Polinomi 1
Nerazcepnost

Luka Urbanc

Avgust 2023

1 Čemu?

Definicijo že poznamo. Zakaj nas torej zanimajo nerazcepni polinomi? Najprej seveda zato, ker so na olimpijadah včasih naloge iz nerazcepnosti. Manj pomembni razlogi so še, da so analog praštevil in so praštevila super, da dokazi nerazcepnosti poudarijo veliko pomembnih motivov v splošnejši teoriji polinomov, da lahko pogosto probleme zreduciramo na podprobleme, kjer so polinomi nerazcepni, ...
Na žalost dokazovanje nerazcepnosti ni vedno lahko.

2 $\mathbb{Z}[x]$ in Gaussova lema

$\mathbb{Z}$ ni polje, zato ne moremo direktno uporabiti nekaterih prej izpeljanih izrekov. Pravzaprav se zalomi že pri deljenju:

$$x = 2 \cdot q(x) + r(x).$$

Ne moremo izbrati $q(x) \in \mathbb{Z}[x]$-a, ki bi dal $d(r(x)) < d(x) = 1$. Razlog za to je, da se dokaz izreka o deljenju z ostanki zanaša na to, da lahko vodilne koeficiente prosto delimo, tj. da so elementi polja. Temu se v splošnem pač ne moremo izogniti, in se je treba zadovoljiti s količniki in ostanki v $\mathbb{Q}[x]$.

Na srečo pa ni vse upanje izgubljeno. Namreč, če gledaš razcep raznih polinomov $p(x) \in \mathbb{Z}[x]$ v $\mathbb{Q}[x]$, opaziš, da lahko vedno izbereš take faktorje, ki pristanejo v $\mathbb{Z}[x]$.

$3x^2 - 12$	$(6x - 12)(\frac{1}{2}x + 1)$	$3(x - 2)(x + 2)$
x^2	$1585x \cdot \frac{1}{1585}x$	$x \cdot x$
$x^5 - x$	$\frac{1}{320}x(16x - 16)(x + 1)(20x^2 + 20)$	$x(x - 1)(x + 1)(x^2 + 1)$

Izgleda torej, da če je $p(x)$ razcepen v $\mathbb{Q}[x]$, je razcepen tudi v $\mathbb{Z}[x]$. Obratna smer implikacije je očitna, zato bi sledilo, da je nerazcepnost polinoma s

celoštevilskimi koeficienti v $\mathbb{Q}[x]$ (in to, da je gcd njegovih koeficientov 1)[1] ekvivalentna njegovi nerazcepnosti v $\mathbb{Z}[x]$. To bi bilo super, ker je razcepnost v $\mathbb{Z}[x]$ dosti "močnejša" izjava (v grobem zato: ker je 1 najmanjša možna neničelna absolutna vrednost celega števila imamo veliko več informacij o kompleksnih ničlah polinoma v $\mathbb{Z}[x]$ kot v $\mathbb{Q}[x]$. Poleg tega pa lahko brezskrbno uporabljamo redukcijo mod p).

A le kako bi to dokazali? No, zgornji primeri že nakazujejo pravo smer razmišljanja. Najprej, izjavo lahko dokazujemo le za razcep na dva faktorja, saj bi splošni primer sledil po indukciji. Drugič, predpostavimo lahko, da je gcd koeficientov polinoma enak 1, ker če lahko na faktorje razcepimo tako verzijo polinoma, lahko enega od njih preprosto pomnožimo z želeno konstanto in dobimo razcep prvotnega polinoma. In tretjič, izgleda, da bi v takem primeru moralo delovati, da vsak faktor pomnožimo z neko racionalno konstanto, da so njegovi koeficienti celoštevilski in je njihov gcd $= 1$ (tu imamo $p(x) \in \mathbb{Z}[x]$, $a(x), b(x) \in \mathbb{Q}[x]$, $A, B \in \mathbb{Q}$):

$$p(x) = a(x)b(x) \iff AB \cdot p(x) = Aa(x) \cdot Bb(x) = c(x)d(x),$$

kjer sta $c(x), d(x) \in \mathbb{Z}[x]$, z gcd-jem koeficientov enakim 1. Če označimo še $C = AB$, sledi, da je $C \in \mathbb{Z}$ (sicer leva stran ne bi bila v $\mathbb{Z}[x]$). Kar bi si dejansko želeli je $C = \pm 1$, saj bi iz tega sledil želeni zapis $p(x)$-a kot produkt dveh celoštevilskih polinomov. To lahko dokažemo, če dokažemo, da ne obstaja praštevilo $q \in \mathbb{Z}$, ki deli C. Predpostavimo nasprotno ($q \mid C$)! Glede na to, da zdaj delamo z nekim določenim praštevilom, se morda splača preiti v polje $\mathbb{Z}/q\mathbb{Z}$, oziroma končno polje reda q – $\mathbb{F}_q$. Kako? Uporabimo najnaravnejšo preslikavo $\phi\colon \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$, in sicer redukcijo mod q. Torej, vse koeficiente polinomov zreduciramo mod q in dobimo $0 = \bar{c}(x)\bar{d}(x)$, kjer sta $\bar{c}(x), \bar{d}(x) \in \mathbb{F}_q[x]$ redukciji $c(x)$-a in $d(x)$-a. A ker je gcd koeficientov $c(x)$-a in $d(x)$-a v $\mathbb{Z}$ enak 1, vsaj en koeficient ni deljiv s q. Torej je njuna stopnja ≥ 0 in imamo protislovje, saj je stopnja leve strani enakosti enaka $-\infty$.

Dokazali smo:

Izrek 2.1 (Gaußova lema)**.** *Za nek polinom $p(x) \in \mathbb{Z}[x]$ označimo s $c(p(x))$* gcd *njegovih koeficientov. Potem velja*

$$(c(a(x)) = 1 \wedge c(b(x)) = 1) \implies c(a(x)b(x)) = 1$$

za vse $a(x), b(x) \in \mathbb{Z}$.

In posledico:

Izrek 2.2 (Tudi Gaussova lema)**.** *Nekonstanten polinom $p(x) \in \mathbb{Z}[x]$ je nerazcepen v $\mathbb{Z}[x]$, če in samo če je nerazcepen v $\mathbb{Q}[x]$ in je $c(p(x)) = 1$.*

[1] To mora veljati, saj je definicija nerazcepnosti v $\mathbb{Z}[x]$ malo drugačna kot tista, ki sem jo napisal za polja: nerazcepen polinom v $\mathbb{Z}[x]$ ni 0, nima multiplikativnega inverza (torej ni ± 1), in ni zmnožek dveh neinvertibilnih polinomov. Edina razlika je torej, da se cela števila $\neq 0, \pm 1$ štejejo kot faktorji. Torej so praštevila (razumljena kot konstantni polinomi) nerazcepna, 6 in $2x + 2$ (npr.) pa nista.

3 Nekaj kriterijev za nerazcepnost

Izrek 3.1. *Če ima polinom $p(x) \in \mathbb{Z}[x]$ natanko eno ničlo $\alpha \in \mathbb{C}$ izven odprte enotske krožnice (torej $|\alpha| \geq 1$), njegov vodilni koeficient je 1, konstantni koeficient pa ni 0, je nerazcepen v $\mathbb{Q}[x]$.*

Dokaz. Zaradi Gaussove leme je dovolj pokazati, da ne obstajata nekonstantna $f(x), g(x) \in \mathbb{Z}[x]$, da je $p(x) = f(x)g(x)$. Predpostavimo nasprotno in se postavimo v $\mathbb{C}[x]$. Tu se polinomi popolnoma razcepijo, torej jih lahko zapišemo kot produkt čez njihove ničle α_k:

$$p(x) = a_m \prod_{k=1}^{m} (x - \alpha_k).$$

Iz tega sledi, da je konstantni koeficient a_0 enak $a_m(-1)^m \prod_{k=1}^{m} \alpha_k$. Po predpostavki je $a_m = 1$. Opazimo, da je (ker so linearni polinomi nerazcepni) unija večkratnih množic[2] ničel $f(x)$-a in $g(x)$-a natanko večkratna množica ničel $p(x)$-a. Torej ima eden od njiju (recimo $f(x)$, ki naj bo stopnje $n \geq 1$) vse ničle β_k v odprti enotski krožnici $|\beta_k| < 1$ in nobena od njih ni 0. Potem je njegov konstantni koeficient celo število absolutne vrednosti $0 < |b_0| = \prod_{k=1}^{n} |\beta_k| < 1$, kar je nemogoče. □

Izpeljali smo zelo zanimivo dejstvo: $p(x) = f(x)g(x) \implies p(0) = a(0)b(0)$.

Izrek 3.2. *Če ima polinom $p(x) \in \mathbb{Z}[x]$ vse ničle izven zaprte enotske krožnice (torej $|\alpha| > 1$), konstantni koeficient pa je praštevilo, je nerazcepen v $\mathbb{Q}[x]$.*

Dokaz. Spet zapišemo $p(x) = f(x)g(x)$. Potem je eden od $|f(0)|, |g(0)|$ enak 1, ker je $p(0)$ praštevilo. Naj bo to $|f(0)|$ in naj bo stopnja $d(f(x)) = m$, njegov vodilni koeficient b_m, njegove ničle pa β_k. To je protislovje, ker je $1 = |f(0)| = |b_m| \prod_{k=1}^{m} |\beta_k| > 1$. □

Iz tega sledi še

Izrek 3.3. *Če ima polinom $p(x) \in \mathbb{Z}[x]$ praštevilski konstantni koeficient in je $|a_0| > |a_1| + |a_2| + \cdots + |a_m|$, je nerazcepen v $\mathbb{Q}[x]$.*

Dokaz. Po prejšnjem izreku je dovolj dokazati da vse ničle $p(x)$-a ležijo izven zaprte enotske krožnice. To sledi iz trikotniške neenakosti, ki pravi, da je absolutna vrednost vsote vektorjev manjša ali enaka vsoti absolutnih vrednosti. Naj bo α ničla z $|\alpha| \leq 1$. Potem dobimo

$$\begin{aligned}
0 &= p(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m \\
-a_0 &= a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m \\
|a_0| &= |a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m| \leq |a_1\alpha| + |a_2\alpha^2| + \cdots + |a_m\alpha^m| = \\
&= |a_1||\alpha| + |a_2||\alpha|^2 + \cdots + |a_m||\alpha|^m \leq |a_1| + |a_2| + \cdots + |a_m|,
\end{aligned}$$

protislovje. □

[2] Množice, kjer dovolimo več enakih elementov.

Iz zgornjega izreka sledi npr., da za vsak polinom $p(x) \in \mathbb{Z}[x]$ obstaja neskončno $a \in \mathbb{Z}$ (lahko tudi $\mathbb{N}$), za katere je $p(x) + a$ nerazcepen v $\mathbb{Q}[x]$. Podam še eno zanimivo lemo, ki kdaj utegne biti uporabna.

Lema 3.1. *Naj bo $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$ s padajočimi pozitivnimi koeficienti: $a_n \geq \cdots \geq a_1 \geq a_0 > 0$. Potem njegove kompleksne ničle ležijo v zaprti enotski krožnici $|z| \leq 1$.*

Dokaz. Naj bo z ničla polinoma z $|z| > 1$. Potem je tudi ničla polinoma $(1 - x)p(x) = -a_n x^{n+1} + (a_n - a_{n-1})x^n + \cdots + (a_1 - a_0)x + a_0$, torej $a_n z^{n+1} = (a_n - a_{n-1})z^n + \cdots + (a_1 - a_0)z + a_0$.

$$\begin{aligned} |a_n z^{n+1}| &= |(a_n - a_{n-1})z^n + \cdots + (a_1 - a_0)z + a_0| \leq \\ &\leq |a_n - a_{n-1}||z|^n + \cdots + |a_1 - a_0||z| + |a_0| = \\ &= (a_n - a_{n-1})|z|^n + \cdots + (a_1 - a_0)|z| + a_0 < \\ &< (a_n - a_{n-1})|z|^n + \cdots + (a_1 - a_0)|z|^n + a_0|z|^n = \\ &= a_n|z|^n, \end{aligned}$$

kar je protislovje. □

Zdaj pa nekaj kriterijev, ki zahtevajo znanje praštevilske faktorizacije koeficientov.

Izrek 3.4 (**Eisensteinov** kriterij)**.** *Če obstaja praštevilo q, da za koeficiente polinoma $p(x) \in \mathbb{Z}[x]$ stopnje m velja*

- $q \nmid a_m$,
- $q \mid a_k \ \forall 0 \leq k < m$ *in*
- $q^2 \nmid a_0$,

potem je $p(x)$ nerazcepen v $\mathbb{Q}[x]$.

Dokaz. Naj bo $p(x) = f(x)g(x)$. Kot pri dokazu Gaussove leme zreduciramo $p(x), f(x), g(x)$ v $\bar{p}(x), \bar{f}(x), \bar{g}(x) \in \mathbb{F}_q[x]$. Potem v $\mathbb{F}_q[x]$ velja $x^m = \bar{p}(x) = \bar{f}(x)\bar{g}(x)$; sledi $\bar{f}(x) = x^j$, $\bar{g}(x) = x^{m-j}$ za nek $0 < j < m$. Torej sta njuna konstantna koeficienta 0 v $\mathbb{F}_q$, kar pomeni da ju q deli v $\mathbb{Z}$. A to je protislovje, ker bi pomenilo $q^2 \mid a_0$. □

Pri uporabi teh izrekov je včasih potrebno najprej uporabiti kako substitucijo, ki polinom spravijo v želeno obliko. Kot primer dokažemo nerazcepnost p-tega ciklotomičnega polinoma, $\Phi_p(x)$, kjer je p praštevilo.

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

Izkaže se, da je tu dobra substitucija $p(x) \leftarrow p(x+1)$ (prepričaj se, da ta substitucija res ohrani nerazcepnost. $p(x) \leftarrow x^m p\left(\frac{1}{x}\right)$ je tudi zanimiva, razmisli še za njo):

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \frac{\sum_{k=1}^{p} \binom{p}{k} x^k}{x} = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k.$$

Ta polinom zadostuje pogojem Eisensteinovega kriterija, zato smo končali. (O nerazcepnosti drugih ciklotomičnih polinomov več kdaj drugič). Na tekmovanjih se ta kriterij v svoji osnovni obliki zelo redko pojavlja, ideja njegovega dokaza, torej redukcija modulo neko praštevilo, pa je veliko pogostejša:

Naloga 3.1 (IMO 1993 P1)**.** Dokaži, da je $x^n + 5x^{n-1} + 3$ nerazcepen v $\mathbb{Q}[x]$ za vse $n \geq 1$.

Poleg tega obstaja še sledeč kriterij, ki je strogo močnejši od Eisensteinovega, objavljen pa je bil nekaj let pred njim:

Izrek 3.5 (Schönemannov kriterij)**.** *Naj bo $p(x) = a(x)^n + q \cdot b(x)$, kjer je $n \in \mathbb{N}$, q praštevilo, $a(x), b(x) \in \mathbb{Z}[x]$ z $n \cdot d(a(x)) > d(b(x))$ in $c(p(x)) = 1$. Če z $\bar{a}(x), \bar{b}(x)$ označimo redukcije teh polinomov v $\mathbb{F}_q[x]$ in zahtevamo še, da je $\bar{a}(x)$ tam nerazcepen in da ne deli $\bar{b}(x)$-a, potem je $p(x)$ nerazcepen v $\mathbb{Q}[x]$.*

Dokaz. Naj bo $p(x) = f(x)g(x)$ za nekonstantne $f(x), g(x) \in \mathbb{Z}[x]$; njune redukcije označimo kot običajno. Potem imamo $\bar{f}(x)\bar{g}(x) = \bar{a}(x)^n$ v $\mathbb{F}_q[x]$, in ker je $\bar{a}(x)$ nerazcepen, dobimo $\bar{f} = \bar{a}(x)^k, \bar{g} = \bar{a}(x)^{n-k}$ za nek $k \geq 0$. Sledi, da lahko zapišemo $f(x) = a(x)^k + q \cdot b_1(x), g(x) = a(x)^{n-k} + q \cdot b_2(x)$. Torej je $a(x)^n + q \cdot b(x) = p(x) = f(x)g(x) = a(x)^n + q \cdot (a(x)^{n-k} b_1(x) + a(x)^k b_2(x) + q b_1(x) b_2(x)) \implies b(x) = a(x)^{n-k} b_1(x) + a(x)^k b_2(x) + q b_1(x) b_2(x) = a(x)h(x) + q b_1(x) b_2(x)$ za nek $h(x) \in \mathbb{Z}[x]$ (tu smo uporabili pogoj za stopnje $n \cdot d(a(x)) > d(b(x))$, saj ta prepreči $k = 0$ ali n). A če to ponovno reduciramo, dobimo $\bar{b}(x) = \bar{a}(x)\bar{h}(x)$ v $\mathbb{F}_q[x]$, kar je protislovje, saj smo predpostavili, da $\bar{a}(x)$ ne deli $\bar{b}(x)$-a. □

Schönemannov kriterij naredi sledečo nalogo skoraj trivialno:

Naloga 3.2. Naj bo $p \equiv 3 \pmod 4$ praštevilo in naj bo $n \in \mathbb{N}$. Dokaži, da je $(x^2+1)^n + p$ nerazcepen v $\mathbb{Q}[x]$.

Obstaja še nešteto drugih manj znanih kriterijev za nerazcepnost, a so njihovi dokazi zelo tehnični, zato jih bom le nakazal. Tu je nekaj zanimivejših.

Izrek 3.6 (Perronov kriterij)**.** *Če za $p(x) \in \mathbb{Z}[x]$ s stopnjo m in koeficienti a_k velja $a_m = 1, a_0 \neq 0$ in $|a_{m-1}| > 1 + |a_{m-2}| + |a_{m-3}| + \cdots + |a_1| + |a_0|$, je $p(x)$ nerazcepen čez $\mathbb{Q}[x]$. Če pa nimamo stroge neenakosti lahko včasih vseeno dobimo nerazcepnost s sledečimi pogoji: če $a_m = 1, a_0 \neq 0, |a_{m-1}| = 1 + |a_{m-2}| + |a_{m-3}| + \cdots + |a_1| + |a_0|$ in $p\left(-\frac{a_{m-1}}{|a_{m-1}|}\right) \neq 0$, potem je $p(x)$ prav tako nerazcepen.*

Dokaz. Uporabimo Rouchéjev izrek iz kompleksne analize: če sta $f(z), g(z)$ diferenciabilni kompleksni funkciji na in v notranjosti neke preproste (take, ki sama sebe ne seka) zaprte ravninske krivulje, in za vse z-je na krivulji velja $|f(z)+g(z)| < |f(z)|+|g(z)|$, potem imata $f(z)$ in $g(z)$ enako število ničel (z večkratnostmi) v notranjosti krivulje. Za Perronov kriterij je dovolj preprosto vzeti $f(z) = p(z)$, $g(z) = -a_{m-1}z^{m-1}$, za krivuljo pa enotsko krožnico. Potem je za z na krivulji $|z| = 1$ in imamo $|f(z)+g(z)| = |z^m + a_{m-2}z^{m-2} + \cdots + a_1 z + a_0| \leq |z|^m + |a_{m-2}||z|^{m-2} + \cdots + |a_1||z| + |a_0| = 1 + |a_{m-2}| + \cdots + |a_1| + |a_0| < |a_{m-1}| = |a_{m-1}z^{m-1}| = |g(z)| \leq |f(z)| + |g(z)|$. Sledi, da ima $p(x)$ natanko $m-1$ ničel v odprti enotski krožnici, torej natanko 1 izven nje, in kriterij sledi po izreku 2.1. Izrek z enakostjo se dobi tako, da preučiš primere enakosti v zgornjem. □

Težji del dokaza kriterija se da izvesti tudi brez kompleksne analize, a je precej nemotivirano in dolgo.
Po Perronovem kriteriju IMO 1993 P1 sledi iz izjave $5 > 4$.

Sledeč kriterij je še en (precej zahtevnejši) primer omejevanja ničel.

Izrek 3.7 (**Brauerjev** kriterij)**.** *Za $a_{m-1} \geq a_{m-2} \geq \cdots \geq a_0 \in \mathbb{N}$ je polinom $p(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_1 x - a_0$ nerazcepen v $\mathbb{Q}[x]$.*

Dokaz. Za $m = 1$ je izjava očitna, torej naj bo $m \geq 2$. Kot pri Perronu bomo dokazali, da je natanko ena ničla takega polinoma zunaj enotske krožnice. Kot pri lemi 3.1 je pametno pogoj o monotonosti zaporedja pretvoriti v pogoj o pozitivnosti. Zatorej se bomo raje bili ukvarjali s polinomom $q(x) = (x-1)p(x) = x^{m+1} - b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$, kjer je $b_m = a_{m-1}+1, b_{m-1} = a_{m-1} - a_{m-2}, b_{m-2} = a_{m-2} - a_{m-3}, \ldots, b_1 = a_1 - a_0, b_0 = a_0$. Torej so b_k nenegativni in imamo $b_m = 1 + b_{m-1} + \cdots + b_0$. Ker ima $q(z)$ ničlo $z = 1$ zagotovo ne bo možno uporabiti enotske krožnice kot krivuljo pri Rouchéjevem izreku. Zato vzamemo raje krožnice s polmerom $1+\varepsilon$ in želeno dokazujemo za vse dovolj majhne $\varepsilon > 0$.
Naj bo $f(z) = q(z)$. Izkaže se, da je pametna izbira za $g(z)$ enaka $b_m z^m - b_{m-1}z^{m-1} - \cdots - b_1 z - b_0$, saj je $|f(z)+g(z)| = |z|^{m+1} < |g(z)| \leq |f(z)|+|g(z)|$:

$$\begin{aligned} |g(z)| - |z|^{m+1} &\geq b_m(1+\varepsilon)^m - \cdots - b_1(1+\varepsilon) - b_0 - (1+\varepsilon)^{m+1} = \\ &= b_m - \cdots - b_1 - b_0 - 1 + \varepsilon(m b_m - \cdots - 1 \cdot b_1 - (m+1)) + \\ &+ \varepsilon^2(\ldots) = \varepsilon \cdot c + \varepsilon^2(\ldots) > 0, \end{aligned}$$

kjer je c neko pozitivno število, tisto v oklepajih pa je omejeno z neko konstanto (pri razširanju $(1+\varepsilon)^k$ smo uporabili binomski izrek). Če vzamemo dovolj majhen ε, je $\varepsilon \cdot c$ veliko večji od $\varepsilon^2(\ldots)$ po absolutni vrednosti, torej je njuna vsota res pozitivna. Preostalo nam je še dokazati, da so vse ničle $g(z)$-ja v enotski krožnici. A za $|z| \geq 1$ velja $|g(z)| \geq b_m|z|^m - b_{m-1}|z|^{m-1} - \cdots - b_1|z| - b_0 \geq b_m|z|^m - b_{m-1}|z|^m - \cdots - b_1|z|^m - b_0|z|^m = |z|^m > 0$. Torej ima $g(z)$ m ničel v enotski krožnici, zato ima $f(z) = q(z)$ tudi m ničel v krožnici s polmerom $1+\varepsilon$ za poljubno majhne $\epsilon > 0$. Sledi, da je natanko ena ničla $q(z)$-ja izven **zaprte**

enotske krožnice, torej enako velja tudi za $p(z)$.
Dejansko še ne moremo uporabiti izreka 2.1, saj dosihmal še nismo izločili možnosti, da vse ostale ničle ležijo ravno na enotski krožnici. Potem bi bilo možno polinom razcepiti tako, da ima tisti faktor s konstantnim koeficientom ± 1 natanko te "enotske" ničle. No, recimo, da je $p(x)$ res tak. Potem mora njegova edina neenotska ničla biti celo število absolutne vrednosti a_0. A ker je $p(1) < 0$ in $p(x) \to \infty$ ko $x \to \infty$, vemo, da ima vsaj eno ničlo na intervalu $(1, \infty)$, torej ima natanko eno in je ta ravno a_0. A to je nemogoče, ker je $a_0^m - a_{m-1}a_0^{m-1} \leq 0$, torej je $p(a_0) < 0$. □

Dovolj trikotniške neenakosti zaenkrat.

Izrek 3.8 (Ljunggrenov izrek)**.** *Če sta $m > n > 0$ naravni števili, potem je **ne**ciklotomični del polinoma $p(x) = x^m \pm x^n \pm 1$ nerazcepen v $\mathbb{Q}[x]$ (ali pa enak 1). (Ciklotomični del je produkt čez natanko tiste ničle, ki ležijo na enotski krožnici. Preveri, da je enak $\gcd(p(x), x^m p(\frac{1}{x}))$, torej ga je za te polinome precej lahko izračunati.)*

Dokaz. Ideja je gledati polinom $p(x) \cdot x^m p(\frac{1}{x})$ in njegove razcepe oblike $f(x) \cdot x^m f(\frac{1}{x})$. Če dokažeš, da so edini taki razcepi $f(x) = \pm p(x)$, se izkaže, da sledi ravno to, kar želimo: da je neciklotomični del nerazcepen. Za dokaz $f(x) = \pm p(x)$ pa izraziš koeficient x^m-ja v polinomu $p(x) \cdot x^m p(\frac{1}{x})$ iz koeficientov $p(x)$-a, in opaziš, da sledi, da ima $f(x)$ tudi natanko 3 neničelne koeficiente ter so vsi ± 1. Lahek izračun konča dokaz. □

Če želiš, lahko natančneje izpelješ podrobnosti zgornjega dokaza... verjetno bi bilo kar poučno. Velja tudi verzija izreka s štirimi členi (neciklotomični del $x^m \pm x^n \pm x^p \pm 1$ je nerazcepen). Seveda pa se je tudi pojavil na olimpijadah:

Naloga 3.3 (IMO 2002 P3)**.** Najdi vse pare naravnih števil $m, n \geq 3$, za katere obstaja neskončno naravnih števil a, za katere je

$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$

celo število.

Problem je seveda rešljiv tudi brez Ljunggrenovega izreka, a je precej težji. Namigi so zapisani tudi za ta pristop; priporočam, da ga poskusiš (naloga 5.11).

Zdaj pa zelo splošen kriterij, ki zelo pomaga pri dokazovanju nerazcepnosti kompozicij polinomov, a ga je morda malo težje razumeti. Zahteva namreč osnovno znanje teorije polj.

Izrek 3.9 (Capellijev kriterij)**.** *Naj sta $p(x), q(x) \in \mathbb{F}[x]$. Naj bo α ničla polinoma $p(x)$ v algebraično zaprti razširitvi polja $\mathbb{F}$. Potem je $p(q(x))$ nerazcepen v $\mathbb{F}[x]$ če in samo če je $p(x)$ nerazcepen v $\mathbb{F}[x]$ in je $q(x) - \alpha$ nerazcepen v $\mathbb{F}(\alpha)[x]$. Poleg tega, tudi če ne vemo, ali je $q(x) - \alpha$ nerazcepen v $\mathbb{F}(\alpha)[x]$, velja, da so stopnje nerazcepnih faktorjev $p(q(x))$-a deljive s stopnjo $p(x)$-a.*

Dokaz. Dokaz zahteva osnovno znanje teorije polj, česar na žalost tu res ne morem natančno razložiti. Skratka, polju $\mathbb{F}$ lahko "dodamo" elemente, ki so ničle polinomov v $\mathbb{F}[x]$, da dobimo polje $\mathbb{F}(\alpha)$. $\mathbb{F}(\alpha)$ je potem množica elementov oblike $p(\alpha)$ za vse $p(x) \in \mathbb{F}[x]$. To je podobno dodajanju x-a, da iz $\mathbb{F}$ dobimo $\mathbb{F}[x]$, le da ničle polinomov po svoji definiciji zadostujejo nekim dodatnim algebraičnim relacijam, npr. ničle x^2+1 zadostujejo $\alpha^2 = -1$. Sledi, da lahko potence α^m za $m \geq 2$ pretvorimo v take z $m = 0$ ali 1. To velja v splošnem, zato ima $\mathbb{F}(\alpha)$ končno dimenzijo kot vektorski prostor čez $\mathbb{F}$. Poleg tega lahko v njem množimo in delimo, torej je res polje. Izkaže se, da nam dimenzija tega polja čez bazno polje (ki jo označimo z $[\mathbb{F}(\alpha) : \mathbb{F}]$) veliko pove o polinomu (in obratno): enaka je stopnji polinoma natanko tedaj, ko je polinom nerazcepen. Poleg tega, če polju dodamo še neko drugo ničlo, velja $[\mathbb{F}(\alpha,\beta) : \mathbb{F}] = [\mathbb{F}(\alpha,\beta) : \mathbb{F}(\alpha)] \cdot [\mathbb{F}(\alpha) : \mathbb{F}]$. Pri Capellijevem kriteriju gledamo $[\mathbb{F}(\beta) : \mathbb{F}] = [\mathbb{F}(\beta) : \mathbb{F}(q(\beta))] \cdot [\mathbb{F}(q(\beta)) : \mathbb{F}]$, kjer je β ničla $p(q(x))$-a. Potem je $q(\beta)$ ravno ničla $p(x)$-a, in ker je ta polinom nerazcepen, je $[\mathbb{F}(q(\beta)) : \mathbb{F}] = d(p(x))$. Iz tega sledi, da je $p(q(x))$ nerazcepen, če in samo če je $[\mathbb{F}(\beta) : \mathbb{F}(q(\beta))] = d(q(x))$. To pa je ravno ekvivalentno nerazcepnosti $q(x) - q(\beta)$ v $\mathbb{F}(q(\beta))$. Ne glede na to nerazcepnost pa je $[\mathbb{F}(\beta) : \mathbb{F}]$ deljiv z $d(p(x))$, torej so stopnje vseh nerazcepnih faktorjev $p(q(x))$ deljive z $d(p(x))$. □

Drugi pogoj torej pravi, da ne moremo zapisati $q(x) - \alpha$ kot produkt dveh polinomov iz $\mathbb{F}(\alpha)[x]$, tj. s koeficienti oblike $a_0 + a_1 \cdot \alpha + \cdots + a_{m-1} \cdot \alpha^{m-1}$ za neke $a_i \in \mathbb{F}$ in $m = d(p(x))$. To je včasih še zmeraj težko dokazati, a pogosto veliko lažje kot direktno dokazovanje nerazcepnosti $p(q(x))$-a, posebej, ko je $q(x)$ npr. kvadratni polinom. Za primer rešimo

Naloga 3.4. Če je $f(x) \in \mathbb{Z}[x]$ nerazcepen v $\mathbb{Q}[x]$, ima stopnjo m in vodilni koeficient 1, $f(x^2)$ pa je razcepen, je $(-1)^m f(0)$ popolni kvadrat.

Dokaz. Naj bo $\alpha \in \mathbb{C}[x]$ ničla $f(x)$-a. Po Capellijevem kriteriju je $x^2 - \alpha$ razcepen v $\mathbb{Q}(\alpha)[x]$. Ker je ta polinom kvadraten, je razcepnost ekvivalentna obstoju ničle, torej mora obstajati element $\beta \in \mathbb{Q}(\alpha)$, za katerega je $\beta^2 = \alpha$. Potem obstaja polinom $p(x) \in \mathbb{Q}[x]$, za katerega je $p(\alpha)^2 = \beta^2 = \alpha$. Ker je $f(x)$ nerazcepen in deli ničlo s $p(x)^2 - x$, sledi $f(x) \mid p(x)^2 - x$, torej je v resnici $p(\alpha_k)^2 = \alpha_k$ za vse ničle $f(x)$-a $\alpha_k \in \mathbb{C}$. Če te izraze zmnožimo, sledi

$$\left(\prod_{k=1}^{m} p(\alpha_k)\right)^2 = \prod_{k=1}^{m} \alpha_k = (-1)^m a_0.$$

Ampak, ker je $\displaystyle\prod_{k=1}^{m} p(\alpha_k)$ simetričen polinom iz α_k, se ga po osnovnem izreku simetričnih polinomov[3] da izraziti kot racionalen polinom v elementarnih sime-

[3] Če je polinom v n spremenljivkah tak, da ga permutacije spremenljivk ne spremenijo (takim pravimo simetrični), se ga da zapisati kot polinom v elementarnih simetričnih polinomih $(1,\ x_1 + \cdots + x_n,\ x_1x_2 + x_1x_3 + \cdots + x_2x_3 + \cdots + x_{n-1}x_n,\ \ldots,\ x_1x_2\ldots x_n)$. To se dokaže z ogabno indukcijo. Če so x_k ničle polinoma, so elementarni simetrični polinomi po Vietovih formulah ± koeficienti tega polinoma.

tričnih polinomih α_k, ki so ravno koeficienti $f(x)$-a. Sledi torej, da je $(-1)^m a_0$ kvadrat racionalnega števila, torej je kvadrat celega števila. □

Iz tega sledi npr., da izjava naloge 3.2 velja tudi, če ne zahtevamo $p \equiv 3 \pmod 4$.
In v resnici lahko dokažemo še več: dovolj je predpostaviti, da je vodilni koeficient pozitiven in da je $c(f(x)) = 1$. Vzamemo polinom $g(x) \in \mathbb{Z}[x]$ minimalne stopnje s $c(g(x)) = 1$ z ničlo β. Dokazati se da, da je $d(g(x)) = m$. Potem vzamemo $g(x)g(-x) = h(x^2)$, in dobimo, da je $(-1)^m h(x) = f(x)$, iz česar sledi enak zaključek.
To nalogo (in njeno močnejšo različico) je precej lahko rešiti tudi na veliko elementarnejši način, brez Capellijevega kriterija (glej nalogo 5.5). A ta kriterij pride prav tudi pri veliko težjih nalogah:

Naloga 3.5. Dokaži, da je $(x^2 + x)^{2^n} + 1$ nerazcepen v $\mathbb{Z}[x]$.

Dokaz. Obstaja bolj elementarna rešitev (naloga 5.8), katere se je veliko težje spomniti. A s Capellijem je naloga praktično enaka zgornji. Za $p(x)$ vzamemo $x^{2^n} + 1$, ki je ciklotomični polinom in je zato nerazcepen v $\mathbb{Q}[x]$. Dovolj je torej dokazati, da $x^2 + x - \zeta_{2^{n+1}}$ nima ničel v $\mathbb{Q}(\zeta_{2^{n+1}})$, kjer je $\zeta_{2^{n+1}}$ 2^{n+1}-ti primitivni koren, torej ničla $x^{2^n} + 1$. Predpostavimo torej, da ničla obstaja. Po kvadratni enačbi je to ekvivalentno obstoju elementa $\beta \in \mathbb{Q}(\zeta_{2^{n+1}})$, za katerega je $\beta^2 = \frac{1}{4} - \zeta_{2^{n+1}}$. Spet zapišemo $\beta = f(\zeta_{2^{n+1}})$ za nek $f(x) \in \mathbb{Q}[x]$, in spet sledi $p(x) \mid f(x)^2 + x - \frac{1}{4}$. Po množenju čez vse ničle ponovno dobimo, da je

$$\prod_{k=0}^{2^n-1} \left(\frac{1}{4} - \zeta_{2^{n+1}}^{2k+1} \right) = \left(\frac{1}{4} \right)^{2^n} + 1$$

kvadrat nekega racionalnega števila, torej je $4^{2^n} + 1$ kvadrat celega, kar je očitno nemogoče. □

S Capellijevim izrekom se lahko dokaže tudi ta presenetljivo težek kriterij (ki se mu tudi reče Capellijev):

Izrek 3.10 (Capellijev kriterij)**.** *$x^n - a \in \mathbb{F}[x]$ je nerazcepen v $\mathbb{F}[x]$ če in samo če $a \neq b^p$ $\forall b \in \mathbb{F}$ za vsa praštevila $p \mid n$ in, če $4 \mid n$, $a \neq -4b^4$ $\forall b \in \mathbb{F}$.*

4 Še nekaj, kar ne paše nikamor drugam

Dokaz tega izreka je eden mojih najljubših. Priporočam.

Izrek 4.1 (Kronecker)**.** *Če ima $p(x) \in \mathbb{Z}[x]$ vodilni koeficient 1 in vse ničle v zaprti enotski krožnici, potem velja $p(x) \mid x^a(x^n - 1)^b$ za neke $a, b, n \in \mathbb{N}$.*

Dokaz. Brez izgube za splošnost naj $p(0) \neq 0$ ($x^a p(x)$ je želene oblike, če in samo če je $p(x)$). Potem moramo v bistvu dokazati, da so vse ničle takega polinoma neki primitivni koreni. Najprej, ker je $|p(0)| \geq 1$, vemo, da morajo

vse ničle ležati nekje na enotski krožnici $|z| = 1$. Torej jih lahko zapišemo kot $\alpha_k = e^{2\pi i \varphi_k}$ za neke realne φ_k, $1 \leq k \leq m = d(p(x))$. Hočemo, da so φ_k racionalni. Zato bi se morda splačalo raziskati $n\varphi_k$ za različne naravne n in upati, da so enkrat cela števila, oziroma da je $\alpha_k^n = 1$. Iz $p(x) = p_0(x)$-a lahko konstruiramo celoštevilski polinom stopnje m $p_1(x)$, ki ima za ničle ravno kvadrate ničel $p_0(x)$-a: $p_1(x^2) = p_0(x)p_0(-x)$. Ta proces lahko ponavljamo in dobimo zaporedje polinomov $p_j(x)$, ki imajo ničle $\alpha_k^{2^j}$.
S pomočjo Vietovih formul in trikotniške neenakosti (ups) lahko izpeljemo zgornje meje za koeficiente takih polinomov: $|a_k| \leq \binom{m}{k}$ (ker je v koeficientu po $\binom{m}{k}$ členov z absolutnimi vrednostmi 1). Sledi, da jih v našem neskončnem zaporedju le končno mnogo različnih, ker imajo za vsak koeficient le končno mnogo izbir! Izjemno. Torej nujno obstajata dva enaka polinoma $p_i(x) = p_j(x)$ za $i < j$. Sledi, da sta večkratni množici njunih ničel enaki: $\{\alpha_1^{2^i}, \dots\} = \{\alpha_1^{2^j}, \dots\}$. Torej obstaja neka permutacija števil od 1 do m σ, da imamo $\alpha_k^{2^i} = \alpha_{\sigma(k)}^{2^j}$ za vse $1 \leq k \leq m$.
A zdaj smo tako rekoč končali, ker je znano, da je za vse permutacije na množici m elementov $\sigma^{m!}(k) = \underbrace{\sigma(\sigma(\dots(\sigma(k))\dots))}_{\text{m!-krat}} = k$. Torej je

$$\begin{aligned}
\alpha_k^{2^{m!i}} &= \left(\alpha_k^{2^i}\right)^{2^{(m!-1)i}} = \left(\alpha_{\sigma(k)}^{2^j}\right)^{2^{(m!-1)i}} = \alpha_{\sigma(k)}^{2^{(m!-1)i+j}} = \\
&= \left(\alpha_{\sigma(k)}^{2^i}\right)^{2^{(m!-2)i+j}} = \left(\alpha_{\sigma(\sigma(k))}^{2^j}\right)^{2^{(m!-2)i+j}} = \alpha_{\sigma(\sigma(k))}^{2^{(m!-2)i+2j}} = \\
&= \dots = \alpha_{\sigma^{m!}(k)}^{2^{m!j}} = \alpha_k^{2^{m!j}}.
\end{aligned}$$

Sledi, da je $\alpha_k^{2^{m!j}-2^{m!i}} = 1$, torej $p(x) \mid (x^{2^{m!j}-2^{m!i}} - 1)^b$ za nek dovolj velik b. □

5 Naloge

Namigi so na zadnji strani.

Naloga 5.1. Najdi vse trojice $m, n, p \in \mathbb{N}$, kjer je p praštevilo, za katere je $x^m + x^n + p$ razcepen v $\mathbb{Q}[x]$.

Naloga 5.2. Najdi vse naravne $n \geq 3$, za katere velja, da so vsi enakokoti n-kotniki s celoštevilskimi dolžinami stranic tudi enakostranični.

Naloga 5.3. Najdi vse kvadratne polinome $p(x) \in \mathbb{Z}[x]$, za katere obstaja nek $q(x) \in \mathbb{Z}[x]$, da ima polinom $p(x)q(x)$ vse koeficiente oblike ± 1.

Naloga 5.4. Naj bo $p(x) \in \mathbb{Z}[x]$ nerazcepen v $\mathbb{Q}[x]$. Če ima dve ničli, katerih produkt je 1, dokaži, da je njegova stopnja soda.

Naloga 5.5. Če je $p(x) \in \mathbb{Z}[x]$, s pozitivnim vodilnim koeficientom in stopnjo m, nerazcepen v $\mathbb{Z}[x]$, $p(x^2)$ pa ni, brez uporabe Capellijevega kriterija dokaži,

da lahko zapišemo $p(x^2) = (-1)^m q(x)q(-x)$ za nek nerazcepni $q(x) \in \mathbb{Z}[x]$. Dokaži še, da lahko potem zapišemo $p(x) = (-1)^m \left(f(x)^2 - xg(x)^2\right)$ za neke $f(x), g(x) \in \mathbb{Z}[x]$.

Naloga 5.6. Naj bo p praštevilo. Dokaži, da je $x^{p-1} + 2x^{p-2} + \cdots + (p-1)x + p$ nerazcepen v $\mathbb{Q}[x]$.

Naloga 5.7. Dokaži, da je $x^p - x - a$ nerazcepen v $\mathbb{Z}[x]$ za vsa praštevila p in cela števila a, ki niso deljiva s p.

Naloga 5.8. Brez uporabe Capellijevega kriterija dokaži, da je $(x^2 + x)^{2^n} + 1$ nerazcepen v $\mathbb{Z}[x]$.

Naloga 5.9. Dokaži, da za polinom $p(x) \in \mathbb{C}[x]$ z vodilnim koeficientom 1 obstaja vsaj en z na enotski krožnici $|z| = 1$, da je $|p(z)| \geq 1$.

Naloga 5.10. Dokaži, da je za vse neničelne $a \in \mathbb{Z}$ in vse naravne n polinom $x^n + ax^{n-1} + ax^{n-2} + \cdots + ax - 1$ nerazcepen v $\mathbb{Q}[x]$.

Naloga 5.11. Brez uporabe Ljunggrenovega izreka najdi vse pare naravnih števil $m, n \geq 3$, za katere obstaja neskončno naravnih števil a, za katere je

$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$

celo število.

Naloga 5.12. Najdi vse kvadratne polinome $p(x) \in \mathbb{Z}[x]$, za katere je $p(x)^{2^n} + 1$ nerazcepen za vsaj en $n \geq 1$.

Naloga 5.13. Naj bodo $a_1, a_2, \ldots, a_n \in \mathbb{Z}[i]$ (torej kompleksna števila $x + yi$ s celoštevilskima x, y) in $|a_1 - a_k| > 2$ za vse $k \geq 2$. Dokaži, da je polinom $(x - a_1)(x - a_2) \ldots (x - a_n) + 1$ nerazcepen v $\mathbb{Z}[i][x]$.

Naloga 5.14. Naj bodo $a_1 < a_2 < \cdots < a_n \in \mathbb{Z}$. Dokaži:

a) nerazcepnost $\prod_{k=1}^{n}(x - a_k) - 1$ v $\mathbb{Q}[x]$,

b) nerazcepnost $\prod_{k=1}^{n}(x - a_k) + 1$ v $\mathbb{Q}[x]$, razen če je $n = 2$ in $a_1 = a_2 - 2$ ali če je $n = 4$ in $a_1 = a_2 - 1 = a_3 - 2 = a_4 - 3$,

c) nerazcepnost $\prod_{k=1}^{n}(x - a_k)^2 + 1$ v $\mathbb{Q}[x]$, in

d) (*) nerazcepnost $\prod_{k=1}^{n}(x - a_k)^4 + 1$ v $\mathbb{Q}[x]$.

Sledeče imajo malo manj direktnega opravka z nerazcepnostjo, so pa vseeno lepe algebraične naloge.

Naloga 5.15. a, b, c so neničelna cela števila, za katera sta $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}, \frac{a}{c} + \frac{b}{a} + \frac{c}{b} \in \mathbb{Z}$. Dokaži, da velja $|a| = |b| = |c|$.

Naloga 5.16. Če za $x \in \mathbb{R}, n \in \mathbb{N}, a \in \mathbb{Q}$, $a \neq 0$ velja, da sta x^n in $(x + a)^n$ racionalna, dokaži, da je tudi x racionalen.

Naloga 5.17. Naj bo $p(x) = ax^3 + bx^2 + cx + d$ za neke $a, b, c, d \in \mathbb{Z}$, $a \neq 0$. Če je $xp(x) = yp(y)$ za neskončno parov celih števil $x \neq y$, dokaži, da ima $p(x)$ celoštevilsko ničlo.

NAMIGI!!!
3.1.: Kopiraj dokaz Eisensteinovega kriterija, a se malo bolj potrudi na koncu
3.2.: $x^2 + 1$ je nerazcepen v $\mathbb{F}_p[x]$ za $p \equiv 3 \pmod 4$
3.3.: Želeni pogoj je ekvivalenten deljivosti polinomov, pazi na ciklotomične faktorje
5.1.: Absolutne vrednosti, potem pa zabavna modularna aritmetika
5.2.: Ciklotomični polinomi
5.3.: Omeji ničle
5.4.: Glej $x^m p(\frac{1}{x})$
5.5.: Vzemi nerazcepni delitelj $p(x^2)$ in uporabi neko simetrijo, da dobiš nek delitelj $p(x)^2$
5.6.: Malo "amortiziraj" koeficiente z množenjem z nekim preprostim faktorjem, potem uporabi trikotniško neenakost
5.7.: Redukcija mod p, uporabi zanimivo lastnost tega polinoma
5.8.: Redukcija mod 2. Tam je $x^2 + x + 1$ nerazcepen
5.9.: Rouchéjev izrek. Uporabi dejstvo o vodilnem koeficientu
5.10.: (Skoraj) direktna uporaba Brauerjevega kriterija
5.11.: Obstaja realna ničla, z njo dokaži $m \leq 2n$
5.12.: Capelli, potem pa spust s pitagorejskimi trojicami
5.13.: Uporabi izrek brez imena $(a - b \big| p(a) - p(b))$
5.14.: Za a) in b) določi n vrednosti faktorjev polinoma, za c) uporabiš še pozitivnost ali pa Capellijev kriterij, za d) pa ne vem, če obstaja kakšna lepša rešitev, a moja je nekako združitev Capellijevega kriterija, netrivialnih lastnosti polja $\mathbb{Q}(\zeta_8)$, naloge 5.13 in ogromno caseworka
5.15.: Konstruiraj polinom, ki ima vsoti za koeficiente
5.16.: $\gcd(z^n - x^n, (z + a)^n - (x + a)^n)$
5.17.: Zapiši kot polinom v $s = x + y, t = xy$