Lösningar till tentamen i Introduktionskurs i Matematik

Distanskurs

18 januari, 2003 kl. 9.00 – 13.00

Maxpoäng: 30p. **Betygsgränser**: 12p: betyg G, 18p: betyg VG. **Hjälpmedel**: Inga.
Kursansvarig: Eric Järpe (035-16 76 53, 070-306 95 89).

1. Formulera och bevisa Aritmetikens fundamentalsats. (3p)

   Lösning: (Se Diskret matematik av Bergström, Sats 2.9, s. 22.) □

2. Avgör om följande utsagor är tautologi, kontradiktion eller ingetdera.

   (a) $(\neg Q \;\Rightarrow\; P) \Leftrightarrow (Q \Rightarrow \neg P)$ (1p)

   (b) $\neg\Big((P \;\Rightarrow\; Q) \vee \neg Q\Big)$ (1p)

   (c) $(P \wedge Q \;\Rightarrow\; R) \vee (P \wedge Q \wedge \neg R)$ (1p)

   Lösning:

   (a)

P	Q	$(\neg Q$	$\boxed{\Rightarrow}$	$P)$	$\boxed{\Leftrightarrow}$	$(Q$	$\boxed{\Rightarrow}$	$\neg P)$
S	S	F	S	S	$\boldsymbol{F}$	S	F	F
S	F	S	S	S	$\boldsymbol{S}$	F	S	F
F	S	F	S	S	$\boldsymbol{S}$	S	S	S
F	F	S	F	F	$\boldsymbol{F}$	F	S	S

   Alltså <u>ingetdera</u>.

   (b) $\neg((P \Rightarrow Q) \vee \neg Q) \;\Leftrightarrow\; \neg(P \Rightarrow Q) \wedge Q \;\Leftrightarrow$
   $\Leftrightarrow\; (P \wedge \neg Q) \wedge Q \;\Rightarrow\; \neg Q \wedge Q$

   Alltså <u>kontradiktion</u>.

   (c)

P	Q	R	$(P \wedge Q$	$\boxed{\Rightarrow}$	$R)$	$\boxed{\vee}$	$(P \wedge Q \wedge \neg R)$
S	S	S	S	S	S	$\boldsymbol{S}$	F
S	S	F	S	F	F	$\boldsymbol{S}$	S
S	F	S	F	S		$\boldsymbol{S}$	F
S	F	F	F	S		$\boldsymbol{S}$	F
F	S	S	F	S		$\boldsymbol{S}$	F
F	S	F	F	S		$\boldsymbol{S}$	F
F	F	S	F	S		$\boldsymbol{S}$	F
F	F	F	F	S		$\boldsymbol{S}$	F

   Alltså <u>tautologi</u>. □

3. Vad blir heltalsresten då $123 \cdot 231^{312}$ divideras med 13? (3p)

Lösning: $123 \equiv 6$ och $231 \equiv -3 \pmod{13}$ vilket innebär att
$123 \cdot 231^{312} \equiv 6 \cdot (-3)^{312} = 6 \cdot ((-3)^4)^{78} = 6 \cdot 81^{78} \equiv 6 \cdot 3^{78} = 6 \cdot 9^{39} =$
$= 6 \cdot (9^3)^{13} = 6 \cdot (81 \cdot 9)^{13} \equiv 6 \cdot (3 \cdot 9)^{13} = 6 \cdot 27^{13} \equiv 6 \cdot 1^{13} = 6$

Alltså blir resten 6. □

4. Visa att $\overline{(z/w)} = \bar{z}/\bar{w}$ för alla komplexa tal z och $w \neq 0$. (3p)

Lösning:
Eftersom $\overline{zw} = \bar{z} \cdot \bar{w}$
(ty $\overline{zw} = \overline{(a+bi)(c+di)} = \overline{ac - bd + (ad+bc)i} = ac - bd - (ad+bc)i$
och $\bar{z} \cdot \bar{w} = (a-bi)(c-di) = ac - bd - (ad+bc)i)$
så är $\bar{z} = \overline{w \cdot z/w} = \bar{w} \cdot \overline{(\frac{z}{w})} \;\Rightarrow\; \bar{z}/\bar{w} = \overline{(z/w)}$ □

5. På hur många sätt kan man i poker få två par i given om man ej tar hänsyn till ordningen? (3p)

Lösning: Första kortet kan man alltid få på 52 sätt.
Andra kortet (säg för att bilda par med det första) kan man få på 3 sätt.
Tredje kortet måste ha annan valör än de två första varmed det finns 48 sätt.
Fjärde kortet (för att bilda par med det tredje) kan fås på 3 sätt.
Femte kortet måste ha annan valör än de två paren och kan således fås på 44 sätt.
Alltså blir det totala antalet sätt utan hänsyn till ordningen $52 \cdot 3 \cdot 48 \cdot 3 \cdot 44 = \underline{988\,416}$. □

6. Ekvationen $x^4 - 6x^3 + 14x^2 + 10x + 125 = 0$ har roten $x = 2i - 1$.
Bestäm de andra rötterna. (3p)

Lösning: $x_1 = 2i - 1$ rot $\Rightarrow$ $x_2 = -2i - 1$ rot $\Rightarrow$ $(x - x_1)(x - x_2)$ kan brytas ut ur vänsterledet. $(x - x_1)(x - x_2) = (x - 2i + 1)(x + 2i + 1) = x^2 + 2x + 5 \;\Rightarrow$
$\Rightarrow\; 0 = x^4 - 6x^3 + 14x^2 + 10x + 125 = (x^2 + 2x + 5)(x^2 - 8x + 25)$. Faktorn $x^2 - 8x + 25$ har nollställena $x = 4 \pm \sqrt{16 - 25} = 4 \pm 3i$ varmed rötterna är $\underline{-1 \pm 2i \text{ och } 4 \pm 3i}$. □

7. Visa att för alla positiva heltal n är $\displaystyle\sum_{k=1}^{n}\left(\sum_{j=1}^{k} j\right) = \sum_{k=1}^{n}\frac{k(n+2)}{3}$. (4p)

Lösning: Klart att $\sum_{j=1}^{k} j = \frac{k(k+1)}{2}$ (se s. 127) och att $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ (se s. 135). Vi ska visa att

$$\text{V.L.} = \sum_{k=1}^{n}\left(\sum_{j=1}^{k} j\right) = \sum_{k=1}^{n}\frac{k(n+2)}{3} = \text{H.L}$$

$$\begin{aligned}
\text{V.L.} &= \sum_{k=1}^{n}\frac{k(k+1)}{2}\\
&= \frac{1}{2}\left(\sum_{k=1}^{n} k^2 + \sum_{k=1}^{n} k\right)\\
&= \frac{1}{2}\left(\frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2}\right)\\
&= \frac{n(n+1)(2n+1)+3n(n+1)}{12}\\
&= \frac{2n^3+3n^2+n+3n^2+3n}{12}\\
&= \frac{2n^3+6n^2+4n}{12}\\
&= \frac{n^3+3n^2+2n}{6}
\end{aligned}$$

$$\begin{aligned}
\text{H.L.} &= \frac{n+2}{3}\sum_{k=1}^{n} k\\
&= \frac{n+2}{3}\cdot\frac{n(n+1)}{2}\\
&= \frac{n(n+1)(2n+1)}{6}
\end{aligned}$$

Därmed är V.L. = H.L. och beviset är klart. $\square$

8. För vilka heltal n är $8^n + 61$ en jämn kub? (4p)

Lösning: För att avgöra detta, låt $x^3 = 8^n + 61$. Eftersom $8^n = (2^3)^n$ så är $61 = x^3 - (2^n)^3 = (x - 2^n)(x^2 + 2^n x + 2^{2n})$.

Eftersom 61 är ett primtal är $1 \cdot 61$ och $(-1) \cdot (-61)$ de enda möjliga faktoriseringarna i två heltal och därmed har vi ekvationssystemen

$$\text{A:} \begin{cases} x - 2^n &= -1 \quad (1) \\ x^2 + 2^n x + 2^{2n} &= -61 \quad (2) \end{cases} \quad \text{och} \quad \text{B:} \begin{cases} x - 2^n &= 1 \quad (1) \\ x^2 + 2^n x + 2^{2n} &= 61 \quad (2) \end{cases}$$

A: (1) $\Rightarrow\ x = 2^n - 1$. (2) $\Rightarrow$
$\Rightarrow\ -61 = (2^n - 1)^2 + 2^n(2^n - 1) + 2^{2n} = 2^{2n} - 2 \cdot 2^n + 1 + 2^{2n} - 2^n + 2^{2n}\ \Rightarrow$
$\Rightarrow\ 3 \cdot 2^{2n} - 3 \cdot 2^n = 62$
Men denna ekvation har ingen heltalslösning n eftersom $3 \nmid 62$.

B: (1) $\Rightarrow\ x = 2^n + 1$. (2) $\Rightarrow\ 61 = (2^n + 1)^2 + 2^n(2^n + 1) + 2^{2n} =$
$= 2^{2n} + 2 \cdot 2^n + 1 + 2^{2n} + 2^n + 2^{2n}\ \Rightarrow\ 3 \cdot 2^{2n} + 3 \cdot 2^n = 60\ \Rightarrow$
$\Rightarrow\ 2^n(2^n + 1) = 20$. Därmed är det klart att $n < 3$
ty $2^3(2^3 + 1) = 72$ och $2^n(2^n + 1)$ är *växande med* n så
$2^n(2^n + 1) \geq 72$ för alla $n \geq 3$.
För $n = 1$ är $2^1(2^1 + 1) = 6$ och för $n = 2$ är $2^2(2^2 + 1) = 20$.

Därmed är $\underline{n = 2 \text{ den enda lösningen}}$. □

9. Visa att om p är ett primtal och $n \in \mathbb{Z}^+ : p \nmid n$ så är $n^{p-1} \equiv 1 \pmod{p}$. (4p)
(Tips: visa att p delar $\binom{p}{k}$.)

Lösning: Detta är den så kallade *Fermats lilla sats* som har stor betydelse för kryptering. Den kan bevisas på flera sätt varav ett är induktion.

<u>Basfall</u> $n = 1$: $\quad 1^{p-1} = 1 \equiv 1 \pmod{p}$ ok!

<u>Induktionsantagande</u> Antag nu att
p är ett primtal, $n \in \mathbb{Z}^+ : p \nmid n$ och att $n^{p-1} \equiv 1 \pmod{p}$ dvs att p delar $n^p - n$.

<u>Induktionssteg</u> Vi ska (mha induktionsantagandet) visa att p delar $(n+1)^p - (n+1)$.
Vi har att $(n+1)^p = n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \ldots + \binom{p}{p-1}n + 1$
dvs $(n+1)^p - (n+1) = (n^p - n) + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \ldots + \binom{p}{p-1}n \quad (*)$
Enligt induktionsantagandet gäller att p delar $n^p - n$.
Det återstår att visa att p delar $\binom{p}{k}$ för $k = 1, 2, \ldots, p-1$.
Vi har att $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ dvs att $\binom{p}{k}k!(p-k)! = p!$. Eftersom $p!$ är delbart med p måste vänsterledet vara det också. Eftersom p är ett primtal är åtminstone någon av faktorerna i vänterledet delbar med p. Men om $k!$ vore delbart med p skulle någon av faktorerna i $k(k-1)\cdots 2 \cdot 1$ (där $k \leq p-1$) vara delbar med p vilket är omöjligt eftersom dessa faktorer är $< p$ och p är ett primtal. Detsamma gäller för $(p-k)!$ eftersom $k \geq 1$. Alltså är det $\binom{p}{k}$ som delas av p.

Därmed är det klart att p delar högerledet i $(*)$ och följdaktligen att p delar vänsterledet $(n+1)^p - (n+1)$ varmed satsen är bevisad enligt induktionsprincipen! □