Kapitel 3 Grundläggande 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, ± 1, ± 2, ± 3,… osv. Man brukar ofta följa Gauss konvention att beteckna mängden av de hela talen med symbolen **Z** efter tyskans *zahl* (tal.)

3.1 Delbarhet och primtal

Om man väljer två godtyckliga heltal ur **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 **Z** om vi använder de vanliga operationerna addition, subtraktion och multiplikation. 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 ett heltal. Här inför vi vårt första begrepp: delbarhetsbegreppet.

Definition 3.1: 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 $a \mid b$. 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 $a \mid b \Leftrightarrow \exists k \in \boldsymbol{Z} : b = k \cdot a$.

Exempel:

- $3 \mid 12$ ty det finns ett tal *k* som uppfyller $12 = k \cdot 3$, talet *k* är här 4.

- $3 \nmid 13$ 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, $2 \mid 0$ ty det finns ett tal *k* som uppfyller $0 = k \cdot 2$, nämligen talet 0 självt. Vi kan fortsätta på samma sätt: $3 \mid 0$, ty vi kan välja *k* = 0 här också. $0 = 0 \cdot 3$. Alltså gäller $3 \mid 0$. Efter detta resonemang inser vi att alla tal delar 0. Vi har en sats:

Sats 3.1: Alla tal delar 0.
Bevis: Vi ska visa att $n \mid 0$ 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 $n \mid 0$. Eftersom *n* var godtyckligt valt måste $n \mid 0$ gälla för alla *n* vilket skulle bevisas.

Vi kan få en bättre förståelse för sats 1 om vi begrundar delbarhetsbegreppet. Att $3 \mid 12$ 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. $3 \mid 0$, javisst för $0 = 0 + 0 + 0$ (tre nollor.) $5 \mid 0$, 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 3.2: 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 tar ett exempel.

Exempel:

- 25 är delbart med 1 ty $25 = 25 \cdot 1$ så vårt k i delbarhetsdefinitionen blir 25 själv.
- 25 är delbart med –1 ty $25 = -25 \cdot -1$ så vårt k i delbarhetsdefinitionen blir –25.
- 25 är delbart med 25 ty $25 = 1 \cdot 25$ så vårt k i delbarhetsdefinitionen blir 1.
- 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 3.3: 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 sats 4 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 $\pm$ sig själva och ± 1 spelar en mycket viktig roll inom talteorin och kryptering. Dessa tal kallas primtal och vi ger en formell definition.

Definition 3.2: Låt p vara ett givet positivt heltal. Om p inte har några andra delare än $\pm p$ och ± 1 kallas p ett primtal.

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 $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 4 \cdot 2$, $9 = 3 \cdot 3$, $10 = 5 \cdot 2$, $12 = 6 \cdot 2$, $14 = 7 \cdot 2$, $15 = 5 \cdot 3$, $16 = 4 \cdot 4$, $18 = 9 \cdot 2$, $20 = 5 \cdot 4$, $21 = 7 \cdot 3$, $22 = 11 \cdot 2$, $24 = 6 \cdot 4$, $25 = 5 \cdot 5$, $26 = 13 \cdot 2$, $27 = 9 \cdot 3$ och $28 = 14 \cdot 2$.

Vi ger en alternativ defintion av primtal med kvantorer:

Definition 3.3: Låt n vara ett positivt heltal större än 1. Då kallas n ett primtal omm $\forall r \in Z : \forall s \in Z : n = r \cdot s \Rightarrow r = 1 \vee s = 1$.

Vad definitionen säger är att ett tal är primtal omm det bara kan delas upp i faktorer som är 1 eller sig själv.

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 för 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 således $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$. Vi ser på ett par exempel.

Exempel:

- $36 = 6 \cdot 6 = 3 \cdot 2 \cdot 3 \cdot 2 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$.
- $120 = 12 \cdot 10 = 4 \cdot 3 \cdot 5 \cdot 2 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 2 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$.
- $252 = 2 \cdot 126 = 2 \cdot 2 \cdot 63 = 2 \cdot 2 \cdot 9 \cdot 7 = 2^2 \cdot 3^2 \cdot 7$.

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 3.4: Låt n vara ett positivt heltal med primtalsfaktorerna p_1, p_2, …, p_k angivna i storleksordning och låt n innehålla a_1 stycken faktorer p_1, a_2 stycken faktorer p_2, … , 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:

Sats 3.4 Aritmetikens fundamentalsats: Låt n vara ett godtyckligt positivt heltal. Då finns en och endast en standardmässig primtalsfaktorisering av n.

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.

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

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

Vi kan välja vilket positivt tal som helst och faktorisera det hur som helst, plocka isär det i vilken ordning vi vill, vi kommer ändå alltid fram till precis en standardmässig primtalsfaktorisering av varje tal. Detta tack vare aritmetikens fundamentalsats vars bevis ligger utanför ramen för denna kurs.

3.2 Gemensamma delare

Vi startar med en definition på en gång.

Definition 3.5: 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 ju talet 1 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. Med *klass* menas mängd av element som har en viss egenskap. Vi ska börja med att studera den klass av tal som alla är delbara med 2.

Definition 3.6: Ett tal *a* sägs vara jämnt om och endast om det är delbart med 2.

De jämna talen är dessa: 0, ± 2, ± 4, ± 6, ± 8, ± 10, … och så vidare. Vi kan skriva dem med mängdnotation: Alla jämna tal = $\{2 \cdot k \mid k \in \mathbf{Z}\}$. 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, till exempel $73 \cdot 34 + 5 \cdot 10$ så får vi ett jämnt tal, i det här fallet 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 i själva verket 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 kan formulera det i en sats.

Sats 3.5: Antag att *d* är en gemensam delare till *a* och *b*. (Talet *d* var 2 ovan då vi alltså studerade jämna tal.) Då gäller:
(i) $d \mid a + b$ (Summan av två tal delbara med *d* blir alltså delbar med *d*, liksom summan av två jämna tal också är jämn.)
(ii) $d \mid k \cdot a$ för alla *k*. (Alla multiplar av ett tal delbart med *d* är också delbart med *d*.)
(iii) $d \mid x \cdot a + y \cdot b$ 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 det. Här blir alltså $x = 73$ och $y = 5$.)

Bevis: Eftersom $d \mid a$ och $d \mid b$ 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 (i), (ii) och (iii) gäller.

(i) 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 just att $d \mid a + b$ och (i) är bevisad.

(ii) 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 $d \mid k \cdot a$ vilket skulle bevisas.

(iii) Lämnas som övning.

Vi formulerar också beviset med kvantorer:
Vi har $d \mid a$ och $d \mid b \Rightarrow \exists t_1 \exists t_2 : a = t_1 \cdot d \wedge b = t_2 \cdot d$. Detta får till följd att $a + b = t_1 \cdot d + t_2 \cdot d = (t_1 + t_2) \cdot d = td$. Detta visar att $\exists k : a + b = k \cdot d$, nämligen $k = d$. Detta visar att $d \mid a + b$ vilket skulle bevisas.

Exempel:

Vi vet att $3 \mid 6$ och $3 \mid 21$. Talet 3 är alltså en gemensam delare till 6 och 21. Av satsen ovan kan vi alltså dra slutsatsen att $3 \mid 21 + 6$, $3 \mid 17 \cdot 21$, samt att $3 \mid 73 \cdot 3 - 2 \cdot 6$. Om vi kontrollerar vilka tal vi påstår är delbara med 3 så ser vi att det också stämmer. De tre talen är $21 + 6 = 27 = 9 \cdot 3$, $17 \cdot 21 = 357 = 119 \cdot 3$ och $73 \cdot 3 - 20 \cdot 6 = 213 - 60 = 153 = 51 \cdot 3$.

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: $\forall a \in Z : \forall b \in Z : 1 \mid a \wedge 1 \mid b$), och det kan som vi sett finnas flera gemensamma delare. Men det kan inte finnas hur stora gemensamma delare som helst. Alla 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*.

Definition 3.6: Låt *a* och *b* vara två givna positiva heltal. Med största gemensamma delaren 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*).

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, 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 drar slutsatsen 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 3.7: Två tal *a* och *b* kallas relativt prima varandra om de saknar andra gemensamma delare andra än 1 och –1. (Alla tal är delbara med 1 och –1.)

Enligt denna definition gäller alltså:

a och *b* är relativt prima varandra $\Leftrightarrow$ GCD(*a*, *b*) = 1.

Exempel:

- De enda tal som delar både 17 och 24 är talen 1, och –1. Alltså är 17 och 24 relativt prima varandra.

- 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.)

- Talen 12 och 15 går båda att dela med 3 (som är större än 1), alltså är dessa två tal inte relativt prima varandra.

- 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.)

Ett annat sätt att säga samma sak är att tal som är relativt prima varandra saknar gemensamma faktorer andra än talen 1 och –1.

3.3 Divisionsalgoritmen och Euklides algoritm

Om man dividerar b med a och $a \mid b$ 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 rest 3 vilket uttrycker att vi kan stuva in 2 stycken 4:or i 11 men sedan blir det 3 över. Vi illustrerar det i figur 3.1

Elva kryss kan placeras i 2 grupper om 4 var och då blir det 3 över.

xxxx xxxx xxx

$11 = 4 \cdot 2 + 3$

Figur 3.1

Vi kan formulera en allmän sats om hur vi dividerar tal med varandra även om vi inte divisionen skulle går jämnt ut.

Sats 3.6 Divisionsalgoritmen: Låt n vara ett givet heltal. För varje positivt heltal d finns då entydigt bestämda tal q och r med $0 \le r \le d - 1$ sådana att

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

Talet d kallas här divisor och r kallas här rest.

Villkoret $0 \le r \le d - 1$ 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 $n = q \cdot d + r$ då vi lägger på det extra kravet $0 \le r \le d - 1$. Vi ska införa lite terminologi i en definition innan vi tar ett par exempel.

Definition 3.8: 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.

Exempel:

- 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 $n = q \cdot d + r$ eftersom talet r ligger i intervallet 0 till och med 4 – 1 = 3. Kvoten i divisionen måste således vara 2 och resten 3. Divisionen går inte jämnt ut. Som vi sett i figur 3.1 illustreras kvoten som det antal grupper av d element som n element räcker till. Har vi 11 kryss som i figur 1.3 räcker det till att formera 2 grupper av 4 kryss i och kvoten blir således 2. Det blir 3 kryss över och det kallas då divisionens rest.

- Låt $n = 56$ och $d = 17$. Vi har $56 = 3 \cdot 17 + 5$. Kvoten blir således 3 och resten blir 5.

- 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.

- 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).

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* en liten stund. 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 multipler av *d*. (12259 och 3887 är båda multipler av *d*.) Men detta innebär att *d* även delar 598 eftersom ju $598 = 12259 - 3 \cdot 3887$. 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*' som är större än *d* och som delar både 598 och 3887. Det talet *d*' 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 just det största talet som delar både 12259 och 3887. Således 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 således reducerat till att finna GCD(3887, 598). Vi upprepar nu steget 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

$$598 = 2 \cdot 299 + \mathbf{0}.$$

Nollan är en stoppsignal i Euklides algoritm. I nästa steg ska vi beräkna 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:

$$d = \text{GCD}(12259, 3887) = \text{GCD}(3887, 598) = \text{GCD}(598, 299) = \underline{299}.$$

Vi tar ett exempel till.

Exempel (Hämtat från tentamen i diskret matematik den 23 oktober 2003):

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)
$910 = 5 \cdot 182 + \mathbf{0}$ (kvot 5, rest **0**, stoppsignal!)

GCD(18200, 3822) = GCD(3882, 2912) = GCD(2912, 910) = GCD(910, 182) = <u>182</u>.

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