KTH Matematik

KTHs Matematiska Cirkel

Talteori

Andreas Enblom
Alan Sola

Institutionen för matematik, 2008
Finansierat av Marianne och Marcus Wallenbergs Stiftelse

5 Modulär aritmetik

5.1 Moduloräkning

Vi kommer nu fram till moduloräkning. Detta är ett lite annorlunda sätt att räkna med heltal på, även om det egentligen bygger på de vanliga räknesätten. Allt utgår från följande definition:

Definition 5.1.1. Låt $n \geqslant 1$ vara ett heltal. Vi säger att heltalen a och b är *kongruenta modulo* n, och skriver

$$a \equiv b \pmod{n},$$

om $n \mid (a-b)$.

Exempel 5.1.2. Låt $n = 12$. Exempelvis har vi att

$$16 \equiv 4 \pmod{12}, \quad -27 \equiv -3 \pmod{12} \quad \text{och} \quad 22 \equiv -2 \pmod{12},$$

eftersom 12 är en delare till alla tre talen $16-4=12$, $(-27)-(-3)=-24$ och $22-(-2)=24$. ▲

När man räknar modulo ett tal, exempelvis 12, kan man se det som att man betraktar alla tal som är kongruenta med varandra som samma tal. Enligt exemplet ovan är 16 och 4 "samma tal" modulo 12, liksom 22 och -2. Därför verkar det inte alldeles orimligt, så länge man räknar modulo 12, att $16+22$ borde bli "samma tal" som $4-2$. Mer korrekt kan vi skriva detta som

$$16+22 \equiv 4-2 \pmod{12}.$$

Denna kongruens gäller eftersom

$$16+22-(4-2) = 36 = 12 \cdot 3.$$

Detta beteende är ingen speciellt för $n = 12$, utan gäller i allmänhet, vilket visas nedan.

Sats 5.1.3. *Låt n vara ett positivt heltal. Antag att heltalen $a, \tilde{a}$ samt $b, \tilde{b}$ uppfyller*

$$a \equiv \tilde{a} \pmod{n} \quad \textit{och} \quad b \equiv \tilde{b} \pmod{n}.$$

Då gäller

$$a+b \equiv \tilde{a}+\tilde{b} \pmod{n}$$

samt

$$a \cdot b \equiv \tilde{a} \cdot \tilde{b} \pmod{n}.$$

Bevis. Per definition vet vi att $n \mid (a-\tilde{a})$ och $n \mid (b-\tilde{b})$. Det betyder att det finns heltal x och y sådana att

$$a-\tilde{a} = nx \quad \text{och} \quad b-\tilde{b} = ny.$$

Nu följer

$$\begin{aligned}(a+b)-(\tilde{a}+\tilde{b}) &= (a-\tilde{a})+(b-\tilde{b})\\ &= nx+ny\\ &= n\cdot(x+y).\end{aligned}$$

Alltså gäller $n \mid (a+b)-(\tilde{a}+\tilde{b})$, vilket betyder att

$$a+b \equiv \tilde{a}+\tilde{b} \pmod{n}.$$

Vidare,

$$\begin{aligned}ab-\tilde{a}\tilde{b} &= ab-a\tilde{b}+a\tilde{b}-\tilde{a}\tilde{b}\\ &= a\cdot(b-\tilde{b})+(a-\tilde{a})\cdot b\\ &= a\cdot ny+nx\cdot b\\ &= n\cdot(ya+xb),\end{aligned}$$

och därmed $n \mid (ab-\tilde{a}\tilde{b})$, det vill säga

$$ab \equiv \tilde{a}\tilde{b} \pmod{n}. \qquad \square$$

Denna sats visar en av de stora fördelarna med moduloräkning. Genom att använda den kan vissa beräkningar förenklas väsentligt. Låt oss illustrera detta med ett par exempel.

Exempel 5.1.4. Låt $a = 228 \cdot 115$. Vi vet att det finns heltal q och r sådana att $a = 8 \cdot q + r$, där $0 \leqslant r < 8$. Bestäm r.

Lösning. Börja med att utföra heltalsdivision med 8 av talen 228 och 115:

$$228 = 8 \cdot 28 + 4 \quad \text{och} \quad 115 = 8 \cdot 14 + 3.$$

Detta betyder att $228 - 4 = 8 \cdot 28$ och $115 - 3 = 8 \cdot 14$, det vill säga att $8 \mid (228-4)$ och $8 \mid (115-3)$. Alltså gäller

$$228 \equiv 4 \pmod{8} \quad \text{och} \quad 115 \equiv 3 \pmod{8}.$$

Enligt satsen ovan får vi

$$a = 228 \cdot 115 \equiv 4 \cdot 3 = 12 \pmod{8}.$$

Men eftersom det uppenbarligen är så att $12 \equiv 4 \pmod{8}$ så följer

$$a \equiv 4 \pmod{8}$$

Alltså har vi $8 \mid (a-4)$, vilket per definition betyder att det finns ett heltal q sådant att $a - 4 = 8 \cdot q$. Vi får alltså

$$a = 8 \cdot q + 4, \quad \text{och därmed} \quad r = 4. \qquad \blacktriangle$$

Poängen med ovanstående exempel är att det är mycket enklare att heltalsdividera talen 228 och 115 med 8 än vad det är att utföra heltalsdivisionen med deras produkt $a = 228 \cdot 115 = 26\,200$.

Exempel 5.1.5. Låt $a = 3^{100}$. Det finns heltal q och r, där $0 \leqslant r < 6$ sådana att $a = 6 \cdot q + r$. Bestäm r.

Lösning. Observera att

$$3^3 = 27 = 6 \cdot 4 + 3 \equiv 3 \pmod{6}.$$

Alltså gäller

$$a = 3^{100} = 3 \cdot 3^{99} = 3 \cdot (3^3)^{33} \equiv 3 \cdot 3^{33} = 3 \cdot (3^3)^{11} \equiv 3 \cdot 3^{11} = 3^{12} \pmod{6}.$$

Vidare följer

$$a \equiv 3^{12} = (3^3)^4 \equiv 3^4 = 3 \cdot 3^3 \equiv 3 \cdot 3 = 9 \equiv 3 \pmod{6},$$

vilket betyder att vi kan skriva

$$a = 6 \cdot q + 3,$$

för något heltal q. Alltså får vi att $r = 3$. ▲

I detta exempel får vi en väldigt stor vinst. Talet $a = 3^{100}$ är enormt stort, om man skriver ut det så består det av 48 siffror, och antagligen alldeles för stort för de flesta miniräknare. Så utan moduloräkning blir det mycket svårt att bestämma r.

Sats 5.1.6. *Låt $n \geqslant 1$ vara ett heltal. För varje heltal a som är relativt prima med n gäller följande:*

1. *Det finns ett heltal x som löser ekvationen $ax \equiv 1 \pmod{n}$.*
2. *Om heltalen b, c uppfyller $ab \equiv ac \pmod{n}$ så måste $b \equiv c \pmod{n}$.*

Bevis. Eftersom a och n är relativt prima finns enligt Sats 2.2.3 heltal x, y sådana att

$$1 = xa + yn.$$

Detta betyder att $1 - xa = n \cdot y$, det vill säga att $n \mid (1 - xa)$, och därmed gäller $1 \equiv xa \pmod{n}$, vilket visar punkt 1.

För att visa punkt 2, antag att heltalen b, c uppfyller $ab \equiv ac \pmod{n}$. Per definition gäller

$$n \mid (ab - ac) = a \cdot (b - c).$$

Men eftersom n och a är relativt prima följer det från Sats 2.2.5 att $n \mid (b - c)$. Alltså får vi

$$b \equiv c \pmod{n}.$$ □

5.2 Ringen $\mathbb{Z}_n$

Låt oss nu införa ett alternativt sätt att se på moduloräkning. Detta sätt kan i vissa fall vara behändigare. Låt $n \geqslant 1$ vara ett fixerat heltal.

Givet ett heltal a, vet vi enligt Sats 1.3.1 att det finns heltal q och r, där r uppfyller $0 \leqslant r < n$, sådana att

$$a = n \cdot q + r.$$

Talet r är alltså resten vid heltalsdivision av a med n. Notera att

$$a \equiv r \pmod{n},$$

eftersom n uppenbarligen delar $a - r = nq$. I själva verket är r det enda tal som uppfyller både $a \equiv r \pmod{n}$ och $0 \leqslant r < n$. Vi kallar hädanefter r för *resten av a modulo n* och skriver

$$r = \mathrm{R}_n(a).$$

Det är alltså skillnad på att skriva $\mathrm{R}_n(a)$ och $a \equiv b \pmod{n}$. Det första uttrycket, $\mathrm{R}_n(a)$ är ett tal r som uppfyller $0 \leqslant r < n$, medan det andra uttrycket beskriver en relation mellan talen a och b.

Exempel 5.2.1. Låt $n = 13$ och $a = 15$. Vi har att

$$\mathrm{R}_n(a) = 2,$$

eftersom

$$a = n \cdot 1 + 2.$$

Observera igen att $\mathrm{R}_n(a)$ är ett tal r som uppfyller *både* $0 \leqslant r < n$ *och* $a \equiv r \pmod{n}$. Det finns oändligt många tal b som uppfyller $a \equiv b \pmod{n}$, exempelvis har vi att

$$15 \equiv -11 \pmod{13}, \quad 15 \equiv 81 \pmod{13}, \quad \text{och} \quad 15 \equiv 11\,015 \pmod{13}.$$

Men det är bara talet 2 bland dessa tal som ligger i intervallet $0 \leqslant b < n$. ▲

Exempel 5.2.2. Låt $n = 15$. Då gäller

$$\mathrm{R}_n(19) = 4, \quad \mathrm{R}_n(-27) = 3, \quad \mathrm{R}_n(11) = 11, \quad \mathrm{R}_n(30) = 0. \qquad ▲$$

Ännu enklare blir det för tal som 10 och 100:

Exempel 5.2.3. Vi har att

$$\mathrm{R}_{10}(67) = 7, \quad \mathrm{R}_{10}(4\,711) = 1, \quad \mathrm{R}_{10}(-118) = 2\,(= 10 - 8).$$

Dessutom gäller

$$\mathrm{R}_{100}(1\,234) = 34, \qquad \mathrm{R}_{100}(-256) = 44\,(= 100 - 56). \qquad ▲$$

Nu inför vi *ringen* $\mathbb{Z}_n$. Vi låter helt enkelt detta vara mängden

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Observera att $\mathrm{R}_n(a)$ är ett element i ringen $\mathbb{Z}_n$ för alla heltal a, eftersom $\mathrm{R}_n(a)$ per definition uppfyller $0 \leqslant \mathrm{R}_n(a) < n$. Mängden $\mathbb{Z}_n$ innehåller helt enkelt alla "rester modulo n".

Den stora vinsten med att införa dessa begrepp är att det förenklar språket för oss. Vi tillåter oss nämligen att "räkna", det vill säga utföra addition och multiplikation, *i ringen* $\mathbb{Z}_n$. Detta fungerar som vanlig addition och multiplikation, men resultatet av uträkningarna väljs *modulo* n.

Alltså: när vi räknar i ringen $\mathbb{Z}_n$ menar vi med $a+b$ egentligen talet $\mathrm{R}_n(a+b)$, och med $a \cdot b$ menar vi talet $\mathrm{R}_n(a \cdot b)$. På detta sätt kommer vi att som resultat av uträkningarna få ett tal r som uppfyller $0 \leqslant r < n$, det vill säga $r \in \mathbb{Z}_n$, och som är kongruent modulo n med det "vanliga" resultatet av uträkningen.

Exempel 5.2.4. Låt $n = 5$. Eftersom exempelvis

$$3 + 8 = 11 \equiv 1 \pmod{n},$$

så säger vi att

$$3 + 8 = 1 \text{ i ringen } \mathbb{Z}_n.$$

På samma sätt säger vi att

$$3 \cdot 8 = 4 \text{ i ringen } \mathbb{Z}_n,$$

eftersom $3 \cdot 8 = 24 \equiv 4 \pmod{n}$. ▲

En av de allra mest självklara matematiska identiteterna är $1 + 1 = 2$. Det visar sig dock när man använder moduloräkning att denna identitet kanske inte är så självklar när allt kommer omkring:

Exempel 5.2.5. Observera att

$$1 + 1 \equiv 0 \pmod{2}.$$

Utan att vara det minsta inkorrekt kan man alltså säga att

$$1 + 1 = 0,$$

om vi bara lägger till "i ringen $\mathbb{Z}_2$". ▲

5.3 Satser av Euler och Fermat

Nu kommer vi till en av matematikens mest berömda satser: *Fermats lilla sats.* Vi börjar med att bevisa *Eulers sats*, från vilken Fermats lilla sats följer.

Definition 5.3.1. Låt $n \geqslant 1$ vara ett heltal, och $\phi(n)$ vara antalet tal x med $1 \leqslant x < n$ som är relativt prima med n. Vi kallar ϕ *Eulers ϕ-funktion.*

Exempel 5.3.2. Om $n = 12$, så tittar vi på talen $x = 1, 2, \ldots, 11$. Vi observerar följande:

$$\begin{array}{llll} \text{sgd}\,(1,12) = 1, & \text{sgd}\,(2,12) = 2, & \text{sgd}\,(3,12) = 3, & \text{sgd}\,(4,12) = 4, \\ \text{sgd}\,(5,12) = 1, & \text{sgd}\,(6,12) = 6, & \text{sgd}\,(7,12) = 1, & \text{sgd}\,(8,12) = 4, \\ \text{sgd}\,(9,12) = 3, & \text{sgd}\,(10,12) = 2, & \text{sgd}\,(11,12) = 1. & \end{array}$$

Alltså är det precis de fyra talen 1, 5, 7 och 11 som är relativt prima med 12. Detta betyder att $\phi(12) = 4$. ▲

Exempel 5.3.3. Om p är ett primtal kommer alltid $\phi(p) = p - 1$, eftersom alla talen $1, 2, 3, \ldots, p-1$ är relativt prima med p. ▲

Sats 5.3.4 (Eulers sats). *Let $n \geqslant 1$ vara ett heltal. Låt a vara ett heltal sådant att a och n är relativt prima. Då gäller*

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

Bevis. Låt $m = \phi(n)$. Enligt definitionen av ϕ-funktionen, finns det m tal bland $1, 2, \ldots, n-1$ som är relativt prima med n. Kalla dessa tal $b_1, b_2, \ldots, b_m$. Låt

$$c_1 = ab_1, \quad c_2 = ab_2, \quad \ldots, \quad c_m = ab_m.$$

Vi vet enligt Sats 1.3.1 att det finns tal $r_1, r_2, \ldots, r_m$ med $0 \leqslant r_j < n$, och tal $q_1, q_2, \ldots, q_m$ sådana att

$$c_j = n \cdot q_j + r_j, \quad j = 1, 2, \ldots, m.$$

Detta betyder bland annat att

$$c_j \equiv r_j \pmod{n}, \quad j = 1, 2, \ldots, m. \tag{5.1}$$

Till att börja med måste alla talen $r_1, r_2, \ldots, r_m$ vara olika, ty om $r_j = r_k$, där $j \neq k$, så får vi att $c_j - c_k = n \cdot q_j - n \cdot q_k = n \cdot (q_j - q_k)$, vilket betyder att

$$n \mid (c_j - c_k) = a \cdot (b_j - b_k),$$

och eftersom n och a är relativt prima måste enligt Sats 2.2.5 $n \mid (b_j - b_k)$, vilket är omöjligt eftersom både $1 \leqslant b_j \leqslant n - 1$ och $1 \leqslant b_k \leqslant n - 1$, och dessutom $b_j \neq b_k$.

Vidare, låt oss visa att r_j och n är relativt prima. Antag motsatsen, det vill säga att $\text{sgd}\,(r_j, n) > 1$. Då finns det ett tal $x > 1$ som delar både r_j och n. Vi kan skriva $r_j = x\tilde{r}$ och $n = x\tilde{n}$, för några heltal $\tilde{r}$ och $\tilde{n}$. Vi har att $\text{sgd}\,(x, a) = 1$ eftersom om det fanns ett tal $y > 1$ som delade både x och a så skulle det talet också dela $n = x\tilde{n}$, vilket skulle betyda att y vore en gemensam delare till a och n och detta är omöjligt eftersom a och n är relativt prima. Nu har vi

$$c_j = n \cdot q_j + r_j = x \cdot (\tilde{n} q_j + \tilde{r}),$$

vilket betyder att x är en delare till $c_j = ab_j$. Eftersom a och x är relativt prima måste $x \mid b_j$, enligt Sats 2.2.5. Men detta är omöjligt, eftersom $x > 1$ i så fall skulle vara en gemensam delare till n och b_j. Men vi vet från definitionen av b_j att n och b_j är relativt prima. Alltså är det inledande antagandet omöjligt, vilket betyder att r_j och n är relativt prima, för varje $j = 1, 2, \ldots, m$.

Notera i förbifarten att detta innebär att $r_j \neq 0$, eftersom om det vore så att $r_j = 0$ så skulle $\operatorname{sgd}(r_j, n) = n$ (se Exempel 2.1.6), men vi vet ju nu att $\operatorname{sgd}(r_j, n) = 1$.

Vi har alltså visat att $r_1, r_2, \ldots, r_m$ är m stycken olika tal som alla uppfyller $1 \leqslant r_j \leqslant n-1$, och att r_j och n är relativt prima. Men enligt definitionen av talen $b_1, b_2, \ldots, b_m$ var dessa alla tal som uppfyllde detta. Alltså har vi att

$$r_1, r_2, \ldots, r_m \quad \text{är precis talen} \quad b_1, b_2, \ldots, b_m,$$

även om ordningen på talen möjligtvis skiljer sig i de två fallen. Det följer att

$$b_1 b_2 \cdots b_m = r_1 r_2 \cdots r_m.$$

Från (5.1) får vi nu att

$$\begin{aligned} b_1 b_2 \cdots b_m \cdot a^m &= (ab_1)(ab_2) \cdots (ab_m) \\ &= c_1 c_2 \cdots c_m \\ &\equiv r_1 r_2 \cdot r_m = b_1 b_2 \cdots b_m \pmod{n}, \end{aligned}$$

det vill säga att

$$b_1 b_2 \cdots b_m \cdot a^m \equiv b_1 b_2 \cdots b_m \cdot 1 \pmod{n}.$$

Eftersom b_j och n är relativt prima, för alla $j = 1, 2, \ldots, m$, så kommer också talen $b_1 b_2 \cdots b_m$ och n vara relativt prima (att visa detta var Övning 3.4). Nu följer det från Sats 5.1.6 att

$$a^m \equiv 1 \pmod{n}. \qquad \square$$

Följdsats 5.3.5 (Fermats lilla sats)**.** *Låt p vara ett primtal. Då gäller*

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

för alla heltal a som inte delas av p.

Bevis. Eftersom a och p är relativt prima så fort p inte delar a, och eftersom $\phi(p) = p - 1$ så följer detta från Eulers sats. $\square$

Övningar

Övning 5.1. Beräkna $4 + 3$ i ringen $\mathbb{Z}_5$, $8 \cdot 7$ i ringen $\mathbb{Z}_9$ och 3^{100} i ringen $\mathbb{Z}_{10}$.

Övning 5.2. Fixera ett heltal $n \geqslant 1$. Visa följande egenskaper för modulo-relationen:

1. För varje heltal a gäller $a \equiv a \pmod{n}$.
2. Låt a och b vara heltal. Om $a \equiv b \pmod{n}$ så gäller också $b \equiv a \pmod{n}$.
3. Antag att heltalen a, b, c uppfyller $a \equiv b \pmod{n}$ och $b \equiv c \pmod{n}$. Då gäller $a \equiv c \pmod{n}$.

Anmärkning: Detta visar att modulorelationen är en så kallad *ekvivalensrelation.*

Övning 5.3. Låt $n \geqslant 1$ vara ett heltal. Antag att $a \equiv b \pmod{n}$. Visa att $-a \equiv -b \pmod{n}$.

Övning 5.4. Bevisa följande variant av Fermats lilla sats:

Låt p vara ett primtal, och $a \in \mathbb{Z}$. Då gäller

$$a^p \equiv a \pmod{n}.$$