KAPITEL 4 - INLEDANDE TALTEORI

Talteori, eller den högre aritmetiken, är studiet av de hela talen. Denna gren av matematiken lades på fast grund av Carl Friedrich Gauss (1777-1855), en av tidernas främsta matematiker.

De hela talen är $0, \pm 1, \pm 2, \pm 3, \ldots$ osv. Man brukar ofta följa Gauss konvention att beteckna mängden av de hela talen med symbolen $\mathbb{Z}$ efter tyskans Zahl (tal.)

I delar av texten kommer vi att bara skriva "tal" men vi *menar* ändå heltal.

1. Delbarhet och primtal

Om man väljer två godtyckliga heltal ur $\mathbb{Z}$, låt oss kalla de talen a och b. Då kan vi addera dessa tal $(a+b)$, vi kan subtrahera dessa tal $(a-b)$ eller multiplicera dessa tal $(a \cdot b)$ och vi får alltid ett heltal som resultat. Detta brukar kallas för att mängden av heltal är *sluten* under addition, subtraktion och multiplikation. Vi kommer inte utanför $\mathbb{Z}$ om vi använder dessa vanliga operationer.

Däremot kan vi inte utan vidare *dividera* heltal med varandra och förvänta oss att få ett nytt heltal. Vi har till exempel att $1/2$ är 0.5 som *inte* är ett heltal. $3/2$ är inte heller ett heltal. Ibland får vi dock ett heltal då vi dividerar två heltal. Exempelvis är $6/3 = 2$, och talet 2 är förstås ett heltal. Här inför vi vårt första begrepp: delbarhet.

Definition: Ett heltal b sägs vara *delbart* med ett heltal a om det finns ett heltal k sådant att $b = k \cdot a$. Vi säger också att a delar b och använder beteckningen $a|b$. Vi kan också säga att b är en *multipel* av a. Vi kan också säga att a är en *faktor* i b. Om b inte är delbart med a skriver vi $a \nmid b$ och vi utläser detta som att a delar *inte* b. (Eller b är *inte* en multipel av a, eller a är *inte* en faktor i b etc.) Med kvantorer kan vi skriva $a|b \Leftrightarrow \exists k \in \mathbb{Z} : b = k \cdot a$.

Exempel: $3|12$ ty det finns ett heltal k som uppfyller $12 = k \cdot 3$, talet k är här 4.

Exempel: $3 \nmid 13$ ty hur vi än väljer k kan vi aldrig uppfylla $13 = k \cdot 3$ för ett *heltal* k. Hur vet vi det? Vi använder ett indirekt bevis. Antag att vi funnit ett k som uppfyller $13 = k \cdot 3$. Vilket skulle detta vara? Undersök ekvationen $13 = k \cdot 3 \Leftrightarrow k = 13/3 = 4.33333...$, men detta k är ju inget heltal! Vi får en motsägelse, k måste ju vara ett heltal, och alltså kan inte 3 dela 13, det vill säga vi har fastställt att $3 \nmid 13$.

Vilka tal delar 0? Testa, $2|0$ ty det finns ett tal k som uppfyller $0 = k \cdot 2$, nämligen talet 0 självt. Vi kan fortsätta på samma sätt: $3|0$, ty vi kan välja $k = 0$ här också. $0 = 0 \cdot 3$. Alltså gäller 3—0. Efter detta resonemang inser vi att alla tal delar 0. Vi har en sats:

Sats: Alla tal delar 0.

Bevis: Vi ska visa att $n|0$ för ett godtyckligt valt n. Låt således n vara vilket tal som helst. Identiteten $0 = 0 \cdot n$ visar att n finns som faktor i 0 vilket är samma sak som att $n|0$. Eftersom n var godtyckligt valt måste $n|0$ gälla för alla n vilket skulle bevisas.

Vi kan få en bättre förståelse för satsen om vi begrundar delbarhetsbegreppet. Att $3|12$ innebär ju att 12 kan delas upp i 3 lika stora delar, $12 = 4 + 4 + 4$, varje del är här 4. Givetvis kan ju 0 delas upp i hur många lika stora delar vi vill eftersom varje del är 0 själv. $3|0$? Javisst, för $0 = 0 + 0 + 0$ (tre nollor.) $5|0$? Javisst för $0 = 0 + 0 + 0 + 0 + 0$ (fem nollor).

Vilka tal är delbara med 1? Vi undersöker några fall. Är det så att $1|4$? Finns ett k sådant att $4 = k \cdot 1$? Ja, 4 själv fungerar som k. På ett liknande sätt som då vi insåg att alla tal är delar 0 kan vi också inse att 1 delar alla tal. Vi har en till sats vars bevis vi lämnar som övning åt läsaren.

Sats: Talet 1 delar alla tal.

Bevis: Genomför beviset själv.

Alla tal är delbara med 1 och -1. Alla tal är också delbara med minus sig själv och sig själv. Vi tittar på några exempel.

Exempel:

(1) 25 är delbart med 1 ty $25 = 25 \cdot 1$ så vårt k i delbarhetsdefinitionen blir 25 själv.
(2) 25 är delbart med -1 ty $25 = -25 \cdot -1$ så vårt k i delbarhetsdefinitionen blir -25.
(3) 25 är delbart med 25 ty $25 = 1 \cdot 25$ så vårt k i delbarhetsdefinitionen blir 1.
(4) 25 är delbart med -25 ty $25 = -1 \cdot -25$ så vårt k i delbarhetsdefinitionen blir -1.

Exemplet leder oss att formulera följande sats:

Sats: Låt n vara ett godtyckligt heltal. Då är n delbart med $\pm n$ samt ± 1.

Bevis: Genomför beviset själv med exemplet med 25 som underlag.

Som den sista satsen säger är alltså alla heltal delbara med ± 1 och $\pm$ sig själv. Heltal kan också vara delbara med andra tal än dessa, till exempel är 25 delbart med ± 5. Tal som emellertid inte har några andra delare än dessa spelar en mycket viktig roll inom talteorin och kryptering. Dessa tal kallas *primtal* och vi ger en formell definition. Detta är en av de viktigaste definitionerna i talteorin.

Definition: Låt $p > 1$ vara ett givet positivt heltal. Om p inte har några andra delare än $\pm p$ och ± 1 kallas p ett *primtal*.

Vi räknar *inte* talet 1 som ett primtal av skäl som kommer att klarna senare.

Exempel: De första 10 primtalen är 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Dessa tal går inte att faktorisera i andra faktorer än $\pm$ sig själva och ± 1.

Exempel: De andra talen i intervallet 2 till 31 är 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28. Dessa tal går alla att dela upp i faktorer som inte är $\pm$ talet själv eller ± 1. Vi har $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 4 \cdot 2$, $9 = 3 \cdot 3$, $10 = 5 \cdot 2$, $12 = 6 \cdot 2$, och så vidare. Alla tal kan skrivas som produkten av två tal där inget av talen är ± 1.

Vi ger en alternativ definition av primtal med kvantorer (vi går också över på bara positiva tal i den här formuleringen – vi bortser alltså just här från negativa delare):

Definition 3.3: Låt n vara ett positivt heltal större än 1. Då kallas n ett *primtal* om och endast om

$$\forall r \in \mathbb{Z}^+ : \forall s \in \mathbb{Z}^+ : n = r \cdot s \Rightarrow r = 1 \vee s = 1.$$

Vad definitionen säger är att ett tal är primtal omm det bara kan delas upp i faktorer som är 1 eller sig själv – om en av faktorerna av (r och s) är 1 så blir ju den andra automatiskt lika med själv (n).

Då vi faktoriserar positiva heltal delar vi gradvis upp talet i mindre och mindre faktorer. Till exempel delades 24 upp i faktorerna 6 respektive 4 i exemplet ovan. Vi kan emellertid fortsätta och dela upp 6 i faktorerna 2 och 3 respektive 4 i faktorerna 2 och 2. Nu kommer vi inte längre eftersom *alla* faktorer är primtal.
Vi säger att vi delat upp talet 24 i *primtalsfaktorer* och vi har alltså $24 = 6 \cdot 4 = 3 \cdot 2 \cdot 2 \cdot 2$. När botten är nådd och alla faktorer är primtal brukar man skriva faktorerna i storleksordning och samla alla 2:or för sig, alla 3:or för sig och så vidare.
Vi har alltså $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$. Vi ser på ett par exempel.

Exempel: $36 = 6 \cdot 6 = 3 \cdot 2 \cdot 3 \cdot 2 = 2^2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$.

Exempel: $120 = 12 \cdot 10 = 4 \cdot 3 \cdot 5 \cdot 2 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 2 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$.

Exempel: $252 = 2 \cdot 126 = 2 \cdot 2 \cdot 63 = 2 \cdot 2 \cdot 9 \cdot 7 = 2^2 \cdot 3^2 \cdot 7$.

Vi ser att vi alltid kan sortera primtalsfaktorerna i storleksordning och att vi kan uttrycka varje faktorisering med exponenter på varje primtalsfaktor. Sålunda kan vi säga att talet 36 innehåller 2 stycken 2:or och 2 stycken 3:or. Talet 120 innehåller 3 stycken 2:or, en 3:a och en 5:a. Slutligen, talet 252 innehåller 2 stycken 2:or, 3

stycken 3:or och en 7:a. Den form som heltalen är skrivna på i ovanstående exempel har ett speciellt namn som vi ger i en definition:

Definition: Låt n vara ett positivt heltal med primtalsfaktorerna $p_1, p_2, \ldots, p_k$ angivna i storleksordning och låt n innehålla a_1 stycken faktorer p_1, a_2 stycken faktorer p_2, och så vidare upp till a_k stycken faktorer p_k. Då kallas formen

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

för den *standardmässiga primtalsfaktoriseringen* av n.

En viktig sats i talteorin är aritmetikens fundamentalsats:

Aritmetikens fundamentalsats: Låt n vara ett godtyckligt positivt heltal. Då finns en och endast en standardmässig primtalsfaktorisering av n.

Vi kommer senare att ge ett bevis för denna men det dröjer ett tag.

Exempel: Vi studerar två tal, 720 och 7560, och försöker faktorisera dem på lite olika sätt. Vi ska se att vi alltid når samma standardmässiga primtalsfaktorisering.

$720 = 72 \cdot 10 = 8 \cdot 9 \cdot 2 \cdot 5 = 2^3 \cdot 3^2 \cdot 2 \cdot 5 = 2^4 \cdot 3^2 \cdot 5^1$.
$720 = 2 \cdot 360 = 2 \cdot 6 \cdot 60 = 2 \cdot 3 \cdot 2 \cdot 15 \cdot 4 = 2 \cdot 3 \cdot 2 \cdot 3 \cdot 5 \cdot 2 \cdot 2 = 2^4 \cdot 3^2 \cdot 5^1$.

$7560 = 756 \cdot 10 = 2 \cdot 378 \cdot 2 \cdot 5 = 2 \cdot 3 \cdot 126 \cdot 2 \cdot 5 = 2 \cdot 3 \cdot 3 \cdot 42 \cdot 2 \cdot 5 = 2 \cdot 3 \cdot 3 \cdot 2 \cdot 3 \cdot 7 \cdot 2 \cdot 5 = 2^3 \cdot 3^3 \cdot 5^1 \cdot 7^1$.
$7560 = 8 \cdot 945 = 2^3 \cdot 5 \cdot 189 = 2^3 \cdot 5 \cdot 27 \cdot 7 = 2^3 \cdot 3^3 \cdot 5^1 \cdot 7^1$.

Aritmetikens fundamentalsats säger att vi kan välja vilket positivt heltal som helst och faktorisera det hur som helst, plocka isär det i vilken ordning vi vill, vi kommer ändå alltid fram till precis en och samma standardmässig primtalsfaktorisering för varje positivt heltal.

Övningar

4.1.1 *före detta 3.1.1.* Studera följande utsagor: $4|12$, $3|20$, $3|21$, $5|21$, $5|25$, $5|-35$, $-5|35$, $-5|36$, $6|-36$, $1|20$, $1|-7$, $-1|5$, $-1|-67$, $0|30$, $0|10$, $10|0$, $20|0$, $-23|0$. Ange vilka som är sanna och vilka som är falska och motivera ditt svar.

4.1.2 *före detta 3.1.2.* Formulera med kvantorer vad det innebär att ett tal b inte är delbart med ett annat tal a. Formulera det också i ord. Ge ett par exempel.

4.1.3 *före detta 3.1.3.* Bevisa att alla tal delar 0.

4.1.4 *före detta 3.1.4.* Bevisa att talet 1 delar alla tal.

4.1.5 *före detta 3.1.5.* Bevisa att om n är ett godtyckligt heltal så är n delbart med $\pm n$ samt ± 1.

4.1.6 *före detta 3.1.6.* Lista alla primtal mindre än 100.

4.1.7 *före detta 3.1.7.* Formulera med kvantorer vad det innebär att ett tal inte är ett primtal.

4.1.8 *före detta 3.1.8.* Avgör vilka tal som är primtal i följande lista, om de är primtal, indikera det, om de inte är primtal, faktorisera dem i en standardmässiga primtalsfaktorisering: 811, 812, 877, 1213, 1215, 640, 641.

2. Gemensamma delare

Vi startar med en definition direkt.

Definition: Låt a och b vara två givna heltal. Om talet d delar både a och b så kallas d en *gemensam delare* till a och b.

Exempel:

* Talet 5 delar både talet 30 och 35. Alltså är 5 en gemensam delare till 30 och 35.
* Talet 6 delar både 12 och 18. Alltså är 6 en gemensam delare till 12 och 18.
* Talet 1 är en gemensam delare till vilka två andra tal som helst. Detta gäller eftersom talet 1 ju delar *alla* heltal. Således kan vi välja vilka två tal som helst och hävda att 1 är en gemensam delare till dessa.

Vi ska nu studera klasser av tal som alla är delbara med ett visst tal. Här säger vi återigen "klass" när vi menar en mängd av element (här heltal) som har en viss egenskap. Vi ska börja med att studera den klass av tal som alla är delbara med 2.

Definition: Ett tal a sägs vara *jämnt* om och endast om det är delbart med 2.

De jämna talen är dessa: $0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \ldots$ och så vidare. Vi kan skriva dem med mängdnotation:

$$\text{Alla jämna tal} = \{2 \cdot k : k \in \mathbb{Z}\}.$$

Vi kan observera olika saker kring jämna tal. Om vi summerar två jämna tal så får vi ett nytt jämnt tal. Om vi subtraherar två jämna tal så får vi ett nytt jämnt tal. Om vi multiplicerar två jämna tal så, gissa vad? Jo vi får ett nytt jämnt tal.

Om vi summerar två multiplar av två jämna tal. Tag till exempel de två jämna talen 34 och 10 och bilda

$$73 \cdot 34 + 5 \cdot 10$$

det blir 2532.

Det verkar som om tal som är delbara med 2 ger tal som är delbara med 2 oberoende av hur man adderar, subtraherar eller multiplicerar dem. Och det är riktigt. Vi kan till och med formulera en sats som inte bara har med jämna tal att göra (alltså multiplar av 2), två tal, a och b, vilka som helst som har en gemensam delare d kan adderas och summeras hur som helst, resultatet får ändå samma gemensamma delare d. Vi formulerar en sats.

Sats: Antag att d är en gemensam delare till a och b. (Talet d var 2 ovan då vi alltså studerade jämna tal.) Då gäller:

(1) $d|a + b$ (Summan av två tal delbara med d blir alltså delbar med d, liksom summan av två jämna tal också är jämn.)
(2) $d|k \cdot a$ för alla k. (Alla multiplar av ett tal delbart med d är också delbart med d.)
(3) $d|x \cdot a + y \cdot b$ för alla tal x, y. (Detta betyder att om två tal är delbara med d så är också alla summor av alla multiplar delbara med d. Detta uppträdde i exemplet ovan: $73 \cdot 34 + 5 \cdot 10$ var också var jämnt eftersom 34 och 10 var jämna. Här blir alltså $x = 73$ och $y = 5$.)

Bevis: Eftersom $d|a$ och $d|b$ så finns heltal t_1 och t_2 sådana att $a = t_1 \cdot d$ och $b = t_2 \cdot d$. (I delbarhetsdefinitionen ovan kallade vi talen t_1 och t_2 för k, men här byter vi alltså namn.) Vi ska nu använda denna information för att visa att (1), (2) och (3) gäller.

(1) Vi studerar $a + b$. Eftersom $a = t_1 \cdot d$ och $b = t_2 \cdot d$ kan vi skriva

$$a + b = t_1 \cdot d + t_2 \cdot d.$$

Vi bryter ut d och ser att $a + b = (t_1 + t_2) \cdot d = heltal \cdot d$. Men detta betyder precis att $d|a + b$ vilket skulle visas.
(2) Vi studerar $k \cdot a$ för godtyckligt k. Genom att återigen ersätta a med $t_1 \cdot d$ får vi $k \cdot a = k \cdot t_1 \cdot d = heltal \cdot d$. Men detta betyder just att $d|k \cdot a$ vilket skulle visas.
(3) Lämnas som övning.

Vi formulerar också första delen av beviset med kvantorer:

Vi har $d|a$ och $d|b \Rightarrow \exists t_1 \exists t_2 : a = t_1 \cdot d \wedge b = t_2 \cdot d$. Detta får till följd att $a + b = t_1 \cdot d + t_2 \cdot d = (t_1 + t_2) \cdot d$. Detta visar att $\exists k : a + b = k \cdot d$, nämligen $k = t_1 + t_2$ som betyder att $d|a + b$ vilket skulle bevisas.

Exempel: Vi vet att $3|6$ och $3|21$. Talet 3 är alltså en gemensam delare till 6 och 21. Av satsen ovan kan vi alltså dra slutsatsen att $3|21 + 6$, $3|17 \cdot 21$, och att $3|73 \cdot 3 + 2 \cdot 6$. Räkna ut vad dessa tal är och verifiera att de verkligen är delbara med 3.

Två tal a och b kan alltså ha en gemensam delare d. Talet 1 är alltid en gemensam delare till a och b, vilka som helst (med kvantorer: $\forall a \in \mathbb{Z} : \forall b \in \mathbb{Z} : 1|a \wedge 1|b$), och det kan som vi sett finnas flera gemensamma delare.

Men det kan inte finnas hur stora gemensamma delare som helst för två heltal. Inga tal större än $|a|$ kan inte dela a och samma sak gäller för b. De tal som är större än $|a|$ eller $|b|$ kan alltså *inte* vara gemensamma delare till a och b. Det innebär att det finns en *största gemensam delare* till varje par av tal a och b. Vi ska formulera detta noggrannt.

Definition: Låt a och b vara två givna heltal. Med *största gemensamma delaren* till a och b menas det tal som är en gemensam delare till a och b och som har egenskapen att inget större tal också är gemensam delare till a och b. Vi betecknar största gemensamma delaren till a och b med $\gcd(a, b)$. *(Från engelskans greatest common divisor.)*

Exempel: Sedan tidigare vet vi att $720 = 2^4 \cdot 3^2 \cdot 5^1$ och $7560 = 2^3 \cdot 3^3 \cdot 5^1 \cdot 7^1$. För att finna största gemensamma delaren till 720 och 7560 kan vi studera deras standardmässiga primtalsfaktoriseringar. Vi ser att 2 är en gemensam delare, men vi ser att även $2^3 = 8$ är en gemensam delare till 720 och 7560. Däremot är *inte* $2^4 = 16$ en gemensam delare till 720 och 7560. Visserligen gäller att $2^4 = 16$ delar 720, men $2^4 = 16$ delar *inte* 7560.

Vi ser vidare att 3 är en gemensam delare till båda talen och även $3^2 = 9$, men inga högre potenser av 3 är gemensam delare.

Eftersom 2 och 3 är primtal kan vi bara multiplicera ihop dem och bilda talet $2^3 \cdot 3^2$ som också måste vara en gemensam delare till 720 och 7560.

Men vi kan öka ännu mer. Talet 5 delar båda talen så vi kan även veta att

$$2^3 \cdot 3^2 \cdot 5 = 72 \cdot 5 = 360$$

måste vara en gemensam delare till 720 och 7560.

Kan vi hitta en större gemensam delare än 360? Svaret är nej eftersom vi sugit ut alla primtalsfaktorer som är gemensamma för både 720 och 7560. Talen 720 och 7560 har inte mer att bjuda på av *gemensamma delare* och vi förstår att 360 måste vara den största gemensamma delaren till 720 och 7560. Slutsats: $\gcd(720, 7560) = 360$.

Om två tal, a och b, har en gemensam delare som är större än 1 så avspeglas det alltså i deras standardmässiga primtalsfaktoriseringar och vi kan alltid extrahera $\gcd(a, b)$ på det sätt som illustreras i exemplet ovan.

Om två tal har största gemensamma delare lika med 1 så saknar talen gemensamma delare. Tal som relaterar till varandra på detta sätt spelar en viktig roll i talteori och kryptering så vi inför ett eget namn för detta förhållande.

Definition: Två tal a och b kallas *relativt prima varandra* om de saknar andra gemensamma delare andra än 1 och -1. (Alla tal är ju förstås delbara med 1 och -1.)

Enligt denna definition gäller alltså att a och b är relativt prima varandra $\Leftrightarrow \gcd(a, b) = 1$.

Exempel:

(1) De enda tal som delar både 17 och 24 är talen 1, och -1. Alltså är 17 och 24 relativt prima varandra.
(2) De enda tal som delar både 10 och 21 är talen 1, och -1. Alltså är talen 10 och 21 relativt prima varandra. (Lägg märke till att varken 10 eller 21 är primtal.)
(3) Talen 12 och 15 går båda att dela med 3 (som är större än 1), alltså är dessa två tal *inte* relativt prima varandra.
(4) Talen 7 och 21 går båda att dela med 7 (som är större än 1), alltså är dessa två tal *inte* relativt prima varandra. (Det är ju till och med så att 7 delar 21.)

Övningar

4.2.1 *före detta 3.2.1* Ange alla gemensamma delare till följande par av tal. Ange också den största gemensamma delaren.

56 och 24
30 och 170
18 och 60
76230 och 2772
1320 och 92400

Ledning: Använd den standardmässiga primtalsfaktoriseringen. Till exempel är $56 = 7 \cdot 8 = 2^3 \cdot 7^1$ och $24 = 3 \cdot 8 = 2^3 \cdot 3^1$. Vi läser direkt från faktoriseringarna att de gemensamma delarna är alla potenser av 2, det vill sga 1, 2, 4 och 8. Största gemensamma delaren är då 8 som är den största ingående potensen av 2 i 56 och 24.

4.2.2 *före detta 3.2.3.* Visa att om $d|a$ och $d|b$ så gäller att $d|a-b$, $d|a \cdot b$. Formulera detta med kvantorer. Formulera också den falska motsatsen med kvantorer och ge en formulering med vanliga ord.

4.2.3 *före detta 3.2.4.* Formulera med kvantorer och med vanliga ord att två tal är relativt prima varandra, formulera också motsatsen med kvantorer och med vanliga ord. Ge ett flertal exempel.

4.2.4 *före detta 3.2.5.* Avgör vilka par av tal som är relativt prima varandra. Ge också motiveringar.

456 och 345
123 och 235
346 och 234

3. Divisionsalgoritmen, Euklides algoritm och Bezouts sats

Om man dividerar b med a och $a|b$ så vet vi att divisionen går jämnt ut och vi får ett heltal som kvot. Till exempel gäller att $6|24$ och $24/6 =$ ett heltal $= 4$. Om divisionen inte går jämnt ut så beror det på att a inte delar b. Talet $a = 4$ delar inte talet $b = 11$ och utför vi en division mellan detta a och b får vi en *rest*. Vi skriver att $11/4 = 2$ med resten 3 vilket uttrycker att vi kan stuva in 2 stycken 4:or i 11 men sedan blir det 3 över.

Vi kan illustrera det så här: Elva kryss kan placeras i 2 grupper om 4 var och då blir det 3 över.

```
xxxx xxxx xxx
```
$11 = 2 \cdot 4 + 3$

Vi formulerar en allmän sats om hur vi dividerar tal med varandra även om vi inte divisionen skulle gå jämnt ut.

Sats *Divisionsalgoritmen.* Låt n vara ett givet heltal. För varje positivt heltal d finns då entydigt bestämda tal q och r med $0 \leq r \leq d-1$ sådana att

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

Vi kommer att ge ett bevis av denna sats senare.

Villkoret $0 \leq r \leq d-1$ är det som garanterar entydigheten hos q och r. Det finns förstås fler tal som uppfyller ekvationen $n = q \cdot d + r$, men det finns exakt ett q och exakt ett r som uppfyller ekvationen då vi lägger på det extra kravet $0 \leq r \leq d-1$.

Vi ska införa lite terminologi i en definition innan vi tar ett par exempel.

Definition: Låt n och d vara två givna tal som uppfyller kraven i divisionsalgoritmen. Det entydigt bestämda talet q kallas då divisionens *kvot* och det entydigt bestämda talet r kallas divisionens *rest*. Om talet r är 0 säger vi att divisionen *går jämnt ut* (och det betyder ju att $d|n$).

Exempel:

(1) Låt $n = 11$ och $d = 4$. Ur ekvationen $11 = 4 \cdot 2 + 3$ läser vi $q = 2$ och $r = 3$. Enligt divisionsalgoritmen finns det bara dessa q och r som uppfyller ekvationen $n = q \cdot d + r$ om talet r ska krävas ligga i intervallet 0 till och med $4 - 1 = 3$. Kvoten i divisionen måste då vara 2 och resten 3.
(2) Låt $n = 56$ och $d = 17$. Vi har $56 = 3 \cdot 17 + 5$. Kvoten blir således 3 och resten blir 5.
(3) Låt $n = 56$ och $d = 8$. Vi har $56 = 7 \cdot 8 + 0$. Kvoten blir således 7 och resten blir 0. Den här divisionen gick jämnt ut.
(4) Låt $n = -112$ och $d = 17$. Då gäller $-112 = -7 \cdot 17 + 7$. Kvoten blir här -7 och resten blir 7.

Vi ska nu visa en algoritm för hur man kan ta fram största gemensamma delare för två heltal. Algoritmen heter *Euklides Algoritm* och baserar sig på divisionsalgoritmen. Vi illustrerar metoden i ett exempel.

Exempel: Finn $\gcd(12259, 3887)$. *Lösning:* Vi dividerar 12259 med 3887 enligt divisionsalgoritmen och får

$$12259 = 3 \cdot 3887 + 598.$$

Här är kvoten 3 och resten 598. Vi söker största gemensamma delare till 12259 och 3887. Vi kallar detta tal D. Efter omskrivning av $12259 = 3 \cdot 3887 + 598$ får vi

$$598 = 12259 - 3 \cdot 3887.$$

Eftersom D delar både 12259 och 3887 så måste också D dela högerledet $12259 - 3 \cdot 3887$ eftersom detta är ett uttryck bildat av två multiplar av D. (Det var en av satserna tidigare: 12259 och 3887 är båda multiplar av D.) Men detta innebär att D även delar 598 eftersom vi har funnit $598 = 12259 - 3 \cdot 3887$. Det kan heller inte finnas något större tal än D som delar både 598 och 3887. Varför det? Jo, antag att vi skulle ha ett tal D_2 som är större än D och som delar både 598 och 3887. Det talet D_2 skulle då även dela 12259 eftersom $12259 = 3 \cdot 3887 + 598$. Men då har vi funnit ett tal som är *större* än $D = \gcd(12259, 3887)$ och det går inte för $D = \gcd(12259, 3887)$ är ju precis det *största* talet som delar både 12259 och 3887. Alltså måste talet D inte bara vara en gemensam delare mellan 3887 och 598 utan det måste vara *största* gemensamma delare till 3887 och 598. Vi drar slutsatsen att $D = \gcd(12259, 3887) = \gcd(3887, 598)$ och problemet att finna $\gcd(12259, 3887)$ är alltså reducerat till att finna $\gcd(3887, 598)$.

Vi upprepar nu hela den här proceduren och dividerar 3887 med 598. Det ger oss

$$3887 = 6 \cdot 598 + 299.$$

Samma resonemang ger oss $\gcd(3887, 598) = \gcd(598, 299)$ och vi tecknar alltså nästa division som ger oss

$$598 = 2 \cdot 299 + 0.$$

Nollan är en stoppsignal i Euklides Algoritm. Om vi skulle fortsatt så skulle vi i nästa steg ska vi beräknat $\gcd(598, 299)$, men eftersom denna divisionen $598 = 2 \cdot 299 + 0$ går jämnt ut måste 299 dela 598. Då måste $\gcd(598, 299) = 299$. Vi sammanfattar:

$$D = \gcd(12259, 3887) = \gcd(3887, 598) = \gcd(598, 299) = 299.$$

Vi tar ett exempel till.

Exempel: Finn $\gcd(18200, 3822)$.

Euklides algoritm ger oss med divisioner:

$18200 = 4 \cdot 3822 + 2912$	(kvot 4, rest 2912)
$3882 = 1 \cdot 2912 + 910$	(kvot 1, rest 910)
$2912 = 3 \cdot 910 + 182$	(kvot 3, rest 182)
$910 = 5 \cdot 182 + 0$	(kvot 5, rest 0, stoppsignal!)

Alltså har vi $\gcd(18200, 3822) = \gcd(3882, 2912) = \gcd(2912, 910) = \gcd(910, 182) = 182$.

Allmänt gäller att största gemensamma delare som kommer ut från Euklides algoritm är den sista resten som inte är 0.

Vi kommer senare att ge ett formellt bevis till att Euklides algoritm verkligen fungerar.

Vi ska nu ta upp en speciell sats som vi inte i första taget kan se hur den ska användas, men det kommer att ha mycket stor betydelse den fortsatta utvecklingen av teorin. Vi formulerar den här.

Sats: *(Bezouts sats)* Låt a och b vara två positiva heltal med största gemensamma delare $\gcd(a, b)$. Då finns heltal x, y sådana att

$$x \cdot a + y \cdot b = \gcd(a, b).$$

Innan vi ger beviset kan vi ge ett par kommentarer om likheten $x \cdot a + y \cdot b = \gcd(a, b)$. Från linjär algebra är vi bekanta med begreppet *linjärkombination*, om vi har två vektorer u och v så kan vi bilda nya vektorer på formen

$$x \cdot u + y \cdot v$$

där x och y är reella tal. Nu håller vi på med *heltal* men egenskaperna hos uttrycket $x \cdot a + y \cdot b$ då allting är heltal är förstå liknande egenskaperna hos uttrycket $x \cdot u + y \cdot v$ då vi arbetar med tal och vektorer. Alla vektorer på formen $x \cdot u + y \cdot v$ bildar ett plan med u och v som uppspännande vektorer och det vi gör nu är formulera någonting liknande för heltal. Likheten

$$x \cdot a + y \cdot b = \gcd(a, b)$$

(som vi snart ska visa) säger att största gemensamma delare på något vi kan åstadkommas genom att bilda en linjärkombination av de båda heltalen a och b. Den här identiteten kommer att vara mycket användbar i flera

sammanhang framöver.

Bevis: Antag att $a \leq b$. Utför Enligt Euklides Algoritm på a och b. Då uppstår en följd av ickenegativa tal $r_0, r_1, r_2, \ldots, r_k$ sådana att

$$\begin{array}{rcl} b & = & q_1 \cdot a + r_1 \\ a & = & q_2 \cdot r_1 + r_2 \\ r_1 & = & q_3 \cdot r_2 + r_3 \\ & \ldots & \\ r_{k-1} & = & q_{k+1} \cdot r_k + \gcd(a,b). \end{array}$$

Talen är de successiva resterna som vi beräknar steg för steg till vi når stoppsignalen 0. Om vi tog ett steg till skulle vi se den där 0:an, men vi bryter precis innan.

Vi använder nu det här talschemat och skriver $\gcd(a,b) = r_{k-1} - q_{k+1} \cdot r_k$. Därefter använder vi alla tidigare led i Euklides Algoritm och ersätter alla rester med uttryck i termer av rester som förekommer på de överliggande raderna. Successivt kan vi då ersätta alla rester med uttryck i multiplar av a och b. Detta kommer då att kunna skrivas som

$$\gcd(a,b) = x \cdot a + y \cdot b$$

för lämpligt valda x och y. (Liknande resonemang fungerar om $b < a$.) Beviset är klart.

Exempel: Finn x och y sådana att $x \cdot 5 + y \cdot 7 = 1$.

Lösning: Talen 5 och 7 är relativt prima, dvs $\gcd(5,7) = 1$ så enligt Bezouts sats vet vi säkert att x och y finns. Vi gör som i beviset ovan och sätter upp Euklides Algoritm. Det ger

$$\begin{array}{rcl} 7 & = & 1 \cdot 5 + 2 \\ 5 & = & 2 \cdot 2 + 1 \end{array}$$

Och så arbetar vi precis som i beviset baklänges i talschemat och skriver $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7$. Det betyder att $x = 3$ och $y = -2$ uppfyller $x \cdot 5 + y \cdot 7 = 1$.

Exempel: Finn x och y sådana att $x \cdot 66 + y \cdot 42 = \gcd(66, 42)$.

Lösning: Vi gör Euklides Algoritm på 66 och 42. Det ger

$$\begin{array}{rcl} 66 & = & 1 \cdot 42 + 24 \\ 42 & = & 1 \cdot 24 + 18 \\ 24 & = & 1 \cdot 18 + 6 \end{array}$$

och eftersom $6|18$ skulle vi fått stoppsignalen 0 i nästa steg. Den här första fasen av beräkningarna visar att $\gcd(66, 42) = 6$. Nu arbetar vi baklänges i talschemat ovan och får:

$$6 = 24 - 1 \cdot 18 = 24 - 1 \cdot (42 - 1 \cdot 24) = 2 \cdot 24 - 1 \cdot 42 = 2 \cdot (66 - 1 \cdot 42) - 1 \cdot 42 = 2 \cdot 66 - 3 \cdot 42.$$

Vi avläser alltså att $x = 2$ och $y = -3$ uppfyller $x \cdot 66 + y \cdot 42 = \gcd(66, 42) \quad (= 6)$.

Kommentar: Om $\gcd(a,b) = 1$ så finns alltså heltalen x, y sådana att $x \cdot a + y \cdot b = 1$ enligt Bezouts sats. Men vi kan faktiskt också säga att om den finns heltal x, y som uppfyller $x \cdot a + y \cdot b = 1$ så måste $\gcd(a,b) = 1$. Varför det? Jo för om $\gcd(a,b)$ vore större ä 1 och så skulle vi inte kunna hitta några tal x, y som uppfyllde $x \cdot a + y \cdot b = 1$ eftersom om $\gcd(a,b) = d > 1$ så skulle vi alltid haft

$$x \cdot a + y \cdot b = x \cdot t_1 \cdot d + y \cdot t_2 \cdot d = (x \cdot t_1 + y \cdot t_2) \cdot d = heltal \cdot d$$

så alla tal på formen $x \cdot a + y \cdot b$ är alltså alltid delbara med $d > 1$ så det uttrycket kan aldrig bli 1 hur vi än väljer x och y. Då skulle vi få att 1 är delbart med heltalen $d > 1$ vilket är en motsägelse.

Så om vi har två heltal a, b kan vi alltså först använda Euklides Algoritm för att hitta $\gcd(a,b)$. Beviset för Bezouts sats inkluderar just en användning av Euklides Algoritm men den satsen säger också att vi kan gå vidare och hitta talen x, y som uppfyller $x \cdot a + y \cdot b = \gcd(a,b)$. När vi går vidare på sättet som beskrivs i beviset till Bezouts sats för att hitta x och y så kallar vi det för *Euklides Utvidgade Algoritm.*

Övningar

4.3.1 *före detta 3.3.1* Divisionsalgoritmen säger att om n är ett givet heltal och d är ett positivt heltal så finns entydigt bestämda heltal q och r sdana att $n = q \cdot d + r$ och $0 \leq r < d$. Ange q och r för följande val av n och d:

$n = 11$ och $d = 2$ $n = 23$ och $d = 3$ $n = 45$ och $d = 9$
$n = 67$ och $d = 8$ $n = 34$ och $d = 7$ $n = -34$ och $d = 6$
$n = -11$ och $d = 2$ $n = -23$ och $d = 3$ $n = -45$ och $d = 9$

Vad innebär det att $r = 0$?

4.3.2 *före detta 3.3.2.* Finn största gemensamma delare för följande par av tal med Euklides algoritm. Ange även båda talens standardmässiga primtalsfaktorisering.
540 och 7350 204750 och 32760 35640 och 8316

4.3.3 *före detta 3.3.3.* Finn största gemensamma delare för följande par av tal med Euklides algoritm
7920 och 7020 151470 och 18700 3740 och 5733

4.3.4 *före detta 3.3.4.* Kan du finna två på varandra följande tal som inte är relativt prima? Varför? Varför inte?

4.3.5 *före detta 3.3.5.* Kan du finna två tal med differens 2 som inte är relativt prima? I så fall ge ett exempel.

4. Kongruenser

Division lämnar ibland rester. Vi vet att $3 \nmid 28$, men i den mening som införs med divisionsalgoritmen så kan vi ändå utföra divisionen $28/3$ och vi får då kvoten 9 och resten 1. Likheten som ger oss detta är $28 = 9 \cdot 3 + 1$.

Vi påminner om terminologin och där kallas talet 3 *divisor*, talet 9 kallas *kvot* och talet 1 kallas *rest* och vi säger att 28 *ger* kvoten 9 och resten 1 vid division med 3.

Vart tredje tal ger resten 1 vid division med 3. Dessa tal bildar en speciell följd av tal:

$$\ldots, -8, -5, -2, 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, \ldots$$

Punkterna i början och i slutet symboliserar att följden av tal fortsätter i all oändlighet. Vi kan på liknande sätt rada upp de tal som ger resten 2 vid division med 3. De är $\ldots, -4, -1, 2, 5, 8, \ldots$. De tal som ger resten 0 vid division med 3 är de tal som är delbara med 3 och de bildar också en följd. Dessa tre följder av tal utgör tillsammans alla heltal och vi kan illustrera dem i ett schema av följande utseende

...	−9			−6			−3			0			3			6			9			12	...	...	...
...	...	−8			−5			−2			1			4			7			10			13	...	...
...	...	...	−7			−4			−1			2			5			8			11			14	...

Vi har som sagt tre rader och i översta raden har vi alla tal som är delbara med 3, det vill säga alla tal som ger resten 0 vid division med 3. Detta är talen $\ldots, -9, -6, -3, 0, 3, 6, 9, 12, \ldots$ och vi säger att dessa tal tillhör en och samma *restklass*. Ordet ”klass” betyder i det här fallet mängd av tal med en viss egenskap och vi klassificerar dessa tal genom att de ger resten 0 vid division med 3, det vill säga de är alla delbara med 3. För att betona att det är 3 det är frågan om brukar man säga *restklass modulo 3*. Den här figuren ovan illustrerar alltså de tre restklasserna modulo 3.

Vi säger på samma sätt att talen $\ldots, -8, -5, -2, 1, 4, 7, \ldots$ tillhör samma restklass modulo 3 och liknande gäller för den undre talföljden.

Med mängdnotation kan restklassen hörande till resten 0 skrivas så här:

$$\{3k + 0 : k \in \mathbb{Z}\}.$$

Och det här är alltså mängden av alla tal som finns på översta raden i talschemat ovan. På liknande sätt kan vi beskriva de andra två restklasserna (talen på de andra två raderna) med

$$\{3k + 1 : k \in \mathbb{Z}\} \quad \text{respektive} \quad \{3k + 2 : k \in \mathbb{Z}\}.$$

Vi inför nu beteckningssättet $x \equiv 1 \pmod 3$ (utläses ”x är kongruent med 1 modulo 3”) som betyder att talet x ger resten 1 vid division med 3. (Med mängdnotation har vi då $x \in \{3k + 1 : k \in \mathbb{Z}\} = \{y : y \equiv 1 \pmod 3\}$.)

På liknande sätt betyder $x \equiv 2 \pmod 3$ att talet x ger resten 2 vid division med 3 och $x \equiv 0 \pmod 3$ betyder att talet x ger resten 0 vid division med 3, det vill säga att x är delbart med 3.

Om $x \equiv 1 \pmod 3$ betyder alltså detta att talet x är ett steg större än en multipel av 3. Det betyder i sin tur att talet $x-1$ är *precis* en multipel av 3, det vill säga talet $x-1$ är *delbart* med 3 som vi också kan skriva som $x - 1 \equiv 0 \pmod 3$. Resonemanget går i båda riktningar så vi har alltså:

$$x \equiv 1 \pmod 3 \Leftrightarrow x - 1 \equiv 0 \pmod 3.$$

Detta kan vi tolka som att vi subtraherat 1 från båda sidor om kongruenstecknet ($\equiv$) och det leder oss till att utvidga skrivsättet $x \equiv tal \pmod 3$ till att innefatta andra tal än 0, 1 och 2. Vi skriver då $x \equiv y \pmod 3$ om och endast om skillnaden mellan x och y är jämnt delbar med 3. Det vill säga

$$x \equiv y \pmod 3 \Leftrightarrow x - y \equiv 0 \pmod 3 \Leftrightarrow 3|x - y.$$

Men att $3|x - y$ betyder att det finns ett tal k sådant att

$$x - y = 3k \Leftrightarrow x = y + 3k.$$

För att komma från y till x lägger vi alltså på k stycken 3:or. Det nya skrivsättet innebär att vi anser att tal x och y är kongruenta med varandra modulo 3 om vi kan komma från det ena talet till det andra talet genom att lägga på lämpligt antal 3:or. I figuren som illustrerar restklasser har varje rad av tal just den egenskapen att vi kan komma från varje tal i den raden till varje annat tal i samma rad genom att lägga på (eller dra ifrån) lämpligt antal 3:or.

Exempel: I figuren med restklasser ovan så ligger 8 och -4 på samma rad. Och mycket riktigt, $8 \equiv -4 \pmod 3$ för $-4 + 4 \cdot 3 = 8$, här behövs alltså 4 stycken 3:or för att komma från -4 till 8.

Exempel: $2 \equiv 5 \pmod 3$ för $5 = 2 + 1 \cdot 3$, här behövs 1 stycken 3:a.

Exempel: $5 \equiv 2 \pmod 3$ för $2 = 5 - 1 \cdot 3$, och här behövs -1 stycken 3:a.

Vi kan även införa flera räknesätt på kongruenstecknet. Vi kan addera (och därmed subtrahera) andra tal på båda sidor om kongruenstecknet, så här:

Om $x \equiv y \pmod 3$ gäller för alla tal a att $x + a \equiv y + a \pmod 3$. Till exempel har vi som vi såg tidigare $5 \equiv 2 \pmod 3$, efter addition av 4 till båda sidor fås $5 + 4 \equiv 2 + 4 \pmod 3 \Leftrightarrow 9 \equiv 6 \pmod 3$. Att verkligen 9 är kongruent med 6 modulo 3 kan vi inse genom att studera figuren med restklasserna igen eller genom att observera att vi kan lägga en 3:a till 6, då får vi 9.

På samma sätta kan vi även *multiplicera* båda sidor av en kongruens med ett tal c: Om $x \equiv y \pmod 3$ gäller för alla tal c att $cx \equiv cy \pmod 3$. Vi formulerar allt det här i följande *mycket* användbara sats:

Sats: Om $x \equiv y \pmod n$ så gäller

(1) $x + a \equiv y + a \pmod n$ för alla tal a. Vi har även det starkare $u \equiv z \pmod n \Rightarrow x + u \equiv y + v \pmod n$.
(2) $cx \equiv cy \pmod n$ för alla tal c.
(3) $x^2 \equiv y^2 \pmod n$ och $x^3 \equiv y^3 \pmod n, \ldots, x^m \equiv y^m \pmod n$ för alla tal m.

Här skriver vi "tal" när vi menar heltal.

Bevis: Bevis av (1) och (2) lämnas som övning till läsaren. Vi visar endast första delen av (3):
Vi ska visa att $x^2 \equiv y^2 \pmod n$, det vill säga vi ska visa att $n|x^2 - y^2$. Vi har som förutsättning att $x \equiv y \pmod n$, det vill säga att $n|x - y$. Studera alltså talet $x^2 - y^2$. Enligt konjugatregeln vet vi att $x^2 - y^2 = (x - y)(x + y)$, men $n|x - y$ så det finns alltså ett k sådant att $x - y = k \cdot n$. Nu kan vi skriva

$$x^2 - y^2 = (x - y)(x + y) = k \cdot n \cdot (x + y) = n \cdot heltal.$$

Vi har alltså visat att $n|x^2 - y^2$ vilket är ekvivalent med $x^2 \equiv y^2 \pmod n$ vilket skulle visas.

Exempel: Vi studerar ett par exempel på konsekvenser av den sista satsen.

* $121^{1000} = (120 + 1)^{1000} = (40 \cdot 3 + 1)^{1000} \equiv 1^{1000} \pmod 3 \equiv 1 \pmod 3$. Här har vi observerat att 121 är kongruent med 1 modulo 3. Det betyder att 121^{1000} måste vara kongruent med 1. ((mod 3).)

* $98^{99} = (99-1)^{99} = ((33\cdot 3)-1)^{99} \equiv (-1)^{99} \pmod 3 \equiv -1 \pmod 3$. Här har vi återigen använt samma satsen på samma sätt. Vi har också observerat att $(-1)^{99} = (-1)^{\text{udda tal}} = -1$.

* Nu använder vi de första delarna av detta exempel tillsammans med första delen av satsen och får

$$121^{1000} + 98^{99} \equiv 1 - 1 \equiv 0 \pmod 3,$$

det vill säga vi har alltså funnit att $3|121^{1000} + 98^{99}$. Det finns nog inga tillämpningar av detta men det är ändå anmärkningsvärt att vi kan dra en slutsats om det fullkomligt obegripligt stora talet $121^{1000} + 98^{99}$ mämligen att det är jämnt delbart med 3.

Vi kallar detta sätt att räkna för *kongruensräkning* vilket innebär att vi kastar alla multiplar av 3 eller något annat n. Kongruensräkning är en viktig del av talteorin och har stor betydelse för kryptografin och vilket vi kommer att studera senare.

Vi kan uttrycka detta på ett annat sätt, kongruensräkning modulo 3 betyder att vi samlar alla tal kongruenta med 0 modulo 3 (alltså alla tal delbara med 3) och räknar med dem som om de alla vore 0. På samma sätt samlar vi alla tal kongruenta med 1 modulo 3 och räknar med dem som om de alla vore 1. Slutligen samlar vi alla tal som är kongruenta med 2 modulo 3 och räknar med dem som om alla de vore 2. Alla tal delbara med 3 representeras alltså av 0, alla tal kongruenta med 1 representeras av 1 och alla tal kongruenta med 2 representeras av 2.

Och det *riktigt* eleganta och fascinerande är att vi faktiskt har friheten att välja representant. I exemplet ovan räknade vi så här $98^{99} = (99-1)^{99} = ((33\cdot 3)-1)^{99} \equiv (-1)^{99} \pmod 3 \equiv -1 \pmod 3$, vi låter alltså det stora ohanterliga talet 98^{99} ersättas av den lätthanterliga representanten -1. Saken är den att vi faktiskt kan räkna med alla tal kongruenta med 0 i en klump och symbolisera allihop med $\overline{0}$ (alltså 0 med ett streck över). På samma sätt symboliserar $\overline{1}$ och $\overline{2}$ alla tal kongruenta med 1 respektive 2 modulo 3.

Vi inför alltså följande notation:

Symbol	Exempel på tal	Beskrivning av talen	Mängdnotation
$\overline{0}$	$0, \pm 3, \pm 6,\ 9, \ldots$	alla multiplar av 3	$\{3k : k \in \mathbb{Z}\}$
$\overline{1}$	$1, 1 \pm 3, 1 \pm 6, 1 \pm 9, \ldots$	alla tal som ger rest 1 vid division med 3	$\{3k+1 : k \in \mathbb{Z}\}$
$\overline{2}$	$2, 2 \pm 3, 2 \pm 6, 2 \pm 9, \ldots$	alla tal som ger rest 2 vid division med 3	$\{3k+2 : k \in \mathbb{Z}\}$

Symbolen $\overline{0}$ betecknar alltså inte ett tal utan en hel klass av tal. Vi har kallat den klassen för en *restklass* tidigare. Det är nu möjligt att definiera räkneoperationer mellan restklasser. Vi illustrerar detta för tal kongruenta modulo 3 i följande exempel:

Exempel: Studera figuren med alla restklasser modulo 3 igen, den med de tre raderna av tal.

* Välj $x = 1$ ur rad 2 och $y = 2$ ur rad 3. Addera dessa tal, det ger $x + y = 1 + 2 = 3 = z$, $z = 3$ ligger i rad 1.
* Välj $x = 4$ ur rad 2 och $y = 8$ ur rad 3. Addera dessa tal, det ger $x + y = 4 + 8 = 12 = z$, $z = 12$ ligger i rad 1.
* Välj $x = 7$ ur rad 2 och $y = -1$ ur rad 3. Addera dessa tal, det ger $x + y = 7 + -1 = 6 = z$, $z = 6$ ligger i rad 1.

Det gäller alltså *alltid* (bevisa detta!) att tal ur rad 2 adderade till rad 3 alltid ger tal i rad 1! Talen i rad 2 är restklassen $\overline{1}$ och talen i rad 3 är restklassen $\overline{2}$ och talen i rad 1 är restklassen $\overline{0}$. Vi kan därför anse att vi kan addera hela rader (eller restklasser) till varandra, rad 1 adderad till rad 2 ger rad 1 vilket tolkas som att restklassen $\overline{1}$ adderad till restklassen $\overline{2}$ ger restklassen $\overline{0}$. Vi har alltså $\overline{1} + \overline{2} = \overline{0}$. De tre restklasserna $\overline{0}$, $\overline{1}$ och $\overline{2}$ brukar man sammantagna kalla $\mathbb{Z}_3$ som alltså är en ny mängd matematiska objekt.

Det är *mycket* viktigt att observera att när vi skriver likheten

$$\overline{1} + \overline{2} = \overline{0}$$

så är detta en likhet som involverar tre mängder (alltså restklasser). Och plustecknet mellan $\overline{1}$ och $\overline{2}$ markerar alltså en operation på två *mängder* (restklasser) av tal. Likaså anger.

Baserat på samma additionsexperiment som i exemplet ovan kan vi skapa en additionstabell för $\mathbb{Z}_3$. Den får följande utseende:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Tabellen är alltså en tabell över modulo-3 addition i $\mathbb{Z}_3$. Vi kan även skapa en multiplikationstabell på samma sätt. (Genomför beräkningarna i exemplet ovan, men byt ordet "addera" mot "multiplicera" för att se att detta går att genomföra även för multiplikation). Så här ser den ut:

$*$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Symbolen $\mathbb{Z}_3$ betecknar alltså $\{\overline{0}, \overline{1}, \overline{2}\}$ = mängden av de tre restklasserna modulo 3. (Alltså en mängd av mängder.)

Vi kan göra detta för andra tal än 3, till exempel har vi additions- och multiplikationstabellerna för $\mathbb{Z}_4$ givna nedan:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$*$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Vi ger också multiplikationstabellerna för $\mathbb{Z}_5$ och $\mathbb{Z}_7$:

$*$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$*$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

och $\mathbb{Z}_{10}$:

$*$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{2}$	$\overline{5}$	$\overline{8}$	$\overline{1}$	$\overline{4}$	$\overline{7}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{8}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{8}$	$\overline{5}$	$\overline{2}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Någonting som är ganska spännande att lägga märke till är att raderna i multiplikationstabellen hörande till $\mathbb{Z}_7$ innehåller, på varje rad, *varje* element ur $\mathbb{Z}_7$ och varje element förekommer *exakt* en gång i varje rad. Till exempel innehåller rad 3 i multiplikationstabellen för $\mathbb{Z}_7$ elementen $\overline{0}, \overline{3}, \overline{6}, \overline{2}, \overline{5}, \overline{1}, \overline{4}$ vilket är alla element i $\mathbb{Z}_7$ fast i en omkastad ordning. Detta gäller som sagt alla rader. Varje rad i multiplikationstabellen för $\mathbb{Z}_7$ ger oss alltså en omordning av alla element i $\mathbb{Z}_7$. Detta är något som utnyttjas i kryptering, fast i en annan form som vi senare ska se. Motsvarande gäller *inte* för $\mathbb{Z}_{10}$, till exempel består rad 5 i tabellen för $\mathbb{Z}_{10}$ *bara* av elementen $\overline{0}$ och $\overline{5}$. Nyckelegenskapen är att 7 är ett primtal och 10 är inte ett primtal. i det

fäoljande avsnittet och det kommande kapitlet kommer vi att se den teoretiska grunden till varför det här gäller.

övningar till detta avsnitt följer efter nästa avsnitt

5. Lösning av kongruensen $a \cdot x \equiv b \pmod{n}$

Vi ska nu formulera och bevisa en sats som uttrycker precis när vi kan lösa en kongruens av typen

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

Lösningen (som uttrycks i x) kommer också att vara en kongruens, alltså ett uttryck på formen

$$x \equiv x_0 \pmod{n}.$$

Vi gör detta genom ett exempel.

Exempel: Finn alla x som uppfyller $5 \cdot x \equiv 11 \pmod{17}$.

Lösning: Vi startar med att ta fram tal s, t som uppfyller $s \cdot 5 + t \cdot 17 = 1$. Detta är talen x och y i Bezouts sats, fast vi har bytt namn på dem till s och t (variabeln x är ju upptagen).

Vi använder Euklides Utvidgade Algoritm på talen 5 och 17 (vi kommer så småningom att förstå varför). Vi får då:

$$\begin{aligned} 17 &= 3 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

och härifrån kan vi skriva $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (17 - 3 \cdot 5) = 7 \cdot 5 - 2 \cdot 17$ alltså har vi

$$7 \cdot 5 - 2 \cdot 17 = \gcd(5, 17) = 1.$$

Men då kan vi också skriva

$$7 \cdot 5 \equiv 1 \pmod{n}$$

och det här en *mycket viktig* likhet. Att vi har hittat talen 7 som har egenskapen att $7 \cdot 5 \equiv 1 \pmod{n}$ är helt i analogi med att ha hittat en matrisinvers, rent tekniskt säger vi att talet 7 är den *multiplikativa inversen* till 5 modulo 17. Nu kan vi resonera så här:

$$5 \cdot x \equiv 11 \pmod{17} \Rightarrow$$

$$7 \cdot 5 \cdot x \equiv 7 \cdot 11 \pmod{17} \Rightarrow$$

$$1 \cdot x \equiv 77 \pmod{17} \Leftrightarrow x \equiv 9 \pmod{17}.$$

Så $5 \cdot x \equiv 11 \pmod{17} \Rightarrow x \equiv 9 \pmod{17}$. Men nu kan vi också gå åt andra hållet:

$$x \equiv 9 \pmod{17} \Rightarrow 5 \cdot x \equiv 5 \cdot 9 \pmod{17} \Leftrightarrow 5 \cdot x \equiv 45 \pmod{17}$$

och den sista kongruensen är just återigen $5 \cdot x \equiv 11 \pmod{17}$. Den här utredningen betyder alltså att

$$5 \cdot x \equiv 11 \pmod{17} \Leftrightarrow x \equiv 9 \pmod{17}$$

och det var just den multiplikativa inversen av 5 modulo 17 (som var 7) som gjorde att vi kunde hitta den här ekvivalensen. Och det faktum att ekvivalensen gäller innebär alltså att vi hittat alla x som uppfyller kongruensen och det är precis det som vi menar med att lösa en kongruens. Svaret är alltså $x \equiv 9 \pmod{17}$.

Den viktiga åtgärden här var användningen av Bezouts sats. Och det finns ingenting i det här exemplet som bara gäller just talen 5 11 och 17. Talet 11 (högerledet) spelar knappt någon roll alls i resonemangen. Så vi kan formulera en allmän sats om lösningarna till sådana här kongruenser.

Sats: Kongruensen $a \cdot x \equiv b \pmod{n}$ har en lösningar i x i form av en kongruensklass för varje heltal b om och endast om $\gcd(a, n) = 1$.

Bevis: Vi antar först att $\gcd(a, n) = 1$. Enligt Bezouts sats finns då heltal s, t sådana att $s \cdot a + t \cdot n = 1$. Talet s kallas här som sagt en multiplikativ invers till a. Men då har vi denna följd av implikationer:

$$a \cdot x \equiv b \pmod{n} \Rightarrow s \cdot a \cdot x \equiv s \cdot b \pmod{n} \Rightarrow 1 \cdot x \equiv s \cdot b \pmod{n} \Rightarrow x \equiv s \cdot b \pmod{n} \Rightarrow$$

$$a \cdot x \equiv a \cdot s \cdot b \pmod{n} \Rightarrow a \cdot x \equiv 1 \cdot b \pmod{n} \Rightarrow a \cdot x \equiv b \pmod{n}$$

och vi har alltså funnit att $a \cdot x \equiv b \pmod{n} \Leftrightarrow x \equiv s \cdot b \pmod{n}$ det vill säga kongruensen har precis de lösningar som hävdades: i form av en kongruensklass. (Talet b var godtyckligt under hela resonemanget.)

Omvänt antar vi nu att $a \cdot x \equiv b \pmod{n}$ har en lösningar i x i form av en kongruensklass för varje heltal b. Specifikt finns då en lösning (i form av en kongruensklass) för heltalet $b = 1$. Vi betecknar denna kongruenssklass med $x \equiv s \pmod{n}$ och alltså har vi

$$a \cdot s \equiv 1 \pmod{n}$$

som kan skrivas ut som $s \cdot a = 1 + k \cdot n \Leftrightarrow s \cdot a - k \cdot n = 1$. Men denna identitet kan bara gälla om $\gcd(a, n) = 1$ (enligt kommentaren som följde Bezouts sats). Alltså gäller $\gcd(a, n) = 1$ och beviset är klart.

Exempel: Ta fram den multiplikativa inversen till $\overline{11}$ i $\mathbb{Z}_{36}$ och använd den för att hitta alla heltal sådana att $11x \equiv 7 \pmod{36}$.

Lösning: Vi börjar med att hitta den största gemensamma delaren till 11 och 36, den är 1, men vi vill hitta s, t sådana att $s \cdot 11 + t \cdot 36 = 1$, då kommer $\overline{s}$ att vara den multiplikativa inversen till $\overline{11}$ i $\mathbb{Z}_{36}$. Vi genomför Euklides utvidgade algoritm:
$36 = 3 \cdot 11 + 3$, $11 = 3 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, vi ser här botten (gcd=1) så vi går baklänges:
$1 = 3 - 2 \cdot 1$, $1 = 3 - (11 - 3 \cdot 3) \cdot 1 \Leftrightarrow 1 = 4 \cdot 3 - 1 \cdot 11$, $1 = 4 \cdot (36 - 3 \cdot 11) - 1 \cdot 11$, $1 = 4 \cdot 36 - 13 \cdot 11$.
Detta betyder att $-13 \cdot 11 \equiv 1 \pmod{36}$, men om vi vill ha ett s i intervallet $0, 1, \ldots, 35$ så kan vi använda att $x \cdot y \equiv 1 \pmod{n} \Leftrightarrow (x + k \cdot n) \cdot y \equiv 1 \pmod{n}$ och skriva

$$-13 \cdot 11 \equiv 1 \pmod{36} \Leftrightarrow (36 - 13) \cdot 11 \equiv 1 \pmod{36} \Leftrightarrow 23 \cdot 11 \equiv 1 \pmod{36}$$

och detta ger oss att $s = 23$ så att den multiplikativa inversen av $\overline{11}$ i $\mathbb{Z}_{36}$ är $\overline{23}$.
Nun kan vi lösa kongruensekvationen $11x \equiv 7 \pmod{36}$. Vi börjar med att skriva om den i $\mathbb{Z}_{36}$. Eftersom $\overline{11}$ tydligen har en multiplikativ invers i $\mathbb{Z}_{36}$ kan vi skriva kongruensen som ekvationen

$$\overline{11} \cdot \overline{x} = \overline{7}.$$

När vi nu multiplicerar båda sidor med den multiplikativa inversen av $\overline{11}$, som är $\overline{23}$ får vi

$$\overline{11} \cdot \overline{x} = \overline{7} \Leftrightarrow \overline{23} \cdot \overline{11} \cdot \overline{x} = \overline{23} \cdot \overline{7} \Leftrightarrow \overline{23} \cdot \overline{11} \cdot \overline{x} = \overline{161} = \overline{17} \Leftrightarrow$$

$$\overline{23} \cdot \overline{11} \cdot \overline{x} = \overline{1} \cdot \overline{x} = \overline{x} = \overline{17}.$$

Så lösningen i $\mathbb{Z}_{36}$ är $\overline{17}$. Detta ger att lösningen till den ursprunliga kongruensen är alla tal på formen

$$17 + 36 \cdot k, \quad k = 0, \pm 1, \pm 2, \ldots.$$

Övningar

4.4.1 *före detta 5.1.1* Gör en egen figur liknande figurren i början av detta avsnitt som var en karta över alla restklasser modulo 3 men basera din figur på restklasser modulo 5. Hur mnga rader (restklasser) blir det i din figur?

4.4.2 *före detta 5.1.2.* Skriv restklasserna hörande den första figuren i detta avsnitt (alltså kartan över alla restklasser modulo 3) med mängdnotation. (Klamrar osv.) Vad blir unionen av alla dessa restklasser? Vad blir snittet mellan två av dessa restklasser? Motivera dina påståenden.

4.4.3 *före detta 5.1.3.* Avgör vilka av följande påståenden som är sanna och vilka som är falska:
$2 \equiv 5 \pmod{3}$ $2 \equiv 5 \pmod{4}$ $2 \equiv -5 \pmod{6}$
$2 \equiv -5 \pmod{7}$ $-8 \equiv 4 \pmod{12}$ $-8 \equiv 4 \pmod{4}$
$-8 \equiv 4 \pmod{3}$ $-8 \equiv 4 \pmod{5}$ $23 \equiv 72 \pmod{7}$
$23 \equiv 72 \pmod{7}$
Motivera dina påståenden.

4.4.4 *före detta 5.1.4.* Bevisa del (i) och (ii) av satsen där dessa två delar utelämnades. ("Om $x \equiv y \pmod{n}$ så gäller ... ") Studera din egen figur från övning 4.4.1 för ett antal tal fr att se att satsen stämmer.

4.4.5 *före detta 5.1.5.* Bevisa följande räkneregler för kongruenser och ge ett par exempel på tal från din egen tabell från vning 4.4.1 fr att se att reglerna stämmer:

$$x_1 \equiv x_2 \pmod{n} \text{ och } y_1 \equiv y_2 \pmod{n} \Rightarrow x_1 + y_1 \equiv x_2 + y_2 \pmod{n} \text{ samt } x_1 \cdot x_2 \equiv y_1 \cdot y_2 \pmod{n}.$$

4.4.6 *före detta 5.1.6.* Vilken rest fås då $411 \cdot 821 + 376 \cdot 297$ divideras med 7?

4.4.7 *före detta 5.1.7.* Vilken rest får då 207^{61} divideras med 13? Vilken rest fås då 207^{6100} divideras med 13?

4.4.8 *före detta 5.1.8.* Är $(17^{47} + 2^{12})^{14} - 4$ delbart med 13? Varför? Varför inte?

4.4.9 *före detta 5.1.9.* Studera följande additionstabell och multiplikationstabell för $\mathbb{Z}_3$:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

*	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Här symboliserar som vanligt $\overline{0}$, $\overline{1}$ och $\overline{2}$ restklasserna som uppkommer vid modulo 3. Visa, genom att välja exempel på tal ur de olika restklasserna att tabellerna troligen är korrekta. (Till exempel gäller, enligt additionstabellen, att $\overline{1}+\overline{2}=\overline{0}$. Detta exemplifieras av att talen 31 (som ligger i $\overline{1}$) och 14 (som ligger i $\overline{2}$) har summan $31 + 14 = 45$ och 45 ligger i $\overline{0}$.)

4.4.10 *före detta 5.1.10.* Gör om föregående övning fast med dessa tabeller för $\mathbb{Z}_4$ respektive $\mathbb{Z}_5$.

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

*	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

4.4.11 *före detta 5.1.11.* Konstruera additions- och multiplikationstabeller för $\mathbb{Z}_9$.

4.4.12 *före detta 5.1.12.* Konstruera additions- och multiplikationstabeller för $\mathbb{Z}_{11}$.

4.4.13 *före detta 5.1.13.* Kan du se någon intressant skillnad mellan multiplikationstabellerna från de två föregående uppgifterna? Kan du förklara denna skillnad?

6. Praktiska räkningar med kongruenser och liknande

Med kongruenser, delbarhet och bevismetoder som vi studerat i kapitel 1 och 2 har vi nu en del verktyg som kan använda för att göra olika utredningar och insikter om de hela talen. Detta avsnitt är tänkt som en paus, nu tittar vi på exempel på hur en del av det här används. De två kapitlen om relationer och fördjupad talteori kommer att bli mer teoretiska så deta här avsnittet är tänkt som en paus som sagt.

Vi tar ett par exempel.

Exempel: Visa att alla tal som är på formen $n^2 - n$ alltid är delbara med 2.

Lösning: Alla tal n kan enligt divisionsalgoritmen skrivas på formen $n = 2 \cdot q + r$ där $r = 0$ eller 1. Vi får således 2 fall:

Fall 1: $n = 2q$. Då får vi $n^2 - n = (2q)^2 - (2q) = 4q^2 - 2q = 2 \cdot (2q^2 - q)$. Detta är ett tal som är delbart med 2 och vi har alltså visa att $2|n^2 - n$ då $n = 2q$.

Fall 2: $n = 2q + 1$. Då får vi $n^2 - n = (2q + 1)^2 - (2q + 1) = 4q^2 + 4q + 1 - 2q - 1 = 4q^2 + 2q = 2 \cdot (2q^2 + q)$ vilket också är delbart med 2. Således har vi visat att $2|n^2 - n$ då $n = 2q + 1$.

Eftersom de enda två fallen som kan inträffa är $n = 2q$ och $n = 2q + 1$ och uttrycket $n^2 - n$ visade sig vara delbart med 2 i *båda* dessa möjliga fall saken klar.

Anmärkning: Vi skulle kunna löst detta med kongruenser också. Vi studerar ett liknande exempel där vi löser en uppgift av detta slag med kongruenser.

Exempel: Visa att alla tal som är på formen $n^3 - n$ alltid är delbara med 3.

Lösning: Vi ska alltså visa att $\forall n \in \mathbb{Z} : 3|n^3 - n$. Ett tal är delbart med 3 om och endast om det är kongruent med 0 modulo 3. Det betyder att om vi kan visa att $\forall n \in \mathbb{Z} : n^3 - n \equiv 0 (\text{mod } 3)$ så är vi klara. Alla tal n ligger i någon av de tre restklasserna $\overline{0}$, $\overline{1}$ eller $\overline{2}$ av $\mathbb{Z}_3$ så vi behöver bara kontrollera att $\overline{n}^3 - \overline{n} = \overline{0}$

för $n = 0$, 1 och 2 (tre representanter för alla elementen i $\mathbb{Z}_3$). Vi beräknar således

$0^3 - 0 \equiv 0 \pmod 3$ vilket visar att alla heltal ur $\overline{0}$ uppfyller kongruensen och $1^3 - 1 = 1 - 1 = 0 \equiv 0 \pmod 3$ vilket visar att alla heltal ur $\overline{1}$ uppfyller kongruensen och slutligen $2^3 - 2 = 8 - 2 = 6 \equiv 0 \pmod 3$ vilket visar att alla heltal i $\overline{2}$ uppfyller kongruensen.

Eftersom vi fann att alla heltal, från alla tre kongruensklasser uppfyller kongruensen må alltså kongruensen $n^3 - n \equiv 0 \pmod 3$ gälla för alla heltal, det till säga vi har visat

$$\forall n \in \mathbb{Z} : n^3 - n \equiv 0 \pmod 3.$$

Övningar

4.6.1 *före detta 5.2.1.* Visa att om ett tal inte är delbart med 3 så är kvadraten på talet kongruent med 1 modulo 3.

4.6.2 *före detta 5.2.2.* Visa att kvadraten på varje heltal antingen är kongruent med 0 eller 1 modulo 4.

4.6.3 *före detta 5.2.3.* Visa att $5|n^5 - n$ för alla positiva heltal n.

4.6.4 *före detta 5.2.4.* Gäller $6|n^6 - n$ för alla positiva heltal n? Gäller det för något heltal alls förutom 0 och 1?

Blandade övningar

4.1 *före detta 3.1.* Bilda mängderna

$$R = \{x \in \mathbb{Z} : x \text{ är jämnt}\}, \quad S = \{x \in \mathbb{Z} : x \text{ är delbart med } 3\}, \quad T = \{x \in \mathbb{Z} : x \text{ är delbart med } 6\}.$$

Vilka av följande påståenden är korrekta?

$$R \subset T \qquad T \subset R \qquad T \subset S \qquad R \cap S = T.$$

Ingen motivering krävs.
Från tentamen i diskret matematik den 28 augusti 2000.

4.2 *före detta 3.2.* Bevisa att ett heltal är delbart med 4 om och endast om det tal som bildas av de två sista siffrorna i talet också är delbart med 4. Exempel 12793742 är inte delbart med 4 eftersom 42 inte är delbart med 4. 12793724 är delbart med 4 eftersom 24 är delbart med 4.
Från tentamen i diskret matematik den 28 augusti 2000.

4.3 *före detta 3.3.* Finn största gemensamma delaren till talen 15400 och 990 med Euklides algoritm. Redovisa varje division.
Från tentamen i diskret matematik den 11 januari 2001. (Inte så lämplig som tentauppgift idag.)

4.4 3.4. Finn största gemensamma delaren till talen 77350 och 50050. Använd Euklides algoritm och redovisa varje enskild division.
Från tentamen i diskret matematik den 18 april 2001. (Inte så lämplig som tentauppgift idag.)

4.5 *före detta 3.5.* Visa att $3|n \cdot (2n+1) \cdot (4n+1)$ fr alla $n \geq 0$. *Ledning:* Divisionsalgoritmen säger att alla heltal n kan skrivas p formen $3q$, $3q+1$ eller $3q+2$. Utred varje fall. (Bevis genom trilemma.))
Från tentamen i diskret matematik den 13 januari 2004.

4.6 *före detta 3.6.* Visa att om n är ett udda tal s gller $8|n^2 - 1$. *Ledning:* Om n är udda, så kan n lämna två olika rester vid division med 4. Studera dessa båda fall.

4.7 *före detta 3.7.* Visa att $n \cdot (n^2 - 1)$ är delbart med 6 fr alla heltal n. *Ledning:* Utför 6 beräkningar, en då $n = 6q$, en då $n = 6q + 1$, en då $n = 6q + 2$, en då $n = 6q + 3$, en då $n = 6q + 4$ och en då $n = 6q + 5$.

4.8 *före detta 3.8.* Använd Euklides algoritm för att finna största gemensamma delare till talen 63063 och 2310. Varje kvot och rest i Euklides algoritm ska redovisas.
Från tentamen i diskret matematik den 13 januari 2004. (Inte så lämplig som tentauppgift idag.)

4.9 *före detta 3.10.* En lite mer omfattande uppgift som består av ett par deluppgifter som leder fram till en intressant sats om så kallade *primtalsöknar*. Det finns oändligt många primtal. Likväl finns det hur långa sekvenser som helst av heltal som följer på varandra där inget av talen är primtal.

(a) Visa att $2|n! + 2$ för alla $n \geq 2$.
(b) Visa att $k|n! + k$ för alla $n \geq 2$ och alla $k = 2, 3, \ldots, n$.
(c) Ange ett positivt heltal som har egenskapen att inget av de 999 därpå följande talen är primtal.
(d) Ange ett positivt heltal som har egenskapen att inget av de 9999 därpå följande talen är primtal.
(e) Lt N vara vilket tal som helst. Ange ett positivt heltal som har egenskapen att inget av de N därpå följande talen är primtal.

Anmärkning: Med $n!$ menas talet $n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot \ldots \cdot 4 \cdot 3 \cdot 2 \cdot 1$. Till exempel är $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 20 \cdot 6 \cdot 1 = 120$ och $3! = 3 \cdot 2 \cdot 1 = 6 \cdot 1 = 6$.)

Sista uppgift på tentamen i diskret matematik den 28 augusti 2000.