Explorativ övning 4

PRIMTALEN, MULTIPLIKATION OCH DIOFANTISKA EKVATIONER*

Syftet med detta avsnitt är att bekanta sig med delbarhetsegenskaper hos heltalen.

De viktigaste begreppen är

- Aritmetikens fundamentalsats
- Diofantiska ekvationer

Detta avsnitt kan betraktas som en kort inledning till talteorin. Eftersom talteorin ger en möjlighet till flera mycket intressanta problem, som ofta kan formuleras enkelt och elementärt, är antalet övningar ganska stort. Flera av dessa övningar finns som illustration för att visa att talteorin verkligen är en källa till roliga problem och kan med fördel redan mycket tidigt utnyttjas i skolarbete.

Vi återkommer till talteorin senare i avsnittet om "Restaritmetiker" (som ofta kallas för "klockaritmetiker").

ARITMETIKENS FUNDAMENTALSATS

Nu kan vi förklara primtalens viktiga roll som byggstenar för alla heltal – varje heltal större än 1 är en entydig produkt av primtal. T ex

$$\begin{aligned} 100 &= 2^2 \cdot 5^2, \\ 108 &= 2^2 \cdot 3^3, \\ 2002 &= 2 \cdot 7 \cdot 11 \cdot 13. \end{aligned}$$

Ett primtal t ex 5 betraktas också som produkt av primtal – produkt med endast en faktor 5 (dvs $5 = 5$). En sådan överenskommelse har stora fördelar – den förenklar många formuleringar (t ex kan vi säga att varje naturligt tal större än 1 är en produkt av primtal).

*preliminär version

Först visar vi en mycket viktig egenskap hos primtalen som egentligen är nyckeln till aritmetikens fundamentalsats:

(4.1) Sats. *En primdelare till en produkt av två heltal är en delare till (minst) en av faktorerna dvs om $p|ab$ så $p|a$ eller $p|b$, då p är ett primtal och a, b är heltal.*

Bevis. Antag att $p \nmid a$. Då är SGD$(p, a) = 1$ därför att p är ett primtal. Enligt (4.7) existerar två heltal x, y sådana att $px + ay = 1$. Om man multiplicerar den likheten med b får man $b = pbx + aby$. Men enligt förutsättningen är $ab = pq$ för ett heltal q. Alltså är $b = p(bx + qy)$ dvs $p|b$. □

Observera att det inte har någon betydelse att den sista satsen handlar av ett primtal som delar en produkt av två faktorer – ett primtal som delar en produkt av ett godtyckligt antal faktorer måste dela någon av dessa. Vi utnyttjar denna egenskap av primtal i beviset av aritmetikens fundamentalsats:

(4.2) Aritmetikens fundamentalsats. *Varje heltal större än 1 är en entydig produkt av primtal dvs om*

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

där p_i och q_j är primtal så är $r = s$ och vid en lämplig numrering av faktorerna är $p_i = q_i$.

Bevis. Först visar vi att varje naturligt tal $n > 1$ är en produkt av primtal. Låt oss anta att det finns naturliga tal som inte kan skrivas som en sådan produkt. Låt oss välja bland dessa naturliga tal det minsta. Vi betecknar detta tal med n. Detta innebär att $n > 1$ är det minsta naturliga tal som inte är en produkt av primtal. Talet n är inte ett primtal (ett primtal är en produkt av primtal med bara en faktor). Alltså är n ett sammansatt tal dvs $n = n_1 n_2$, där både n_1 och n_2 är äkta delare till n dvs $1 < n_1 < n$ och $1 < n_2 < n$. Eftersom både $n_1 > 1$ och $n_2 > 1$ är mindre än n så måste dessa tal kunna skrivas som produkt av primtal (ty n är det minsta som inte kan skrivas). Men detta betyder att också n kan skrivas som produkt av primtal. På det sättet får vi att det inte finns något naturligt tal som inte kan skrivas som produkt av primtal.

Nu visar vi att varje naturligt tal $n > 1$ kan skrivas som produkt av primtal bara på ett sätt om man bortser från faktorernas ordningsföljd. På samma sätt som tidigare låt oss anta att det finns ett naturligt tal större än 1 som kan skrivas på olika sätt som en sådan produkt och låt $n > 1$ beteckna det minsta av alla naturliga tal som har olika framställningar:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

där $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ är primtal. Observera att n inte är ett primtal (ett primtal har endast en framställning). Eftersom p_1 är ett primtal och p_1 delar produkten $q_1 q_2 \cdots q_s$ så måste p_1 dela en av dess faktorer t ex p_1 delar q_1. Men q_1 är också ett primtal så att $p_1 = q_1$ (om ett primtal delar ett primtal så måste det vara samma primtal). Nu får vi:

$$\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s$$

så att talet $1 < \frac{n}{p_1} < n$ har två olika framställningar som produkt av olika primtal. Detta är dock omöjligt eftersom n var det minsta naturliga talet med olika framställningar. Slutsatsen är att det inte finns något minsta naturliga tal $n > 1$ med två olika framställningar som produkt av primtal. □

(4.3) Anmärkning. Ofta kallar man sats (4.1) för aritmetikens fundamentalsats. Även om formuleringen ovan handlar om positiva heltal så kan vi säga rent allmänt att varje heltal $N \neq 0, \pm 1$ är en produkt

$$N = \varepsilon p_1 p_2 \cdots p_n,$$

där p_i är primtal och $\varepsilon = \pm 1$. Enligt aritmetikens fundamentalsats är en sådan framställning entydig så när som på faktorernas ordningsföljd. Faktoruppdelningar av liknande typ är kända t ex för polynom. Vi diskuterar både faktoruppdelningar för heltalen och för polynom i ett senare avsnitt. □

Primfaktoruppdelningar av heltal ger en möjlighet att beräkna SGD(a, b) och MGM(a, b) utan Euklides algoritm. Även om denna möjlighet inte är särskilt praktisk används den flitigt i skolan.

(4.4) Exempel. Vi vill bestämma SGD(a, b) och MGM(a, b) då $a = 90$ och $b = 150$. Eftersom $a = 90 = 2 \cdot 3 \cdot 3 \cdot 5$ och $b = 2 \cdot 3 \cdot 5 \cdot 5$, så är SGD$(90, 150) = 2 \cdot 3 \cdot 5 = 30$. samt MGM$(90, 150) = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 450$. En primfaktor p ingår i SGD(a, b) om den ingår i både a och b. Dess exponent är minimum av exponenterna i a och b. En primfaktor p ingår i MGM(a, b) om den ingår i minst ett av talen a eller b. Dess exponent är maximum av exponenterna i a och b. □

(4.5) Anmärkning. Vi avslutar detta avsnitt med några kommentarer om primfaktoruppdelningar av heltal. Det är inte lätt att faktoruppdela ett helt godtyckligt heltal N i primfaktorer. Om N är ett relativt litet så kan man testa små primtal och kontrollera om de dividerar N. T ex om $N = 420$ så dividerar man först med 2, därefter med 2 igen, med 3, 5 och 7. Man brukar ibland skriva resultaten på följande sätt

420	2
210	2
105	3
35	5
7	7
1	

dvs $420 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 7$.

Den metoden förutsätter att vi känner till en lista över de små primtalen. Det är också viktigt att relativt snabbt kunna bedömma om talet är delbart med t ex 2, 3, 5, 7 osv. Sådana "delbarhetskriterier" diskuterar vi i ett senare avsnitt om restaritmetiker. Tyvärr fungerar sådana metoder endast då talen är små. För faktoruppdelningar av stora heltal krävs mycket avancerade metoder. De bästa kända algoritmerna för primtalsfaktorisering kräver c:a $N^{1/5}$ räkneoperationer för att hitta en primfaktor till N (om N är sammansatt och "slumpmässigt" valt). Om en räkneoperation tar $1\mu s$ och talet har 200

siffror, så krävs det $10^{40}\mu s \approx 3 \cdot 10^{26}$ år för att genomföra beräkningarna för N (10^6 datorer var och en kapabel att utföra en operation på $1\mu s$ skulle behöva $3 \cdot 10^{20}$ år för att klara dessa beräkningar!). Dessa omständigheter gör att tal $N = pq$, där p och q är stora primtal (med, säg, 100 siffror) används för säkerhetskryptering av känsliga uppgifter som t ex bankkoder. Vi diskuterar ett sådant system i samband med ett senare avsnitt om restaritmetiker. □

Övning A

1. Låt $a = 45$ och $b = 50$. Bestäm minsta gemensamma multipeln till dessa tal.
2. Låt a och b vara två heltal. Försök beskriva en procedur som ger MGM(a, b).
3. Visa att SGD(a, b) MGM$(a, b) = ab$ och förklara hur denna formel kan användas till beräkningar av MGM(a, b). Använd formeln i den första uppgiften ovan.

   Ledning. Låt $a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ och $b = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$ vara faktoruppdelningar av a och b i produkt av olika primtal $p_1, p_2, \ldots, p_r$ (några av exponenterna $k_1, k_2, \ldots, k_r$ och $l_1, l_2, \ldots, l_r$ kan vara lika med 0). Med vilken exponent ingår t ex p_1 i SGD(a, b), MGM(a, b) och ab? Jämför exponenterna för p_1 i SGD(a, b) MGM(a, b) och i ab.

• Se även Vretblad-Ekstig, avsnitt 2.4 och tillhörande övningar.

Övning B

Diofantiska[†] ekvationer. Termen "Diofantisk ekvation" gäller ekvationer vars heltaliga eller rationella lösningar man vill bestämma. T ex att bestämma alla heltaliga lösningar (x, y, z) till ekvationen

$$x^2 + y^2 = z^2$$

eller alla heltalspar (x, y) som löser ekvationen

$$3^x - 2^y = 1.$$

Den första ekvationen ovan kallas Pythagoras ekvation och har oändligt många lösningar (t ex alla $(n^2 - 1, 2n, n^2 + 1)$, där n är ett heltal – $n = 2$ ger $(3, 4, 5)$). Den andra ekvationen (ett specialfall av Catalans[‡] ekvation) har en lösning $(2, 3)$. Den mest berömda av alla Diofantiska ekvationer är Fermats ekvation:

$$x^n + y^n = z^n,$$

[†]Diofantos (eller Diophantus) var en grekisk matematiker som levde i Alexandria omkring 250 e.Kr.. Troligen skrev han 13 volymer av ett verk under namnet "Arithmetica". 6 av dessa volymer finns bevarade.

[‡]Catalans ekvation är

$$x^y - z^t = 1.$$

Det är inte känt om denna ekvation har en lösning i naturliga tal skild från $x = 3$, $y = 2$, $z = 2$, $t = 3$.

där $n > 2$. Det tog mer än 350 år att lösa den ekvationen. I september 1994 visade den engelske matematikern Andrew Wiles att ekvationen saknar heltaliga lösningar (x, y, z) med $xyz \neq 0$[§].

I talteorin finns många närbesläktade problem som fortfarande väntar på sin lösning. Vi skall i denna övning syssla med mycket enkla Diofantiska ekvationer av typen $ax + by = N$.

1. Bestäm ett heltalspar (x_0, y_0) sådant att $2x+5y = 1$ (Du kan försöka gissa en lösning!). Bestäm därefter alla heltalspar (x, y) sådana att $2x + 5y = 1$.

   Ledning. Observera att om $2x + 5y = 2x_0 + 5y_0$ så är $2(x - x_0) = 5(y - y_0)$. Detta ger att $y - y_0 = 2k$ för ett heltal k. Uttryck y med hjälp av y_0 och därefter x med hjälp av x_0.

2. Låt (x_0, y_0) vara en lösning till ekvationen $ax+by = N$, där a och b saknar gemensamma delare (dvs a och b är relativt prima). Bestäm alla lösningar till denna ekvation dvs alla heltalspar (x, y) sådana att $ax + by = N$.

   Ledning. Gör som ovan.

Exempel : Linjära Diofantiska ekvationer.

Vi skall bestämma alla heltaliga lösningar (x, y) till ekvationen $12x + 28y = 20$. Först dividerar vi alla koefficienter med 4 och får den ekvivalenta ekvationen $3x + 7y = 5$. Nu behöver vi en *partikulär* lösning till denna ekvation. En sådan lösning kan vi rent allmänt beräkna med Euklides algoritm, men vi kan också gissa en lösning utan större problem. Först tar vi ekvationen $3x + 7y = 1$ och ser direkt att $x = -2$, $y = 1$ är en lösning. För att få en lösning till vår ekvation måste vi multiplicera denna med 5 dvs $x_0 = -10$, $y_0 = 5$ är en partikulär lösning till ekvationen $3x + 7y = 5$ (kontrollera!). Låt (x, y) beteckna en godtycklig heltalig lösning. Då är $3x + 7y = 3x_0 + 7y_0$. Alltså är $3(x - x_0) = 7(y_0 - y)$. Likheten visar att 3 dividerar högerled och eftersom 3 saknar gemensamma delare med 7 måste $3 \mid y_0 - y$ dvs $y_0 - y = 3k$, där k är ett heltal. Vi får $y = y_0 - 3k$ och insättning ger $3(x - x_0) = 7 \cdot 3k$ dvs $x - x_0 = 7k$. Alltså är $x = x_0 + 7k = -10 + 7k$, $y = y_0 - 3k = 5 - 3k$ med ett godtyckligt heltal k den allmänna lösningen till den givna ekvationen. □

• Se även Vretblad-Ekstig, avsnitt 2.7 och tillhörande övningar, speciellt 2.88, 2.89, 2.95. och blandade övningar till kap 2 speciellt: 2.105, 2.106, 2.107, 2.112.

• Läs övningarna nedan och välj ut några att fundera på! De anknyter till forskningsfrågor i talteori. För mer om primtal rekommenderas websajten "The Prime Pages´´ vid primes.utm.edu som innehåller mycket intressant om primtal känt fram till år 2012.

Övning C

Primtalstvillingar. Man säger att två primtal p och q är **tvillingar** om $q - p = 2$.

1. Skriv ut alla primtalstvillingar < 100.

[§]Det finns en mycket intressant bok av Simon Singh "Fermats gåta" som berättar om olika turer kring Fermats problem och dess lösning. Även filmen "Fermat's Enigma´´ som Simon Singh gjorde för BBC Discovery rekomenderas varmt till både matematiker och icke-matematiker. Den hittas på YouTube.

2. 3, 5 och 7 är "primtalstrillingar". Motivera att det inte finns några andra primtal p, q, r sådana att $r - q = q - p = 2$.

   Anmärkning. Primtalstvillingar intresserade människor redan under antiken. De nämns i Euklides böcker. Man vet inte om det finns oändligt många sådana primtalspar, men stora framsteg i denna fråga publicerades år 2013.

Övning D

Aritmetiska följder av primtal. Vi repeterar att en aritmetisk följd med differansen d är en följd av talen a, $a + d$, $a + 2d$, ..., $a + nd, \ldots$. (detta betyder att om $a_i = a + id$ och $a_{i+1} = a + (i + 1)d$, så är $a_{i+1} - a_i = d$ dvs differensen av två efterföljande tal i följden är lika med d). T ex är 11, 17, 23 en aritmetisk följd med differansen 6.

1. Skriv ut alla aritmetiska följder av primtal som är < 50 och som består av minst tre stycken primtal.

2. Försök skriva ut en aritmetisk följd bestående av 4 primtal.

   Anmärkning. Man vet att det finns godtyckligt långa aritmetiska följder av primtal. Men det finns godtyckligt långa avsnitt av de naturliga talen som saknar primtal t ex är $11! + 2$, $11! + 3, \ldots, 11! + 11$ tio efterföljande sammansatta tal (varför?). Vi har $11! = 1 \cdot 2 \cdots 11$ och rent allmänt $n! = 1 \cdot 2 \cdots n$ dvs $n!$ är produkten av alla naturliga tal från 1 till n.

3. Skriv ut en följd av 100 efterföljande sammansatta tal och generalisera Din konstruktion till en följd av n efterföljande sammansatta tal.

   Anmärkning. Dirichlet* visade 1828 att varje aritmetisk följd $a + nd$, där a och d är relativt prima (dvs SGD$(a, d) = 1$) och $n = 1, 2, 3, \ldots$ innehåller oändligt många primtal. T ex finns det enligt Dirichlets sats oändligt många primtal på formen $1 + 4n$ och oändligt många på formen $3 + 4n$.

Övning E

Goldbachs† förmodan. År 1742 formulerade Goldbach påståendet att varje jämnt heltal större än 2 är en summa av två primtal. T ex $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7$ osv. Ännu har man inte lyckats bevisa detta påstående.

1. Kontrollera Goldbachs förmodan för alla jämna heltal < 50.

2. Visa att Goldbachs förmodan implicerar att varje udda heltal större än 5 är en summa av tre primtal.

   Anmärkning. En rysk matematiker I.M. Vinogradov visade 1937 att varje udda heltal som är större än $3^{3^{15}}$ verkligen är en summa av tre primtal. Vingradovs konstant är så stor (mer än 7 miljoner siffror!) att det inte finns en chans att kontrollera hans sats för heltal mindre än $3^{3^{15}}$

*Peter Gustav Lejeune Dirichlet (13/2 1805 – 5/5 1859) var en mycket framstående tysk matematiker som bidrog med resultat till flera matematikgrenar.

†Christian Goldbach (18/3 1690 – 20/11 1764) var en tysk matematiker. Läs om Goldbachs förmodan i "Matte med mening" på sid. 36.

med hjälp av datorer. Nyligen reducerades storleken av den konstanten betydligt, men gränsen är fortfarande utom räckhåll för datorberäkningar. Det finns en Internet–sida där man kan skriva in ett godtyckligt jämnt heltal som därefter testas och presenteras som summa av två primtal – om detta är möjligt (talet kan inte vara för stort).

Övning F

Mersenne–primtal. De största kända primtalen hittar man bland så kallade Mersenne–tal $M_n = 2^n - 1$. Marin Mersenne började studera dessa tal år 1644. Talen M_n då $n = 2, 3, 5, 7, 13, 17, 19$ är primtal. T ex är $M_{19} = 2^{19} - 1 = 524287$ ett primtal. Man känner 35 Mersenne–primtal – det sista $2^{1398269} - 1$ upptäcktes i november 1996. Senaste nytt om Mersenne–talen kan fås på Internet (sök "Mersenne Prime").

1. Visa att talet M_{23} inte är ett primtal – kontrollera att $47|2^{23} - 1$.

2. Motivera att Mersenne–talen M_n inte är primtal då n är sammansatt.

   Ledning. Börja med jämna n.

Övning G

Formler för primtal. Man har studerat olika "formler" $f(n)$ som för varje n ger ett primtal (och helst alla).

1. L. Euler[‡] fann att $f(n) = n^2 + n + 41$ ger primtal då $n = 0, 1, 2, \ldots, 40$ (Du kan kontrollera detta fast det är lite jobbigt). Visa att det finns oändligt många n sådana att $f(n)$ är sammansatt.

   Anmärkning. Både C. Goldbach och L. Euler visade att varje polynom $f(n)$ med heltaliga koefficienter ger ett sammansatt tal för något n. Vi visar den satsen som en enkel övning i avsnittet om polynom.

2. Fermat trodde att hans tal $F_n = 2^{2^n} + 1$ är primtal för varje $n = 0, 1, 2, 3, \ldots$. Vi vet redan (se stencilen "Induktion och deduktion") att hans förmodan var falsk. Kontrollera med miniräknare att $641|F_5$.

   Anmärkning. Man har studerat andra "formler" för primtal. T ex vet man att det finns ett positivt reellt tal a sådant att heltalsdelen av talet a^{3^n} (dvs det största heltalet mindre än detta tal) är ett primtal för varje n. Men man känner tyvärr inte talet a. Det finns ett polynom i 26 variabler (av grad 25) som alltid ger primtal då variablerna antar icke–negativa heltaliga värden och polynomets värde är större än 0. Man får alla primtal, men de kommer inte i någon naturlig ordning. Man lyckades minska antalet variabler i liknande polynom, men man var tvungen att öka dess grad (se en mycket intressant bok av Paulo Ribenboim, "The Little Book of Big Primes", Springer–Verlag, 1991.

[‡]Leonhard Euler (15/4 1707 – 18/9 1783) var en schweizisk matematiker. Men han var verksam under många år i St Petersburg och Berlin. Eulers sysslade mest med matematik, men han gjorde också viktiga insatser i andra vetenskaper. Han var en av de mest produktiva vetenskapsmänen i historien och skrev hundratals artiklar och böcker. Under de sista åren av sitt liv var han blind, men han publicerade lika mycket som tidigare – han dikterade sina artiklar och böcker som skrevs av en betjänt. Euler hade 13 barn. Läs om Euler i "Matte med mening".

Övning H

Primtal i intressanta former.

1. Man visar att det finns oändligt många primtal p som är summor av två heltaliga kvadrater dvs $p = a^2 + b^2$, för två heltal a och b. Varje primtal p som lämnar resten 1 vid division med 4 kan skrivas på detta sätt (se vidare avsnittet om restaritmetiker). Visa att varje primtal som lämnar resten 3 vid division med 4 inte är en summa av två heltaliga kvadrater.

   Ledning. Både a och b i $p = a^2 + b^2$ måste vara udda.

   Anmärkning. Ganska nyligen visade två matematiker – J. Friedlander (University of Toronto) och H. Iwaniec (Rutgers University) – att det finns oändligt många primtal p som kan skrivas på formen $p = a^2 + b^4$ med heltal a och b. Detta resultat betraktas som en stor matematisk sensation.

2. Försök hitta 5 primtal p som kan skrivas på formen $p = a^2 + b^4$, där a och b är heltal.

3. Det är inte känt om $n^2 + 1$ är ett primtal för oändligt många n (men man tror att det är så). Visa att $n^2 + 1$ är sammansatt för oändligt många n.

   Anmärkning. Det finns många obesvarade frågor av liknande karaktär. Är t ex $n^2 + 2$ ett primtal för oändligt många n? Man vet inte om talet $n! + 1$ är ett primtal för oändligt många n. Vi nämnde Fermat–talen $F_n = 2^{2^n} + 1$ – man vet inte heller om det finns oändligt många primtal bland dessa.

APPENDIX: NÅGRA BEVIS

(4.6) Divisionsalgoritmen. *Om a och b är heltal och $b \neq 0$ så är*

$$a = bq + r, \quad \textit{där} \;\; 0 \leq r < |b|.$$

Både q (kallad **kvoten***) och r (kallad* **resten***) är entydigt definierade av a och b.*

Bevis. Först noterar vi att det räcker om vi bevisar satsen då $b > 0$ eftersom $b < 0$ innebär att $|b| = -b > 0$. Om satsen gäller då delaren är positiv, så är $a = (-b)q + r$, med $0 \leq r < |b|$. Denna likhet kan skrivas om till $a = b(-q) + r$. Alltså förutsätter vi vidare att $b > 0$.

Låt oss nu välja det största möjliga heltalet k sådant att $q \leq \frac{a}{b}$. Alltså är $q + 1 > \frac{a}{b}$. Dessa olikheter säger att $a - bq \geq 0$ och $a - bq < b$. Om vi betecknar $a - bq$ med r så får vi $a = bq + r$ och $0 \leq r < b$.

Slutligen visar vi att kvoten q och resten r definieras entydigt av a och b. Antag att:

$$a = bq + r = bq' + r,'$$

där $0 \leq r < |b|$ och $0 \leq r' < |b|$ dvs både q och q' är kvoter samt r och r' är rester. Då är $b(q - q') = r' - r$, så att b delar $r' - r$. Men både r och r' är mindre än $|b|$, vilket innebär att deras skillnad är delbar med b endast om de är lika dvs $r = r'$. Alltså är $bq = bq'$, så att $q = q'$ eftersom $b \neq 0$. □

(4.7) Sats. *Om a och b är heltal och $d = SGD(a, b)$ så existerar två heltal x_0 och y_0 sådana att*

$$d = ax_0 + by_0.$$

Bevis. Om $a = b = 0$ så är påståendet klart (som x och y kan man välja helt godtyckliga heltal). Anta att a eller b inte är 0. Det är klart att det finns positiva heltal som kan skrivas på formen $ax + by$ t ex om $a \neq 0$ så är $\pm a = a \cdot (\pm 1) + b \cdot 0$ och antingen a eller $-a$ är ett positivt heltal. Även $b = a \cdot 0 + b \cdot 1$ kan skrivas på formen $ax + by$. Låt d_0 vara det minsta positiva heltal som kan skrivas på den önskade formen dvs

$$(*) \qquad d_0 = ax_0 + by_0.$$

Vi påstår att $d_0 = d$. Först observerar vi att varje heltal $ax + by$ är delbart med d_0. För att bevisa detta delar vi $ax + by$ med d_0. Då är

$$ax + by = qd_0 + r,$$

där resten r är mindre än delaren d_0. Men

$$r = ax + by - qd_0 = ax + by - q(ax_0 + by_0) = a(x - qx_0) + b(y - qy_0)$$

så att r måste vara 0 ty annars får man ett tal som är mindre än d_0 och som kan skrivas på den önskade formen. Alltså dividerar d_0 både a och b ty bägge kan skrivas på formen $ax + by$. Ekvationen $(*)$ visar att om d' är en delare till a och b, så är d' en delare till d_0. Alltså är d_0 den största gemensamma delaren till a och b. □