Högskolan i Halmstad

forts. Kapitel 2: De hela talen

En stor del av området algebra handlar om att kunna lösa ekvationer. Då det gäller polynomekvationer av grad 1 (dvs linjära ekvationer) kan dessa alltid skrivas på formen $a + bx = 0$ där $b \neq 0$. De har lösningen $x = -a/b$. Då det gäller polonekvationer av grad 2 (dvs andragradsekvationer) kan dessa skrivas $x^2 + ax + b$. De har lösningarna $x = -a/2 \pm \sqrt{(a/2)^2 - b}$. Vad gäller polynomekvationer av grad 3 och 4 har även dessa allmänna (dock mer komplicerade) lösningar på sluten form. För polomekvationer av grad ≥ 5 kan man dock ej skriva någon allmänt giltig lösningsformel med ett ändlgit antal rotutdragningar. Emellertid kan man lösa många specialfall av ekvationer av grad såväl 3, 4 som 5 och högre.

Polynomekvationer med rationella rötter

Sats 2.10
Antag att polynomet $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ där $a_0, \ldots, a_n \in \mathbb{R}$ och $a_n \neq 0$. Då gäller att $p(\frac{b}{c}) = 0 \;\Rightarrow\; b|a_0 \,\wedge\, c|a_n$.

Exempel Lös ekvationen $105x^3 - 307x^2 + 199x + 35 = 0$.

Lösning: Under antagandet att ekvationen har minst en rationell rot, b/c, skulle $b|35$ och $c|105$, dvs vi kan välja bland alla kombinationer av $b = \pm 1, \pm 5 \pm 7 \pm 35$ och $c = \pm 1, \pm 3, \pm 5 \pm 7, \pm 15, \pm 21, \pm 35, \pm 105$, dvs 36 distinkta kandidater (efter att har räknat bort dubletter). Med $b = 1$ börjar vi t.ex. med $x = \pm 1, \pm\frac{1}{3}, \pm\frac{1}{5}, \pm\frac{1}{7}, \ldots$ och finner att

x	$p(x)$
1	$105 - 307 + 199 + 35 > 0$
-1	$-105 - 307 - 199 + 35 < 0$
$\frac{1}{3}$	$\frac{35}{9} - 3079 + \frac{199}{3} + 35 = \frac{35}{9} - 3079 + \frac{3\cdot 199}{9} + 35 > \frac{35}{9} + 35 > 0$
$-\frac{1}{3}$	$-\frac{35}{9} - 3079 - \frac{199}{3} + 35 = -\frac{35}{9} - 3079 - \frac{199}{3} + \frac{105}{3} < 0$
$\frac{1}{5}$	$\frac{21}{25} - \frac{307}{25} + \frac{199}{5} + 35 = \frac{21}{25} - \frac{307}{25} + \frac{5\cdot 199}{25} + 35 > \frac{21}{25} + 35 > 0$
$-\frac{1}{5}$	$-\frac{21}{25} - \frac{307}{25} - \frac{199}{5} + 35 = -\frac{21}{25} - \frac{307}{25} - \frac{199}{5} + \frac{175}{5} < 0$
$\frac{1}{7}$	$\frac{15}{49} - \frac{307}{49} + \frac{199}{7} + 35 = \frac{15}{49} - \frac{307}{49} + \frac{7\cdot 199}{49} + 35 > 0$
$-\frac{1}{7}$	$-\frac{15}{49} - \frac{307}{49} - \frac{199}{7} + 35 = -\frac{15}{49} - \frac{307}{49} - \frac{1393}{49} + \frac{49\cdot 35}{49} = \frac{-15-307-1393+1715}{49} = 0$

Alltså är $x_1 = -\frac{1}{7}$ en rot, varmed $7x+1$ kan brytas ut: $105x^3 - 307x^2 + 199x + 35 = (7x+1)(15x^2 - 46x + 35) = 0$. Andragradaren $x^2 - \frac{46}{15}x + \frac{7}{3} = 0$ löses på vanligt sätt: $x = \frac{23}{15} \pm \sqrt{(23/15)^2 - 7/3} = \frac{23}{15} \pm \sqrt{(529 - 525)/225} = \frac{23 \pm 2}{15}$ varmed $x_2 = \frac{21}{15} = \frac{7}{5}$ och $x_3 = \frac{25}{15} = \frac{5}{3}$. □

Diofantiska ekvationer

Ekvationer där man bara beaktar heltalslösningar kallas "Diofantiska ekvationer".

Ekvationen $ax + by = c$

En **(partikulär-) lösning** är ett heltalspar, (x_1, y_1), sådant att $ax_1 + by_1 = c$.

Sats (partikulärlösning)
Antag att $\text{SGD}(a, b) = 1$. Då ges en *partikulärlösning*, (x_1, y_1), till ekvationen $ax + by = c$ av Euklides algoritm.

Den **allmänna lösningen** är produktmängden $\{(x, y) : ax + by = c\}$.

Sats (allmän lösning)
Om (x_1, y_1) är partikulärlösning till $ax + by = c$
så är den allmänna lösningen
$\{\, (x_1 - bm\ ,\ y_1 + am)\ :\ m \in \mathbb{Z}\}$.

Exempel Bestäm alla positiva heltalslösningar (x, y) till $7x + 12y = 107$.

Lösning: Hjälpekvationen är $7x + 12y = \text{SGD}(7, 12)$. Euklides algoritm ger att

$$\begin{array}{rrcl} \text{SGD}(7,12): & 12 & = & 1 \cdot 7 + 5 \\ & 7 & = & 1 \cdot 5 + 2 \\ & 5 & = & 2 \cdot 2 + 1 \\ & 2 & = & 2 \cdot 1 + 0 \ \Rightarrow\ \text{SGD}(7,12) = 1 \end{array}$$

så hjälpekvationen är $7x + 12y = 1$. Baklängesräkning i Euklides algoritm ger nu en lösning till hjälpekvationen:

$$\begin{array}{rcl} 1 & = & 5 - 2 \cdot 2 \\ & = & 5 - 2 \cdot (7 - 1 \cdot 5) \\ & = & 3 \cdot 5 - 2 \cdot 7 \\ & = & 3 \cdot (12 - 1 \cdot 7) - 2 \cdot 7 \\ & = & 3 \cdot 12 - 5 \cdot 7 \end{array}$$

varmed en partikulärlösning till $7x{+}12 = 1$ är $(x_1, y_1) = (-5, 3)$. En partikulärlösning till $7x + 12y = 107$ är $107 \cdot (-5, 3) = (-535, 321)$. Därmed fås alla lösningar som $(-535 + 12m, 321 - 7m)$ där $m \in \mathbb{Z}$ så den enda lösningen där både x och y är positiva fås då $m = 45$ så att $(x, y) = (5, 6)$. $\square$

Ekvationer med tre obekanta, dvs av typen $ax + by + cz = d$ kan också lösas om de har ett bivillkor.

Exempel Börje ska köpa godis för exakt 500 kronor. Han väljer mellan lakritskolor för 3 kronor/st, chokladkakor för 10 kronor/st och påsar med blandat smågodis för 15 kronor/st. På vilka sätt kan Börje handla precis 131 godisvaror?

Lösning: Vi antar att Börje köper x chokladkakor, y påsar och z kolor. Då ska $10x + 15y + 3z = 500$ och antalet godisvaror ska vara 131, dvs $x + y + z = 131$. Det senare villkoret innebär att $z = 131 - x - y$ och sätts detta in i den första ekvationen har vi $10x+15y+3(131-x-y)=500$, dvs $(10-3)x+(15-3)y=500-3\cdot 131$, dvs $7x+12y=107$ vilket är precis den ekvation vi löste i förra exemplet! Denna hade lösningen $(x,y)=(5,6)$, den enda där både $x>0$ och $y>0$. Eftersom det inte finns någon lösning med $x=0$ eller $y=0$ är $(x,y,z)=(x,y,131-x-y)=(5,6,120)$ enda lösningen till detta problem! $\square$

Exempel
Beräkna den principala resten vid heltalsdivision av $(15^{51}+2^{16})^{18}$ med 13.

Lösning: Om man räknar (mod 13) är

$$\begin{aligned}
(15^{51}+2^{16})^{18} &\equiv \Big((15-13)^{51}+2^{16}\Big)^{18} \\
&= (2^{48+3}+2^{6\cdot 2+4})^{18} \\
&= (2^{6\cdot 8}\cdot 2^3+(2^6)^2\cdot 2^4)^{18} \\
&= (64^8\cdot 2^3+64^2\cdot 2^4)^{18} \\
&\equiv \Big((64-5\cdot 13)^8\cdot 2^3+(64-5\cdot 13)^2\cdot 2^4\Big)^{18} \\
&= \Big((-1)^8\cdot 2^3+(-1)^2\cdot 2^4\Big)^{18} \\
&= (8+16)^{18} \\
&\equiv (24-2\cdot 13)^{18} \\
&= (-2)^{18} \\
&= ((-2)^6)^3 \\
&= 64^3 \\
&\equiv (64-5\cdot 13)^3 \\
&= (-1)^3 \\
&= -1 \\
&\equiv -1+13 \\
&= 12
\end{aligned}$$

dvs 12 är den principala resten vid division av $(15^{51}+2^{16})^{18}$ med 13.

Sats
Om $p(x)$ polynom med heltalskoefficienter
$x\equiv y \pmod n$
så $p(x)\equiv p(y) \pmod n$

Genom att använda satsen ovan förenklar man lösandet av "kongruens-ekvationer" genom insättning av n heltal i följd (t.ex. talen $0,1,\ldots,n-1$ eller (om n udda) talen $-\frac{n-1}{2},-\frac{n-1}{2}+1,\ldots,0,\ldots,\frac{n-1}{2}$ eller (om n jämnt) talen $-\frac{n}{2}+1,-\frac{n}{2}+2,\ldots,0,\ldots,\frac{n}{2}$) som värde på den obekanta, x.

Exempel Lös ekvationen $5x^{12}-10001x\equiv 6 \pmod 4$.

Lösning: Det räcker att kontrollera $x = -1, 0, 1, 2$. Då är (mod 4)

x	$5x^{12} - 10001x$
-1	$5 + 10001 \equiv 10006 - 4 \cdot 2500 = 6 \equiv 6$ (ok)
0	$0 \not\equiv 6$ (nej!)
1	$5 - 10001 \equiv 9996 - 4 \cdot 2499 = 0 \not\equiv 6$ (nej!)
2	$5 \cdot (2^6)^2 - 10001 \cdot 2 = 5 \cdot 4096 - 20002 \equiv 478 - 4 \cdot 118 = 6 \equiv 6$ (ok)

$x = -1$ lösning $\Rightarrow$ $x = -1 + 4n$ där $n \in \mathbb{Z}$ är lösningar.
$x = 2$ lösning $\Rightarrow$ $x = 2 + 4n$ där $n \in \mathbb{Z}$ är lösningar.

dvs lösningsmängden är $\{-1 + 4n : n \in \mathbb{Z}\} \cup \{2 + 4n : n \in \mathbb{Z}\}$. □

Talsystem

Heltalet 12 345 kan skrivas $10\,000 + 2\,000 + 300 + 40 + 5$
dvs $1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0$
vilket hade varit till hjälp om man varit ovan vid det decimala talsystemet (dvs det talsystem med bas 10). Emellertid är det decimala talsystemet det vanligaste men ibland förekommer t.ex. det binära (med bas 2), det oktala (med bas 8) eller det hexadecimala (med bas 16). Innan vi försöker oss på att översätta mellan olika talsystem, låt oss införa begreppen *heltalsdivion* och *rest*.

Exempel Skriv talet 768 på
a) binär form b) oktal form c) hexadecimal form

Lösning:

a) Att skriva 768 på binär form innebär att vi ska hitta $(a_0, a_1, \ldots, a_n) \in \{0, 1\}^{n+1}$ så att $a_n \cdot 2^n + \ldots + a_1 \cdot 2^1 + a_0 \cdot 2^0 = 768$.
Vi börjar med a_n: vi vill hitta n och resten vid heltalsdivision av 768 med 2^n sådan att kvoten blir 1. Detta innebär att vi söker det största talet $2^n \leq 768$. Vi har att $2^0 = 1,\ 2^1 = 2, \ldots,\ 2^8 = 256,\ 2^9 = 512,\ 2^{10} = 1024$ så 2^9 är den sökta nämnaren. Resten blir $768 - 2^9 = 256$ och eftersom $2^8 = 256$ har vi att $768 = 2^9 + 2^8 = 1 \cdot 2^9 + 1 \cdot 2^8 + 0 \cdot 2^7 + \ldots + 0 \cdot 2^0$ varmed 768 på binär form blir 1100000000 och man skriver $(768)_{10} = (1100000000)_2$.

b) Vi ska nu hitta $(a_0, \ldots, a_n) \in \{0, 1, \ldots, 7\}^{n+1}$ så att $a_n \cdot 8^n + \ldots + a_0 \cdot 8^0 = 768$. Vi har att $8^0 = 1, 8^1 = 8, 8^2 = 64, 8^3 = 4096$ så $1 \cdot 512$ är det mesta vi kan ta av 8^3. Kvar blir $768 - 512 = 256$ och eftersom vi nu kan välja bland koefficienterna $0, 1, \ldots, 7$ ser vi att koefficienten 4 ger $4 \cdot 8^2 = 256$ så då är vi klara: $768 = 1 \cdot 8^3 + 4 \cdot 8^2 + 0 \cdot 8^1 + 0 \cdot 8^0$ dvs $(768)_{10} = (1400)_8$.

c) Vi ska hitta $(a_0, \ldots, a_n) \in \{0, 1, \ldots, 9, \underbrace{10}_{\text{A}}, \underbrace{11}_{\text{B}}, \underbrace{12}_{\text{C}}, \underbrace{13}_{\text{D}}, \underbrace{14}_{\text{E}}, \underbrace{15}_{\text{F}}\}^{n+1}$
så att $a_n \cdot 16^n + \ldots + a_0 \cdot 16^0 = 768$. Vi har att $16^0 = 1, 16^1 = 16, 16^2 = 256, 16^3 = 4096$ varmed $3 \cdot 16^2 = 768$ är det största talet $a_n \cdot 16^n$ som är mindre än eller lika med 768. Därmed är $(768)_{10} = (300)_{16}$. □