Skaičių teorija

2017 m. gegužės 17 d.

Pirma dalis

1 Vienareikšmis išskaidymas

1.1 Vienareikšmis išskaidymas $\mathbb{Z}$

1, 2, 3, 4 lemos; 1 teorema; 1.1.1 teiginys; 1, 2 išvados.

1.2 Žiedai $\mathbb{Z}[i]$ ir $\mathbb{Z}[\omega]$

1.4.1, 1.4.2 teiginiai.

2 Vienareikšmio išskaidymo taikymai

2.1 Be galo daug pirminių

1 teorema.

2.2 Aritmetinės funkcijos

Mobuso funkcijos apibrėžimas, Oilerio funkcijos apibrėžimas; 2.2.2, 2.2.3, 2.2.4, 2.2.5 teiginiai; 2 teorema.

3 Lyginiai

3.1 Lyginys $ax \equiv b \pmod{m}$

3.3.2 teiginys; visos išvados.

3.2 Kinų liekanų teorema

1, 2 lemos; 1 teorema.

4 $U(\mathbb{Z}/n\mathbb{Z})$ struktūra

Primityviosios šaknies apibrėžimas; 1, 2, 3 lemos; 4.1.1, 4.1.2 teiginiai; 1, 2 teoremos.

Antra dalis

5 Kvadratinės liekanos

5.1 Kvadratinės liekanos

Ležandro simbolio apibrėžimas; 5.1.2, 5.1.3 teiginiai; 1, 2, 3 išvados; Gauso lema.

5.2 Kvadratinio apverčiamumo dėsnis

1, 2, 3 teoremos; Jakobio simbolio apibrėžimas.

6 Difantinės lygtys (17 skyrius)

6.1 Pelio lygtis

17.5.1, 17.5.2 teiginiai; 1 lema.