Po bližnjici do končnih polj

dr. Boštjan Kuzman
Univerza v Ljubljani, Pedagoška fakulteta

MARS 2013, Bohinj, 21. avgust 2013

Štoparski uvod

Na začetku je bilo ustvarjeno Vesolje. To je povzročilo veliko jeze in nasploh velja za slabo potezo.

Douglas Adams, Štoparski vodič po galaksiji

Zadnja novica: končno je bolj zanimivo od neskončnega

Ogrlice

Naj bo p praštevilo. Koliko *različnih* ogrlic s p kroglicami lahko naredimo, če imamo na voljo dovolj kroglic v a različnih barvah?

Ogrlice

Naj bo p praštevilo. Koliko *različnih* ogrlic s p kroglicami lahko naredimo, če imamo na voljo dovolj kroglic v a različnih barvah?

Pojasnilo: Dve ogrlici smatramo za enaki, če lahko iz prve dobimo drugo le s krožnim premeščanjem kroglic, zrcaljenja ogrlice pa ne dovolimo (npr. $ABC = BCA \neq ACB$).

Ogrlice

Naj bo p praštevilo. Koliko *različnih* ogrlic s p kroglicami lahko naredimo, če imamo na voljo dovolj kroglic v a različnih barvah?

Pojasnilo: Dve ogrlici smatramo za enaki, če lahko iz prve dobimo drugo le s krožnim premeščanjem kroglic, zrcaljenja ogrlice pa ne dovolimo (npr. $ABC = BCA \neq ACB$).

Odgovor: $\frac{a^p - a}{p} + a$. *Premisli!*

Ogrlice

Naj bo p praštevilo. Koliko *različnih* ogrlic s p kroglicami lahko naredimo, če imamo na voljo dovolj kroglic v a različnih barvah?

Pojasnilo: Dve ogrlici smatramo za enaki, če lahko iz prve dobimo drugo le s krožnim premeščanjem kroglic, zrcaljenja ogrlice pa ne dovolimo (npr. $ABC = BCA \neq ACB$).

Odgovor: $\frac{a^p - a}{p} + a$. *Premisli!*

Torej je $\frac{a^p - a}{p}$ celo število. Dokazali smo...

Mali Fermatov izrek

Izrek

Za vsako praštevilo p in pozitivno celo število a je število $a^p - a$ deljivo s p. Torej,

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

Mali Fermatov izrek

Izrek

Za vsako praštevilo p in pozitivno celo število a je število $a^p - a$ deljivo s p. Torej,

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

Posledica

Če p ne deli a, je $a^{p-1} \equiv 1 \pmod{p}$.

Zgledi uporabe MFI

- Koliko je ostanek deljenja števila 3^{50} s številom 7?

Zgledi uporabe MFI

- Koliko je ostanek deljenja števila 3^{50} s številom 7?
  Odgovor: Po MFI je $3^6 \equiv 1 \pmod 7$, *zato je*
  $3^{50} = 3^{6 \cdot 8 + 2} = (3^6)^8 \cdot 9 \equiv 2 \pmod 7$.

Zgledi uporabe MFI

- Koliko je ostanek deljenja števila 3^{50} s številom 7?
  Odgovor: Po MFI je $3^6 \equiv 1 \pmod 7$, *zato je*
  $3^{50} = 3^{6 \cdot 8 + 2} = (3^6)^8 \cdot 9 \equiv 2 \pmod 7$.
- S katerim številom lahko pomnožim 5, da bo imel rezultat ostanek 1 pri deljenju s 7?

Zgledi uporabe MFI

- Koliko je ostanek deljenja števila 3^{50} s številom 7?
  Odgovor: Po MFI je $3^6 \equiv 1 \pmod 7$, *zato je*
  $3^{50} = 3^{6 \cdot 8 + 2} = (3^6)^8 \cdot 9 \equiv 2 \pmod 7$.
- S katerim številom lahko pomnožim 5, da bo imel rezultat ostanek 1 pri deljenju s 7?
  Odgovor: 5^5, *saj je* $5 \cdot 5^5 = 5^6 \equiv 1 \pmod 7$.
  Opomba: $5^5 \equiv 3 \pmod 7$, kar bi lahko tudi uganili, saj je $3 \cdot 5 \equiv 1 \pmod 7$.

Zgledi uporabe MFI

- Koliko je ostanek deljenja števila 3^{50} s številom 7?
  Odgovor: Po MFI je $3^6 \equiv 1 \pmod 7$, *zato je*
  $3^{50} = 3^{6 \cdot 8+2} = (3^6)^8 \cdot 9 \equiv 2 \pmod 7$.
- S katerim številom lahko pomnožim 5, da bo imel rezultat ostanek 1 pri deljenju s 7?
  Odgovor: 5^5, *saj je* $5 \cdot 5^5 = 5^6 \equiv 1 \pmod 7$.
  Opomba: $5^5 \equiv 3 \pmod 7$, kar bi lahko tudi uganili, saj je $3 \cdot 5 \equiv 1 \pmod 7$.
- Dokaži, da 42 deli $n^7 - n$ za vsako naravno število n.

Zgledi uporabe MFI

- Koliko je ostanek deljenja števila 3^{50} s številom 7?
  Odgovor: Po MFI je $3^6 \equiv 1 \pmod 7$, *zato je*
  $3^{50} = 3^{6 \cdot 8 + 2} = (3^6)^8 \cdot 9 \equiv 2 \pmod 7$.
- S katerim številom lahko pomnožim 5, da bo imel rezultat ostanek 1 pri deljenju s 7?
  Odgovor: 5^5, *saj je* $5 \cdot 5^5 = 5^6 \equiv 1 \pmod 7$.
  Opomba: $5^5 \equiv 3 \pmod 7$, kar bi lahko tudi uganili, saj je $3 \cdot 5 \equiv 1 \pmod 7$.
- Dokaži, da 42 deli $n^7 - n$ za vsako naravno število n.
  Odgovor: Domača naloga.

Polje - približna definicija

Polje (angleško *field*) je množica elementov, s katerimi lahko izvajamo 4 osnovne računske operacije: seštevanje, odštevanje, množenje in deljenje.

Polje - približna definicija

Polje (angleško *field*) je množica elementov, s katerimi lahko izvajamo 4 osnovne računske operacije: seštevanje, odštevanje, množenje in deljenje.

Ali poznamo kakšen primer polja?

Polje - približna definicija

Polje (angleško *field*) je množica elementov, s katerimi lahko izvajamo 4 osnovne računske operacije: seštevanje, odštevanje, množenje in deljenje.

Ali poznamo kakšen primer polja?

- Racionalna števila $\mathbb{Q}$,
- Realna števila $\mathbb{R}$,
- Kompleksna števila $\mathbb{C}$.

Še kakšno?

Polje - približna definicija

Polje (angleško *field*) je množica elementov, s katerimi lahko izvajamo 4 osnovne računske operacije: seštevanje, odštevanje, množenje in deljenje.

Ali poznamo kakšen primer polja?

- Racionalna števila $\mathbb{Q}$,
- Realna števila $\mathbb{R}$,
- Kompleksna števila $\mathbb{C}$.

Še kakšno?

Oglejmo si bolj natančno definicijo...

”Ljudje, ki vedo, o čem govorijo, ne potrebujejo PowerPointa.”

Steve Jobs, o nezaželeni uporabi prosojnic na sestankih.

Polje - natančna definicija

Polje je urejena trojica $(\mathbb{F}, +, \cdot)$, ki jo sestavljajo neprazna množica $\mathbb{F}$ ter dvočleni operaciji $+$ in $\cdot$, za kateri velja:

1. $\forall a, b \in \mathbb{F}\colon a + b \in \mathbb{F}$ (zaprtost za $+$)
2. $\forall a, b, c \in \mathbb{F}\colon (a + b) + c = a + (b + c)$ (asociativnost za $+$).
3. $\forall a, b \in \mathbb{F}\colon a + b = b + a$ (komutativnost za $+$).
4. $\exists e \in \mathbb{F}\colon e + a = a + e = a$ (obstoj nevt. elementa za $+$). Oznaka: $0_{\mathbb{F}}$.
5. $\forall a \in \mathbb{F} \exists b \in \mathbb{F}\colon a + b = b + a = 0_{\mathbb{F}}$ (obstoj obratov za $+$). Oznaka: $-a$.
6. $\forall a, b \in \mathbb{F}\colon a \cdot b \in \mathbb{F}$ (zaprtost za $\cdot$)
7. $\forall a, b, c \in \mathbb{F}\colon (ab)c = a(bc)$ (asociativnost za $\cdot$).
8. $\forall a, b \in \mathbb{F}\colon ab = ba$ (komutativnost za $\cdot$).
9. $\exists e \in \mathbb{F}\colon ea = ae = a$ (obstoj nevtralnega elementa za $\cdot$). Oznaka: $1_{\mathbb{F}}$.
10. $\forall a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\} \exists b \in \mathbb{F}\colon ab = ba = 0_{\mathbb{F}}$ (obstoj obratov za $+$). Oznaka: a^{-1}.
11. $\forall a, b, c \in \mathbb{F}\colon a(b + c) = ab + ac$ (distributivnost $+$ in $\cdot$).
12. $1_{\mathbb{F}} \neq 0_{\mathbb{F}}$.

Najmanjše polje

- Kako veliko je najmanjše polje?

Najmanjše polje

- Kako veliko je najmanjše polje?
- Vsako polje vsebuje vsaj dva elementa: $0_{\mathbb{F}}$ in $1_{\mathbb{F}}$. Ali polje reda 2 res obstaja?

Najmanjše polje

- Kako veliko je najmanjše polje?
- Vsako polje vsebuje vsaj dva elementa: $0_{\mathbb{F}}$ in $1_{\mathbb{F}}$. Ali polje reda 2 res obstaja?
- Množica $\{0, 1\} \subset \mathbb{Q}$ z običajnima operacijama **ni** polje, saj $1 + 1 \notin \{0, 1\}$!

Najmanjše polje

- Kako veliko je najmanjše polje?
- Vsako polje vsebuje vsaj dva elementa: $0_{\mathbb{F}}$ in $1_{\mathbb{F}}$. Ali polje reda 2 res obstaja?
- Množica $\{0, 1\} \subset \mathbb{Q}$ z običajnima operacijama **ni** polje, saj $1 + 1 \notin \{0, 1\}$!
- Ideja: seštevanje definiramo malo drugače.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Najmanjše polje

- Kako veliko je najmanjše polje?
- Vsako polje vsebuje vsaj dva elementa: $0_{\mathbb{F}}$ in $1_{\mathbb{F}}$. Ali polje reda 2 res obstaja?
- Množica $\{0, 1\} \subset \mathbb{Q}$ z običajnima operacijama **ni** polje, saj $1 + 1 \notin \{0, 1\}$!
- Ideja: seštevanje definiramo malo drugače.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- Interpretacija: gledamo ostanke celih števil pri deljenju z 2 (0 predstavlja soda števila, 1 pa liha števila).
- Množica $\{0, 1\}$ s tema operacijama je polje (premisli). Oznaka: $\mathbb{Z}_2$.

Polje $\mathbb{Z}_3$

Po analogiji od prej gledamo ostanke pri deljenju s 3 in dobimo naslednji tabeli operacij:

Polje $\mathbb{Z}_3$

Po analogiji od prej gledamo ostanke pri deljenju s 3 in dobimo naslednji tabeli operacij:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Polje $\mathbb{Z}_3$

Po analogiji od prej gledamo ostanke pri deljenju s 3 in dobimo naslednji tabeli operacij:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Ali res veljajo vse zahtevane lastnosti za polje?

Polje $\mathbb{Z}_3$

Po analogiji od prej gledamo ostanke pri deljenju s 3 in dobimo naslednji tabeli operacij:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Ali res veljajo vse zahtevane lastnosti za polje?

- Zaprtost za $+$ in $\cdot$: Da. Očitno?
- Komutativnost, asociativnost, distributivnost: Da, se dedujejo iz $\mathbb{Z}$.
- Obstoj nevtralnih elementov: Da, 0 in 1 iz $\mathbb{Z}_3$.
- Obstoj obratov: Da, $-0 = 0$, $-1 = 2$, $-2 = 1$, $1^{-1} = 1$, $2^{-1} = 2$.

Torej, $\mathbb{Z}_3$ je polje s tremi elementi.

Polje reda 4

Kot prej sestavimo tabeli operacij v $\mathbb{Z}_4$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Polje reda 4

Kot prej sestavimo tabeli operacij v $\mathbb{Z}_4$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Element 2 nima obrata za množenje. $\mathbb{Z}_4$ **ni polje!**

Polje reda 4

Kot prej sestavimo tabeli operacij v $\mathbb{Z}_4$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Element 2 nima obrata za množenje. $\mathbb{Z}_4$ **ni polje!**

To pa ne pomeni, da polje reda 4 ne obstaja. Z nekaj spretnosti si lahko izmislimo "boljši"operaciji na štirielementni množici $\{0, 1, a, b\}$.

Polje reda 4

Kot prej sestavimo tabeli operacij v $\mathbb{Z}_4$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Element 2 nima obrata za množenje. $\mathbb{Z}_4$ **ni polje!**

To pa ne pomeni, da polje reda 4 ne obstaja. Z nekaj spretnosti si lahko izmislimo "boljši"operaciji na štirielementni množici $\{0, 1, a, b\}$.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Izkaže se, da je to res polje (rigorozen dokaz: DN).
Oznaka $GF(4)$: (Galois' field - Galoisjevo polje reda 4).

Pomembna vprašanja

1. Kdaj je $\mathbb{Z}_n$ polje?
2. Ali obstajajo polja reda n za vsak $n \geq 2$?
3. Ali lahko za kakšen n obstaja več različnih polj reda n?
4. Kako najti oziroma "konstruirati" vsa končna polja?

Polja $\mathbb{Z}_p$

Izrek

Množica $\mathbb{Z}_n$ z operacijama $+, \cdot \mod n$ je polje natanko tedaj, ko je n praštevilo.

Polja $\mathbb{Z}_p$

Izrek

Množica $\mathbb{Z}_n$ z operacijama $+, \cdot \mod n$ je polje natanko tedaj, ko je n praštevilo.

Dokaz:
Če je $n = p$ praštevilo, po MFI velja $a^{p-1} \equiv 1 \pmod{p}$, če p ne deli a. Torej ima vsak neničelni $a \in \{1, \ldots, p-1\}$ obrat $a^{p-2} \in \mathbb{Z}_p \setminus \{0\}$. Tudi ostale lastnosti polj so izpolnjene (premisli!), zato je $\mathbb{Z}_p$ polje.

Polja $\mathbb{Z}_p$

Izrek

Množica $\mathbb{Z}_n$ z operacijama $+, \cdot \pmod n$ je polje natanko tedaj, ko je n praštevilo.

Dokaz:
Če je $n = p$ praštevilo, po MFI velja $a^{p-1} \equiv 1 \pmod p$, če p ne deli a. Torej ima vsak neničelni $a \in \{1, \ldots, p-1\}$ obrat $a^{p-2} \in \mathbb{Z}_p \setminus \{0\}$. Tudi ostale lastnosti polj so izpolnjene (premisli!), zato je $\mathbb{Z}_p$ polje.

Če je n sestavljeno število, je $n = ab$ za $a, b \in \mathbb{Z}$, $2 \geq a, b < n$. Za ustrezna ostanka $a, b \in \mathbb{Z}_n$ potem velja $ab = 0$. Če bi imel a obrat za množenje, bi sledilo

$$b = (a^{-1}a)b = a^{-1} \cdot 0 = 0,$$

torej $b = 0 \pmod n$, protislovje.

Opomba: računanje obratov v $\mathbb{Z}_p$

MFI pove, da obrat za $a \in \mathbb{Z}_p \setminus \{0\}$ vedno obstaja in je enak a^{p-2}, saj je $a^{p-1} \equiv 1 \pmod{p}$. Za računanje to ni najbolj praktično...

Opomba: računanje obratov v $\mathbb{Z}_p$

MFI pove, da obrat za $a \in \mathbb{Z}_p \setminus \{0\}$ vedno obstaja in je enak a^{p-2}, saj je $a^{p-1} \equiv 1 \pmod{p}$. Za računanje to ni najbolj praktično...

Primer: Koliko je $7^{-1} \in \mathbb{Z}_{311}$?

Opomba: računanje obratov v $\mathbb{Z}_p$

MFI pove, da obrat za $a \in \mathbb{Z}_p \setminus \{0\}$ vedno obstaja in je enak a^{p-2}, saj je $a^{p-1} \equiv 1 \pmod{p}$. Za računanje to ni najbolj praktično...

Primer: Koliko je $7^{-1} \in \mathbb{Z}_{311}$?

MFI: $7^{-1} = 7^{309} = \ldots$ (precej računanja).

Opomba: računanje obratov v $\mathbb{Z}_p$

MFI pove, da obrat za $a \in \mathbb{Z}_p \setminus \{0\}$ vedno obstaja in je enak a^{p-2}, saj je $a^{p-1} \equiv 1 \pmod{p}$. Za računanje to ni najbolj praktično...

Primer: Koliko je $7^{-1} \in \mathbb{Z}_{311}$?

MFI: $7^{-1} = 7^{309} = \ldots$ (precej računanja).

Obrate raje računamo z (razširjenim) Evklidovim algoritmom. V našem primeru za števili 311 in 7 dobimo enakosti $311 = 44 \cdot 7 + 3$ in $7 = 2 \cdot 3 + 1$. Od tod lahko izrazimo $1 = 7 - 2 \cdot 3$ in $3 = 311 - 44 \cdot 7$, kar nam da enakost oblike $1 = a \cdot 311 + b \cdot 7$ za $a = -2$ in $b = 89$. Če jo delimo s 311, dobimo $1 \equiv b \cdot 7 \pmod{311}$, torej je b iskani obrat za 7. Sledi $7^{-1} = 89 \in \mathbb{Z}_{311}$.

Druga polja

Izrek

Če je $\mathbb{F}$ končno polje, potem je njegov red lahko le p^k, kjer je p neko praštevilo in k pozitivno celo število.

Druga polja

Izrek

Če je $\mathbb{F}$ končno polje, potem je njegov red lahko le p^k, kjer je p neko praštevilo in k pozitivno celo število.

Dokaz: 2. letnik faksa?

Druga polja

Izrek

Če je $\mathbb{F}$ končno polje, potem je njegov red lahko le p^k, kjer je p neko praštevilo in k pozitivno celo število.

Dokaz: 2. letnik faksa?

Izrek

Če sta $\mathbb{F}$ in $\mathbb{F}'$ končni polji istega reda, potem sta "v bistvu"enaki (izomorfni).

Druga polja

Izrek

Če je $\mathbb{F}$ končno polje, potem je njegov red lahko le p^k, kjer je p neko praštevilo in k pozitivno celo število.

Dokaz: 2. letnik faksa?

Izrek

Če sta $\mathbb{F}$ in $\mathbb{F}'$ končni polji istega reda, potem sta "v bistvu"enaki (izomorfni).

Dokaz: 2. letnik faksa?

Druga polja

Izrek

Če je $\mathbb{F}$ končno polje, potem je njegov red lahko le p^k, kjer je p neko praštevilo in k pozitivno celo število.

Dokaz: 2. letnik faksa?

Izrek

Če sta $\mathbb{F}$ in $\mathbb{F}'$ končni polji istega reda, potem sta "v bistvu"enaki (izomorfni).

Dokaz: 2. letnik faksa?

Izrek

Za vsako praštevilo p in pozitivno celo število k obstaja polje reda p^k.

Druga polja

Izrek

Če je $\mathbb{F}$ končno polje, potem je njegov red lahko le p^k, kjer je p neko praštevilo in k pozitivno celo število.

Dokaz: 2. letnik faksa?

Izrek

Če sta $\mathbb{F}$ in $\mathbb{F}'$ končni polji istega reda, potem sta "v bistvu"enaki (izomorfni).

Dokaz: 2. letnik faksa?

Izrek

Za vsako praštevilo p in pozitivno celo število k obstaja polje reda p^k.

Ideja dokaza: Zdaj.

Konstrukcija Galoisjevih polj

- Podobno kot cela števila lahko med seboj delimo tudi polinome s celoštevilskimi koeficienti in opazujemo ostanke:

Konstrukcija Galoisjevih polj

- Podobno kot cela števila lahko med seboj delimo tudi polinome s celoštevilskimi koeficienti in opazujemo ostanke:

  PRIMER: $x^2 + 1 \equiv 2 \pmod{x+1}$,
  ker je $x^2 + 1 = (x+1)(x-1) + 2$.

Konstrukcija Galoisjevih polj

- Podobno kot cela števila lahko med seboj delimo tudi polinome s celoštevilskimi koeficienti in opazujemo ostanke:

  PRIMER: $x^2 + 1 \equiv 2 \pmod{x+1}$,
  ker je $x^2 + 1 = (x+1)(x-1) + 2$.

- Namesto koeficientov v $\mathbb{Z}$ lahko vzamemo koeficiente v $\mathbb{Z}_p$.

Konstrukcija Galoisjevih polj

- Podobno kot cela števila lahko med seboj delimo tudi polinome s celoštevilskimi koeficienti in opazujemo ostanke:

  PRIMER: $x^2 + 1 \equiv 2 \pmod{x+1}$,
  ker je $x^2 + 1 = (x+1)(x-1) + 2$.

- Namesto koeficientov v $\mathbb{Z}$ lahko vzamemo koeficiente v $\mathbb{Z}_p$.

  PRIMER: $x^2 + 1 \equiv 0 \pmod{x+1}$ nad $\mathbb{Z}_2$, ker je
  $x^2 + 1 = (x+1)(x+1) + 0$.

Konstrukcija Galoisjevih polj

- Podobno kot cela števila lahko med seboj delimo tudi polinome s celoštevilskimi koeficienti in opazujemo ostanke:

  PRIMER: $x^2 + 1 \equiv 2 \pmod{x+1}$,
  ker je $x^2 + 1 = (x+1)(x-1) + 2$.

- Namesto koeficientov v $\mathbb{Z}$ lahko vzamemo koeficiente v $\mathbb{Z}_p$.

  PRIMER: $x^2 + 1 \equiv 0 \pmod{x+1}$ nad $\mathbb{Z}_2$, ker je
  $x^2 + 1 = (x+1)(x+1) + 0$.

  PRIMER: Nad $\mathbb{Z}_2$ je polinom $x^2 + 1$ razcepen, polinom $x^2 + x + 1$ pa ne.

Konstrukcija Galoisjevih polj

- Podobno kot cela števila lahko med seboj delimo tudi polinome s celoštevilskimi koeficienti in opazujemo ostanke:

  PRIMER: $x^2 + 1 \equiv 2 \pmod{x+1}$,
  ker je $x^2 + 1 = (x+1)(x-1) + 2$.

- Namesto koeficientov v $\mathbb{Z}$ lahko vzamemo koeficiente v $\mathbb{Z}_p$.

  PRIMER: $x^2 + 1 \equiv 0 \pmod{x+1}$ nad $\mathbb{Z}_2$, ker je
  $x^2 + 1 = (x+1)(x+1) + 0$.

  PRIMER: Nad $\mathbb{Z}_2$ je polinom $x^2 + 1$ razcepen, polinom $x^2 + x + 1$ pa ne.

- Če je $p(x)$ nerazcepen polinom stopnje k nad $\mathbb{Z}_p$, imamo p^k različnih ostankov pri deljenju s $p(x)$.

Konstrukcija Galoisjevih polj

- Podobno kot cela števila lahko med seboj delimo tudi polinome s celoštevilskimi koeficienti in opazujemo ostanke:

  PRIMER: $x^2 + 1 \equiv 2 \pmod{x+1}$,
  ker je $x^2 + 1 = (x+1)(x-1) + 2$.

- Namesto koeficientov v $\mathbb{Z}$ lahko vzamemo koeficiente v $\mathbb{Z}_p$.

  PRIMER: $x^2 + 1 \equiv 0 \pmod{x+1}$ nad $\mathbb{Z}_2$, ker je
  $x^2 + 1 = (x+1)(x+1) + 0$.

  PRIMER: Nad $\mathbb{Z}_2$ je polinom $x^2 + 1$ razcepen, polinom $x^2 + x + 1$ pa ne.

- Če je $p(x)$ nerazcepen polinom stopnje k nad $\mathbb{Z}_p$, imamo p^k različnih ostankov pri deljenju s $p(x)$.

  PRIMER: Ostanki pri deljenju z $x^2 + x + 1$ nad $\mathbb{Z}_2$ so vsi polinomi nižje stopnje, torej 0, 1, x in $x + 1$.

Konstrukcija Galoisjevih polj

- Podobno kot cela števila lahko med seboj delimo tudi polinome s celoštevilskimi koeficienti in opazujemo ostanke:

  PRIMER: $x^2 + 1 \equiv 2 \pmod{x+1}$,
  ker je $x^2 + 1 = (x+1)(x-1) + 2$.

- Namesto koeficientov v $\mathbb{Z}$ lahko vzamemo koeficiente v $\mathbb{Z}_p$.

  PRIMER: $x^2 + 1 \equiv 0 \pmod{x+1}$ nad $\mathbb{Z}_2$, ker je
  $x^2 + 1 = (x+1)(x+1) + 0$.

  PRIMER: Nad $\mathbb{Z}_2$ je polinom $x^2 + 1$ razcepen, polinom $x^2 + x + 1$ pa ne.

- Če je $p(x)$ nerazcepen polinom stopnje k nad $\mathbb{Z}_p$, imamo p^k različnih ostankov pri deljenju s $p(x)$.

  PRIMER: Ostanki pri deljenju z $x^2 + x + 1$ nad $\mathbb{Z}_2$ so vsi polinomi nižje stopnje, torej 0, 1, x in $x + 1$.

- **Seštevanje in množenje teh ostankov nam da ravno polje reda p^k.**

Še enkrat polje reda 4.

Prva različica - abstraktni operaciji nad simboli $0, 1, a, b$:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Še enkrat polje reda 4.

Prva različica - abstraktni operaciji nad simboli $0, 1, a, b$:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Druga različica - ostanki pri deljenju z nerazcepnim polinomom $x^2 + x + 1$ s koeficienti v $\mathbb{Z}_2$:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

V bistvu gre za isto polje!!!

Zaključek

- Polje reda p^k "konstruiramo" kot množico ostankov pri deljenju z nerazcepnim polinomom nad $\mathbb{Z}_p$.
  - Ostanki pri deljenju z nerazcepnim polinomom $x^3 + x + 1$ nad $\mathbb{Z}_2$ dajo polje reda $2^3 = 8$.
  - Ostanki pri deljenju z nerazcepnim polinomom $x^2 + 1$ nad $\mathbb{Z}$ dajo polje reda $3^2 = 9$.
  - ...
- Za konstrukcijo polja reda p^k potrebujemo (vsaj en) nerazcepen polinom stopnje k nad $\mathbb{Z}_p$. Izkaže se, da je polinom $x^k + x^{k-1} + \ldots + x + 1$ nad $\mathbb{Z}_p$ nerazcepen za vsak k.
- Zakaj imajo neničelni ostanki vedno obrate za množenje? Ker smo izbrali nerazcepni polinom in ker za polinome nad polji velja Evklidov algoritem. (Rigorozna utemeljitev zahteva precej teorije).

- Evariste Galois: beri življenjepis na Wikipediji.

Uporaba končnih polj

- Kriptografija, kodiranje podatkov, digitalne komunikacije (FFT)
- Razne veje matematike: algebra, teorija grafov, algebraična geometrija...
- Letošnji Abelov nagrajenec Pierre Deligne je v 70.-tih letih prejšnjega stoletja zaslovel z reševanjem Weillovih domnev, ki so povezane s končnimi polji.
- Preproste primere praktične uporabe najdemo v kombinatoriki (npr. sestavljanje razporeda nogometne lige - ideja za marsovski projekt 2014).
- ...

Štoparski zaključek

Obstaja teorija, ki pravi, da bo v tistem hipu, ko bo nekdo odkril, zakaj obstaja in čemu natanko služi Vesolje, le-to v hipu izginilo in ga bo zamenjalo nekaj še bolj bizarnega in nerazložljivega.

Obstaja pa še druga teorija, ki pravi, da se je to že zgodilo...

Douglas Adams, Štoparski vodič po vesolju.