Mat-1.1510 Grundkurs i matematik 1, del III

G. Gripenberg

TKK

2 december 2010

Variabelbyte

$$\int_a^b F'(g(x))g'(x)\,\mathrm{d}x = \int_a^b \frac{\mathrm{d}}{\mathrm{d}x}F(g(x))\,\mathrm{d}x$$
$$= \Big|_a^b F(g(x)) = F(g(b)) - F(g(a)),$$

eller så här om $F' = f$:

- *Vi gör variabelbytet $t = g(x)$*
- *Då $x = a$ är $t = g(a)$ och då $x = b$ är $t = g(b)$*
- *Eftersom $\frac{\mathrm{d}t}{\mathrm{d}x} = g'(x)$ är $g'(x)\,\mathrm{d}x = \mathrm{d}t$*

och därför blir

$$\int_a^b f(g(x))g'(x)\,\mathrm{d}x = \int_{g(a)}^{g(b)} f(t)\,\mathrm{d}t.$$

Variabelbyte II

Man kan också gä ät motsatt håll, dvs. om man skall räkna integralen $\int_a^b f(x)\,\mathrm{d}x$ gör man så här:

- *Vi gör variabelbytet $x = h(t)$*
- *Då $x = a$ är $t = h^{-1}(a)$ och då $x = b$ är $t = h^{-1}(b)$*
- *Eftersom $\frac{\mathrm{d}x}{\mathrm{d}t} = h'(t)$ är $\mathrm{d}x = h'(t)\,\mathrm{d}t$*

och därför blir

$$\int_a^b f(x)\,\mathrm{d}x = \int_{h^{-1}(a)}^{h^{-1}(b)} f(h(t))h'(t)\,\mathrm{d}t.$$

Obs!

Om man tex. i integralen $\int f(x)\,\mathrm{d}x$ gör variablebytet $x = h(t)$ så att $\mathrm{d}x = h'(t)\,\mathrm{d}t$ och får integralen $\int f(h(t))h'(t)\,\mathrm{d}t$ som man sedan räknar ut och får som svar $G(t) + C$ skall man sedan sätta in $t = h^{-1}(x)$ för att få $\int f(x)\,\mathrm{d}x = G(h^{-1}(x)) + C$.

Partiell integrering

$$\int f'(x)g(x)\,\mathrm{d}x = f(x)g(x) - \int f(x)g'(x)\,\mathrm{d}x$$
$$\int_a^b f'(x)g(x)\,\mathrm{d}x = \Big|_a^b f(x)g(x) - \int_a^b f(x)g'(x)\,\mathrm{d}x$$

Exempel

Om vi skall räkna $\int \ln(x)\,\mathrm{d}x$ kan vi skriva $\ln(x) = 1 \cdot \ln(x)$ och välja $f(x) = x$ så att $f'(x) = 1$ och $g(x) = \ln(x)$. Då får vi

$$\int \ln(x)\,\mathrm{d}x = x\ln x - \int x\frac{1}{x}\,\mathrm{d}x = x\ln(x) - \int 1\,\mathrm{d}x = x\ln(x) - x + C.$$

Taylorutveckling med partiell integrering

Om f är $k+1$ gånger kontinuerligt deriverbar så är

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2}(x-a)^2 + \frac{f'''(a)}{3!}(x-a)^3 + \ldots + \frac{f^{(k)}(a)}{k!}(x-a)^k + \int_a^x \frac{(x-t)^k}{k!} f^{(k+1)}(t)\,\mathrm{d}t.$$

Hur visar man detta?
Av analysens huvudsats följer att $f(x) = f(a) + \int_a^x f'(t)\,\mathrm{d}t$ vilket ger ovanstående formel för $k = 0$. Nu kan man integrera partiellt så att man skriver $1 = \frac{\mathrm{d}}{\mathrm{d}t}(-(x-t))$ och man får

$$f(x) = f(a) + \int_a^x 1 \cdot f'(t)\,\mathrm{d}t = f(a) + \Big/_a^x (-(x-t))f'(t)$$
$$- \int_a^x (-(x-t))f''(t)\,\mathrm{d}t = f(a) + f'(a)(x-a) + \int_a^x (x-t)f''(t)\,\mathrm{d}t,$$

vilket är formeln för $k = 1$. Sedan fortsätter man "på samma sätt".

Integrering av rationella funktioner

En rationell funktion $f(x) = \frac{p(x)}{q(x)}$ kan integreras förutsatt att man hittar nämnarens nollställen.

Exempel

Räkna $\int_0^2 \frac{1}{x^2+8x+17}\,\mathrm{d}x$

Först konstaterar vi att nämnarens nollställen är $-4 \pm \sqrt{16-17} = -4 \pm \mathrm{i}$ och eftersom de är komplexa kan man gå tillväga på lite olika sätt. Ett sätt ar att "komplettera kvadraten" och skriva $x^2+8x+17 = (x+4)^2+1$ och sedan göra variabelbytet $x+4 = t$ så att då $x = 0$ är $t = 4$, då $x = 2$ är $t = 6$ och $\mathrm{d}x = \mathrm{d}t$. Den integral vi skall räkna ut blir då

$$\int_4^6 \frac{1}{t^2+1}\,\mathrm{d}t = \Big/_4^6 \arctan(t) = \arctan(6) - \arctan(4),$$

eftersom $\frac{\mathrm{d}}{\mathrm{d}t}\arctan(t) = \frac{1}{1+t^2}$.

Hur man hittar integralen till en rationell funktion

- *Skriv funktionen i formen $f(x) = s(x) + \frac{r(x)}{q(x)}$ där $s(x)$ är ett polynom och gradtalet av $r(x)$ är mindre än gradtalet av $q(x)$;*
- *Skriv $q(x)$ i formen $q(x) = a(x-x_1)^{k_1} \cdot \ldots \cdot (x-x_m)^{k_m}$;*
- *Bestäm koefficienterna $A_{j,k}$ så att*

$$\frac{r(x)}{q(x)} = \sum_{j=1}^{m} \sum_{k=1}^{k_j} \frac{A_{j,k}}{(x-x_j)^k};$$

- *Integrera!*

Observera att för de nollställen x_j som är komplexa måste man antingen räkna med komplexa logaritmer eller så skall man kombinera uttryck med rötter som är varandras konjugat så att man får termer med kvadrater i nämnaren.

Exempel

Om vi skall bestämma lösningen till differentialekvationen

$$y'(t) = ay(t)(1-y(t)),$$

då $0 < y(0) < 1$ så kan vi dividera båda sidorna med $y(t)(1-y(t))$ och integrera över $(0,s)$ så att resultatet blir

$$\int_0^s \frac{y'(t)}{y(t)(1-y(t))}\,\mathrm{d}t = \int_0^s a\,\mathrm{d}t.$$

I integralen på vänstra sidan kan vi göra variabelbytet $y(t) = u$ så att $y'(t)\,\mathrm{d}t = \mathrm{d}u$ och $u = y(0)$ då $t = 0$ och $u = y(s)$ då $t = s$. Då får vi

$$\int_{y(0)}^{y(s)} \frac{1}{u(1-u)}\,\mathrm{d}u = as.$$

Exempel, forts.

För att kunna räkna integralfunktionen $\int \frac{1}{u(1-u)}\,\mathrm{d}u$ *gör vi en partialbråksuppdelning*

$$\frac{1}{u(1-u)} = \frac{A}{u} + \frac{B}{1-u},$$

och koefficienterna A *och* B *kan vi räkna ut så att*

$$A = \lim_{u\to 0}\left(u\frac{A}{u} + u\frac{B}{1-u}\right) = \lim_{u\to 0}\frac{u}{u(1-u)} = 1,$$
$$B = \lim_{u\to 1}\left((1-u)\frac{A}{u} + (1-u)\frac{B}{1-u}\right) = \lim_{u\to 1}\frac{1-u}{u(1-u)} = 1.$$

Exempel, forts.

Detta innebär att

$$as = \int_{y(0)}^{y(s)}\left(\frac{1}{u} + \frac{1}{1-u}\right)\mathrm{d}u = \Big/_{y(0)}^{y(s)}\left(\ln(u) - \ln(1-u)\right)$$
$$= \ln(y(s)) - \ln(1-y(s)) - \ln(y(0)) + \ln(1-y(0)) = \ln\left(\frac{y(s)(1-y(0))}{y(0)(1-y(s))}\right).$$

Av detta följer i sin tur att

$$\frac{y(s)(1-y(0))}{y(0)(1-y(s))} = \mathrm{e}^{as},$$

och sedan, efter diverse räkningar, att

$$y(s) = \frac{\mathrm{e}^{as}y(0)}{1 + (\mathrm{e}^{as}-1)y(0)}.$$

Trapetsregeln

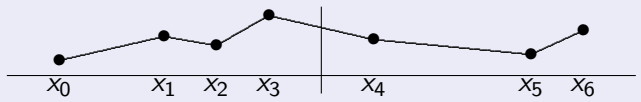
Antag att man känner till funkionens f *värden i punkterna* $a = x_0 < x_1 < \ldots, < x_n = b$ *och man vill räkna*

$$\int_a^b f(x)\,\mathrm{d}x.$$

Vad kan man göra? Till exempel så här:

- *Vi bildar någon enkel funktion* f_* *så att* $f_*(x_j) = f(x_j)$ *och räknar* $\int_a^b f_*(x)\,\mathrm{d}x$.
- *Hur skall vi välja* f_**?*
- *Tex. med linjär interpolering så att*

$$f_*(x) = \frac{x_j - x}{x_j - x_{j-1}}f(x_{j-1}) + \frac{x - x_{j-1}}{x_j - x_{j-1}}f(x_j), \quad x_{j-1} \le x \le x_j.$$



Trapetsregeln, forts.

Vad är $\int_a^b f_*(x)\,\mathrm{d}x$*?*

$$\int_a^b f(x)\,\mathrm{d}x \approx \int_a^b f_*(x)\,\mathrm{d}x = \sum_{j=1}^n \int_{x_{j-1}}^{x_j} f_*(x)\,\mathrm{d}x$$
$$= \sum_{j=1}^n \int_{x_{j-1}}^{x_j}\left(-\frac{(x_j - x)^2}{2(x_j - x_{j-1})}f(x_{j-1}) + \frac{(x - x_{j-1})^2}{2(x_j - x_{j-1})}f(x_j)\right)$$
$$= \sum_{j=1}^n \frac{x_j - x_{j-1}}{2}\left(f(x_{j-1}) + f(x_j)\right).$$

Trapetsregeln: Formel

Detta är också en god ide om man känner $f(x)$ i alla punkter x och i synnerhet om delintervallen är lika långa, dvs. $x_j - x_{j-1} = \frac{1}{n}(b-a)$ och då får man

$$\int_a^b f(x) \approx T_n(f,a,b) = \frac{b-a}{2n}\big(f(x_0) + 2f(x_1) + \dots 2f(x_{n-1}) + f(x_n)\big)$$
$$= \frac{b-a}{n}\big(\tfrac{1}{2}f(x_0) + f(x_1) + \dots f(x_{n-1}) + \tfrac{1}{2}f(x_n)\big).$$

Observera att man räknar värdena av funktionen f i $n+1$ punkter och den första och den sista delar på koefficienten.

När ger trapetsregeln rätt svar?

Åtminstone i de fall då f är kontinuerlig och f är i varje intervall (x_{j-1}, x_j) där $j = 1, \dots, n$ ett polynom med högst gradtalet 1, dvs. $f(x) = \alpha_j x + \beta_j$ kun $x \in (x_{j-1}, x_j)$.

Trapetsregeln: Feluppskattning

Antag att $n = 1$ och intervallet är $[-\frac{h}{2}, \frac{h}{2}]$. Om nu f är tex. två gånger kontinuerligt deriverbar och om $f_0(x) = f(0) + f'(0)x$ så är $f(x) = f_0(x) + f_1(x)$ där $f_1(x)$ är sådan att för någon konstant C_1 gäller $|f_1(x)| \le C_1 x^2$. Nu är

$$\left|\int_{-\frac{h}{2}}^{\frac{h}{2}} f_1(x)\,\mathrm{d}x\right| \le C_1 \int_{-\frac{h}{2}}^{\frac{h}{2}} x^2\,\mathrm{d}x = \frac{C_1 h^3}{12}.$$

På samma sätt ser man att

$$\left|T_1\left(f_1, -\frac{h}{2}, \frac{h}{2}\right)\right| \le \frac{C_1 h^3}{4}.$$

Trapetsregeln: Feluppskattning, forts.

Eftersom $\int_{-\frac{h}{2}}^{\frac{h}{2}} f_0(x)\,\mathrm{d}x = T_1\left(f_0, -\frac{h}{2}, \frac{h}{2}\right)$ så får man med

$$\left|\int_{-\frac{h}{2}}^{\frac{h}{2}} f(x)\,\mathrm{d}x - T_1\left(f, -\frac{h}{2}, \frac{h}{2}\right)\right|$$
$$= \left|\int_{-\frac{h}{2}}^{\frac{h}{2}} f_0(x)\,\mathrm{d}x + \int_{-\frac{h}{2}}^{\frac{h}{2}} f_1(x)\,\mathrm{d}x - T_1\left(f_0, -\frac{h}{2}, \frac{h}{2}\right) - T_1\left(f_1, -\frac{h}{2}, \frac{h}{2}\right)\right|$$
$$\le \left|\int_{-\frac{h}{2}}^{\frac{h}{2}} f_1(x)\,\mathrm{d}x\right| + \left|T_1\left(f_1, -\frac{h}{2}, \frac{h}{2}\right)\right| \le Ch^3.$$

Om man använder n delintervall skall man addera feluppskattningarna så att

$$\left|\int_a^b f(x)\,\mathrm{d}x - T_n(f,a,b)\right| \le C(b-a)h^2 = C\frac{(b-a)^3}{n^2}, \quad h = \frac{b-a}{n}.$$

Med en noggrannare analys kan man visa att konstanten C kan vara $\frac{1}{12}\max_{x\in[a,b]}|f''(x)|$.

Trapetsregeln och extrapolering

Antag att funktionen f är sådan att

$$T_m(f,a,b) \approx \int_a^b f(x)\,\mathrm{d}x + \frac{C}{m^2}.$$

Då är

$$T_{2m}(f,a,b) \approx \int_a^b f(x)\,\mathrm{d}x + \frac{1}{4}\frac{C}{m^2}.$$

Detta är ett "ekvationssystem" där de obekanta är $\int_a^b f(x)\,\mathrm{d}x$ och $\frac{C}{m^2}$ och som "lösning " får man (då man multiplicerar den senare med fyra och subtraherar den första från resultatet)

$$\int_a^b f(x)\,\mathrm{d}x \approx \frac{4}{3}T_{2m}(f,a,b) - \frac{1}{3}T_m(f,a,b).$$

Om n är ett jämnt tal så är $S_n(f,a,b) = \frac{4}{3}T_n(f,a,b) - \frac{1}{3}T_{\frac{n}{2}}(f,a,b)$ och man får Simpsons regel!

Simpsons regel

Om man delar intervallet $[a,b]$ i två delar $[x_0,x_1]$ och $[x_1,x_2]$ där $x_j = a + j\frac{b-a}{2}$ så skall man enligt Simpsons regel räkna

$$\begin{aligned}\int_a^b f(x)\,\mathrm{d}x \approx S_2(f,a,b) &= \frac{4}{3}T_2(f,a,b) - \frac{1}{3}T_1(f,a,b)\\ &= \frac{4}{3}\frac{b-a}{4}(f(x_0+2f(x_1)+f(x_2) - \frac{1}{3}\frac{b-a}{2}(f(x_0)+f(x_2))\\ &= \frac{b-a}{6}(f(x_0)+4f(x_1)+f(x_2)).\end{aligned}$$

Simpsons regel, forts.

Om antalet delintervall är n där n är ett jämnt tal så får man genom att addera (då man skriver $x_j = a + j\frac{b-a}{n}$)

$$\begin{aligned}\int_a^b f(x)\,\mathrm{d}x \approx S_n(f,a,b) = \frac{b-a}{3n}\big(&f(x_0)+4f(x_1)+2f(x_2)\\ &+4f(x_3)+2f(x_4)+\ldots+2f(x_{n-2})+4f(x_{n-1})+f(x_n)\big).\end{aligned}$$

Observera att termerna $f(x_j)$ där j är udda ges en större vikt 4 än de termer där j är jämn, vilka har vikten 2 bortsett från den första och den sista termen som delar på vikten 2.

När ger Simpsons regel rätt svar?

Antag att $n = 2$ och att intervallet är $[-h,h]$. En räkning visar att

$$f(x) = 1 \Rightarrow \int_{-h}^{h} f(x)\,\mathrm{d}x = 2h \text{ och } S_2(f,-h,h) = \frac{2h}{6}(1+4\cdot 1+1) = 2h,$$

$$f(x) = x \Rightarrow \int_{-h}^{h} f(x)\,\mathrm{d}x = 0 \text{ och } S_2(f,-h,h) = \frac{2h}{6}(-h+4\cdot 0+h) = 0,$$

$$f(x) = x^2 \Rightarrow \int_{-h}^{h} f(x)\,\mathrm{d}x = \Big/_{-h}^{h}\frac{1}{3}x^3 = \frac{2h^3}{3}$$

$$\text{och } S_2(f,-h,h) = \frac{2h}{6}(h^2+4\cdot 0+h^2) = \frac{2h^3}{3},$$

$$f(x) = x^3 \Rightarrow \int_{-h}^{h} f(x)\,\mathrm{d}x = 0 \text{ och } S_2(f,-h,h) = \frac{2h}{6}(-h^3+4\cdot 0+h^3) = 0,$$

(men om $f(x) = x^4$ så är $\int_{-h}^{h} x^4\,\mathrm{d}x = \frac{2h^5}{5} \neq S_2(f,-h,h) = \frac{2h^5}{3}$).

När ger Simpsons regel rätt svar? forts

Av detta ser man att Simpsons regel ger rätt svar åtminstone om f är kontinuerlig och f är ett polynoim med gradtalet högst 3 på varje intervall $(x_{2(j-1)}, x_{2j})$ där $j = 1,\ldots,\frac{n}{2}$.

Simpsons regel: Feluppskattning

Antag att $n = 2$ och intervallet är $[-h,h]$. Om nu f är tex. fyra gånger kontinuerligt deriverbar och om $f_0(x) = f(0) + f'(0)x + \frac{1}{2}f''(0)x^2 + \frac{1}{6}f'''(0)x^3$ så är $f(x) = f_0(x) + f_1(x)$ där $f_1(x) = O(x^4)$ dvs. det finns någon konstant C_1 så att $|f_1(x)| \le C_1x^4$.Nu är

$$\left|\int_{-h}^{h} f_1(x)\,\mathrm{d}x\right| \le C_1\int_{-h}^{h} x^4\,\mathrm{d}x = \frac{2C_1h^5}{5}.$$

På samma sätt ser man att

$$|S_2(f_1,-h,h)| \le \frac{C_1h^5}{3}.$$

Simpsons regel: Feluppskattning, forts.

Eftersom $\int_{-h}^{h} f_0(x)\,\mathrm{d}x = S_2(f_0, -h, h)$ *får man av föregående olikheter*

$$\left|\int_{-h}^{h} f(x)\,\mathrm{d}x - S_2(f,-h,h)\right| = \left|\int_{-h}^{h} f_0(x)\,\mathrm{d}x + \int_{-h}^{h} f_1(x)\,\mathrm{d}x - S_2(f_0,-h,h) - S_2(f_1,-h,h)\right| \le \left|\int_{-h}^{h} f_1(x)\,\mathrm{d}x\right| + |S_2(f_1,-h,h)| \le C_2 h^5.$$

Om man använder n *intervall skall man räkna ihop* $\frac{n}{2}$ *feluppskattningar där* $h = \frac{b-a}{n}$ *så att*

$$\left|\int_a^b f(x)\,\mathrm{d}x - S_n(f,a,b)\right| \le C(b-a)h^4 = C\frac{(b-a)^5}{n^4}.$$

Med en noggrannare analys kan man visa att man som konstant C *kan välja* $\frac{1}{180}\max_{x\in[a,b]}|f^{(4)}(x)|$.

Mittpunktsregeln

En annan, mycket enkel och naturlig, metod är att dela upp integrationsintervallet i n *delar (som ofta men inte alltid är lika långa), räkna ut funkionens värde i delintervallens mittpunkter och multiplicera dessa med intervallens längd och sedan addera. Om intervallen är lika långa får man*

$$M_n(f,a,b) = \sum_{j=0}^{n-1} \frac{b-a}{n} f\left(a + \frac{b-a}{n}(j+\tfrac{1}{2})\right).$$

Mittpunktsregeln ger rätt svar om funktionen som skall integreras är ett polynom med högst gradtalet 1 *i varje delintervall. Som feluppskattning får man*

$$\left|M_n(f,a,b) - \int_a^b f(x)\,\mathrm{d}x\right| \le \frac{K(b-a)^3}{24n^2}, \quad \text{ifall } |f''(x)| \le K \text{ då } x \in (a,b).$$

Obs!

Det som här sägs om numerisk integrering berör inte bara frågan hur man skall räkna ut någon integral utan också hur man kan resonera allmänt beträffande numeriska räkningar och approximationer.

Feluppskattning: Grundide

Man räknar på åtminstone två (tillräckligt olika) sätt och jämför resultaten. I de flesta fall kan absolutbeloppet av skillnaden användas som en övre gräns för absolutbeloppet av felet i den bättre metoden!

Ett numeriskt exempel

Man skall räkna integralen $I = \int_{-1}^{1} \sqrt{|x|}\,\mathrm{d}x$ *vars exakta värde naturligtvis är* $I = \frac{4}{3} \approx 1.333333333$. *Derivatan av funktionen* $\sqrt{|x|}$ *är inte begränsad i närheten av origo så man kan inte vänta sig att man med de metoder som här presenterats kan få speciellt exakta resultat.Med trapetsmetoden får man följande värden*

n	8	16	32	64
T_n	1.286566	1.316260	1.327162	1.331118
$\lvert T_n - I\rvert$	0.046767	0.017073	0.006170	0.002215
$\lvert T_n - T_{\frac{n}{2}}\rvert$		0.029694	0.010902	0.003955

n	128	256	512	1024
T_n	1.332542	1.333051	1.333233	1.333298
$\lvert T_n - I\rvert$	0.000792	0.000282	0.000100	0.000036
$\lvert T_n - T_{\frac{n}{2}}\rvert$	0.001424	0.000510	0.000182	0.000065

Ett numeriskt exempel, forts.

Om man använder Simpsons metod för att räkna integralen $\int_{-1}^{1} \sqrt{|x|}\,\mathrm{d}x$ *så är resultaten följande:*

n	8	16	32	64
S_n	1.3130525	1.3261586	1.3307964	1.3324364
$\lvert S_n - I\rvert$	0.0202808	0.0071748	0.002537	0.000897
$\lvert S_n - S_{\frac{n}{2}}\rvert$		0.0131060	0.0046378	0.001640

n	128	256	512	1024
S_n	1.3330162	1.3332212	1.3332937	1.3333193
$\lvert S_n - I\rvert$	0.0003171	0.0001121	0.0000396	0.0000140
$\lvert S_n - S_{\frac{n}{2}}\rvert$	0.0005798	0.0002050	0.0000725	0.0000256

Ett numeriskt exempel, forts.

Vi skall ännu närmare undersöka hur snabbt de approximationer man får med trapetsregeln och Simpsons regel konvergerar mot integralens värde, utan att utnyttja det faktum att man kan räkna ut integralen. Låt $T_n = T_n(\sqrt{|x|}, -1, 1)$ *och antag att*

$$T_n \approx I + \frac{C_T}{n^\tau},$$

Där alltså $I = \int_{-1}^{t} \sqrt{|x|}\,\mathrm{d}x$. *Då är*

$$T_{2n} \approx I + \frac{C_T}{2^\tau n^\tau},$$

så att

$$T_n - T_{2n} \approx (1 - 2^{-\tau})\frac{C_T}{n^\tau},$$

och

$$\frac{T_n - T_{2n}}{T_{2n} - T_{4n}} \approx \frac{(1 - 2^{-\tau})\frac{C_T}{n^\tau}}{(1 - 2^{-\tau})\frac{C_T}{2^\tau n^\tau}} = 2^\tau$$

Ett numeriskt exempel, forts.

Som en approximation av parametern τ *får man alltså*

$$\tau \approx \log_2\left(\frac{T_n - T_{2n}}{T_{2n} - T_{4n}}\right).$$

De numeriska värdena ger följande approximationer för τ*:*

n	8	16	32	64	128
$\log_2\left(\frac{T_n - T_{2n}}{T_{2n} - T_{4n}}\right)$	1.4456	1.4627	1.4742	1.4820	1.4874

n	256	512	1024	2048	4096
$\log_2\left(\frac{T_n - T_{2n}}{T_{2n} - T_{4n}}\right)$	1.4912	1.4938	1.4956	1.4969	1.4978

Ett numeriskt exempel, forts.

Skriv $S_n = S_n(\sqrt{|x|}, -1, 1)$ *och antag att*

$$S_n \approx I + \frac{C_S}{n^\sigma}.$$

Då får man med samma slags resonemang

$$\sigma \approx \log_2\left(\frac{S_n - S_{2n}}{S_{2n} - S_{4n}}\right).$$

och följande numeriska värden:

n	8	16	32	64	128
$\log_2\left(\frac{S_n - S_{2n}}{S_{2n} - S_{4n}}\right)$	1.4987	1.4998	1.5000	1.5000	1.5000

Feluppskattning, forts.

Med hjälp av ovanstående räkningar och antaganden $T_n \approx I + \frac{C_T}{n^\tau}$ *och* $S_n \approx I + \frac{C_S}{n^\sigma}$ *får man också*

$$|T_n - I| \approx \frac{1}{2^\tau - 1}\left|T_n - T_{\frac{n}{2}}\right|,$$

och

$$|S_n - I| \approx \frac{1}{2^\sigma - 1}\left|S_n - S_{\frac{n}{2}}\right|.$$

Variabelbyte

Om integrationsintervallet är oändligt långt eller om funktionen inte är begränsad i närheten av någon eller några punkter så kan det vara omöjligt att använda trapets+ eller Simpsons regel direkt. (I somliga fall kan mittpunktsregeln fungera bättre.) Dessutom kan det vara så att fast funktionen är kontinuerlig och intervallet är ändligt långt så kan dessa metoder fungera onödigt långsamt om f *inte är tillräckligt många gånger deriverbar.*
Då kan ett variabelbyte vara till hjälp men det finns många fall då man inte har nytta av det.

Variabelbyte: Exempel 1

$$\int_0^3 \frac{1}{\sqrt{9-x^2}}\,\mathrm{d}x = ?$$

Här är problemet att funktionen som skall integreras inte är begränsad då $x \to 3-$. *Nu är* $\sqrt{9-x^2} = \sqrt{3+x}\sqrt{3-x}$ *och endast den senare faktorn skapar problem. Vi gör variabelbytet* $3 - x = t^2$ *så att* $-\mathrm{d}x = 2t\,\mathrm{d}t$, $t = \sqrt{3}$ *då* $x = 0$ *och* $t = 0$ *då* $x = 3$ *och dessutom gäller* $x = 3 - t^2$ *så att*

$$\int_0^3 \frac{1}{\sqrt{9-x^2}}\,\mathrm{d}x = \int_{\sqrt{3}}^0 \frac{1}{\sqrt{3+3-t^2}\sqrt{t^2}}(-2t)\,\mathrm{d}t$$
$$= \int_0^{\sqrt{3}} \frac{2}{\sqrt{6-t^2}}\,\mathrm{d}t.$$

Nu är funktionen som skall integreras oändligt många gånger deriverbar i integrationsintervallet $[0, \sqrt{3}]$.

Variabelbyte: Exempel 2

$$\int_0^\infty \frac{1}{1+x^5}\,\mathrm{d}x = ?$$

Här är problemet det att integrationsintervallet är oändligt långt och vi börjar med att dela upp integralen i två integraler

$$\int_0^\infty \frac{1}{1+x^5}\,\mathrm{d}x = \int_0^1 \frac{1}{1+x^5}\,\mathrm{d}x + \int_1^\infty \frac{1}{1+x^5}\,\mathrm{d}x.$$

I den senare gör vi variabelbytet $x = \frac{1}{t}$. *Då är* $\mathrm{d}x = -\frac{1}{t^2}\,\mathrm{d}t$, $t = 1$ *då* $x = 1$ *och* $t = 0$ *då* $x = \infty$ *så att*

$$\int_0^\infty \frac{1}{1+x^5}\,\mathrm{d}x = \int_0^1 \frac{1}{1+x^5}\,\mathrm{d}x + \int_1^0 \frac{1}{1+(\frac{1}{t})^5}\,\frac{-1}{t^2}\mathrm{d}t$$
$$\int_0^1 \frac{1}{1+x^5}\,\mathrm{d}x + \int_0^1 \frac{t^3}{t^5+1}\,\mathrm{d}t = \int_0^1 \frac{1+x^3}{1+x^5}\,\mathrm{d}x.$$

Det är inga problem att numeriskt räkna denhär integralen.

Sammandrag

- *Mittpunktsregeln:*

$$\int_a^b f(x)\,\mathrm{d}x \approx M_n(f,a,b) = \frac{b-a}{n}\sum_{j=0}^{n-1} f\left(a+\frac{b-a}{n}(j+\tfrac{1}{2})\right).$$

- *Trapetsregeln:* ($x_0 = a$, $x_1 = a+\frac{b-a}{n}$, $x_j = a+\frac{b-a}{n}j$)

$$\int_a^b f(x)\,\mathrm{d}x \approx T_n(f,a,b) = \frac{b-a}{2n}\left(f(x_0)+2f(x_1)+\ldots 2f(x_{n-1})+f(x_n)\right).$$

- *Simpsons regel:*

$$\int_a^b f(x)\,\mathrm{d}x \approx S_n(f,a,b) = \frac{b-a}{3n}\left(f(x_0)+4f(x_1)+2f(x_2)\right.$$
$$\left.+4f(x_3)+2f(x_4)+\ldots+2f(x_{n-2})+4f(x_{n-1})+f(x_n)\right).$$

Laplace-transformer

$$\mathcal{L}(f)(s) = \int_0^\infty \mathrm{e}^{-st} f(t)\,\mathrm{d}t$$

Exempel

- $\mathcal{L}(1)(s) = \frac{1}{s}$
- $\mathcal{L}(\mathrm{e}^{at})(s) = \frac{1}{s-a}$
- $\mathcal{L}(\cos(\omega t))(s) = \frac{s}{s^2+\omega^2}$
- $\mathcal{L}(\sin(\omega t))(s) = \frac{\omega}{s^2+\omega^2}$

Obs!

$\mathcal{L}$ är en funktion vars argument inte är ett tal utan en funktion (definerad i $(0,\infty)$ och som uppfyller vissa villkor) och värdet av $\mathcal{L}(f)$ är en annan funktion (definierad åtminstone för alla komplexa tal s med $\mathrm{Re}\,(s) > \alpha$ för något tal α).

Laplace-transformen är linjär!

$$\mathcal{L}(\alpha f+\beta g) = \alpha\mathcal{L}(f)+\beta\mathcal{L}(g)$$

Teorem

Ifall

- *För varje $T > 0$ är funktionen f är integrerbar i intervallet $(0,T)$.*
- $\lim_{T\to\infty}\int_0^T \mathrm{e}^{-s_0 t} f(t)\,\mathrm{d}t$ *existerar för något tal* $s_0 \in \mathbb{C}$

så gäller att

- $F(s) = \lim_{T\to\infty}\int_0^T \mathrm{e}^{-st} f(t)\,\mathrm{d}t$ *existerar då* $\mathrm{Re}\,(s) > \mathrm{Re}\,(s_0)$,
- *$F(s)$ är analytisk i mängden $\{\, s\in\mathbb{C} : \mathrm{Re}\,(s) > \mathrm{Re}\,(s_0)\,\}$ dvs.* $F(s) = \sum_{n=0}^\infty \frac{1}{n!}F^{(n)}(s_1)(s-s_1)^n$ *åtminstone då* $|s-s_1| < \mathrm{Re}\,(s_1-s_0)$.

Laplace-transformen är entydig

Om $\mathcal{L}(f)(s) = \mathcal{L}(g)(s)$ då $\mathrm{Re}\,(s) > \alpha$ så är $f(t) = g(t)$ för nästan alla $t \geq 0$.

Räkneregler, derivator mm. då $F(s) = \mathcal{L}(f)(s)$

- $\mathcal{L}(f')(s) = sF(s) - f(0)$
- $F'(s) = \mathcal{L}(-tf(t))(s)$
- $\mathcal{L}\left(\int_0^t f(\tau)\,\mathrm{d}\tau\right)(s) = \frac{1}{s}F(s)$

Räkneregler, förskjutningsregler mm. då $F(s) = \mathcal{L}(f)(s)$

- $\mathcal{L}(\mathrm{e}^{at}f(t))(s) = F(s-a)$
- $\mathcal{L}(f(t-a)u(t-a))(s) = \mathrm{e}^{-as}F(s)$
  där $u(t) = 1$ då $t > 0$, $u(t) = 0$ då $t < 0$ och $a \geq 0$.
- $\mathcal{L}(f(at))(s) = \frac{1}{a}F\left(\frac{s}{a}\right)$, $a > 0$

Exempel

Antag att $y(t)$ är lösningen till ekvationen

$$y'(t) + 2y(t) = 3, \quad y(0) = 4.$$

Om $Y(s) = \mathcal{L}(y)(s)$ så är $\mathcal{L}(y')(s) = sY(s) - y(0) = sY(s) - 4$. Eftersom Laplace-transformen är linjär och $\mathcal{L}(3)(s) = \frac{3}{s}$ så får man när man tar Laplace-transformen av båda sidorna i ekvationen

$$sY(s) - 4 + 2Y(s) = \frac{3}{s},$$

vilket betyder att

$$Y(s) = \frac{4}{s+2} + \frac{3}{s(s+2)}.$$

Exempel, forts.

Om man nu vill bestämma $y(t)$ så kan man göra en partialbråksuppdelning

$$\frac{4}{s+2} + \frac{3}{s(s+2)} = \frac{A}{s} + \frac{B}{s+2},$$

och man får

$$A = \lim_{s\to 0}\left(s\frac{A}{s} + s\frac{B}{s+2}\right) = \lim_{s\to 0}\left(s\frac{4}{s+2} + s\frac{3}{s(s+2)}\right) = \frac{3}{2},$$

$$B = \lim_{s\to -2}\left((s+2)\frac{A}{s} + (s+2)\frac{B}{s+2}\right)$$

$$= \lim_{s\to -2}\left((s+2)\frac{4}{s+2} + (s+2)\frac{3}{s(s+2)}\right) = \frac{5}{2}.$$

Detta innebär att

$$y(t) = \mathcal{L}^{-1}\left(\frac{3}{2}\cdot\frac{1}{s}\right) + \mathcal{L}^{-1}\left(\frac{5}{2}\cdot\frac{1}{s+2}\right) = \frac{3}{2} + \frac{5}{2}\cdot \mathrm{e}^{-2t}.$$

Konvolution (faltning)

$$(f * g)(t) = \int_0^t f(t-\tau)g(\tau)\,\mathrm{d}\tau$$

$$\mathcal{L}(f * g) = \mathcal{L}(f)\mathcal{L}(g)$$

Delta-funktionalen

$$\delta_T = \frac{\mathrm{d}}{\mathrm{d}t}u(t-T)$$

men $u(t-T)$ är inte deriverbar så δ_T är en "generaliserad" funktion, så att

$$\int_{-\infty}^{\infty} f(t)\delta_T(\mathrm{d}t) = f(T).$$

$$\mathcal{L}(\delta_T)(s) = \mathrm{e}^{-sT}, \quad T \geq 0$$

$$(\delta_T * f)(t) = u(t-T)f(t-T), \quad T \geq 0$$

Delbarhet

Ett tal a delar ett tal b, dvs. $a|b$ (eller b är delbart med a) om det finns ett **heltal** *k så att $b = ak$.*

Kongruens modulo

Två tal a och b är kongruenta modulo n vilket skrivs $a \equiv b \pmod{n}$ eller $a \equiv_n b$ om de har samma rest då de divideras med n, dvs. om n delar $a - b$:

$$a \equiv b \pmod{n} \Leftrightarrow a \equiv_n b \Leftrightarrow n|(a-b) \Leftrightarrow a = b + kn, \quad k \in \mathbb{Z}.$$

$\mathbb{Z}_n$, kongruensklasser

Relationen $a \equiv b \pmod{n}$ *är en ekvivalensrelation i* $\mathbb{Z}$ *(*$x \sim x$, $x \sim y \Rightarrow y \sim x$, $x \sim y, y \sim z \Rightarrow x \sim z$*) och delar upp* $\mathbb{Z}$ *i ekvivalensklasser, som kallas* **kongruensklasser** *(eller restklasser), dvs. delmängder* $\{\ldots, -2n, -n, 0, n, 2n \ldots\}$, $\{\ldots, -2n+1, -n+1, 1, n+1, 2n+1 \ldots\}$, $\ldots$, $\{\ldots, -n-1, -1, n-1, 2n-1, \ldots\}$ *där alla element i samma ekvivalensklass är kongruenta modulo n med varandra.*
Man kan använda följande beteckningar:

$$[k]_n \stackrel{\text{def}}{=} \{\, m \in \mathbb{Z} : m \equiv k \pmod{n} \,\}$$

$$\mathbb{Z}_n \stackrel{\text{def}}{=} \{\, [k]_n : k = 0, 1, 2, \ldots, n-1 \,\}, \quad \text{om } n > 0$$

Addition, subtraktion och multiplikation i $\mathbb{Z}_n$

Man kan visa att om

$$a_1 \equiv a_2 \pmod{n} \quad \text{och} \quad b_1 \equiv b_2 \pmod{n}$$

så är

$$(a_1 + b_1) \equiv (a_2 + b_2) \pmod{n}$$
$$(a_1 - b_1) \equiv (a_2 - b_2) \pmod{n}$$
$$(a_1 b_1) \equiv (a_2 b_2) \pmod{n}$$

Därför kan man definiera räkneoperationer i $\mathbb{Z}_n$ *med*

$$[a]_n + [b]_n = [a+b]_n,$$
$$[a]_n - [b]_n = [a-b]_n,$$
$$[a]_n \cdot [b]_n = [a \cdot b]_n,$$

och alla "normala" räkneregler gäller (bortsett från de som gäller olikheter).

Modulofunktionen mod

Om $n > 0$ *så är* $\mathrm{mod}\,(m, n)$ *det minsta icke-negativa heltalet i kongurensklassen* $[m]_n$*, dvs.* $\mathrm{mod}\,(m, n) = k$ *om* $0 \le k < n$ *och* $m \equiv k \pmod{n}$*, (men* $\mathrm{mod}\,(m, 0) = m$ *och* $\mathrm{mod}\,(m, n) = -\mathrm{mod}\,(m, -n)$ *om* $n < 0$*).*

$$\mathrm{mod}\,(m_1, n) = \mathrm{mod}\,(m_2, n) \quad \Leftrightarrow \quad [m_1]_n = [m_2]_n$$

Obs!

Om m och n är positiva tal så är $\mathrm{mod}\,(m, n)$ *den rest som erhålls då man dividerar m med n men om* $m < 0$ *är denna rest inte positiv.*

Obs!

Ofta väljer man elementet $\mathrm{mod}\,(m, n)$ *för att representera kongruensklassen* $[m]_n$ *så att man tex. kan tala om talen* $0, 1, 2, \ldots, 5$ *som elementen i* $\mathbb{Z}_6$ *istället för mängderna* $[0]_6, [1]_6, \ldots, [5]_6$

Exempel

Om en björn går i ide en dag kl 17 och sover i 2557 *timmar och man vill veta vid vilket klockslag den vaknar dividerar man först* 2557 *med* 24 *och får* $2557 = 106 \cdot 24 + 13$*, dvs.* $2557 \equiv 13 \pmod{24}$*. Därför är* $(17 + 2557) \equiv (17 + 13) \pmod{24} = 6 \pmod{24}$ *vilket betyder att björnen vaknar kl 6.*

Exempel

Teknolog T uppgav att början på hans personnummer är 141089-151. Om man skall räkna ut kontrolltecknet skall man räknar resten då det tal som bildas av de nio första numrorna divideras med 31 *så att talen* 10, 11, ... ,30 *ersätts med respektive A, B, C, D, E, F, H, J, K, L, M, N, P, R, S, T, U, V, W, X, Y. Nu blir*

$$\mathrm{mod}\,(141989151, 31) = 29,$$

så det fullständiga personnumret blir 141089-151X.

Exempel

Om $j \geq 0$ så är

$$[10^j]_9 = [10]_9^j = [1]_9^j = [1^j]_9 = [1]_9.$$

Om nu x är ett tal som i decimalform är $x_n x_{n-1} \ldots x_1 x_0$ så är $x = x_0 \cdot 10^0 + x_1 \cdot 10 + \ldots x_n \cdot 10^n$ och

$$\begin{aligned}[x]_9 &= [x_0 \cdot 10^0]_9 + \ldots + [x_n \cdot 10^n]_9 \\ &= [x_0]_9 \cdot [10^0]_9 + [x_1]_9 \cdot [10^1]_9 + \ldots + [x_n]_9 \cdot [10^n]_9 \\ &= [x_0]_9 \cdot [1]_9 + [x_1]_9 \cdot [1]_9 + \ldots + [x_n]_9 \cdot [1]_9 = [x_0 + x_1 + x_2 + \ldots + x_n]_9.\end{aligned}$$

Av detta följer (den välkända) regeln att 9 delar x om och endast om 9 delar summan av siffrorna i decimalformen av x.

Största gemensamma delare

Om m och n är heltal som inte båda är noll så är deras största gemensamma delare

$$\operatorname{sgd}(m, n) = \max\{\, d \in Z : d|m \text{ och } d|n \,\}.$$

(sgd=största gemensamma delare, gcd= greatest common divisor, och vanligen definierar man $\operatorname{sgd}(0, 0) = 0$)
Om $\operatorname{sgd}(m, n) = 1$ sägs talen m och n vara relativt prima.
Observera att av defintionen följer att $\operatorname{sgd}(m, n) = \operatorname{sgd}(n, m)$.

Inverser i $\mathbb{Z}_n$

Om $[m]_n \in \mathbb{Z}_n$ och det finns en kongruensklass $[j]_n \in \mathbb{Z}_n$ så att $[m]_n \cdot [j]_n = [1]_n$, dvs $m \cdot j \equiv 1 \pmod{n}$ så säger man att $[m]_n$ (eller bara m) är inverterbar i Z_n och inversen är $[j]_n = [m]_n^{-1}$. Detta innebär att man kan dividera med $[m]_n$ för det är det samma som att multiplicera med $[j]_n$. Eftersom $m \cdot j \equiv 1 \pmod{n}$ så finns det ett heltal k så att $m \cdot j = 1 + k \cdot n$. Om nu $d|m$ och $d|n$ så gäller $d|(m \cdot j - k \cdot n)$ dvs. $d|1$ och då är $d = 1$. Därför måste $\operatorname{sgd}(m, n) = 1$. Man kan också visa att det omvända gäller så man får att

$$[m]_n \text{ är inverterbar i } \mathbb{Z}_n \quad \Leftrightarrow \quad \operatorname{sgd}(m, n) = 1.$$

Obs

Om p är ett primtal så är alla element i $\mathbb{Z}_p$ som inte är $[0]_p$ inverterbara.

Exempel

Kongruensklasserna $[1]_6$ och $[5]_6$ är de enda som är inverterbara i $\mathbb{Z}_6$.

Euklides algoritm för att räkna $\operatorname{sgd}(m, n)$

- *Antag att $m > n$ ($\operatorname{sgd}(m, m) = m$).*
- *Låt $r_0 = m$ och $r_1 = n$.*
- *Räkna ut q_i och r_i så att $0 \leq r_i < r_{i-1}$ och*

$$r_{i-2} = q_i r_{i-1} + r_i$$

  då $i \geq 2$ så länge $r_{i-1} \neq 0$.
- $\operatorname{sgd}(m, n) = r_{k-1}$ *om* $r_k = 0$.

Varför fungerar Euklides algoritm?

Det följer av ett allmänt resultat att om $r_{i-2} = q_i r_{i-1} + r_i$ så är $\operatorname{sgd}(r_{i-2}, r_{i-1}) = \operatorname{sgd}(r_{i-1}, r_i)$ för alla $i \geq 2$ för vilka $r_{i-1} \neq 0$. Eftersom $d|0$ för alla d gäller $\operatorname{sgd}(r_{k-1}, 0) = r_{k-1}$ vilket innebär att $\operatorname{sgd}(m, n) = \operatorname{sgd}(r_0, r_1) = \ldots = \operatorname{sgd}(r_{k-1}, r_k) = \operatorname{sgd}(r_{k-1}, 0) = r_{k-1}$ om $r_k = 0$.

Exempel

Om vi vill räkna ut $\operatorname{sgd}(634, 36)$ *så får vi följande resultat:*

$$\begin{aligned} 634 &= 17 \cdot 36 + 22 \\ 36 &= 1 \cdot 22 + 14 \\ 22 &= 1 \cdot 14 + 8 \\ 14 &= 1 \cdot 8 + 6 \\ 8 &= 1 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

så att $\operatorname{sgd}(634, 36) = 2$.

Euklides algoritm och inversa element i $\mathbb{Z}_n$

Om man i Euklides algoritm valt $r_0 = m$, $r_1 = n$ *och sedan räknat* q_i *och* r_i *för* $i = 2, \ldots, k$ *med formeln* $r_{i-2} = q_i r_{i-1} + r_i$ *tills* $r_k = 0$, *så att* $r_{k-1} = \operatorname{sgd}(m, n)$ *så kan man räkna baklänges så att man startar med ekvationen* $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ *så får man*

$$\operatorname{sgd}(m, n) = r_{k-1} = r_{k-3} - q_{k-1} r_{k-2}.$$

Sedan sätter man in r_{k-2} *ur ekvationen* $r_{k-2} = r_{k-4} - q_{k-2} r_{k-3}$ *och uttrycker* $\operatorname{sgd}(m, n)$ *med hjälp av* r_{k-4} *och* r_{k-3} *och fortsätter tills man får*

$$\operatorname{sgd}(m, n) = am + bn.$$

Om nu $\operatorname{sgd}(m, n) = 1$ *betyder detta att*

$$[a]_n \cdot [m]_n = [1]_n \quad \textit{dvs.} \quad [a]_n = [m]_n^{-1},$$

och

$$[b]_m \cdot [n]_m = [1]_m \quad \textit{dvs.} \quad [b]_m = [n]_m^{-1}.$$

Exempel

Om man vill räkna $[23]_{67}^{-1}$ *räknar man först ut* $\operatorname{sgd}(67, 23)$ *och får*

$$\begin{aligned} 67 &= 2 \cdot 23 + 21 \\ 23 &= 1 \cdot 21 + 2 \\ 21 &= 10 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

För att uttrycka $\operatorname{sgd}(67, 23)$ *med hjälp av* 67 *och* 23 *räknar vi baklänges:*

$$\begin{aligned} \operatorname{sgd}(67, 23) = 1 &= 21 - 10 \cdot 2 = 1 \cdot 21 - 10 \cdot (23 - 1 \cdot 21) \\ &= -10 \cdot 23 + 11 \cdot 21 = -10 \cdot 23 + 11 \cdot (67 - 2 \cdot 23) \\ &= 11 \cdot 67 - 32 \cdot 23 \end{aligned}$$

Detta innebär att $(-32) \cdot 23 = 1 - 11 \cdot 67$ *så att* $(-32) \cdot 23 \equiv 1 \pmod{67}$ *vilket är det samma som att* $[23]_{67}^{-1} = [-32]_{67} = [-32 + 67]_{67} = [35]_{67}$.

Eulers φ-funktion

$$\begin{aligned} \varphi(n) &= \textit{antalet tal i mängden } \{\, m \in \mathbb{Z} : 0 \le m \le n - 1, \operatorname{sgd}(m, n) = 1 \,\}, \\ &= \textit{antalet element i } \mathbb{Z}_n \textit{ som har en en invers.} \end{aligned}$$

Eulers teorem

Om $\operatorname{sgd}(a, n) = 1$ *och* $n > 1$ *så är*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Fermats lilla teorem

Om p är ett primtal och $\text{sgd}\,(a,p)=1$ *så är*

$$a^{p-1}\equiv 1 \pmod{p}.$$

Potenser i $\mathbb{Z}_p$ då p är ett primtal

Om man skall räkna ut $\text{mod}\,(a^m,p)$ *då p är ett primtal får man naturligtvis 0 om* $\text{sgd}\,(a,p)\neq 1$ *(för då är* $\text{sgd}\,(a,p)=p$ *och $p|a$ eftersom p är ett primtal) och annars kan man utnyttja det faktum att* $a^{p-1}\equiv 1 \pmod{p}$ *för det innebär att* $a^m\equiv a^{\text{mod}\,(m,p-1)} \pmod{p}$ *vilket kan vara mycket enklare att räkna ut.*

Eulers teorem, bevis

Antag att $\alpha_1,\dots,\alpha_{\phi(n)}$ *är de invertibla elementen i* $\mathbb{Z}_n$. *Eftersom* $\text{sgd}\,(a,n)=1$ *har också* $[a]_n$ *en invers och eftersom* $\alpha\cdot\beta$ *är invertibelt on* α *och* β *är det, är också* $[a]_n\cdot\alpha_j$ *invertibelt för alla j. Om nu* $[a]_n\cdot\alpha_j=[a]_n\cdot\alpha_k$ *så är* $\alpha_j=[a]_n^{-1}\cdot[a]_n\alpha_j=[a]_n^{-1}\cdot[a]_n\cdot\alpha_k=\alpha_k$ *vilket innebär att elementen* $[a]_n\alpha_1,\dots[a]_n\alpha_{\varphi(n)}$ *är elementen* $\alpha_1,\dots,\alpha_{\phi(n)}$ *eventuellt i en annan ordning. Men produkterna är de samma, dvs.*

$$[a]_n^{\varphi(n)}\Pi_{i=1}^{\varphi(n)}\alpha_i=\Pi_{i=1}^{\varphi(n)}\left([a]_n\cdot\alpha_i\right)=\Pi_{i=1}^{\varphi(n)}\alpha_i.$$

Eftersom varje element α_i *är inverterbart, kan vi dividera bort alla* α_i *och slutresultatet är att* $[a]_n^{\varphi(n)}$ *är "ett", dvs.* $a^{\varphi(n)}\equiv 1 \pmod{n}$.

RSA-algoritmen

I RSA-algoritmen används en publik nyckel (n,k) *för kryptering och en privat nyckel* (n,d) *för dekryptering:*

- *Kryptering: "Meddelandet" a, som är ett tal mellan 0 och* $n-1$ *krypteras till* $b=\text{mod}\,(a^k,n)$.
- *Det mottagna meddelandet b dekrypteras till* $a=\text{mod}\,(b^d,n)$.

Ideen är den att vem som helst kan skicka meddelanden krypterade med den publika nyckeln men bara den som känner till den privata nyckeln, som är "svår" at räkna ut bara med hjälp av n och k, kan dekryptera meddelandet.

Hur skall nycklarna i RSA-algoritmen väljas?

- $n=pq$ *där p och q är två olika "mycket stora" primtal.*
- k *är ett "inte alltför litet" tal så att* $\text{sgd}(k,m)=1$ *där* $m=(p-1)\cdot(q-1)$ *(och det "svåra" med att räkna ut d är att bestämma p och q och därmed m om man bara känner till n).*
- *Med hjälp av Euklides algoritm kan d bestämmas så att* $[d]_m=[k]_m^{-1}$.

Varför fungerar RSA-algoritmen?

- *Antag för enkelhets skull att* $\text{sgd}\,(a,n)=1$.
- *Man kan visa att* $\varphi(n)=m$.
- *Enligt Eulers teorem gäller* $a^m\equiv 1 \pmod{n}$
- *Eftersom* $k\cdot d=1+r\cdot m$ *är*

$$\left[b^d\right]_n=\left[a^{k\cdot d}\right]_n=\left[a^{1+r\cdot m}\right]_n=[a]_n\cdot[a^m]_n^r=[a]_n\cdot[1]_n^r=[a]_n,$$

vilket betyder att $\text{mod}\,(b^d,n)=\text{mod}\,(a,n)=a$.

Vad händer om $\text{sgd}\,(a,n) \neq 1$?

- *Eftersom man antar att* $0 < a < n$ *så är* $\text{sgd}\,(a,n) \neq 1$ *endast då* $p|a$ *eller* $q|a$. *Anta att* $p|a$ *så att* $a = p^j \cdot c$ *där* $\text{sgd}\,(c,n) = 1$
- *Nu är* $[b^d]_n = [((p^j \cdot c)^k)^d]_n = [(p^k)^d]_n^j \cdot [(c^k)^d]_n$ *och eftersom* $\text{sgd}\,(c,n) = 1$ *så är* $[(c^k)^d]_n = [c]_n$ *och det återstår att visa att* $[[(p^k)^d]_n = [p]_n$ *för då är* $[b^d]_n = [p]_n^j \cdot [c]_n = [p^j \cdot c]_n = [a]_n$.
- *Eftersom* q *är ett primtal och* $p \neq q$ *så är* $\text{sgd}\,(p,q) = 1$ *och därför följer det av enligt Fermats teorem att* $p^{q-1} \equiv 1 \pmod{q}$.
- *Då är också* $p^{(q-1)(p-1)r} \equiv 1 \pmod{q}$ *dvs.* $p^{(q-1)(p-1)r} = 1 + sq$ *och därför också* $p^{1+(q-1)(p-1)r} = p + spq$ *dvs.* $[p^{1+m\cdot r}]_n = [p]_n$ *vilket visar att* $[(p^k)^d]_n = [p]_n = [a]_n$.

Algoritmen fungerar alltså också i detta fall!

Exempel

Om man med RSA-algoritmen skall kryptera meddelandet 9 *och använda den publika nyckeln* $(55,23)$ *så skall man räkna ut* $\text{mod}\,(9^{23},55)$. *För att göra räkningen enklare observerar man först att* $23 = 2^4 + 2^2 + 2^1 + 2^0$ *så att* $9^{23} = (((9^2)^2)^2)^2 \cdot (9^2)^2 \cdot 9^2 \cdot 9$ *och man får*

$$\text{mod}\,(9^2,55) = \text{mod}\,(81,55) = 26,$$
$$\text{mod}\,((9^2)^2,55) = \text{mod}\,(26^2,55) = \text{mod}\,(676,55) = 16,$$
$$\text{mod}\,(((9^2)^2)^2,55) = \text{mod}\,(16^2,55) = \text{mod}\,(256,55) = 36,$$
$$\text{mod}\,((((9^2)^2)^2)^2,55) = \text{mod}\,(36^2,55) = \text{mod}\,((-19)^2,55)$$
$$= \text{mod}\,(361,55) = 31,$$
$$\text{mod}\,(9^2 \cdot 9,55) = \text{mod}\,(26 \cdot 9,55) = \text{mod}\,(234,55) = 14,$$
$$\text{mod}\,((9^2)^2 \cdot 9^2 \cdot 9,55) = \text{mod}\,(16 \cdot 14,55) = \text{mod}\,(224,55) = 4,$$
$$\text{mod}\,((((9^2)^2)^2)^2 \cdot (9^2)^2 \cdot 9^2 \cdot 9,55) = \text{mod}\,(31 \cdot 4,55)$$
$$= \text{mod}\,(124,55) = 14,$$

så att $\text{mod}\,(9^{23},55) = 14$.

Exempel, forts.

Om man vill dekryptera meddelandet 14 *måste man känna till den privata nyckeln och den är* $(55,7)$ *därför att* $55 = 5 \cdot 11$, $(5-1)\cdot(11-1) = 40$ *och* $\text{mod}\,(23 \cdot 7,40) = \text{mod}\,(161,40) = 1$. *För dekryptering observerar man att* $7 = 2^2 + 2^1 + 2^0$ *så att* $14^7 = (14^2)^2 \cdot 14^2 \cdot 14$ *och man får*

$$\text{mod}\,(14^2,55) = \text{mod}\,(196,55) = 31,$$
$$\text{mod}\,((14^2)^2,55) = \text{mod}\,(31^2,55) = \text{mod}\,(961,55) = 26,$$
$$\text{mod}\,(14^2 \cdot 14,55) = \text{mod}\,(31 \cdot 14,55) = \text{mod}\,(434,55) = 49,$$
$$\text{mod}\,((14^2)^2 \cdot 14^2 \cdot 14,55) = \text{mod}\,(26 \cdot 49,55)$$
$$= \text{mod}\,(26 \cdot (-6),55) = \text{mod}\,(-156,55) = 9,$$

så att $\text{mod}\,(14^7,55) = 9$.