Univerza v Ljubljani
Fakulteta za matematiko in fiziko

Praštevila in nerazcepni polinomi
Seminar 1

Jurij Volčič

Škofja Loka, april 2011

1. Uvod

Podobnost med praštevili in nerazcepnimi polinomi s celimi koeficienti ni le na nivoju analogije med kolobarjem celih števil in kolobarjem polinomov nad celimi števili. Zanimivo je vprašanje, ali je polinom s celimi koeficienti, ki zavzame praštevilske vrednosti, nerazcepen v $\mathbb{Z}[x]$ oziroma $\mathbb{Q}[x]$. V splošnem je odgovor ne, izkaže pa se, da je polinom nerazcepen, če ima praštevilsko vrednost v točki, ki je v nekem smislu "dovolj" oddaljena od njegovih ničel. Še bolj nazorno povezavo predstavlja izrek, ki ga je odkril Arthur Cohn ([1], [2] in [5]):

Izrek 1. *Če je praštevilo p v desetiškem sistemu enako $p = a_m 10^m + \cdots + a_1 10 + a_0$, potem je polinom $f(x) = a_m x^m + \cdots + a_1 x + a_0$ nerazcepen v $\mathbb{Q}[x]$.*

Najprej si bomo ogledali splošen kriterij za nerazcepnost v $\mathbb{Z}[x]$ oz. $\mathbb{Q}[x]$ glede na praštevilske vrednosti polinoma, potem pa posplošitev Cohnovega izreka za poljubno osnovo številskega sistema $b \geq 2$.

2. Kriterij za nerazcepnost v $\mathbb{Z}[x]$

Razmislimo, pod kakšnimi pogoji lahko iz praštevilskih vrednosti polinoma sklepamo na nerazcepnost. Če polinom zavzame praštevilske vrednosti na neskončni podmnožici $A \subset \mathbb{Z}$, je nerazcepen v $\mathbb{Z}[x]$. Res; denimo, da lahko $f(x)$ razcepimo, torej $f(x) = g(x)h(x)$, kjer sta $g(x)$ in $h(x)$ nekonstantna polinoma s celimi koeficienti. Ker je $f(x)$ praštevilo za neskončno celih števil x, vsaj eden od polinomov $g(x)$, $h(x)$ zavzame vrednost 1 oz. -1 za neskončno število $x \in \mathbb{Z}$. To pa je protislovje, saj nekonstantni polinom zavzame določeno vrednost le končno mnogokrat.
Naslednji izrek nam bo povedal, da je za ugotavljanje nerazcepnosti polinoma dovolj, da enkrat zavzame praštevilsko vrednost. Še prej pa potrebujemo sledečo lemo.

Lema 1. *Naj bo $f(x) = a_m x^m + \cdots + a_1 x + a_0$ polinom s celimi koeficienti in*

$$H = \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|.$$

Če je $\alpha \in \mathbb{C}$ ničla polinoma $f(x)$, velja

$$|\alpha| < H + 1.$$

Dokaz. Naj bo $\alpha \in \mathbb{C}$ ničla polinoma $f(x)$. Po definiciji je $H \geq 0$. Opazimo, da je $H = 0$ natanko tedaj, ko so vse ničle polinoma $f(x)$ enake 0. V tem primeru lema očitno drži. Naj bo sedaj $H > 0$. Če je $|\alpha| \leq 1$, takoj sledi $|\alpha| < H + 1$. Obravnavajmo še primer $|\alpha| > 1$. Ker je α ničla $f(x)$, velja:

$$0 = a_m \alpha^m + \cdots + a_1 \alpha + a_0$$

oziroma

$$\alpha^m = -\frac{a_{m-1}}{a_m} \alpha^{m-1} - \cdots - \frac{a_1}{a_m} \alpha - \frac{a_0}{a_m}.$$

Naredimo naslednjo oceno:

$$|\alpha^m| \leq |\frac{a_{m-1}}{a_m}||\alpha|^{m-1} + \cdots + |\frac{a_1}{a_m}||\alpha| + |\frac{a_0}{a_m}| \leq$$

$$\leq H(|\alpha|^{m-1} + \cdots + 1) = H\left(\frac{|\alpha|^m - 1}{|\alpha| - 1}\right).$$

Od tu dobimo

$$|\alpha|^{m+1} - |\alpha|^m \leq H|\alpha|^m - H$$

in zato

$$|\alpha|^{m+1} - |\alpha|^m < H|\alpha|^m;$$

sledi $|\alpha| < H + 1$.

■

Lema 1 nam poda oceno absolutnih vrednosti kompleksnih ničel polinoma $f(x)$, ki jo potrebujemo pri dokazu naslednjega izreka.

Izrek 2. *Naj bo $f(x) = a_m x^m + \cdots + a_1 x + a_0$ polinom s celimi koeficienti in*

$$H = \max_{0 \leq i \leq m-1} \left|\frac{a_i}{a_m}\right|.$$

Če je $f(n)$ praštevilo za neko naravno število $n \geq H + 2$, potem je $f(x)$ nerazcepen v $\mathbb{Z}[x]$.

Dokaz. Dokažimo izrek s protislovjem: naj $f(x)$ zadošča predpostavkam izreka in denimo, da je $f(x)$ razcepen v $\mathbb{Z}[x]$; zato obstajata nekonstantna polinoma $g(x), h(x) \in \mathbb{Z}[x]$, da velja $f(x) = g(x)h(x)$. Ker je $f(n)$ praštevilo, je eno izmed števil $g(n)$ in $h(n)$ enak 1 ali -1. Brez škode za splošnost lahko predpostavimo, da je $g(n) = \pm 1$. V $\mathbb{C}[x]$ je $g(x)$ seveda razcepen in ga lahko zapišemo v obliki

$$g(x) = c\prod_i (x - \alpha_i),$$

kjer je $c \in \mathbb{Z}$ vodilni koeficient in so $\alpha_i \in \mathbb{C}$ ničle polinoma $g(x)$. Ničle $g(x)$ so tudi ničle polinoma $f(x)$, zato po lemi 1 velja $|\alpha_i| < H + 1$ za vse ničle polinoma $g(x)$. Ob predpostavki $n \geq H + 2$ potem velja $n - |\alpha_i| > n - (H + 1) \geq 1$ za vse indekse i. Sedaj ocenimo $|g(n)|$:

$$|g(n)| = |c|\prod_i |n - \alpha_i| \geq \prod_i (n - |\alpha_i|) > \prod_i 1 = 1,$$

torej je $|g(n)| > 1$, to pa je v protislovju z $g(n) = \pm 1$.

■

Poglejmo si nekaj primerov uporabe izreka 2.

Primer. Obravnavajmo polinom $f(x) = x^5 - 2x^4 + 2x^2 - x + 1$. Nerazcepnosti tega polinoma ne moremo dokazati z Eisensteinovim kriterijem. Prav tako si ne moremo pomagati z dejstvom, da je polinom $f(x)$ s celimi koeficienti nerazcepen nad $\mathbb{Z}$, če je nerazcepen nad $\mathbb{Z}_p$ za neko praštevilo

p (pri tem gledamo koeficiente polinoma kot elemente polja $\mathbb{Z}_p$). V našem primeru smo za $p = 2$ ali $p = 3$ v zadregi; $p(x)$ kot element $\mathbb{Z}_2[x]$ je enak $x^5 - x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$, kot element $\mathbb{Z}_3[x]$ pa je enak $x^5-2x^4+2x^2-x+1 = (x^2+1)(x^3+x^2+2x+1)$. Po drugi strani pa je pripadajoča konstanta H, definirana kot v lemi 1 in izreku 2, enaka 2. Preverimo lahko, da je $f(4) = 541$ praštevilo, zato je $f(x)$ po izreku 2 nerazcepen v $\mathbb{Z}[x]$.

Primer. Podobno sklepamo pri polinomu $g(x) = 7x^4-x^3-x^2-4x+1$; ta polinom je razcepen nad $\mathbb{Z}_2$, $\mathbb{Z}_3$ in $\mathbb{Z}_5$: ustrezni polinomi so $(x+1)(x^3+x+1)$, $(x+1)^2(x^2+1)$ in $2(x+2)(x^3+2x+4)$; vendar pa je $g(4) = 1697$ praštevilo, zato je nerazcepen v $\mathbb{Z}[X]$.

Primer. Še bolj skrajen primer je polinom $h(x) = x^4 + 6x^2 + 1$; da se dokazati (dokaz za splošnejši primer je dan v[3]), da je $h(x)$ razcepen v $\mathbb{Z}_p[x]$ za vsako praštevilo p. Prav tako ne moremo uporabiti Eisensteinovega kriterija. Vendar pa je $h(8) = 4481$ praštevilo, zato je $h(x)$ po izreku 2 nerazcepen nad $\mathbb{Z}$.

Izrek 2 lahko torej uporabimo v več primerih, ko drugi kriteriji odpovejo. Poleg tega za polinome s celimi koeficienti ne moremo določiti nižje meje za število n, definirano kot v formulaciji izreka. Za primer lahko vzamemo $f(x) = (x-9)(x^2+1) = x^3-9x^2+x-9$; za ta polinom je $H = 9$, $f(10) = 101$ je praštevilo, vendar je $f(x)$ razcepen. Zato je v splošnem primeru izrek 2 najboljši možen. Kljub temu pa ne zadostuje za dokaz Cohnovega izreka. Števke v desetiškem sistemu so omejene z 9, zato za $f(x)$ (kot v formulaciji izreka 1) velja $H = 9$, po izreku 2 pa ni zadostno preveriti $f(10)$, temveč $f(11)$.

3. Posplošitev Cohnovega izreka

Cohnov izrek bomo posplošili za številski sistem s poljubno osnovo $b \geq 2$. To posplošitev so prvi dokazali John Brillhart, Michael Filaseta in Andrew Odlyzko v [2]. Lema 1 nam ne da dovolj ostre ocene velikosti absolutnih vrednostih ničel danega polinoma; to niti ne preseneča, saj lema 1 obravnava splošni primer, pri Cohnovem izreku pa obravnavamo polinome z nenegativnimi koeficienti. Zato nenegativnost (vsaj nekaterih) koeficientov igra bolj pomembno vlogo pri sledeči lemi.

Lema 2. *Naj bo $f(x) = a_m x^m + \cdots + a_1 x + a_0$ polinom s celimi koeficienti in naj velja $a_m \geq 1$, $a_{m-1} \geq 0$ in $|a_i| \leq H$ za vse $i = 0, \ldots, n-2$, kjer je $H > 0$ konstanta. Potem za vsako ničlo $\alpha \in \mathbb{C}$ polinoma $f(x)$ velja bodisi $\Re(\alpha) \leq 0$ bodisi $|\alpha| < \frac{1+\sqrt{1+4H}}{2}$.*

Dokaz. Če je $|\alpha| \leq 1$, očitno drži $|\alpha| < \frac{1+\sqrt{1+4H}}{2}$, saj je $H > 0$.
Za primer $|\alpha| > 1$ pa pokažimo, da kompleksno število z, za katero velja

$$\Re(z) > 0 \text{ in } |z| \geq \frac{1 + \sqrt{1 + 4H}}{2},$$

ne more biti ničla danega polinoma. Želimo torej pokazati, da velja $|f(z)| > 0$. Ker iz zgornjih dveh pogojev med drugim sledi $z \neq 0$, lahko ocenimo:

$$\begin{aligned}
\left|\frac{f(z)}{z^m}\right| &= \left|a_m + \frac{a_{m-1}}{z} + \cdots + \frac{a_0}{z^m}\right| \geq \\
&\geq \left|a_m + \frac{a_{m-1}}{z}\right| - \left|\frac{a_{m-2}}{z^2} + \ldots \frac{a_0}{z^m}\right| \geq \\
&\geq \Re\left(a_m + \frac{a_{m-1}}{z}\right) - \frac{a_{m-2}}{|z|^2} - \cdots - \frac{a_0}{|z|^m} \geq \\
&\geq a_m + a_{m-1}\Re\left(\frac{1}{z}\right) - \left(\frac{H}{|z|^2} + \cdots + \frac{H}{|z|^m}\right) > \\
&> a_m + a_{m-1}\Re\left(\frac{1}{z}\right) - \frac{H}{|z|^2}\frac{1}{1-\frac{1}{|z|}} \geq 1 + a_{m-1}\Re\left(\frac{1}{z}\right) - \frac{H}{|z|^2 - |z|}
\end{aligned}$$

Prvo neenakost smo dobili iz trikotniške neenakosti $|a| = |a + b - b| \leq \leq |a + b| + |b|$, druga neenakost pa je posledica trikotniške neenakosti in neenakosti $\Re(z) \leq |z|$, ki velja za vsak $z \in \mathbb{C}$. Upoštevali smo tudi $a_m \geq 1$. Sedaj upoštevamo še $\Re(\frac{1}{z}) = \Re(\frac{\bar{z}}{|z|^2}) \geq 0$; sledi

$$\left|\frac{f(z)}{z^m}\right| > \frac{|z|^2 - |z| - H}{|z|^2 - |z|}.$$

Rešitve neenačbe

$$\frac{|z|^2 - |z| - H}{|z|^2 - |z|} \geq 0$$

zadoščajo ob predpostavki $|z| > 1$ natanko pogoju

$$|z| \geq \frac{1 + \sqrt{1 + 4H}}{2}.$$

Zato iz zgornjih pogojev res sledi $|f(z)| > 0$. Torej mora za ničlo α, $|\alpha| > 1$, veljati $\Re(\alpha) \leq 0$ ali $|\alpha| < \frac{1+\sqrt{1+4H}}{2}$.

■

Sedaj lahko dokažemo posplošitev Cohnovega izreka.

Izrek 3. *Naj bo $b \geq 3$ naravno število in $p = a_m b^m + \cdots + a_1 b + a_0$ zapis praštevila p v številskem sistemu z osnovo b. Potem je polinom $f(x) = a_m x^m + \cdots + a_1 x + a_0$ nerazcepen v $\mathbb{Q}[x]$.*

Dokaz. Po Gaussovem izreku je dovolj dokazati, da je $f(x)$ nerazcepen v $\mathbb{Z}[x]$. Predpostavimo nasprotno: denimo, da obstajata nekonstantna polinoma $g(x), h(x) \in \mathbb{Z}[x]$, da velja $f(x) = g(x)h(x)$. Ker je $f(b)$ praštevilo, je $g(b)$ ali $h(b)$ enak 1 ali -1. Brez izgube splošnosti naj bo $g(b) = \pm 1$. $g(x)$ lahko zapišemo v obliki

$$g(x) = c\prod_i (x - \alpha_i),$$

kjer je $c \in \mathbb{Z}\backslash\{0\}$ vodilni koeficient in so $\alpha_i \in \mathbb{C}$ ničle polinoma $g(x)$. Polinom $f(x)$ očitno zadošča pogojem leme 2: vsi koeficienti so elementi množice $\{0,\ 1, \ldots, b-1\}$. Zato za vsako ničlo α_i (saj so ničle polinoma $g(x)$ tudi

ničle polinoma $f(x)$) velja bodisi $\Re(\alpha_i) \leq 0$ bodisi $|\alpha_i| < \frac{1+\sqrt{1+4(b-1)}}{2}$. V prvem primeru velja

$$|b - \alpha_i| \geq \Re(b - \alpha_i) = b - \Re(\alpha_i) \geq b.$$

V drugem primeru pa opazimo, da za $b \geq 3$ velja neenakost

$$\frac{1 + \sqrt{1 + 4(b-1)}}{2} \leq b - 1,$$

zato lahko ocenimo

$$|b - \alpha_i| \geq b - |\alpha_i| > b - \frac{1 + \sqrt{1 + 4(b-1)}}{2} \geq 1.$$

Torej za vsak indeks i velja $|b - \alpha_i| > 1$, zato lahko ocenimo $g(b)$:

$$|g(b)| = |c| \prod_i |b - \alpha_i| > 1,$$

to pa je protislovje.

■

Cohnov izrek je posledica izreka 3, če vzamemo $b = 10$. Zadnji izrek smo dokazali za vsak $b \geq 3$; vendar pa ta izrek velja tudi v primeru $b = 2$. V dokazu je bila predpostavka $b \geq 3$ ključna pri uporabi leme 2; ocena

$$\frac{1 + \sqrt{1 + 4(b-1)}}{2} \leq b - 1$$

namreč ne velja za $b = 2$; zato potrebujemo boljšo oceno za polinome, katerih koeficienti so enaki 0 ali 1.

Lema 3. *Naj bo $\alpha \in \mathbb{C}$ ničla polinoma $f(x) = a_m x^m + \cdots + a_1 x + a_0$ s koeficienti iz množice $\{0, 1\}$. Če je $|\arg \alpha| \leq \frac{\pi}{4}$, potem je $|\alpha| < \frac{3}{2}$. Če pa je $|\arg \alpha| > \frac{\pi}{4}$, velja $\Re(\alpha) < \frac{1+\sqrt{5}}{2\sqrt{2}}$.*

Opomba. Tu je $\arg z$ argument kompleksnega števila z, torej kot med pozitivnim realnim poltrakom ter zveznico 0 in z.

Dokaz. Lema očitno drži v primeru $m = 1$ oziroma $m = 2$: za ničle polinomov x, $x + 1$ in x^2, $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$ (to so 0, -1, $\pm i$, $\frac{-1 \pm i\sqrt{3}}{2}$) namreč veljajo zgornji sklepi. Naj bo sedaj $m \geq 3$.
Za prvi del leme zadostuje dokazati, da $z \in \mathbb{C}$, $|\arg z| \leq \frac{\pi}{4}$ in $|z| \geq \frac{3}{2}$, ne more biti ničla danega polinoma. Opazimo sledeče: iz $|\arg z| \leq \frac{\pi}{4}$ sledi $|\arg z^2| \leq \frac{\pi}{2}$, torej $\Re(z) \geq 0$ in $\Re(z^2) \geq 0$, zato pa tudi $\Re(\bar{z}) \geq 0$ in $\Re(\bar{z}^2) \geq 0$. Ker $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$, sledi $\Re(\frac{1}{z}) \geq 0$ in $\Re(\frac{1}{z^2}) \geq 0$. Sedaj lahko za $z \neq 0$ ocenimo:

$$\left|\frac{f(z)}{z^m}\right| = \left|1 + \frac{a_{m-1}}{z} + \cdots + \frac{a_0}{z^m}\right| \geq$$

$$\geq \left|1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right| - \left(\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^m}\right) \geq$$

$$\geq \Re\left(1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right) - \frac{1}{|z|^3}\left(1 + \frac{1}{|z|} + \cdots + \frac{1}{|z|^{m-3}}\right) >$$

$$> 1 + a_{m-1}\Re\left(\frac{1}{z}\right) + a_{m-2}\Re\left(\frac{1}{z^2}\right) - \frac{1}{|z|^3}\frac{1}{1-\frac{1}{|z|}} \geq$$

$$\geq 1 - \frac{1}{|z|^3 - |z|^2} = \frac{|z|^3 - |z|^2 - 1}{|z|^3 - |z|^2}.$$

Po predpostavki je imenovalec zgornjega ulomka pozitiven. Oglejmo si funkcijo

$$h(x) = x^3 - x^2 - 1.$$

Ker je $h'(x) = 3x^2 - 2x = x(3x-2)$, je $h(x)$ monotono naraščajoča za $x > \frac{2}{3}$. Ker je še $h(\frac{3}{2}) = \frac{1}{8}$, je $h(x)$ strogo pozitivna za $x \geq \frac{3}{2}$. To upoštevajoč v zgornji neenačbi vidimo, da $\left|\frac{f(z)}{z^m}\right| > 0$ oz. $|f(z)| > 0$.
Dokažimo še drugi del leme. Naj bo α, $|\arg\alpha| > \frac{\pi}{4}$, ničla polinoma $f(x)$. Po lemi 2 je bodisi $\Re(\alpha) \leq 0$ bodisi $|\alpha| < \frac{1+\sqrt{1+4\cdot 1}}{2} = \frac{1+\sqrt{5}}{2}$. V drugem primeru lahko ocenimo $\Re(\alpha) = |\alpha|\cos(\arg\alpha) < \frac{1+\sqrt{5}}{2}\frac{\sqrt{2}}{2} = \frac{1+\sqrt{5}}{2\sqrt{2}}$; drugi del leme je tako dokazan.

■

Sedaj lahko dokažemo trditev, ki posploši Cohnov izrek za zapis praštevil v dvojiškem sistemu.

Trditev 1. *Naj bo $p = a_m 2^m + \cdots + a_1 2 + a_0$ zapis praštevila p v dvojiškem številskem sistemu. Potem je polinom $f(x) = a_m x^m + \cdots + a_1 x + a_0$ nerazcepen v $\mathbb{Q}[x]$.*

Dokaz. Naj bo α ničla polinoma $f(x)$. Ta polinom zadošča predpostavkam leme 3, zato lahko ocenimo $\Re(\alpha) < \frac{3}{2}$. Res, prvi del leme nam pove, da v primeru $|\arg\alpha| \leq \frac{\pi}{4}$ velja $\Re(\alpha) < \frac{3}{2}$. V drugem primeru pa velja $\Re(\alpha) \leq |\alpha| < \frac{1+\sqrt{5}}{2\sqrt{2}} < \frac{3}{2}$.
Po Gaussovem izreku je dovolj dokazati, da je $f(x)$ nerazcepen nad $\mathbb{Z}$. Predpostavimo nasprotno: denimo, da obstajata nekonstantna polinoma $g(x)$, $h(x) \in \mathbb{Z}[x]$, da velja $f(x) = g(x)h(x)$. Ker je $f(2)$ praštevilo, je ponovno brez škode za splošnost $g(2) = \pm 1$. $g(x)$ lahko v $\mathbb{C}[x]$ razcepimo na produkt linearnih faktorjev:

$$g(x) = c\prod_i (x - \alpha_i),$$

Oglejmo si sedaj polinom

$$g\left(x + \frac{3}{2}\right) = c\prod_i \left(x + \frac{3}{2} - \alpha_i\right).$$

Ker je $g(x) \in \mathbb{Z}[x]$, ima $g(x + \frac{3}{2})$ realne koeficiente. Pokažimo, da imajo vsi ti koeficienti enak predznak. Če je α_i realno število, ima po zgornji oceni (α_i je namreč tudi ničla $f(x)$) linearni polinom

$$x + \frac{3}{2} - \alpha_i$$

pozitivne koeficiente. Če pa je α_i kompleksno število, je ničla polinoma $g(x)$ tudi $\bar{\alpha_i}$, saj ima $g(x)$ realne koeficiente. Vidimo, da ima tudi kvadratni polinom

$$\left(x+\frac{3}{2}-\alpha_i\right)\left(x+\frac{3}{2}-\bar{\alpha_i}\right)=$$
$$=x^2+2\left(\frac{3}{2}-\frac{\alpha_i+\bar{\alpha_i}}{2}\right)x+\left(\frac{3}{2}-\alpha_i\right)\overline{\left(\frac{3}{2}-\alpha_i\right)}=$$
$$=x^2+2\left(\frac{3}{2}-\Re(\alpha_i)\right)x+\left|\frac{3}{2}-\alpha_i\right|^2$$

pozitivne koeficiente; ker je $g\left(x+\frac{3}{2}\right)$ produkt polinomov zgornjih dveh tipov ter koeficienta c, imajo vsi koeficienti $g(x)$ enak predznak, to je $\operatorname{sgn}(c)$. Zato ima polinom $g\left(-x+\frac{3}{2}\right)$ alternirajoče koeficiente. Ker je $g(x)$ stopnje vsaj 1, sta tudi $g\left(x+\frac{3}{2}\right)$ in $g\left(-x+\frac{3}{2}\right)$ stopnje vsaj 1. Ker ima $g(x)$ nenegativne koeficiente, imata $g\left(x+\frac{3}{2}\right)$ in $g\left(-x+\frac{3}{2}\right)$ vsaj en člen, v katerem je spremenljivka x na liho potenco. Zato za vsak $x>0$ velja

$$\left|g\left(-x+\frac{3}{2}\right)\right|<\left|g\left(x+\frac{3}{2}\right)\right|.$$

Če vstavimo $x=\frac{1}{2}$, dobimo $|g(1)|<|g(2)|$; ker je $g(x)$ polinom s celimi koeficienti, je $g(1)$ celo število, različno od nič; če bi namreč veljalo $g(1)=0$, bi sledilo $f(1)=0$, to pa ni možno, saj so koeficienti polinoma $f(x)$ nenegativni. Zato $1\leq|g(1)|<|g(2)|$, to pa je protislovje s prvotno predpostavko.

■

Poglejmo si posplošeni Cohnov izrek na primeru praštevila $p=2411$. Če zapišemo p v številskih sistemih z osnovami $b=2,3,\ldots,10$, dobimo naslednje nerazcepne polinome:

osnova	polinom
2	$x^{11}+x^8+x^6+x^5+x^3+x+1$
3	$x^7+2x^4+2x^3+2x+2$
4	$2x^5+x^4+x^3+2x^2+2x+3$
5	$3x^4+4x^3+x^2+2x+1$
6	x^4+5x^3+5x+5
7	x^4+x+3
8	$4x^3+5x^2+5x+3$
9	$3x^3+2x^2+6x+8$
10	$2x^3+4x^2+x+1$

4. Sklep

Smiselno se je vprašati, kaj bi bil obrat Cohnovega izreka. Ali zavzame vsak nerazcepen polinom s celimi tujimi koeficienti praštevilsko vrednost? Odgovor je ne; polinom $f(x) = x^2 + x + 4$ je očitno nerazcepen, vendar je $f(n)$ sodo število za vsak $n \in \mathbb{N}$ in $f(n)>4$, torej $f(x)$ ne zavzame praštevilske vrednosti. Zanimivo pa je, da je nekoliko šibkejši obrat še odprt problem. Viktor Jakovljevič Bunjakovski je leta 1857 postavil naslednjo domnevo ([4]): če je polinom $f(x)$ stopnje 2 ali več nerazcepen nad $\mathbb{Z}$, njegov vodilni koeficient pozitiven in ima množica $f(\mathbb{N})$ največji skupni delitelj enak 1, potem ta polinom neskončnokrat zavzame praštevilske vrednosti na naravnih številih. V primeru linearnih polinomov ta trditev drži po Dirichletovem izreku, sicer pa so tudi razni posebni primeri domneve Bunjakovskega še nedokazani, denimo ali je izraz $n^2 + 1$ praštevilo za neskončno naravnih števil n.
Za konec bi omenil še Cohnovemu analogen izrek, ki velja v polju racionalnih funkcij nad končnim poljem. Maruti Ram Murty je v [1] navedel izrek:

Izrek 4. *naj bo $K(x)$ polje racionalnih funkcij nad končnim poljem, $b(x)$ polinom v $K[x]$ in $p(x)$ nerazcepen polinom v $K[x]$. Če $p(x)$ razvijemo po $b(x)$, to je*

$$p(x) = a_m(x)b(x)^m + \cdots + a_1(x)b(x) + a_0(x)$$

in imajo polinomi $a_i(x)$ manjšo stopnjo od polinoma $b(x)$, potem je polinom

$$f(y) = a_m(x)y^m + \cdots + a_1(x)y + a_0(x)$$

nerazcepen nad $K[y]$.

S pomočjo tega izreka pa je možno preverjati nerazcepnost polinomov dveh spremenljivk nad končnim poljem.

Literatura

[1] M. Ram Murti: *Prime numbers and irreducible polynomials*, The American Mathematical Monthly 109 (May 2002), 452-458.

[2] J. Brillhart, M. Filaseta, A. Odlyzko: *On a irreducibility theorem of A. Cohn*, Canadian Journal of Mathematics 33 (1981), 1055-1059.

[3] E. Driver, P. A. Leonard, K. S. Williams: *Irreducible Quartic Polynomials with Factorizations modulo p*, The American Mathematical Monthly 112 (December 2005), 876-890.

[4] S. Lang: *Algebra*, 3rd ed., Addison-Wesley, Reading, MA, 1993.

[5] `http://en.wikipedia.org/wiki/Cohn_irreducibility_criterion`