

Talteori

Vad är talteori?

Jan Snellman¹

¹Matematiska Institutionen
Linköpings Universitet

Föreläsningsanteckningar på kurshemsidan <http://courses.mai.liu.se/GU/TATA54/>



TEKNISKA HÖGSKOLAN
LINKÖPING UNIVERSITET

Analytisk talteori

Primtalsräkning

Partitioner

“Geometry of Numbers”

Gitterpunkter i konvexa kroppar

Aritro-algebraisk geometri

Pythagoreanska tripplar

Kopplingar till algebra

Ingår i kursen:

Inte i kursen

Elementär talteori

Elementär?

Denna kurs

Litteratur

Föreläsningar

Analytisk talteori

Primtalsräkning

Partitioner

“Geometry of Numbers”

Gitterpunkter i konvexa kroppar

Aritro-algebraisk geometri

Pythagoreanska tripplar

Kopplingar till algebra

Ingår i kursen:

Inte i kursen

Elementär talteori

Elementär?

Denna kurs

Litteratur

Föreläsningar

Analytisk talteori

Primtalsräkning

Partitioner

“Geometry of Numbers”

Gitterpunkter i konvexa kroppar

Aritro-algebraisk geometri

Pythagoreanska tripplar

Kopplingar till algebra

Ingår i kursen:

Inte i kursen

Elementär talteori

Elementär?

Denna kurs

Litteratur

Föreläsningar

Analytisk talteori

Primtalsräkning

Partitioner

“Geometry of Numbers”

Gitterpunkter i konvexa kroppar

Aritro-algebraisk geometri

Pythagoreanska tripplar

Kopplingar till algebra

Ingår i kursen:

Inte i kursen

Elementär talteori

Elementär?

Denna kurs

Litteratur

Föreläsningar

Analytisk talteori

Primtalsräkning

Partitioner

“Geometry of Numbers”

Gitterpunkter i konvexa kroppar

Aritro-algebraisk geometri

Pythagoreanska tripplar

Kopplingar till algebra

Ingår i kursen:

Inte i kursen

Elementär talteori

Elementär?

Denna kurs

Litteratur

Föreläsningar

Analytisk talteori

Primtalsräkning

Partitioner

“Geometry of Numbers”

Gitterpunkter i konvexa kroppar

Aritro-algebraisk geometri

Pythagoreanska tripplar

Kopplingar till algebra

Ingår i kursen:

Inte i kursen

Elementär talteori

Elementär?

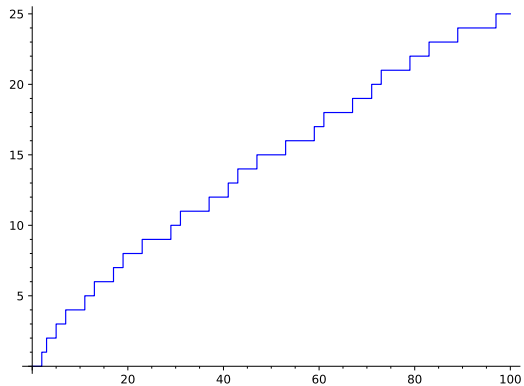
Denna kurs

Litteratur

Föreläsningar

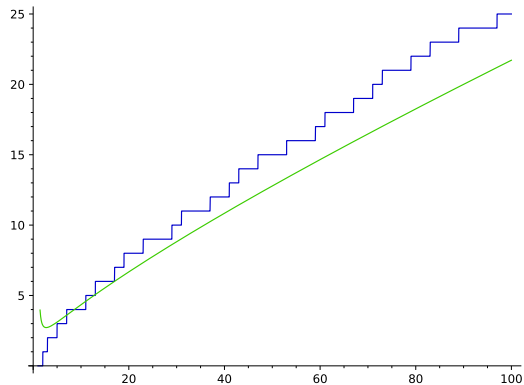
Definition

$$\pi(x) = \sum_{k \leq x} \text{IsPrime}(k)$$



Teorem (Primtalssatsen, Hadamard, de la Vallée Poussin)

$$\pi(x) \sim \frac{x}{\log x} \text{ då } x \rightarrow \infty.$$





J. Hadamard

Definition

Primtalstäthetsfunktion $\pi(x)/x$.

Teorem

$$\pi(x)/x \sim 1/\log(x).$$

Bevis.

Följer av primtalssatsen.

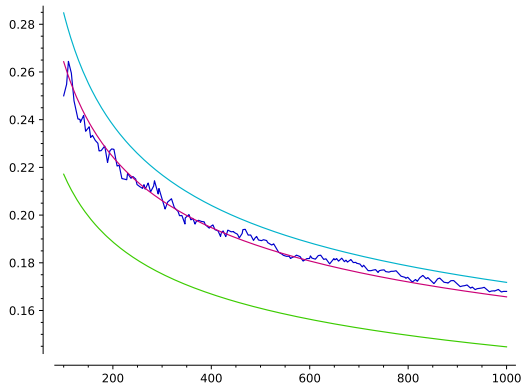


Exempel

Sannolikheten att ett positivt heltal ≤ 1000 är ett primtal är $p(1000)/1000 \approx \frac{1}{\log(1000)} = 0.145$. I själva verket finns 168 primtal ≤ 1000 .

Teorem

$$p(x)/x = \sum_{k=1}^{n-1} \frac{(k-1)!}{\log(x)^k} + \mathcal{O}\left(\frac{(n-1)!}{(\log(x))^n}\right) \text{ as } x \rightarrow \infty.$$



De tre första approximationerna:

Definition

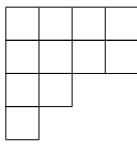
n positivt heltal. En (heltals)partition $\lambda \vdash n$ är en svagt avtagande heltalsföljd som summerar till n .

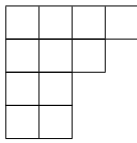
Exempel

$\lambda = (3, 3, 2, 1, 1, 1) \vdash 11$. Det finns 7 partitioner av 5, nämligen

$[[5], [4, 1], [3, 2], [3, 1, 1], [2, 2, 1], [2, 1, 1, 1], [1, 1, 1, 1, 1]]$

- ▶ *Young-diagrammet* av en partition är en hög lådor, svarande mot delarnas storlek
- ▶ Konjugatet till en partition fås genom att svänga runt diagrammet
- ▶

$$\lambda = (4, 4, 2, 1) =$$


$$\lambda^* = (4, 3, 2, 2) =$$


- ▶ Ger bijektion mellan partitioner med högst k delar och partitioner vars delar är $\leq k$

Exempel

- ▶ Högst 4 delar, eller storlek på delar ≤ 4
- ▶ c_j räknar antal sådana partitioner av j
- ▶ $p_4(x) = \sum_{j \geq 0} c_j x^j$ generande funktion
- ▶ $p_4(x) = 1 + 1x + 2x^2 + 3x^3 + 5x^4 + 6x^5 + 9x^6 + \mathcal{O}(x^7)$
- ▶ Lätt att se att $p_4(x) = \frac{1}{(x^4-1)(x^3-1)(x^2-1)(x-1)}$
- ▶ Partialbråksuppdelning: $p_4(x) = \frac{x+1}{9(x^2+x+1)} + \frac{1}{8(x^2+1)} + \frac{1}{8(x+1)} - \frac{17}{72(x-1)} + \frac{1}{32(x+1)^2} + \frac{59}{288(x-1)^2} - \frac{1}{8(x-1)^3} + \frac{1}{24(x-1)^4}$
- ▶ Ger asymptotisk växt av c_j (som funktion av j)

Definition

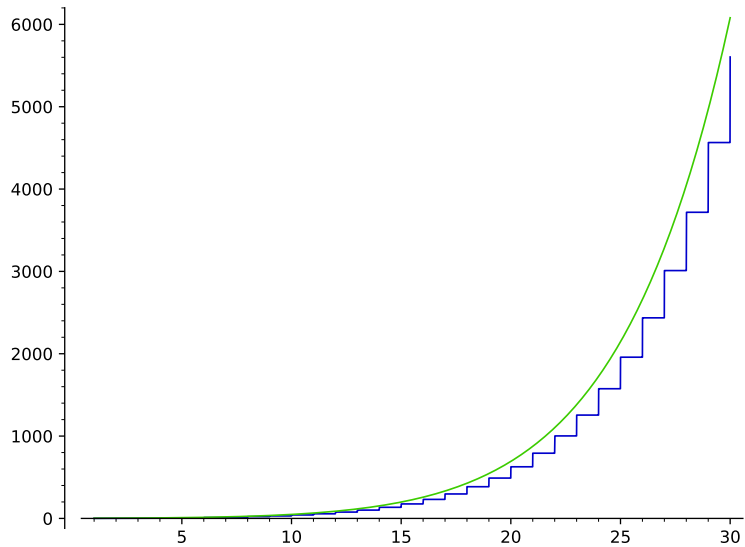
$p(n)$ antal partitioner av n .

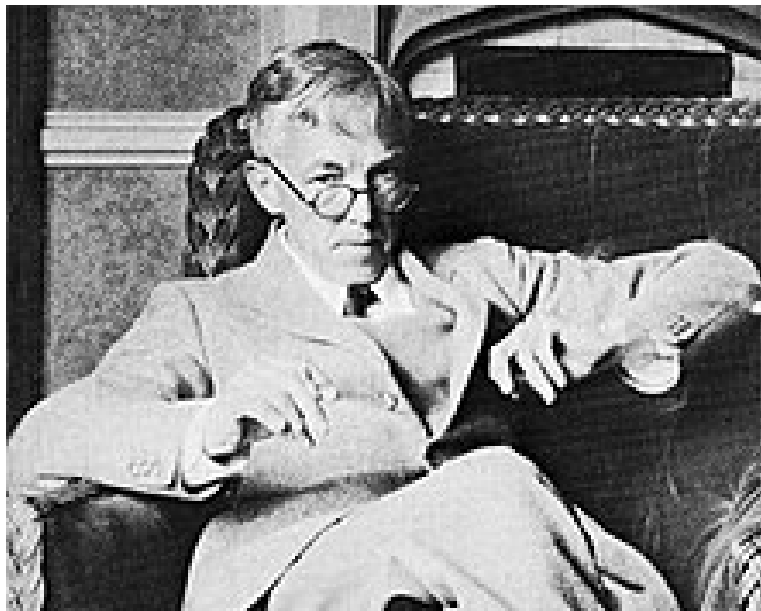
Lemma (Lätt)

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}$$

Teorem (Hardy-Ramanujan)

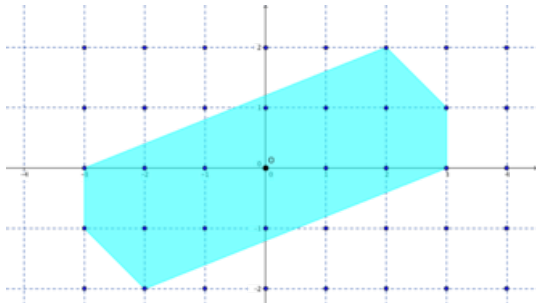
$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right) \text{ as } n \rightarrow \infty.$$





Teorem (Minkowski)

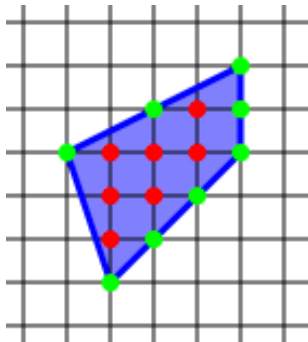
$D \subset \mathbb{R}^n$ konvex, volym $> 2^n$, $-D = D$. Då innehåller D gitterpunkt skild från origo.



Teorem (Pick)

A area av konvex polygon i planet vars hörnpunkter är gitterpunkter, i antal inre gitterpunkter, b antal randpunkter. Då

$$A = i + \frac{b}{2} - 1$$



$$i = 7, b = 8, A = i + b/2 - 1 = 10$$

We kommer att bestämma de Pythagoreanska tripplarna!

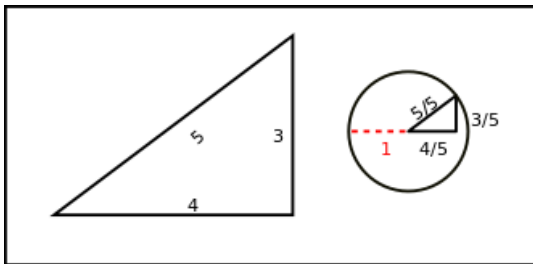
Teorem

Heltalslösningar till

$$a^2 + b^2 = c^2$$

svarar mot rational punkt $(a/c, b/c)$ på enhetscirkeln, kan parametrисeras med

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2$$

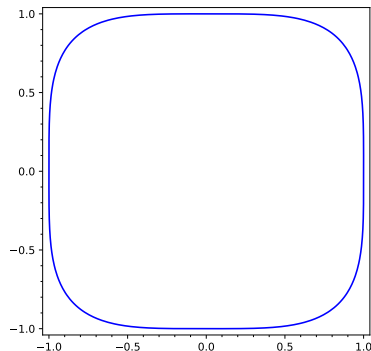


Teorem (Fermats förmodan)

För $n \geq 3$ så saknar ekvationen

$$x^n + y^n = z^n$$

icke-triviala heltalslösningar.



- ▶ Gruppen $\mathbb{Z}_n^*$ är cyclisk då n är primtalspotens
- ▶ $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ omm $\gcd(m, n) = 1$, samma för $\mathbb{Z}_{mn}^*$.
- ▶ $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ är ett huvudidealområde domain
- ▶ Hensel-lyft
- ▶ Möbiusinversion

Algebrarelaterade spörsmål i kursen:

- ▶ Gruppen $\mathbb{Z}_n^*$ är cyclisk då n är primtalspotens
- ▶ $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ omm $\gcd(m, n) = 1$, samma för $\mathbb{Z}_{mn}^*$.
- ▶ $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ är ett huvudidealområde domain
- ▶ Hensel-lyft
- ▶ Möbiusinversion

Algebrarelaterade spörsmål i kursen:

- ▶ Gruppen $\mathbb{Z}_n^*$ är cyclisk då n är primtalspotens
- ▶ $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ omm $\gcd(m, n) = 1$, samma för $\mathbb{Z}_{mn}^*$.
- ▶ $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ är ett huvudidealområde domain
- ▶ Hensel-lyft
- ▶ Möbiusinversion

Algebrarelaterade spörsmål i kursen:

- ▶ Gruppen $\mathbb{Z}_n^*$ är cyclisk då n är primtalspotens
- ▶ $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ omm $\gcd(m, n) = 1$, samma för $\mathbb{Z}_{mn}^*$.
- ▶ $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ är ett huvudidealområde domain
- ▶ Hensel-lyft
- ▶ Möbiusinversion

- ▶ Gruppen $\mathbb{Z}_n^*$ är cyclisk då n är primtalspotens
- ▶ $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ omm $\gcd(m, n) = 1$, samma för $\mathbb{Z}_{mn}^*$.
- ▶ $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ är ett huvudidealområde domain
- ▶ Hensel-lyft
- ▶ Möbiusinversion

- ▶ Permutationer, cykeltyp, partitioner
- ▶ Algebraiska talkroppar, deras heltal, klasstal

- ▶ Permutationer, cykeltyp, partitioner
- ▶ Algebraiska talkroppar, deras heltal, klasstal

- ▶ “Elementär” betyder ingen avancerad analys eller algebra, ingen komplicerad kombinatorik
- ▶ Inte samma som “lätt”
- ▶ Theorin byggs upp från grunden, i princip inga förkunskaper
- ▶ Men behöver mängdlära, induktion
- ▶ Användbart: linjär algebra

- ▶ “Elementär” betyder ingen avancerad analys eller algebra, ingen komplicerad kombinatorik
- ▶ Inte samma som “lätt”
- ▶ Theorin byggs upp från grunden, i princip inga förkunskaper
- ▶ Men behöver mängdlära, induktion
- ▶ Användbart: linjär algebra

- ▶ “Elementär” betyder ingen avancerad analys eller algebra, ingen komplicerad kombinatorik
- ▶ Inte samma som “lätt”
- ▶ Teorin byggs upp från grunden, i princip inga förkunskaper
- ▶ Men behöver mängdlära, induktion
- ▶ Användbart: linjär algebra

- ▶ “Elementär” betyder ingen avancerad analys eller algebra, ingen komplicerad kombinatorik
- ▶ Inte samma som “lätt”
- ▶ Theorin byggs upp från grunden, i princip inga förkunskaper
- ▶ Men behöver mängdlära, induktion
- ▶ Användbart: linjär algebra

- ▶ “Elementär” betyder ingen avancerad analys eller algebra, ingen komplicerad kombinatorik
- ▶ Inte samma som “lätt”
- ▶ Theorin byggs upp från grunden, i princip inga förkunskaper
- ▶ Men behöver mängdlära, induktion
- ▶ Användbart: linjär algebra

- ▶ “Elementary Number Theory” av Rosen
- ▶ Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- ▶ Definierar kursen
- ▶ Jag kommer inte att ta upp allt på föreläsningarna
- ▶ Kommer också att använda “Elementary number Theory” av Stein
- ▶ Hackman’s manuskript rekommenderas som bredvidläsning
- ▶ Gaussiska heltal via Conrads text

- ▶ “Elementary Number Theory” av Rosen
- ▶ Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- ▶ Definierar kursen
- ▶ Jag kommer inte att ta upp allt på föreläsningarna
- ▶ Kommer också att använda “Elementary number Theory” av Stein
- ▶ Hackman’s manuskript rekommenderas som bredvidläsning
- ▶ Gaussiska heltal via Conrads text

- ▶ “Elementary Number Theory” av Rosen
- ▶ Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- ▶ Definierar kursen
- ▶ Jag kommer inte att ta upp allt på föreläsningarna
- ▶ Kommer också att använda “Elementary number Theory” av Stein
- ▶ Hackman’s manuskript rekommenderas som bredvidläsning
- ▶ Gaussiska heltal via Conrads text

- ▶ “Elementary Number Theory” av Rosen
- ▶ Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- ▶ Definierar kursen
- ▶ Jag kommer inte att ta upp allt på föreläsningarna
- ▶ Kommer också att använda “Elementary number Theory” av Stein
- ▶ Hackman’s manuskript rekommenderas som bredvidläsning
- ▶ Gaussiska heltal via Conrads text

- ▶ “Elementary Number Theory” av Rosen
- ▶ Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- ▶ Definierar kursen
- ▶ Jag kommer inte att ta upp allt på föreläsningarna
- ▶ Kommer också att använda “Elementary number Theory” av Stein
- ▶ Hackman’s manuskript rekommenderas som bredvidläsning
- ▶ Gaussiska heltal via Conrads text

- ▶ “Elementary Number Theory” av Rosen
- ▶ Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- ▶ Definierar kursen
- ▶ Jag kommer inte att ta upp allt på föreläsningarna
- ▶ Kommer också att använda “Elementary number Theory” av Stein
- ▶ Hackman’s manuskript rekommenderas som bredvidläsning
- ▶ Gaussiska heltal via Conrads text

- ▶ “Elementary Number Theory” av Rosen
- ▶ Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- ▶ Definierar kursen
- ▶ Jag kommer inte att ta upp allt på föreläsningarna
- ▶ Kommer också att använda “Elementary number Theory” av Stein
- ▶ Hackman’s manuskript rekommenderas som bredvidläsning
- ▶ Gaussiska heltal via Conrads text

- ▶ 19 sessioner
- ▶ Föreläsningar
- ▶ Övningsräkning
- ▶ Lista på rekommenderade övningar på kurshemsidan
<http://courses.mai.liu.se/GU/TATA54/>

- ▶ 19 sessioner
- ▶ Föreläsningar
- ▶ Övningsräkning
- ▶ Lista på rekommenderade övningar på kurshemsidan
<http://courses.mai.liu.se/GU/TATA54/>

- ▶ 19 sessioner
- ▶ Föreläsningar
- ▶ Övningsräkning
- ▶ Lista på rekommenderade övningar på kurshemsidan
<http://courses.mai.liu.se/GU/TATA54/>

- ▶ 19 sessioner
- ▶ Föreläsningar
- ▶ Övningsräkning
- ▶ Lista på rekommenderade övningar på kurshemsidan
<http://courses.mai.liu.se/GU/TATA54/>

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal

1. Heltal, delbarhet
2. Unik faktorisering
3. Sgd, Linjära Diofantiska ekvationer
4. Kongruenser, Kinesiska restsatsen
5. Multiplicativ ordning, Fermat, Euler
6. Arithmetiska funktioner, Möbiusinversion
7. Hensel-lyft
8. Lagrange, Primitiva rötter, Diskreta logaritmer
9. Quadratisk Reciprocitet
10. Kedjerbråk
11. Pell's ekvation
12. Sum of squares
13. Gaussiska heltal