|p} \mu\left(\frac{p}{d}\right) a^d = \mu(p)a + \mu(1)a^p = a^p - a \equiv 0 \pmod{p},$$

in res pridemo do malega Fermatovega izreka, torej gre za posplošitev na vsa cela števila.

Primer 1.15. Poglejmo, kaj dobimo, če vzamemo $a = 7$, $n = 4$.

$$\begin{aligned}\sum_{d|n} \mu\left(\frac{n}{d}\right) a^d &= \sum_{d|4} \mu\left(\frac{4}{d}\right) 7^d \\ &= \mu(4) \cdot 7^1 + \mu(2) \cdot 7^2 + \mu(1) \cdot 7^4 \\ &= 0 + (-49) + 2401 \\ &= 2352,\end{aligned}$$

kar je res deljivo s 4.

2. Delovanje grupe

Prioriteta drugega poglavja bodo delovanja grupe na množici. Osnovno delovanje bomo razširili na inducirano delovanje, podali osnovne pojme povezane z delovanjem, Cauchy-Frobeniusovo lemo in polinomsko lemo, ki nam bo zagotovila veljavnost glavnega izreka tudi za negativna cela števila.

Definicija 2.1. Dani sta grupa G in poljubna množica Ω. *Delovanje* grupe G na množici Ω je preslikava

$$\rho : \Omega \times G \to \Omega,$$
$$\rho(\omega, g) = \omega g,$$

za katero velja:

- $\rho(\omega, 1) = \omega 1 = \omega$,
- $\rho(\omega, gh) = \omega(gh) = (\omega g)h = \rho(\omega g, h)$.

Primer 2.2. Znana delovanja grupe so

(1) Trivialno delovanje: $(\omega, g) \mapsto \omega$ za poljuben $\omega \in \Omega$ in $g \in G$.
(2) G deluje na G z običajnim množenjem: $(g, h) \mapsto gh$ za poljubna $g, h \in G$.
(3) G deluje na G s konjugiranjem: $(g, h) \mapsto h^{-1}gh$ za poljubna $g, h \in G$.

Za vsa tri delovanja z lahkoto preverimo, da ustrezajo zahtevam delovanja.

Definicija 2.3. Osnovni pojmi pri delovanju grupe G na množici Ω:

- *Orbita* elementa $\omega \in \Omega$:
$$\omega^G = \{\omega g : g \in G\}.$$
- *Stabilizator* elementa ω v grupi G:
$$G_\omega = \{g \in G : \omega g = \omega\}.$$
- *Fiksne točke*:
$$\mathrm{Fix}(g) = \{\omega \in \Omega : \omega g = \omega\}.$$

Trditev 2.4. *Množica orbit pri delovanju grupe G na množici Ω predstavlja razbitje množice Ω na disjunktne podmnožice.*

Dokaz. Vsak element $\omega \in \Omega$ je vsebovan v orbiti ω^G, saj $\omega 1 = \omega$. Unija vseh orbit je tako enaka Ω. Naj bosta $\omega, \beta \in \Omega$ in denimo, da imata orbiti ω^G in β^G neprazen presek, tj. obstaja $\gamma \in \omega^G \cap \beta^G$. Hočemo pokazati, da sta v tem primeru orbiti enaki. Najprej dokažemo, da je $\omega^G \subseteq \beta^G$. Vzamemo poljuben element $\delta \in \omega^G$. Obstajajo elementi $g, h, t \in G$, da je $\gamma = \omega g = \beta h$ in $\delta = \omega t$. Iz $\omega g = \beta h$ sledi, da je $\omega = \beta h g^{-1}$. Vstavimo v $\delta = \omega t$ in dobimo $\delta = (\beta h g^{-1})t = \beta h g^{-1} t = \beta h'$, $h' \in G$.

Torej $\delta \in \beta^G$. Če zamenjamo vlogi ω in β, na isti način dobimo še vsebovanost v drugo smer. Tako smo dokazali, da sta orbiti dveh elementov iz Ω disjunktni ali pa enaki. □

Trditev 2.5. *Naj končna grupa G deluje na množici Ω in naj bo ω poljuben element množice Ω. Tedaj velja enakost*

$$|G_\omega||\omega^G| = |G|.$$

Dokaz. Označimo z $G_{\omega,\beta}$ množico elementov grupe G, za katere velja $\omega g = \beta$, $G_{\omega,\beta} = \{g \in G : \omega g = \beta\}$. Če β ni element orbite ω^G, je množica $G_{\omega,\beta}$ prazna. Predpostavimo, da je $\beta \in \omega^G$, izberimo element $g \in G_{\omega,\beta}$ in definiramo preslikavo $f : G_{\omega,\beta} \to G$ s predpisom $f(h) = hg^{-1}$. Lahko je videti, da je f injektivna, saj velja:

$$f(h) = f(k) \text{ za poljubna } h, k \in G_{\omega,\beta} \iff hg^{-1} = kg^{-1} \iff h = k.$$

Slika funkcije f pa je enaka G_ω:

$$\begin{aligned}
\mathrm{Im}f &= \{f(h) : h \in G_{\omega,\beta}\} \\
&= \left\{hg^{-1} : h \in G_{\omega,\beta}, g \in G_{\omega,\beta}\right\} \\
&= \left\{hg^{-1} : \omega h = \beta, \omega g = \beta\right\} \\
&= \left\{hg^{-1} : \omega h = \omega g\right\} \\
&= \left\{hg^{-1} : \omega h g^{-1} = \omega\right\}
\end{aligned}$$

Torej je $\mathrm{Im}f \subseteq G_\omega$. Neenakost v drugo smer: dokazati moramo, da za vsak $g' \in G_\omega$ velja $g' \in \mathrm{Im}f$. Najti moramo tak $h \in G_{\omega,\beta}$, ki se preslika v g'. Preverimo, da je $h = g'g$ dober.

- h je res element $G_{\omega,\beta}$, tj. $\omega h = \beta$:

$$\omega h = \omega g' g = \omega g = \beta, \text{ saj } g' \in G_\omega \text{ in } g \in G_{\omega,\beta}.$$

- Slika elementa h je g':

$$f(h) = f(g'g) = g'gg^{-1} = g'.$$

Iz tega sledi, da je $|G_{\omega,\beta}| = |G_\omega|$, če le β pripada orbiti ω^G. V nasprotnem primeru, ko β leži izven ω^G, je $|G_{\omega,\beta}| = 0$. Definiramo vsoto moči množic $G_{\omega,\beta}$ po vseh $\beta \in \Omega$,

$$S := \sum_{\beta \in \Omega} |G_{\omega,\beta}|.$$

K vsoti S prispevajo samo tisti elementi β, ki ležijo v orbiti ω^G, vsak natanko $|G_\omega|$. Zato je

$$S = \sum_{\beta \in \omega^G} |G_\omega| = |G_\omega||\omega^G|.$$

Po drugi strani pa vsak element grupe G leži v natanko eni množici $G_{\omega,\beta}$, tisti, pri kateri je $\beta = \omega g$. Vsota S je potem enaka tudi $|G|$ in smo končali. □

2.1. **Cauchy-Frobeniusova lema.** Cauchy-Frobeniusovo lemo so najprej pripisali angleškemu matematiku Williamu Burnsideu, ki jo je ponovno odkril leta 1900. Šele kasneje se je razvedelo, da sta lemo že prej poznala Francoz Augustin-Louis Cauchy in Nemec Ferdinand Georg Frobenius. Cauchy je lemo v drugačni obliki zapisal že leta 1845, Frobenius pa jo je v sedanji obliki odkril leta 1887. Nekateri jo imenujejo kar lema, ki ni Burnsideova.

Lema 2.6 (Cauchy-Frobenius)**.** *Naj bo G končna grupa, ki deluje na končni množici Ω. Število orbit m je enako*

$$m = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|,$$

kjer $|\operatorname{Fix}(g)| = |\{\omega \in \Omega : \omega g = \omega\}|$.

Dokaz. Vse orbite delovanja grupe G označimo z $\Omega_1, \Omega_2, \ldots, \Omega_m$. Definirajmo še množico $M = \{(a, g) : a \in \Omega, g \in G_a\}$ in preštejmo njene elemente na dva načina. Najprej vidimo, da je moč množice M enaka vsoti moči vseh stabilizatorjev po vseh elementih a iz Ω. Poznamo že povezavo med močjo orbite in močjo stabilizatorja, $|G_a| = \frac{|G|}{|\Omega_i|}$, kjer je Ω_i orbita, ki vsebuje element a. Potem je

$$|M| = \sum_{a \in \Omega} |G_a| = \sum_{i=1}^{m} \sum_{a \in \Omega_i} \frac{|G|}{|\Omega_i|} = \sum_{i=1}^{m} |G| = m|G|.$$

Po drugi strani pa lahko definiramo množico

$$M_g = \{(a, g) : a \in \Omega, g \in G_a \text{ izbran}\} = \{(a, g) : a \in \operatorname{Fix}(g)\}$$

in tako

$$|M| = \sum_{g \in G} |\operatorname{Fix}(g)|.$$

Izenačimo, delimo z $|G|$ in dobimo želeno enakost. □

Zelo pogosto Cauchy-Frobeniusovo lemo uporabimo za štetje orbit induciranega delovanja.

Definicija 2.7. Naj grupa G deluje na množici Ω in naj bo A poljubna množica. *Inducirano delovanje* na množici S vseh preslikav iz Ω v množico A, $S = \{f : \Omega \to A\}$, definiramo kot preslikavo iz $S \times G$ v S:

$$(f, g) \mapsto fg,$$

$$(fg)(\omega) = f(\omega g^{-1}).$$

Z lahkoto preverimo, da je to res delovanje. Velja namreč

(1) $(f1)(\omega) = f(w1^{-1}) = f(w1) = f(w)$, saj je zaradi delovanja G na Ω $w1 = w$. To velja za vsak $\omega \in \Omega$, zato $f1 = f$.

(2) $(f(gh))(\omega) = f(\omega(gh)^{-1}) = f(\omega(h^{-1}g^{-1})) \overset{(*)}{=} f((\omega h^{-1})g^{-1}) = (fg)(\omega h^{-1}) = ((fg)h)(\omega)$ za vsak $\omega \in \Omega$, kjer smo pri $(*)$ uporabili že znano delovanje grupe G na Ω.

Opomba 2.8. V tem delu bomo imeli opravka s končnimi grupami in končnimi množicami, zato v nadaljevanju pridevnik končna pred grupo in pred množico opuščamo.

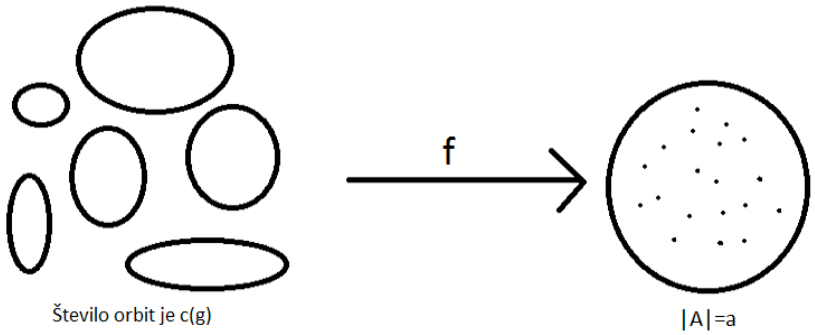
Zanima nas, kdaj element $g \in G$ pribije funkcijo f, tj. $(fg)(\omega) = f(\omega)$ za vsak $\omega \in \Omega$. Po definiciji je $(fg)(\omega) = f(\omega g^{-1})$, torej $f(\omega g^{-1}) = f(\omega)$ za vsak $\omega \in \Omega$. Sledi $f(\omega g^{-1}) = f((\omega g^{-1})g^{-1}) = f(\omega(g^{-1}g^{-1})) = f((\omega g^{-2})$ za vsak $\omega \in \Omega$ in tako naprej pridemo do spoznanja, da g pribije funkcijo f, če je f konstantna na vseh orbitah ciklične grupe $\langle g^{-1} \rangle$, ki deluje na Ω. Ciklična grupa $\langle g^{-1} \rangle$, ki je generirana z elementom g, je oblike $\{1, g^{-1}, g^{-2}, \ldots, g^{-m+1}\}$, kjer je m red elementa g^{-1}. Ciklična grupa $\langle g \rangle = \{1, g^1, g^2, \ldots, g^{m-1}\}$ je enaka ciklični grupi $\langle g^{-1} \rangle$, saj je za vsak element g^{-k} iz grupe $\langle g^{-1} \rangle$ tudi njegov inverz g^k element te grupe.

Koliko je potem $|\operatorname{Fix}(g)|$? Najprej s $c(g)$ označimo število orbit pri delovanju $\langle g \rangle$ na množici Ω. Funkcija f, ki jo g pribije, je določena s sliko enega elementa v vsaki izmed orbit. Naj bo moč množice A enaka a. Potem se vsi elementi iz določene orbite preslikajo v enega izmed elementov v A, vsi seveda v istega. Različnih funkcij, ki ustrezajo tej zahtevi, je tako $a^{c(g)}$. Iz Cauchy-Frobeniusove leme potem izpeljemo, da je število orbit m pri delovanju G na S enako

$$\frac{1}{|G|} \sum_{g \in G} a^{c(g)},$$

iz česar sledi

$$\sum_{g \in G} a^{c(g)} \equiv 0 \pmod{|G|}. \tag{1}$$



Slika 1. Funkcije, ki jih element g pribije.

Opomba 2.9. Delovanje grupe G na Ω je podano in določa $c(g)$, moč množice A pa je poljubno nenegativno celo število, saj končno množico A izberemo poljubno.

Primer 2.10. Naj bo G poljubna grupa moči n in naj G deluje sama na sebi z desnim množenjem. Delovanje je torej podano s preslikavo $G \times G \to G$. Za poljubna $g, h \in G$ velja $(h, g) \mapsto hg$. Za red elementa grupe vemo, da deli moč grupe (po Lagrangevem izreku). Naj ima $g \in G$ red $\operatorname{red}(g) = m$, g generira ciklično podgrupo grupe G: $\langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$. Poglejmo, kako $\langle g \rangle$ razbije G. Izberemo si poljuben $h \in G$ in poiščemo njegovo orbito $h^{\langle g \rangle}$.

$$\begin{aligned} (h, 1) &\mapsto h, \\ (h, g) &\mapsto hg, \\ &\vdots \\ (h, g^{m-1}) &\mapsto hg^{m-1}. \end{aligned}$$

Lahko je videti, da $hg^k \neq hg^l$ za $k \neq l$ in $1 \leq k, l \leq m-1$. Če bi namreč veljalo $hg^k = hg^l$, potem bi s krajšanjem dobili $g^{k-l} = 1$. Brez škode za splošnost predpostavimo $k > l$. Pridemo v protislovje, saj je m red grupe G, $k-l$ pa je gotovo manjše od m. Torej ima orbita elementa h m elementov. Vzemimo sedaj element $h' \in G - h^{\langle g \rangle}$. Podobno kot za h dobimo za h' orbito moči m. Nadaljujemo in ugotovimo, da $\langle g \rangle$ razbije G na $\frac{n}{m}$ orbit moči m. V naših oznakah to pomeni $c(g) = \frac{n}{m} = \frac{n}{red(g)}$. Vstavimo v (1) in dobimo

$$\sum_{g \in G} a^{\frac{n}{red(g)}} \equiv 0 \pmod{n}. \tag{2}$$

Kongruenca velja za vse nenegativne a, saj je moč končne množice A poljubna.

Uporabimo sedaj izpeljano kongruenco za ciklično grupo G praštevilske moči p. Zaradi Lagrangeovega izreka vemo, da imamo en element reda 1 (enota) in $p-1$ elementov reda p. Vstavimo v (2), da pridelamo

$$a^p + (p-1)a \equiv a^p - a \equiv 0 \pmod{p},$$

kar velja za vsa nenegativna cela števila. Do malega Fermatovega izreka nas loči še premislek za negativna cela števila. To pa ni težko, saj za praštevilo $p \neq 2$ z zamenjavo a za $-a$ v izrazu $a^p - a$ dobimo $-a^p + a = -(a^p - a)$, ki ima očitno spet ostanek 0 pri deljenju s p.

Za $p = 2$ nas prav tako čaka zelo malo dela. Za sodi a imata tako a kot a^2 ostanek 0 pri deljenju z 2. Za lihi a pa imata a in a^2 ostanek 1 pri deljenju z 2.
Tako smo na alternativen način prišli do malega Fermatovega izreka.

Opomba 2.11. Z vsako izbiro grupe G dobimo z vsoto $\sum_{g \in G} a^{c(g)}$ polinom v spremenljivki a, ki je zagotovo deljiv z močjo grupe G za vsako nenegativno celo število a. V resnici omejitev na nenegativne a ni potrebna zaradi sledeče leme.

Lema 2.12. *Naj bo f polinom z racionalnimi koeficienti in denimo, da je $f(a) \in \mathbb{Z}$ za vsa cela števila a, $0 \leq a \leq d$, kjer je d stopnja polinoma f. Potem je $f(a) \in \mathbb{Z}$ za vsa cela števila a.*

Opomba 2.13. Lema res poskrbi za negativna cela števila a, saj vemo, da je $\sum_{g \in G} a^{c(g)}$ deljiva z močjo grupe G, ko G deluje na G z desnim množenjem. To pa pomeni, da ima polinom z racionalnimi koeficienti $\frac{1}{|G|} \sum_{g \in G} a^{c(g)}$ za vrednosti cela števila pri nenegativnih celih številih. Lema nam zagotovi, da slednje velja tudi pri negativnih celih številih in je tako $\sum_{g \in G} a^{c(g)}$ deljiva z močjo grupe G, ko G deluje na G z desnim množenjem, tudi pri negativnih celih številih.

Dokaz. Dokazujemo s pomočjo dejstva, da lahko na binomske koeficiente gledamo kot na polinome. Binomski koeficienti so sledeče oblike za nenegativna cela števila m in poljubno kompleksno število X,

$$\binom{X}{m} = \frac{X(X-1)\cdots(X-m+1)}{m!},$$

kar si lahko predstavljamo kot polinom stopnje m z racionalnimi koeficienti. Množica

$$\left\{ \binom{X}{m} : 0 \leq m \leq d \right\}$$

je baza za vektorski prostor vseh polinomov stopnje največ d z racionalnimi koeficienti. Množica namreč vsebuje $d+1$ neodvisnih polinomov (vsi so različnih stopenj). Vsak polinom $f(X)$ v besedilu leme lahko potem zapišemo v obliki

$$f(X) = \sum_{m=0}^{d} a_m \binom{X}{m},$$

kjer so koeficienti a_m racionalni. Vemo $\binom{n}{n} = 1$ in $\binom{n}{m} = 0$, če $m > n$. Tako lahko za celo število n, $0 \leq n \leq d$, zapišemo

$$f(n) = a_0 \binom{n}{0} + a_1 \binom{n}{1} + \cdots + a_{n-1} \binom{n}{n-1} + a_n. \tag{3}$$

Po predpostavki je $f(n) \in \mathbb{Z}$ za $0 \leq n \leq d$, prav tako so binomski koeficienti cela števila, zato z indukcijo pokažemo, da so vsi a_i, $i = 0, 1, \ldots, n$, cela števila. Za $n = 0$ dobimo $f(0) = a_0$, ki je celo število po predpostavki. Naj velja, da so $a_0, a_1, \ldots, a_{n-1}$ cela števila.
Po (3) je $a_n = f(n) - (a_0\binom{n}{0} + a_1\binom{n}{1} + \cdots + a_{n-1}\binom{n}{n-1})$, kar je očitno spet celo število. Posplošimo še na vsa cela števila a. Vemo, da so koeficienti $a_0, a_1, \ldots, a_d$ cela števila in polinom f oblike

$$f(a) = a_0 \binom{a}{0} + a_1 \binom{a}{1} + \cdots + a_{d-1} \binom{a}{d-1} + a_d \binom{a}{d}$$

za vsako celo število a. Torej je dovolj pokazati, da so binomski koeficienti cela števila, kar za nenegativne a že vemo. Za negativna cela števila a pa velja zveza:

$$\begin{aligned} \binom{a}{k} &= \frac{a(a-1)\cdots(a-k+1)}{1 \cdot 2 \cdots k} \\ &= (-1)^k \frac{-a(-a+1)\cdots(-a+k-1)}{1 \cdot 2 \cdots k} \\ &= (-1)^k \binom{-a+k-1}{k}, \end{aligned}$$

kar je spet celo število. □

3. Posplošitev štetja orbit

Naslednja stvar, ki jo potrebujemo pri dokazu glavnega izreka, je posplošitev Cauchy-Frobeniusove formule za štetje orbit. Pomagali si bomo s pojmom λ-dobrih orbit.

Definicija 3.1. Naj bo G grupa, ki deluje na množici Ω, in λ homomorfizem iz G v $\mathbb{C}^*$, tj. grupo za množenje kompleksnih števil, $\mathbb{C}^* = \mathbb{C} - \{0\}$. Naj bo Θ ena izmed orbit, na katere delovanje grupe G razbije množico Ω. Pravimo, da je Θ *λ-dobra*, če je stabilizator G_θ vsake točke $\theta \in \Theta$ vsebovan v jedru homomorfizma λ, tj. $G_\theta \subseteq \ker(\lambda)$ za vsak $\theta \in \Theta$.

Izrek 3.2. *Naj bo λ homomorfizem iz končne grupe G v $\mathbb{C}^*$. Naj G deluje na končni množici Ω in naj bo M število λ-dobrih orbit tega delovanja. Potem je*

$$M = \frac{1}{|G|} \sum_{g \in G} \lambda(g) |\operatorname{Fix}(g)|.$$

Pri dokazovanju potrebujemo še dve lemi.

Lema 3.3. *Naj bo $\lambda : G \to \mathbb{C}^*$ netrivialen homomorfizem, kjer je G končna grupa. Tedaj velja*

$$\sum_{g \in G} \lambda(g) = 0. \tag{4}$$

Dokaz. Označimo $S = \sum_{g \in G} \lambda(g)$. Izberemo tak $h \in G$, da $\lambda(h) \neq 1$. Tak h obstaja, ker je λ netrivialen in ne preslika vseh elementov v enoto grupe za množenje $\mathbb{C}^*$, ki je 1. Vse je jasno v naslednji vrstici:

$$\lambda(h)S = \lambda(h) \sum_{g \in G} \lambda(g) = \sum_{g \in G} \lambda(hg) = S,$$

kjer smo najprej upoštevali, da je λ homomorfizem, nato pa še, da je množica $\{hg : g \in G\} = G'$ enaka grupi G. To je res, saj je preslikava iz G v G', ki elementu g priredi element hg, očitno bijekcija. Surjektivna je, ker je poljubni element hg v G' slika elementa g iz G. Injektivnost pa preverimo tako, da se vprašamo, kdaj imata lahko dva elementa iz G enaki sliki, tj. $hg_1 = hg_2$. S krajšanjem z leve ugotovimo, da le v primeru, ko sta elementa enaka. Torej različna elementa ne moreta imeti enakih slik in je preslikava res injektivna. □

Lema 3.4. *Naj bo Θ poljubna izmed orbit, na katere razpade množica Ω pri delovanju grupe G. Tedaj so si stabilizatorji poljubnih točk iz Θ izomorfni, tj. za poljubni točki α in β iz Θ velja $G_\alpha \cong G_\beta$.*

Opomba 3.5. Lema nam pove tudi, da so moči stabilizatorjev točk iz iste orbite enake, $|G_\alpha| = |G_\beta|$ za poljubni točki α, β v orbiti.

Dokaz. Če sta α,β v orbiti Θ, potem obstajata $g_1, g_2 \in G$, da velja $\alpha = \theta g_1$ in $\beta = \theta g_2$, kjer je θ predstavnik orbite Θ, tj. $\Theta = \theta^G$. Izrazimo θ iz prve enačbe in vstavimo v drugo, da pridemo do $\beta = \alpha g_1^{-1} g_2$. Označimo $g_1^{-1} g_2$ z g_0 in definiramo preslikavo $f : G_\alpha \to G_\beta$ s predpisom $f(g) = g_0^{-1} g g_0$. Preverimo, da je ta preslikava izomorfizem.

- Dobra definiranost: pokazati hočemo, da je za vsak $g \in G_\alpha$ velja $f(g) \in G_\beta$, tj. $\beta f(g) = \beta$. To drži, saj je
$$\beta f(g) = \beta g_0^{-1} g g_0 = \alpha g g_0 = \alpha g_0 = \beta,$$
kjer smo pri prvem in tretjem enačaju upoštevali povezavo med α in β, nato pa še dejstvo, da je $g \in G_\alpha$.
- Homomorfizem: $f(gh) = g_0^{-1} g h g_0 = g_0^{-1} g g_0 g_0^{-1} h g_0 = f(g) f(h)$
- Injektivnost: $f(g) = 1 \iff g_0^{-1} g g_0 = 1 \iff g g_0 = g_0 \iff g = 1$.
- Surjektivnost: preveriti moramo, da za vsak $h \in G_\beta$ obstaja $g \in G_\alpha$, da velja $f(g) = h$. Za h vemo, da je $\beta h = \beta$. Namesto β pišemo αg_0 in dobimo $\alpha g_0 h = \alpha g_0$ oziroma $\alpha g_0 h g_0^{-1} = \alpha$. Označimo $g_0 h g_0^{-1} = g$. Potem je $f(g) = g_0^{-1}(g_0 h g_0^{-1}) g_0 = h$, torej je preslikava res surjektivna. Vse zahteve za izomorfizem so tako izpolnjene.

□

Opomba 3.6. Če je stabilizator neke točke α iz orbite Θ vsebovan v $\ker(\lambda)$, tj. $\lambda(g) = 1$ za vsak $g \in G_\alpha$, so potem stabilizatorji vseh drugih točk prav tako vsebovani v $\ker(\lambda)$. Za poljubno drugo točko β torej velja $\lambda(h) = 1$ za vsak $h \in G_\beta$. To je res, saj zaradi izomorfizma, ki smo ga definirali v dokazu prejšnje leme, vemo, da je $h = g_0^{-1} g g_0$ za nek $g_0 \in G$ in posledično $\lambda(h) = \lambda(g_0^{-1} g g_0) = \lambda(g_0^{-1}) \lambda(g) \lambda(g_0) = \lambda(g_0^{-1}) \lambda(g_0) = \lambda(g_0^{-1} g_0) = \lambda(1) = 1$.

Dokaz izreka 3.2. Naj bodo $\Theta_1, \Theta_2, ..., \Theta_N$ orbite pri delovanju G na Ω. Naj bo $\sigma_i(g)$ število fiksnih točk v orbiti Θ_i, ki jih pribije element g, torej $\sigma_i(g) = |\{\theta \in \Theta_i : \theta g = \theta\}|$. Izberemo orbito Θ_i in definiramo

$$S_i = \sum_{g \in G} \lambda(g)\sigma_i(g).$$

Vsoto $\sum_{g\in G} \lambda(g)|\operatorname{Fix}(g)|$, ki nastopa v izreku, lahko zapišemo kot

$$\sum_{i=1}^{N} S_i.$$

Torej zadošča pokazati, da je

$$S_i = \begin{cases} |G|; & \text{če je } \Theta_i \ \lambda\text{-dobra} \\ 0 \ \ ; & \text{sicer.} \end{cases}$$

V tem primeru namreč dobimo

$$\sum_{g \in G} \lambda(g)|\operatorname{Fix}(g)| = \sum_{i=1}^{N} S_i = M|G|,$$

kar trdi izrek. Pobliže poglejmo vsoto S_i. Vsako kompleksno število $\lambda(g)$ je šteto $\sigma_i(g)$ krat. Drugače rečeno, šteto je enkrat za vsak urejen par (α, g), kjer $\alpha \in \Theta_i$, $g \in G$ in $\alpha g = \alpha$. Sledi, da lahko zapišemo

$$S_i = \sum_{\alpha \in \Theta_i} \sum_{g \in G_\alpha} \lambda(g).$$

Notranja vsota je po lemi 3.3, ki jo uporabimo na grupi G_α, enaka 0, če λ, zožen na G_α, ni trivialen homomorfizem, torej če G_α ni vsebovan v $ker(\lambda)$. V nasprotnem primeru je enaka $|G_\alpha|$, saj je takrat $\lambda(g) = 1$ za vse $g \in G_\alpha$. Od prej že poznamo povezavo med močjo stabilizatorja in orbite, po lemi 3.4 in opombi potem sledi, da je $|G_\alpha| = \frac{|G|}{|\Theta_i|}$, ko α preteče celo orbito Θ_i. V primeru, ko Θ_i ni λ-dobra orbita, tj. G_α ni vsebovan v $ker(\lambda)$, je tako $S = \sum_{\alpha\in\Theta_i} 0 = 0$. Če pa je Θ_i λ-dobra orbita, je $S = \sum_{\alpha\in\Theta_i} |G_\alpha| = |\Theta_i||G_\alpha| = |G|$. □

Opomba 3.7. $G_\alpha = \{g \in G : \alpha g = \alpha\}$ je res grupa, saj je podgrupa grupe G. Vsebuje namreč enoto ($\alpha 1 = \alpha$ po definiciji delovanja), inverz elementa $g \in G_\alpha$ je tudi v G_α ($\alpha g = \alpha \Rightarrow \alpha = \alpha g^{-1}$), prav tako pa je produkt dveh elementov iz G_α spet v G_α, saj $\alpha gh = \alpha h = \alpha$.

Nadaljujemo s posledico izreka 3.2. Vemo že, da je število fiksnih točk pri induciranemu delovanju grupe G na množici S vseh preslikav iz Ω v neko končno množico A, $|A| = a$, enako $a^{c(g)}$, kjer je $c(g)$ število orbit pri delovanju ciklične grupe $\langle g \rangle$ na Ω.

Posledica 3.8. *Naj bo G končna grupa, ki deluje na končni množici Ω. Naj bo λ poljuben homomorfizem iz G v $\mathbb{C}^*$. Potem za vsako celo število a velja*

$$\sum_{g \in G} \lambda(g)a^{c(g)} \equiv 0 \pmod{|G|}. \tag{5}$$

Dokaz. V izreku uporabimo, da je $|\operatorname{Fix}(g)| = a^{c(g)}$. Torej je vsota $\sum_{g\in G} \lambda(g)a^{c(g)}$ po izreku 3.2 deljiva z $|G|$. □

Definicija 4.1. Aritmetična funkcija je funkcija, ki slika iz naravnih števil v kompleksna števila.

4.1. Osnovno o multiplikativnih funkcijah.

Definicija 4.2. Aritmetična funkcija je multiplikativna, če je

$$f(mn) = f(m)f(n)$$

za poljubni tuji si naravni števili m, n, tj. največji skupni večkratnik $D(m, n) = 1$.

Trditev 4.3. *Naj bosta f in g multiplikativni funkciji. Potem velja*

(1) *fg in $\frac{f}{g}$ $(g \neq 0)$ sta multiplikativni.*

(2) *Funkciji*

$$h(n) = \sum_{a|n} f(a)g\left(\frac{n}{a}\right) \quad in \quad k(n) = \sum_{a|n} f(a)g(a)$$

sta prav tako multiplikativni.

Dokaz. (1)

$$\begin{aligned}(fg)(mn) &= f(mn)g(mn)\\ &= f(m)f(n)g(m)g(n)\\ &= f(m)g(m)f(n)g(n)\\ &= (fg)(m)(fg)(n),\end{aligned}$$

$$\begin{aligned}\frac{f}{g}(mn) &= \frac{f(mn)}{g(mn)}\\ &= \frac{f(m)f(n)}{g(m)g(n)}\\ &= \frac{f(m)}{g(m)} \cdot \frac{f(n)}{g(n)}\\ &= \frac{f}{g}(m)\frac{f}{g}(n).\end{aligned}$$

(2) Vsoto razbijemo na dve vsoti, kjer upoštevamo, da sta m in n tuji si števili:

$$\begin{aligned}h(mn) &= \sum_{a|mn} f(a)g\left(\frac{mn}{a}\right)\\ &= \sum_{b|m}\sum_{c|n} f(bc)g\left(\frac{mn}{bc}\right)\\ &= \sum_{b|m}\sum_{c|n} f(b)f(c)g\left(\frac{m}{b}\right)g\left(\frac{n}{c}\right)\\ &= \sum_{b|m} f(b)g\left(\frac{m}{b}\right)\sum_{c|n} f(c)g\left(\frac{n}{c}\right)\\ &= h(m)h(n).\end{aligned}$$

Podobno za k:

$$\begin{aligned} k(mn) &= \sum_{a|mn} f(a)g(a) \\ &= \sum_{b|m}\sum_{c|n} f(bc)g(bc) \\ &= \sum_{b|m}\sum_{c|n} f(b)f(c)g(b)g(c) \\ &= \sum_{b|m} f(b)g(b)\sum_{c|n} f(c)g(c) \\ &= k(m)k(n). \end{aligned}$$

□

4.2. **K Möbiusovi inverziji.**

Lema 4.4. *Möbiusova funkcija μ je multiplikativna.*

Dokaz. Ločimo primera:

- Eno izmed števil m, n je enako 1, denimo $m = 1$. Potem
$$\mu(mn) = \mu(n)$$
in
$$\mu(m)\mu(n) = \mu(1)\mu(n) = \mu(n).$$
- $m, n > 1$:

  (1) Tako m kot n imata v praštevilskem razcepu praštevila zastopana največ s potenco 1. Števili m in n sta tuji, zato bo enako veljalo tudi za produkt mn. Če ima m k faktorjev v praštevilskem razcepu in n l faktorjev, ima potem mn v praštevilskem razcepu $k + l$ faktorjev. Sledi
  $$\mu(m)\mu(n) = (-1)^k(-1)^l = (-1)^{k+l} = \mu(mn).$$
  (2) Če v praštevilskem razcepu m ali n nastopa prafaktor s potenco > 1, enako velja za produkt mn. Zato je $\mu(m)\mu(n) = \mu(mn) = 0$.

□

Trditev 4.5. *Uvedemo aritmetično funkcijo $\nu(n) := \sum_{d|n} \mu(d)$. Zanjo velja $\nu(1) = 1$ in $\nu(n) = 0$ za $n \geq 2$.*

Dokaz. Funkcija ν je multiplikativna po zgornji trditvi, kjer je $f = \mu$ in $g = 1$, ki sta seveda multiplikativni. Zadošča torej poznati vrednosti ν na potencah praštevil. Za vsako naravno število namreč obstaja enoličen praštevilski razcep, zato velja

$$\nu(p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}) = \nu(p_1^{k_1})\nu(p_2^{k_2})\cdots\nu(p_s^{k_s}).$$

Pri $n = 1$ trditev drži:

$$\nu(1) = \sum_{d|1} \mu(d) = \mu(1) = 1.$$

Za praštevilo p pa izračunamo

$$\nu(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) = 1 + (-1)^1 + 0 + \cdots + 0 = 0,$$

torej je res $\nu(n) = 0$ za $n \geq 2$. □

Pomembna je Möbiusova inverzna formula.

Izrek 4.6 (Möbiusova inverzija)**.** *Naj bo f aritmetična funkcija in $g(n) = \sum_{d|n} f(d)$. Potem je $f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$.*

Dokaz. Vse delitelje števila n si predstavljamo v parih. Označimo jih z $d_1, d_1', d_2, d_2', \ldots, d_k, d_k'$, kjer $d_i d_i' = n$, $d_i \leq d_i'$ in d_i, d_i' pretečejo vse delitelje od 1 do n. Potem ni težko videti, kako v nadaljevanju zamenjamo vsoti:

$$\begin{aligned}
\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} f(e) \\
&= \sum_{d|n} \sum_{e|\frac{n}{d}} \mu(d) f(e) \\
&= \sum_{e|n} \sum_{d|\frac{n}{e}} \mu(d) f(e) \\
&= \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) \\
&= \sum_{e|n} f(e) \nu\left(\frac{n}{e}\right) \\
&= f(n) \cdot 1 \\
&= f(n),
\end{aligned}$$

kjer na koncu uporabimo že dokazana dejstva o funkciji ν. □

Posledica 4.7. *Naj bo funkcija f aritmetična in $g(n) = \sum_{d|n} f(d)$ multiplikativna. Potem je f multiplikativna.*

Dokaz. Möbiusova inverzija nam da

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

Vemo, da sta μ in g multiplikativni funkciji, torej je po trditvi 4.3 tudi f multiplikativna. □

4.3. **Inačica glavnega izreka z Eulerjevo funkcijo.**

Lema 4.8 (Gauss)**.** *Za vsako naravno število n drži enakost*

$$\sum_{d|n} \varphi(d) = n$$

Dokaz. Za vsak d, ki deli n, naj bo n_d število elementov v množici $\mathbb{Z}_n$, katerih največji skupni delitelj z n je enak d. Naj bo $N_d \subseteq \mathbb{Z}_n$ množica vseh elementov, katerih največji skupni delitelj z n je d, $N_d = \{k \in \mathbb{Z}_n : D(k, n) = d\}$. Vsak element v $\mathbb{Z}_n$ očitno pripada natanko eni izmed množic N_d, saj je največji skupni delitelj en sam. Zato velja $\sum_{d|n} |N_d| = \sum_{d|n} n_d = n$. V N_d so števila, ki imajo z n skupen ravno d. Če ta števila delimo z d, dobimo števila, ki so tuja $\frac{n}{d}$ in manjša od $\frac{n}{d}$. Torej dobimo elemente v množici $\mathbb{Z}_{\frac{n}{d}}^*$ in to kar vse. Vsak $x \in \mathbb{Z}_{\frac{n}{d}}^*$ je namreč tuj proti $\frac{n}{d}$ ($D(x, \frac{n}{d}) = 1$), zato je $D(dx, d\frac{n}{d}) = D(dx, n) = d$, torej $dx \in N_d$. Sledi, da je

$|N_d| = n_d = |\mathbb{Z}^*_{\frac{n}{d}}| = \varphi(\frac{n}{d})$ in seveda $n = \sum_{d|n} n_d = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$, kjer si pri zadnjem enačaju lahko delitelje spet predstavljamo v parih (d_i, d_i'), $d_i d_i' = n$. □

Primer 4.9. Naj bo $n = 16$. Delitelji števila 16 so $1, 2, 4, 8, 16$. Množice N_d potem izgledajo tako:

$$\begin{aligned} N_1 &= \{1, 3, 5, 7, 9, 11, 13, 15\} \\ N_2 &= \{2, 6, 10, 14\} \\ N_4 &= \{4, 12\} \\ N_8 &= \{8\} \\ N_{16} &= \{0\}. \end{aligned}$$

N_d tvorijo disjunktno razbitje $\mathbb{Z}_n$ in $|N_d|$ je res enaka $\varphi(\frac{n}{d})$: $|N_1| = \varphi(16) = 8$, $|N_2| = \varphi(8) = 4$, $|N_4| = \varphi(4) = 2$, $|N_8| = \varphi(2) = 1$, $|N_{16}| = \varphi(1) = 1$.

Posledica 4.10. *Eulerjeva funkcija φ je multiplikativna.*

Dokaz. Sledi iz posledice 4.7. V našem primeru imamo

$$g(n) = n = \sum_{d|n} \varphi(d),$$

torej je φ res multiplikativna, saj je $g(n) = n$ očitno multiplikativna. □

Posledica 4.11. *Za Eulerjevo funkcijo φ velja:*

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}. \tag{6}$$

Dokaz. Uporabimo Möbiusovo inverzijo na Gaussovi lemi, kjer je $g(n) = n$. Sledi

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

□

Posledica 4.12. *Če je $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, kjer so p_i različna praštevila, potem je*

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right). \tag{7}$$

Dokaz. Izračunamo $\varphi(p^\alpha)$ s pomočjo prejšnje posledice:

$$\begin{aligned} \varphi(p^\alpha) &= \sum_{d|p^\alpha} \mu(d) \frac{p^\alpha}{d} \\ &= \mu(1)p^\alpha + \mu(p)\frac{p^\alpha}{p} + \mu(p^2)\frac{p^\alpha}{p^2} + \cdots \\ &= p^\alpha - \frac{p^\alpha}{p} \\ &= p^\alpha \left(1 - \frac{1}{p}\right). \end{aligned}$$

Upoštevamo multiplikativnost funkcije φ, da dobimo želen rezultat:

$$\begin{aligned}\varphi(n) &= \varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) \\ &= \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) \\ &= \prod_{i=1}^{k} p_i^{\alpha}\left(1-\frac{1}{p_i}\right) \\ &= \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \\ &= n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).\end{aligned}$$

□

Izrek 4.13. *Naj bo a poljubno celo število. Potem za vsako naravno število n velja:*

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) a^d \equiv 0 \pmod{n}.$$

.

Pred dokazom potrebujemo še sledečo trditev.

Trditev 4.14. *Naj bo G ciklična grupa reda n (lahko si jo predstavljamo kot $\mathbb{Z}_n$). Potem za vsak d, ki deli n, velja, da je v G natanko $\varphi(d)$ elementov reda d.*

Dokaz. Vemo $\varphi(d) = |\{(d,i) : i \leq d \text{ tuj proti } d\}|$. Označimo s T_d podmnožico $\mathbb{Z}_n$ vseh elementov reda d, $T_d = \{k \in \mathbb{Z}_n : \text{red}(k) = d\}$. Definiramo preslikavo $u : \{(d,i) : i \leq d \text{ tuj proti } d\} \to T_d$, $(d,i) \mapsto i\frac{n}{d}$ in pokažemo, da je bijekcija.

- Surjekcija: za vsak element k reda d velja $kd = in$ za nek $i \in \mathbb{N}_0$, $i < n$, kjer mora biti i tuj proti d, sicer bi bil red elementa k manjši od d. Torej je k res oblike $i\frac{n}{d}$, $D(d,i) = 1$.
- Injekcija: Recimo, da sta sliki elementov $(d,i_1), (d,i_2)$ enaki, tj. $i_1\frac{n}{d} = i_2\frac{n}{d}$. Očitno je to mogoče le, če je $i_1 = i_2$.

□

Dokaz izreka 4.13. Naj bo G ciklična grupa reda n. Po izpeljani enakosti (2) lahko zapišemo

$$\sum_{g\in G} a^{\frac{n}{red(g)}} \equiv \sum_{d|n} c_d a^d \equiv 0 \pmod{n} \quad \text{za neke koeficiente } c_d.$$

Koeficient c_d pri a^d pa je ravno enak številu elementov reda $\frac{n}{d}$, tj. $\varphi(\frac{n}{d})$ in smo dokazali. □

Primer 4.15. Vzamemo grupo $\mathbb{Z}_{18}$, $|G| = n = 18$. Poglejmo rede elementov:

$$\begin{aligned} &red \quad 1:0\\ &red \quad 2:9\\ &red \quad 3:6,12\\ &red \quad 6:3,15\\ &red \quad 9:2,4,8,10,14,16\\ &red\ 18:1,5,7,11,13,17. \end{aligned}$$

Moči množic elementov reda d res ustrezajo $\varphi(d)$. Za a izberemo 4 in poglejmo vsoto v izreku:

$$\begin{aligned} \sum_{d|18} \varphi\left(\frac{18}{d}\right) 4^d &= \varphi(18)4^1 + \varphi(9)4^2 + \varphi(6)4^3 + \varphi(3)4^6 + \varphi(2)4^9 + \varphi(1)4^{18}\\ &= 6\cdot 4 + 6\cdot 16 + 2\cdot 64 + 2\cdot 4096 + 1\cdot 262144 + 1\cdot 68719476736\\ &= 68719747320\\ &= 18\cdot 3817763740, \end{aligned}$$

torej je vsota res deljiva z 18.

5. Od korenov enote do dokaza glavnega izreka

5.1. **Koreni enote.**

Definicija 5.1. Kompleksno število z je $n-$ti *koren enote*, če velja $z^n = 1$. Pravimo, da je n-ti koren enote *primitiven*, če ni že k-ti koren enote za $k = 1, 2, \ldots, n-1$, $z^n = 1$, $z^k \neq 1$ za $k < n$.

Opomba 5.2. Število n-tih korenov enote je seveda n, saj smo v kompleksnih številih.

Primer 5.3. Za $n = 4$ dobimo korene enote $1, -1, i, -i$. Korena $1, -1$ nista primitivna, sta namreč korena enote že za $n = 2$. Korena $i, -i$ pa sta primitivna, saj nista korena enote za $k = 1, 2, 3$.

Potrebovali bomo DeMoivreovo formulo.

Izrek 5.4 (DeMoivre)**.** *Za $n \in \mathbb{Z}$ velja*

$$(\cos x + i\sin x)^n = \cos(nx) + i\sin(nx).$$

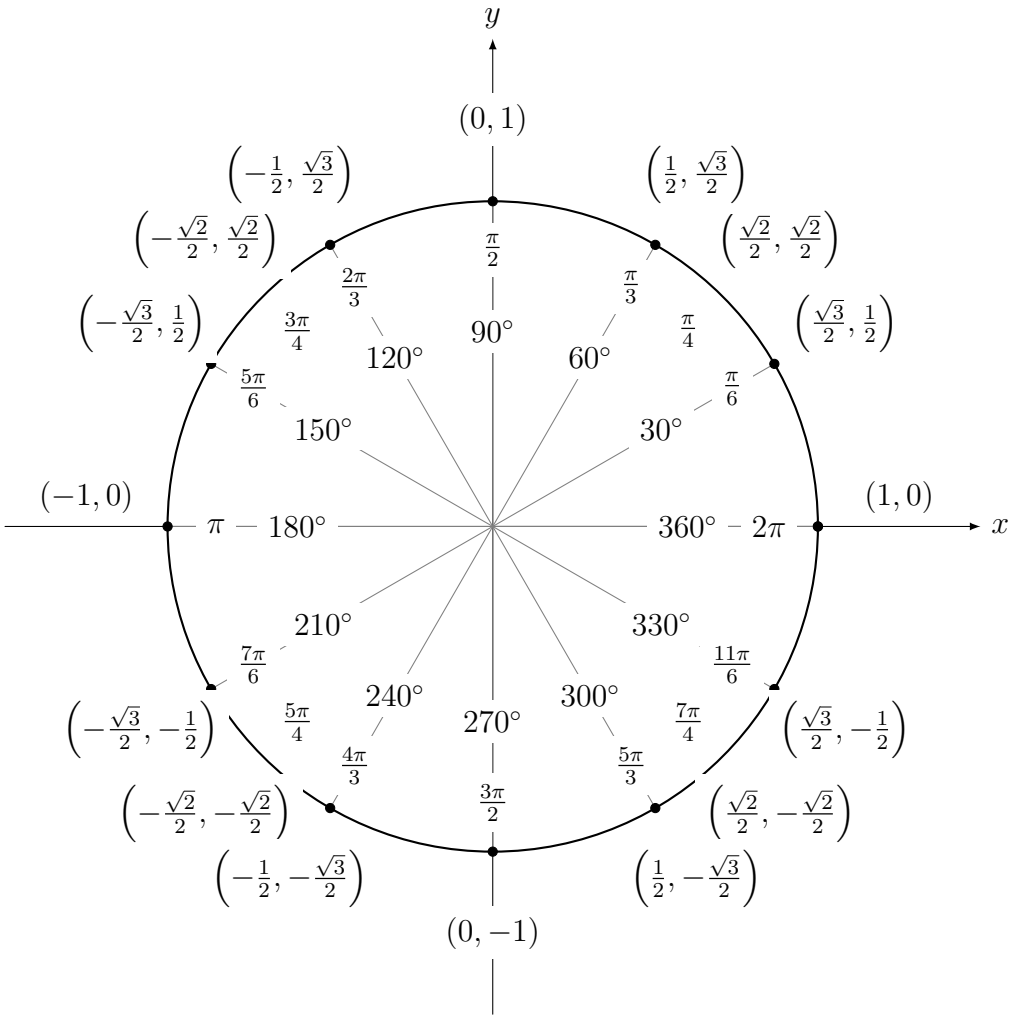
Dokaz. Dokazujemo z indukcijo. Za $n = 1$ izrek očitno velja. Predpostavimo, da velja za naravno število k. Pokažemo, da velja tudi za $k+1$:

$$\begin{aligned} (\cos x + i\sin x)^{k+1} &= (\cos x + i\sin x)^k(\cos x + i\sin x)\\ &= (\cos(kx) + i\sin(kx))(\cos x + i\sin x) \quad \text{(indukcija)}\\ &= \cos(kx)\cos x - \sin(kx)\sin x + i(\cos(kx)\sin x + \sin(kx)\cos x)\\ &= \cos((k+1)x) + i\sin((k+1)x) \quad \text{(trigonometrične enakosti)}. \end{aligned}$$

Torej izrek velja za vsa naravna števila.
Za $n = 0$ izrek drži, za negativna cela števila m pa pokažemo na naslednji način:

$$\begin{aligned}(\cos x + i \sin x)^m &= \frac{1}{(\cos x + i \sin x)^n} \\ &= \frac{1}{\cos(nx) + i \sin(nx)} \\ &= \cos(nx) - i \sin(nx) \\ &= \cos(-nx) + i \sin(-nx) \quad \text{(cos je soda, sin pa liha funkcija)} \\ &= \cos(mx) + i \sin(mx),\end{aligned}$$

kjer je $n = -m$ pozitivno celo število. □



SLIKA 2. n-ti koreni enote

Izrek 5.5. *n-ti koreni enote, tj. kompleksna števila z, ki ustrezajo enačbi $z^n = 1$, n naravno število, so oblike*

$$\cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right),\ k = 0, 1, \ldots, n-1.$$

Dokaz. Za $k = 0, 1, \ldots, n-1$ so ta števila različna, po DeMoivreovi formuli vemo

$$\left(\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)\right)^n = \cos(2k\pi) + i\sin(2k\pi) = 1.$$

□

Opomba 5.6. Če n-te korene enote predstavimo v kompleksni ravnini, tvorijo pravilen n-kotnik.

Trditev 5.7. *n-ti koreni enote sestavljajo grupo za množenje.*

Dokaz. Preverimo vse zahtevane pogoje za grupo:

- Imamo enoto, to je število 1, ki ustreza številu $\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$ pri $k = 0$.
- Zaprtost za množenje:

$$\begin{aligned}
&\left(\cos\left(\frac{2k_1\pi}{n}\right) + i\sin\left(\frac{2k_1\pi}{n}\right)\right)\left(\cos\left(\frac{2k_2\pi}{n}\right) + i\sin\left(\frac{2k_2\pi}{n}\right)\right)\\
&= \cos\left(\frac{2k_1\pi}{n}\right)\cos\left(\frac{2k_2\pi}{n}\right) - \sin\left(\frac{2k_1\pi}{n}\right)\sin\left(\frac{2k_2\pi}{n}\right)\\
&+ i\left(\cos\left(\frac{2k_1\pi}{n}\right)\sin\left(\frac{2k_2\pi}{n}\right) + \sin\left(\frac{2k_1\pi}{n}\right)\cos\left(\frac{2k_2\pi}{n}\right)\right)\\
&= \cos\left(\frac{2(k_1+k_2)\pi}{n}\right) + i\sin\left(\frac{2(k_1+k_2)\pi}{n}\right),
\end{aligned}$$

  kar je zaradi periodičnosti funkcij cos in sin vedno element grupe n-tih korenov enote.
- Asociativnost velja, saj je navadno množenje števil asociativno.
- Inverz elementa $\cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$ je element $\cos(\frac{2(n-k)\pi}{n}) + i\sin(\frac{2(n-k)\pi}{n})$, ki je tudi v grupi.

□

Lema 5.8. *Za vsako naravno število n je vsota vseh n-tih primitivnih korenov enote v $\mathbb{C}$ enaka $\mu(n)$.*

Dokaz. Označimo s $F(n)$ vsoto vseh primitivnih korenov enote v $\mathbb{C}$ in z $G(n)$ vsoto vseh n-tih korenov enote v $\mathbb{C}$. Če je z n-ti koren enote, je gotovo primitiven koren za nek m, kjer $m|n$. Obratno, vsak primitiven m-ti koren, $m|n$, je tudi n-ti koren enote, saj $1 = (1)^{\frac{n}{m}} = (z^m)^{\frac{n}{m}} = z^n$. Zato lahko zapišemo naslednjo enakost

$$G(n) = \sum_{m|n} F(m).$$

Na tej enakosti uporabimo Möbiusovo inverzno formulo, da dobimo

$$F(n) = \sum_{m|n} \mu(m)G(\frac{n}{m}). \tag{8}$$

Vemo, da n-ti koreni enote v kompleksni ravnini predstavljajo oglišča pravilnega n-kotnika. Vidimo, da velja $G(1) = 1$ (očitno) in $G(n) = 0$ za $n > 1$. Slednje lahko pokažemo na alternativen način, in sicer kot posledico enakosti (4). Za G v besedilu leme, ki nam poda to enakost, vzamemo grupo n-tih korenov enote, za homomorfizem λ pa izberemo kar identiteto, $\lambda(z) = z$. Ta homomorfizem ni trivialen

za $n > 1$. Imamo vse potrebne predpostavke, da lahko lemo uporabimo in za $n > 1$ res dobimo

$$\sum_{g \in G} \lambda(g) = G(n) = 0.$$

Sedaj se (8) poenostavi v

$$F(n) = \mu(n)G(1) = \mu(n)$$

in smo končali. □

Imamo vse potrebno za dokaz glavnega izreka.

5.2. **Dokaz glavnega izreka.**

Dokaz izreka 1.14. Naj bo G grupa vseh n-tih korenov enote v $\mathbb{C}$ in naj bo homomorfizem $\lambda : G \to \mathbb{C}^*$ identiteta. Za množico Ω izberemo G in naj G deluje na Ω z desnim množenjem. Grupa G je ciklična, saj je denimo generirana z elementom $\cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Spomnimo se, da je v tem primeru število orbit pri delovanju G na Ω $c(g) = d$, če je g element reda $\frac{n}{d}$. Vrnimo se k posledici 3.8, ki pravi

$$\sum_{g \in G} \lambda(g) a^{c(g)} \equiv 0 \pmod{|G|}$$

in premislimo o koeficientu, ki nastopa pred $a^{c(g)} = a^d$. V njem nastopajo sešteti členi $\lambda(g_1), \lambda(g_2), \ldots, \lambda(g_k)$, $k < n$, kjer so $g_1, g_2, \ldots, g_k$ elementi reda $\frac{n}{d}$. Homomorfizem λ pa je identiteta, zato je koeficient pred a^d ravno $g_1 + g_2 + \cdots + g_k$, kjer so $g_1, g_2, \ldots, g_k$ elementi reda $\frac{n}{d}$ v grupi G n-tih korenov enote. To pa so seveda $\frac{n}{d}$-ti primitivni koreni enote, saj velja $g_i^{\frac{n}{d}} = 1$, $g^l \neq 0$ za $l < \frac{n}{d}$ po definiciji reda elementa. Po zgornji lemi je tako koeficient pred a^d enak $\mu(\frac{n}{d})$. Kongruenca v posledici se potem glasi

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) a^d \equiv 0 \pmod{n},$$

kar trdi naš glavni izrek. □

Tako smo z nekoliko manj razširjeno tehniko pokazali napomembnejši del mojega diplomskega seminarja. Kot zanimivost pa bom podal še dokaz brez znanja o delovanjih grup.

Alternativni dokaz izreka 1.14. Najprej dokažemo za števila n, ki so potence praštevil, $n = p^k$.

$$\begin{aligned}\sum_{d|p^k} \mu\left(\frac{p^k}{d}\right) a^d &= a^{p^k} - a^{p^{k-1}} \\ &= a^{p^{k-1}}(a^{p^{k-1}(p-1)} - 1) \\ &= a^{p^{k-1}}(a^{p^k(1-\frac{1}{p})} - 1).\end{aligned}$$

Po (7) vemo $p^k(1 - \frac{1}{p}) = \varphi(p^k)$, torej

$$\sum_{d|p^k} \mu\left(\frac{p^k}{d}\right) a^d = a^{p^{k-1}}(a^{\varphi(p^k)} - 1).$$

Če je a tuj proti p (posledično proti p^k), nam Eulerjev izrek pove

$$a^{\varphi(p^k)} - 1 \equiv 0 \pmod{p^k}.$$

Če pa a ni tuj proti p, potem $p|a$ in seveda $p^k|a^{p^{k-1}}$, saj $k \leq p^{k-1}$ za vsak k in vsak p. Za $k = 1$ velja $1 \leq 1$, nadaljujemo z indukcijo na k. Naj neenakost velja za k, potem velja tudi za $k + 1$.

$$p^{k+1-1} = p^{k-1}p \geq kp \geq k + 1,$$

saj $p \geq 2$. Torej v vsakem primeru res drži

$$\sum_{d|p^k} \mu\left(\frac{p^k}{d}\right) a^d \equiv 0 \pmod{p^k}.$$

Spopademo se še s splošnim n. Če je p praštevilo, ki deli n, lahko zapišemo $n = p^k m$, kjer sta p in m tuja. To lahko naredimo za vsako praštevilo, ki deli n, zato zadošča pokazati, da

$$p^k \Big| \sum_{d|n} \mu\left(\frac{n}{d}\right) a^d.$$

Računamo

$$\begin{aligned}
\sum_{d|n} \mu\left(\frac{n}{d}\right) a^d &= \sum_{d|p^k m} \mu\left(\frac{p^k m}{d}\right) a^d \\
&= \sum_{d|m} \sum_{e|p^k} \mu\left(\frac{p^k m}{de}\right) a^{de} \\
&= \sum_{d|m} \sum_{e|p^k} \mu\left(\frac{m}{d}\right) \mu\left(\frac{p^k}{e}\right) a^{de} \\
&= \sum_{d|m} \mu\left(\frac{m}{d}\right) \sum_{e|p^k} \mu\left(\frac{p^k}{e}\right) a^{de} \\
&= \sum_{d|m} \mu\left(\frac{m}{d}\right) \sum_{e|p^k} \mu\left(\frac{p^k}{e}\right) (a^d)^e \ (*),
\end{aligned}$$

ampak za potence praštevil že vemo, da p^k res deli $\sum_{e|p^k} \mu(\frac{p^k}{e}) a^e$ za vsako celo število a, torej tudi za a^d. Vsak člen vsote $(*)$ je potem deljiv s p^k in tako $p^k | \sum_{d|n} \mu(\frac{n}{d}) a^d$. □

Literatura

[1] J. Grasselli, *Elementarna teorija števil*, Knjižnica Sigma **87**, DMFA – založništvo, Ljubljana, 2009.

[2] T. W. Hungerford, *Algebra*, Graduate texts in mathematics **73**, Springer, New York, 1974.

[3] I. M. Isaacs in M. R. Pournaki, *Generalizations of Fermat's little theorem via group theory*, Amer. Math. Monthly **112** (2005) 734–740.

[4] P. Potočnik, *Zapiski predavanj iz Diskretne matematike 1*, verzija 1. 4. 2011, [ogled 22. 3. 2012], dostopno na `http://www.fmf.uni-lj.si/~potocnik/Ucbeniki/DM-Zapiski2010.pdf`.

[5] *Root of unity*, [ogled 22. 3. 2012], dostopno na `http://en.wikipedia.org/wiki/%Root_of_unity/`.

[6] *Art of problem solving*, [ogled 24. 3. 2012], dostopno na `http://www.artofproblemsolving.com/Forum/%viewtopic.php?f=57&t=156312&`.
[7] *Example: Unit circle*, [ogled 26. 3. 2012], dostopno na `http://www.texample.net/tikz/examples/unit-circle/`.