Algebra och talteori

MMGL31

Föreläsning 6

VT 2010

Samuel Bengmark

Repetition

- Eulers ϕ-funktion
- Eulers formel
- Att beräkna Eulers ϕ-funktion
- Kinesiska restsatsen

Kinesiska restsatsen

$$\begin{cases} x \equiv_m c \\ x \equiv_n b \end{cases} \Leftrightarrow \begin{cases} x = c + mk \\ x = b + nl \end{cases} \Leftrightarrow \begin{cases} x = c + mk \\ c + mk = b + nl \end{cases} \Leftrightarrow \begin{cases} x = c + mk \\ c - b = nl - mk \end{cases}$$

- Den nedre ekvationen har lösning eftersom
  SGD(m,n)=1|c-b.
  Lösningarna har formen $l=l_p+mr$, $k=k_p+nr$, $r\in\mathbb{Z}$
- Övre ekvationen ger då
  $x=c+m(k_0+nr)=(c+mk_0)+(mn)r$
  Lämpligt val av r ger unikt x i önskat intervall.

Idag

- Primtal/Irreducibla tal i $\mathbb{Z}$
- Antalet primtal $\equiv_4 3$
- Några kända förmodanden
- Mersenne primtal

Primtalen i $\mathbb{Z}$

2,3,5,7,13,17,19,23,29,31,41,43,47,53,59,61,67,71,73,79,83,97,101,103,107,109...

Minns att de är de irreducibla/odelbara talen, byggstenarna med vilka man kan bygga upp alla andra tal genom multiplikation.

De är också prima tal.

Det finns ∞ antal primtal

- Bevisidé: Varje ändlig lista av primtal innehåller inte alla primtal som finns.
- Tag en ändlig listan $\{p_1, \ldots, p_n\}$ av primtal.
- Bilda talet $A=p_1 \cdot \ldots \cdot p_n+1$.
- Då är $A=q_1^{\alpha 1} \cdot \ldots \cdot q_k^{\alpha k}$ enligt Aritm. f. sats, dvs
  $q_1^{\alpha 1} \cdot \ldots \cdot q_k^{\alpha k}=p_1 \cdot \ldots \cdot p_n+1$
- Då är $q_1 \neq p_i$ för alla i ty annars skulle q_1 dela 1 eftersom q_1 då delar de andra två termerna.
- Alltså har vi hittat ett primtal som inte ingick i den första listan.

Betrakta primtalen modulo 4

$$\begin{cases} 5 & 13 & 17 & 29 & 37 & 41 & 53 & 61 & 73 & 89 & 97 & 101 & 109 & 113 & \equiv_4 1 \\ 3 & 7 & 11 & 19 & 23 & 31 & 43 & 47 & 59 & 67 & 71 & 79 & 83 & 103 & \equiv_4 3 \end{cases}$$

- Vi skall senare se att denna uppdelning av primtalen återspeglas i huruvida ett tal kan skrivas som en summa av två kvadrater samt om -1 är en kvadrat i en kongruensring.
- Kan vi bevisa att det finns oändligt många i var och en av dess grupper?

Det finns ∞ antal primtal $\equiv_4 3$

- Bevisidé: Varje ändlig lista av primtal innehåller inte alla primtal som finns.
- Tag en ändlig listan $\{3,p_1, \ldots, p_n\}$ av primtal $\equiv_4 3$.
- Bilda talet $A=4p_1 \cdot \ldots \cdot p_n+3$. (OBS 3 ej medtaget).
- Då är $A=q_1^{\alpha 1} \cdot \ldots \cdot q_k^{\alpha k}$ enligt Aritm. f. sats, dvs $q_1^{\alpha 1} \cdot \ldots \cdot q_k^{\alpha k}=4p_1 \cdot \ldots \cdot p_n+3$
- Minst en av q_i är $\equiv_4 3$ eftersom annars vore VL $\equiv_4 1$ men HL $\equiv_4 3$. Kalla denna q_1.
- Då är $q_1 \neq p_i$ för alla i, ty q_1 dela A men ingen av talen $\{3,p_1, \ldots, p_n\}$ gör det.
- Alltså har vi hittat ett primtal $\equiv_4 3$ som inte ingick i den första listan.

Dirichlets sats för aritmetisk progression

Låt a och n vara heltal med SGD(a,n)=1. Då finns det oändligt många primtal $\equiv_n a$.

Specialfallet n=4, a=3 är avklarat. Bara resten återstår… men det får bli i en annan kurs.

Dock visas fallet n=4 a=1 senare i denna kurs. Fallet n=6, a=5 bevisas i uppgift 12.2.

Räkna primtal

$\pi(x)=|\{\text{primtal} \leq x\}|$.

$\pi(10)=4$
$\pi(100)=25$
$\pi(1000)=168$

Svårberäknad funktion, men man vet följande:

Primtalssatsen

$\pi(x)$ växer som x/ln(x) för stora x,
eller mer precist

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

Fantastiskt resultat!
Här ser man ett exempel på att ln och därmed e dyker upp vid oväntade tillfällen.

Matematik i utveckling

Man kan se resultat som primtalssatsen och tro att människan vet allt om matematiken.
Så är inte fallet. Vi skall nu titta på några exempel tillsynes enkla påståenden som ingen lyckats bevisa om de är sanna eller ej.

Goldbachs förmodan

Förmodan
Varje jämnt tal ≥ 4 kan skrivas som en summa av två primtal.

Exampel
4=2+2, 6=3+3, 8=3+5, …. 102=61+41, …

Retligt enkelt att kolla i enskilda fall, men ingen har klarat att visa det allmänt.

Primtalstvillingar

2,3,5,7,13,17,19,23,29,31,41,43,47,53,59,61,67,71,73,79,83,97,101,103,107,109...

239,241.....269,271,.....281,283,.....

Förmodan
Det finns oändligt många primtalstvillingar.

Förmodan
Om T(X)=|{primtalstvillingspar $\leq$ x}| så gäller att

$$\lim_{x\to\infty}\frac{T(x)}{x/(\ln x)^2} = C, \text{ där } C = \prod_{p>2;\ p \text{ prime}} [1 - 1/((p-1)^2)] \approx 0{,}66$$

Primtal av typen N^2+1

$2^2+1=5$, $4^2+1=17$, $6^2+1=37$, $10^2+1=101$ …
dock inte för alla jämna, tex $8^2+1=5\cdot 13$.

Förmodan
Det finns oändligt många primtal på formen N^2+1.

Förmodan
Om S(X)=|{primtal på formen $N^2+1 \leq$ x}| så gäller att

$$\lim_{x\to\infty}\frac{S(x)}{\sqrt{x}/\ln x} = K$$

Matematik i utveckling

Många tror att matematiken är något statiskt som man får plugga in.
Egentligen är det en levande verkasamhet som i utveckling.
Människan utvecklar sin kunskap och förståelse för matematiken snabbare idag än tidigare. Det publiceras ca 35000 nya rön varje år.
Varje enkild människa är kreativ och löser sina egna problem och skapar sina egna bilder av begreppen.

Först en uppgift: 7.3c

Primtal på formen a^n-1

- $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\ldots+a+1)$, enligt uppg 7.3c
  alltså sammansatt om a heltal >2.
  Väljer alltså a=2.

- Om n=mk får vi på samma sätt
  $2^n-1=2^{mk}-1=(2^m)^k-1=(2^m-1)((2^m)^{k-1}+(2^m)^{k-2}\ldots 2^m+1)$
  Alltså är 2^n-1 sammansatt om n sammansatt.
  Väljer därför n till att vara primtal p.

Sats
För att ett tal a^n-1 skall vara ett primtal måste a=2 och n vara ett primtal.

Mersenneprimtal

Definition
Ett primtal på formen 2^p-1 kallas ett Mersenneprimtal.

Påstående
De första 15 Mersenneprimtalen ges av exponenterna
$p \in \{2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279\}$

Detta är bland Mersenneprimtalen man letar idag när man söker stora primtal.