Övningar till kapitel 3 Grundläggande talteori

3.1 Delbarhet och primtal

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.

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 eller ett par exempel.

3.1.3. Bevisa sats 3.1: Alla tal delar 0.

3.1.4. Bevisa sats 3.2: Talet 1 delar alla tal.

3.1.5. Bevisa sats 3.3: Låt n vara ett godtyckligt heltal. Då är n delbart med $\pm n$ samt ± 1.

3.1.6. Lista alla primtal minde än 100.

3.1.7. Formulera med kvantorer vad det innebär att ett tal inte är ett primtal.

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.

3.2 Gemensamma delare

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 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 8, det vill säga 1, 2, 4 och 8. Största gemensamma delaren är då 8.)

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

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.

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

3.3 Divisionsalgoritmen och Euklides algoritm

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 sådana att $n = q \cdot d + r$ och $0 \le r < d$. Ange q och r för följande 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?

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

3.3.3. Finn största gemensamma delare för följande par av tal med Euklides algoritm

7920 och 7020   151470 och 18700   3740 och 5733

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

3.3.5. Kan du finna två tal med differens 2 som inte är relativt prima?

Blandade Övningar

3.1. Bilda mängderna R = $\{x \in \boldsymbol{Z} \mid x \textit{ är jämnt}\}$, S = $\{x \in \boldsymbol{Z} \mid x \textit{ är delbart med } 3\}$, T = $\{x \in \boldsymbol{Z} \mid x \textit{ är delbart med } 6\}$. Vilka av följande påståenden är korrekta?

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

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

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.

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.

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.

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

3.6. Visa att om n är ett udda tal så gäller $8 \mid n^2 - 1$. (Ledning: Om n är udda, så kan n lämna två olika rester vid division med 4. Studera dessa båda fall.)

3.7. Visa att $n \cdot (n^2 - 1)$ är delbart med 6 för 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 $n = 6q + 5$.)

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.

3.9. En svårare uppgift: Låt $n > d > 0$ vara två givna heltal och låt q och r väljas så att villkoren för divisionsalgoritmen är uppfyllda, det vill säga så att $n = q \cdot d + r$ och $0 \leq r < d$. Visa att GCD(n, d) = GCD(d, r).
Ledning: Försök visa att GCD(n, d) $\leq$ GCD(d, r) och GCD(n, d) $\geq$ GCD(d, r).
Anmärkning: Det är detta som ligger till grund för Euklides algoritm.

3.10. En svårare 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 $2 \mid n!+2$ för alla $n \geq 2$.

b) Visa att $k \mid n!+k$ 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) Låt 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.

Övningar till kapitel 3 Grundläggande talteori

3.1 Delbarhet och primtal

3.1.1.
4 | 12 sann, ty 12 = 4*3.
3 | 20, falsk, ty 3 delar inte 20.
3 | 21, sann ty 21 = 7*3.
5 | 21, falsk ty 5 delar inte 21.
5 | 25, sann ty 25 = 5*5.
5 | -35 sann ty -35 = -7*5.
-5 | 35, sann ty 35 = -7*-5.
-5 | 36, falsk ty -5 delar inte 36.
6 | -36, sann ty -36 = -6*6.
1 | 20, sann ty 1 delar alla tal.
1 | -7 sann ty 1 delar alla tal.
-1 | 5 sann ty -1 delar alla tal.
-1 | -67 sann ty -1 delar alla tal.
0 | 30 falsk ty 0 delar inte 30.
0 | 10 falsk ty 0 delar inte 10.
10 | 0 sann ty alla tal delar 0.
20 | 0 sann ty alla tal delar 0.
-23 | 0 sann ty alla tal delar 0.

3.1.2. $a \nmid b \Leftrightarrow \sim (\exists k \in Z : b = a \cdot k) \Leftrightarrow \forall k \in Z :\sim (b = a \cdot k) \Leftrightarrow \forall k \in Z : b \neq a \cdot k$. Motsatsen till att a delar b blir således $\forall k \in Z : b \neq a \cdot k$, det vill säga ”För alla heltal k gäller att ekvationen $b = a \cdot k$ aldrig är uppfylld.” Exempel på detta är 3 som inte delar 20. Vi kan aldrig finna ett heltal k som uppfyller $20 = 3 \cdot k$. Samma sak gäller 4 som inte delar 30. etc.

3.1.3. Sats 3.1: Alla tal delar 0. Bevis: Låt n vara vilket tal som helst. Vi ska visa att n | 0. Det ska alltså finnas ett tal k sådant att $n \cdot k = 0$. Ett sådant tal är k = 0 ty vi har ju att $n \cdot 0 = 0$. Beviset är klart.

3.1.4. Sats 3.2: Talet 1 delar alla tal. Bevis: Låt n vara vilket tal som helst. Vi ska visa att 1| n. Det ska alltså finnas ett tal k sådant att $1 \cdot k = n$. Ett sådant tal är n själv. Vi säljer alltså k = n och har att $n \cdot 1 = n$. Beviset är klart.

3.1.5. Sats 3.3: Låt n vara ett godtyckligt heltal. Då är n delbart med $\pm n$ samt $\pm$ 1. Bevis: Sats 3.2 som bevisades ovan visa att 1 | n. På samma sätt man visa att -1 | n, vi väljer bara k = - n. Att ett tal n är delbart med sig självt är också klart eftersom k = 1 duger i delbarhetsdefinitionen ($n \cdot 1 = n$). För -n duger k = -1 ($-n \cdot -1 = n$). Beviset är klart.

3.1.6. Alla primtal minde än 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 83, 89, 97.

3.1.7. Formulera med kvantorer vad det innebär att ett tal inte är ett primtal.
Talet n är primtal $\Leftrightarrow \forall r \in Z_+ : \forall s \in Z_+ : r \cdot s = n \Rightarrow r = 1 \vee s = 1$. Negationen till detta blir: $\sim \forall r \in Z_+ : \forall s \in Z_+ : r \cdot s = n \Rightarrow r = 1 \vee s = 1 \Leftrightarrow \exists r \in Z_+ : \exists s \in Z_+ \sim (r \cdot s = n \Rightarrow r = 1 \vee s = 1)$. Vi vill nu negera en implikation. En implikation är falskt endast då dess förled är sant och dess efterled är falskt, så negationen av $r \cdot s = n \Rightarrow r = 1 \vee s = 1$ blir $r \cdot s = n \wedge \sim (r = 1 \vee s = 1)$. Vi använder DeMorgans lag på den sista negationen av disjunktion och får sammantaget

$\exists r \in Z_+ : \exists s \in Z_+ : r \cdot s = n \wedge r \neq 1 \wedge s \neq 1$. Detta utläses ”*n* har par av faktorer som båda inte är 1”. Till exempel är 30 inte ett primtal och 30 kan skrivas som $30 = 5 \cdot 6$. Talet 17 är däremot ett primtal och kan *inte* skrivas som en produkt av två positiva tal *r* och *s* som båda inte är 1. Något av dem måste bli 1 och då blir det andra förstås 17 (Om till exempel *r* = 1 så blir $17 = r \cdot s = 1 \cdot s$. Härav följer att *s* = 17).

3.1.8. 811 är primtal, 812 = $2^2 \cdot 7 \cdot 29$, 877 är primtal, 1213 är primtal, 1215 = $3^5 \cdot 5$, 640 = $2^6 \cdot 5^1$, 641 är primtal.

3.2 Gemensamma delare

3.2.1.

30 och 170:

$30 = 2 \cdot 3 \cdot 5$
$170 = 17 \cdot 10 = 2 \cdot 5 \cdot 17$
Vi läser av största gemensamma delare = $2 \cdot 5 = 10$.

18 och 60:

$18 = 2 \cdot 3^2$
$60 = 15 \cdot 4 = 2^2 \cdot 3 \cdot 5$
Vi läser av största gemensamma delare = $2 \cdot 3 = 6$.

76230 och 2772:

$76230 = 7623 \cdot 10 = 3 \cdot 2541 \cdot 2 \cdot 5 = 3 \cdot 7 \cdot 363 \cdot 2 \cdot 5 = 3 \cdot 7 \cdot 363 \cdot 2 \cdot 5 = 3 \cdot 7 \cdot 3 \cdot 121 \cdot 2 \cdot 5 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11^2$
$2772 = 2^2 \cdot 693 = 2^2 \cdot 3^2 \cdot 77 = 2^2 \cdot 3^2 \cdot 7 \cdot 11$
Vi läser av största gemensamma delare = $2 \cdot 3^2 \cdot 7 \cdot 11 = 1386$.

1320 och 92400:

$1320 = 132 \cdot 10 = 12 \cdot 11 \cdot 2 \cdot 5 = 4 \cdot 3 \cdot 11 \cdot 2 \cdot 5 = 2^3 \cdot 3 \cdot 5 \cdot 11$
$92400 = 924 \cdot 100 = 4 \cdot 231 \cdot 2 \cdot 5 \cdot 2 \cdot 5 = 2^2 \cdot 7 \cdot 33 \cdot 2 \cdot 5 \cdot 2 \cdot 5 = 2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11$
Vi läser av största gemensamma delare = $2^3 \cdot 3 \cdot 5 \cdot 11 = 1320$.
(Anmärkning: Eftersom 1320 | 92400 så blir GCD(92400, 1320) = 1320. Om a | b så blir likaledes GCD(a, b) = a.)

3.2.3. Sats: Låt *a*, *b* och *d* vara heltal. Då gäller $d \mid a$ och $d \mid b \;\Rightarrow\; d \mid a - b$ och $d \mid a \cdot b$. Bevis: $d \mid a$ och $d \mid b$ betyder att det finns tal t_1 och t_2 sådana att $b = t_1 \cdot d$ och $a = t_2 \cdot d$. Vi har då $a - b = t_2 \cdot d - t_1 \cdot d = (t_2 - t_1) \cdot d = heltal \cdot d$. Detta visar att $d \mid a - b$. Vi studerar nu $a \cdot b$ i ljuset av $b = t_1 \cdot d$ och $a = t_2 \cdot d$: $a \cdot b = t_1 \cdot d \cdot t_2 \cdot d = heltal \cdot d$ vilket visar att även $a \cdot b$ är delbart med *d*. Beviset är klart.

Satsen med kvantorer: $\forall a, b, d \in Z : d \mid a \wedge d \mid b \Rightarrow d \mid a - b \wedge d \mid a \cdot b$.

Med vanliga ord: ”Om heltalen *a* och *b* båda är delbara med *d* så måste också deras differens och produkt vara delbara med *d*.”

Motsatsen: (Som är falsk) $\sim (\forall a, b, d \in Z : d \mid a \wedge d \mid b \Rightarrow d \mid a - b \wedge d \mid a \cdot b) \Leftrightarrow \exists a, b, d \in Z : \sim (d \mid a \wedge d \mid b \Rightarrow d \mid a - b \wedge d \mid a \cdot b)$. Vi ska här negera en implikation och minns att negationen av $p \Rightarrow q$ är $p \wedge \sim q$. Vi får den ekvivalenta utsagan $\exists a,b,d \in Z : d \mid a \wedge d \mid b \wedge \sim (d \mid a-b \wedge d \mid a \cdot b)$ som med DeMorgans lag får utseendet $\exists a,b,d \in Z : d \mid a \wedge d \mid b \wedge (d \nmid a-b \vee d \nmid a \cdot b)$. I vanliga ord lyder detta: ”Det finns heltal tal *a*, *b* och *d* som har den egenskapen att *d* delar både *a* och *b*, men trots detta är antingen differensen eller produkten mellan *a* och *b* inte delbar med *d*.” (Detta är alltså en falsk utsaga.)

3.2.4. ”*a*, *b* är relativt prima” $\Leftrightarrow$ GCD(*a*, *b*) = 1 $\Leftrightarrow \forall d \in Z_+ : d \mid a \wedge d \mid b \Rightarrow d = 1$. Att två heltal *a* och *b* är relativt prima innebär att största (positiva) gemensamme delaren till dem är 1. Motsatsen med kvantorer lyder $\sim (\forall d \in Z_+ : d \mid a \wedge d \mid b \Rightarrow d = 1) \Leftrightarrow \exists d \in Z_+ :\sim (d \mid a \wedge d \mid b \Rightarrow d = 1)$. Här ska vi negera en implikation som återigen gör med $\sim (p \Rightarrow q) \Leftrightarrow p \wedge \sim q$. Det ger oss $\sim (\forall d \in Z_+ : d \mid a \wedge d \mid b \Rightarrow d = 1) \Leftrightarrow \exists d \in Z_+ : d \mid a \wedge d \mid b \wedge d \neq 1$. I ord blir detta: ”Det finns ett positivt heltal som är större än 1 och som delar både *a* och *b*”. Exempelvis är 25 och 30 inte relativt prima, de har en gemensam delare större än 1, till exempel 5. 27 och 30 är inte heller relativt prima och 3 är en gemensam delare som är större än 1. 25 och 12 är däremot relativt prima och den enda (och därmed största) gemensamma delaren är således 1.

3.2.5.
456 och 345:
Båda dessa tal är delbara med 3 varför de inte kan vara relativt prima.

123 och 235:
Dessa tal är relativt prima varandra eftersom de saknar gemensamma faktorer. (Kan ses i primtalsfaktoriseringarna.)

346 och 234:
Dessa tal är inte relativt prima varandra för de är båda jämna och därmed båda delbara med 2.

3.3 Divisionsalgoritmen och Euklides algoritm

3.3.1.
n = 11 och *d* = 2: Eftersom 11 = 4*2 + 3 har vi alltså *q* = 4 och *r* = 3. (Detta är figur 3.1 i kompendiet.)
n = 23 och *d* = 3: Eftersom 23 = 7*3 + 2 har vi alltså *q* = 7 och *r* = 2.
n = 45 och *d* = 9: Eftersom 45 = 5*9 + 0 har vi alltså *q* = 5 och *r* = 0.

n = 67 och *d* = 8: Eftersom 67 = 8*8 + 3 har vi alltså *q* = 8 och *r* = 3.
n = 34 och *d* = 7: Eftersom 34 = 4*7 + 6 har vi alltså *q* = 4 och *r* = 6.
n = -34 och *d* = 6: Eftersom -34 = -6*6 + 2 har vi alltså *q* = -6 och *r* = 2.

n = -11 och *d* = 2: Eftersom -11 = -6*2 + 1 har vi alltså *q* = -6 och *r* = 1.
n = -23 och *d* = 3: Eftersom -23 = -8*3 + 1 har vi alltså *q* = -8 och *r* = 1.
n = -45 och *d* = 9: Eftersom -45 = -5*9 + 0 har vi alltså *q* = -5 och *r* = 0.

Att *r* = 0 innebär att divisionen går jämnt ut. Ekvationen *n* = *q***d* + *r* tar då formen *n* = *q***d* vilket uttrycker ett delbarhetsförhållande, nämligen att *d* | *n*.

3.3.2.

540 och 7350:

$540 = 2^2 \cdot 3^2 \cdot 5 \cdot 13$

$7350 = 2 \cdot 3 \cdot 5^2 \cdot 7^2$

Vi läser av största gemensamma delare = $2 \cdot 3 \cdot 5 = 30$.

Euklides algoritm:

$$7350 = 13 \cdot 540 + 330$$
$$540 = 1 \cdot 330 + 210$$
$$330 = 1 \cdot 210 + 120$$
$$210 = 1 \cdot 120 + 90$$
$$120 = 90 + 30$$
$$90 = 3 \cdot \mathit{30} + \mathbf{0}.$$

Vi har nått nollan i Euklides algoritm och konstaterar således att *30* är största gemensamma delaren till 540 och 7350. Det har vi också tidigare kunnat konstatera från primtalsfaktoriseringarna.

204750 och 32760:

$204750 = 2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13$

$32760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$

Vi läser av största gemensamma delare = $2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 = 8190$.

Euklides algoritm:

$$204750 = 6 \cdot 32760 + 8190$$
$$32760 = 4 \cdot \mathit{8190} + \mathbf{0}$$

Vi har nått nollan i Euklides algoritm bara efter två divisioner och konstaterar således att *8190* är största gemensamma delaren till 32760 och 204750. Det har vi också tidigare kunnat konstatera från primtalsfaktoriseringarna.

35640 och 8316:

$35640 = 2^3 \cdot 3^4 \cdot 5 \cdot 11$

$8316 = 2^2 \cdot 3^3 \cdot 7 \cdot 11$

Vi läser av största gemensamma delare = $2^2 \cdot 3^3 \cdot 11 = 1188$.

Euklides algoritm:

$$35640 = 4 \cdot 8316 + 2376$$
$$8316 = 3 \cdot 2376 + 1188$$
$$2376 = 2 \cdot \mathit{1188} + \mathbf{0}$$

Vi har nått nollan i Euklides algoritm efter tre divisioner och konstaterar således att *1188* är största gemensamma delaren till 35640 och 8316. Det har vi också tidigare kunnat konstatera från primtalsfaktoriseringarna.

3.3.3.

7920 och 7020:

$$\begin{aligned}
&7920 = 1 \cdot 7020 + 900\\
&7020 = 7 \cdot 900 + 720\\
&900 = 1 \cdot 720 + 180\\
&720 = 4 \cdot \mathit{180} + \mathbf{0}
\end{aligned}$$

Svar: GCD(7920, 7020) = <u>180</u>.

151470 och 18700:

$$\begin{aligned}
&151470 = 8 \cdot 18700 + 1870\\
&18700 = 10 \cdot \mathit{1870} + \mathbf{0}
\end{aligned}$$

Svar: GCD(151470, 18700) = <u>1870</u>.

3740 och 5733:

$$\begin{aligned}
&5733 = 1 \cdot 3740 + 1993\\
&3740 = 1 \cdot 1993 + 1747\\
&1993 = 1 \cdot 1747 + 246\\
&1747 = 7 \cdot 246 + 25\\
&246 = 9 \cdot 25 + 21\\
&25 = 1 \cdot 21 + 4\\
&21 = 5 \cdot 4 + 1\\
&4 = 4 \cdot \mathit{1} + \mathbf{0}
\end{aligned}$$

Svar: GCD(5733, 3740) = <u>1</u>.
Anmärkning: 5733 och 3740 är alltså relativt prima.

3.3.4. Två på varandra följande tal måste vara relativt prima för om vi tillämpar Euklides algoritm på talet n + 1 och talet n får vi:

$$\begin{aligned}
&n + 1 = 1 \cdot n + 1\\
&n = n \cdot \mathit{1} + \mathbf{0}
\end{aligned}$$

vilket visar att GCD(n + 1, n) = 1. Detta är tydligen oberoende av vilket n vi väljer så två på varandra följande tal måste således alltid vara relativt prima varandra.

3.3.5. Talen 4 och 2 har differensen 2 och är inte relativt prima varandra. Deras största gemensamma delare är just 2.

Blandade Övningar

3.1.

$R \subset T$ är sann.
$T \subset R$ är falsk.
$T \subset S$ Är falsk.
$R \cap S = T$ är sann.

3.2.

Sats: Ett tal är delbart med 4 $\Leftrightarrow$ det tal det tal som bildas av de två sista siffrorna i talet också är delbart med 4.
Bevis: Låt *n* vara ett godtyckligt heltal med de två slutsiffrorna *a* och *b*. Då är $n = k \cdot 100 + a \cdot 10 + b$ för något *k*. En ekvivalens visas i två steg. Antag att *n* är delbart med 4. Vi ska nu visa att talet $a \cdot 10 + b$ också är delbart med 4. Att n är delbart med 4 innebär att det finns ett tal q sådant att $n = 4 \cdot q$. Vi har då $n = 4 \cdot q = k \cdot 100 + a \cdot 10 + b \Leftrightarrow a \cdot 10 + b = 4 \cdot q - k \cdot 100$. Men detta tal är delbart med 4 eftersom $4 \cdot q - k \cdot 100 = 4 \cdot q - 4 \cdot 25 \cdot k = 4 \cdot (q - 25 \cdot k)$. Vi har således visat att $a \cdot 10 + b = 4 \cdot \textit{ett heltal}$ det vill säga att $4 \mid a \cdot 10 + b$. Vi visar nu den andra implikationen och antar att $4 \mid a \cdot 10 + b$. Då finns ett tal q sådant att $a \cdot 10 + b = 4 \cdot q$. Då har vi $n = k \cdot 100 + a \cdot 10 + b = k \cdot 100 + 4 \cdot q = 4 \cdot 25 \cdot k + 4 \cdot q = 4 \cdot (25 \cdot k + q) = 4 \cdot \textit{ett heltal}$. Detta innebär att $4 \mid n$ vilket skulle visas. Sammantaget har vi visat $4 \mid n \Rightarrow 4 \mid a \cdot 10 + b$ och $4 \mid a \cdot 10 + b \Rightarrow 4 \mid n$. Detta betyder att $4 \mid n \Leftrightarrow 4 \mid a \cdot 10 + b$ vilket skulle bevisas.

3.3.

Euklides algortim tillämpad på 15400 och 990:

$$
\begin{aligned}
15400 &= 15 \cdot 990 + 550 \\
990 &= 1 \cdot 550 + 440 \\
550 &= 1 \cdot 440 + 110 \\
440 &= 4 \cdot \mathit{110} + \mathbf{0}
\end{aligned}
$$

Svar: GCD(15400, 990) = <u>110</u>.

3.4.

Euklides algoritm tillämpad på 77350 och 50050:

$$
\begin{aligned}
77350 &= 1 \cdot 50050 + 27300 \\
50050 &= 1 \cdot 27300 + 22750 \\
27300 &= 1 \cdot 22750 + 4550 \\
22750 &= 5 \cdot \mathit{4550} + \mathbf{0}
\end{aligned}
$$

Svar: GCD(77350, 50050) = <u>4550</u>.

3.5.

Sats: $3 \mid n \cdot (2n+1) \cdot (4n+1)$ för alla $n \geq 0$.
Bevis: Varje tal *n* ger antingen rest 0, 1 eller 2 vid division med 3. Således har vi $n = 3q$, $n = 3q + 1$ eller $n = 3q + 2$. Detta är tre fall som vi studerar var för sig.

Första fallet, $n = 3q$:
$n \cdot (2n+1) \cdot (4n+1) = 3 \cdot q \cdot (2 \cdot 3 \cdot q + 1) \cdot (4 \cdot n + 1) = 3 \cdot \textit{ett heltal}$. Detta tal måste således vara delbart med 3.

Andra fallet, $n = 3q + 1$:
$n\cdot(2n+1)\cdot(4n+1)=(3\cdot q+1)\cdot(2\cdot(3\cdot q+1)+1)\cdot(4\cdot(3\cdot q+1)+1)=(3\cdot q+1)\cdot(6\cdot q+2+1)\cdot(12\cdot q+5)=$
$(3\cdot q+1)\cdot(6\cdot q+3)\cdot(12\cdot q+5)=3\cdot(3\cdot q+1)\cdot(2\cdot q+1)\cdot(12\cdot q+5)=3\cdot \textit{ett heltal}$. Även här har vi alltså visat att $3\,|\,n\cdot(2n+1)\cdot(4n+1)$

Sista fallet, $n = 3q + 2$:
$n\cdot(2n+1)\cdot(4n+1)=(3\cdot q+2)\cdot(2\cdot(3\cdot q+2)+1)\cdot(4\cdot(3\cdot q+2)+1)=()\cdot()\cdot(12\cdot q+4\cdot 2+1)=()\cdot()\cdot(12\cdot q+9)=$
$3\cdot()\cdot()\cdot(4\cdot q+3)=3\cdot \textit{ett heltal}$.

I alla tänkbara fall är alltså $n\cdot(2n+1)\cdot(4n+1)$ delbart med 3 vilket skulle visas. Beviset är klart.

3.6.
Sats: Om *n* är ett udda tal så gäller $8\,|\,n^2-1$.
Bevis: Om *n* är udda gäller antingen $n=4\cdot k+1$ eller $n=4\cdot k+3$. Om $n=4\cdot k+1$ har vi
$n^2-1=(4\cdot k+1)^2-1=16\cdot k^2+2\cdot 4\cdot k+1-1=8\cdot(2\cdot k^2+k)=8\cdot \textit{ett heltal}$. Då är således n^2-1 delbart med 8. Om $n=4\cdot k+3$ har vi
$n^2-1=(4\cdot k+3)^2-1=16\cdot k^2+2\cdot 4\cdot k\cdot 3+3^2-1=^2-1=8\cdot 2\cdot k^2+8\cdot k\cdot 3+8=8\cdot(2\cdot k^2+k\cdot 3+1)=$
$8\cdot \textit{ett heltal}$ så även här blir tydligen n^2-1 delbart med 8. I alla tänkbara fall är n^2-1 delbart med 8 vilket skulle visas. Beviset är klart.

3.7.
Sats: Talet $n\cdot(n^2-1)$ är delbart med 6 för alla heltal *n*.
Bevis: Det finns 6 fall: $n = 6q$, $n = 6q + 1$, $n = 6q + 2$, $n = 6q + 3$, $n = 6q + 4$ och $n = 6q + 5$. Vi verfierar att $n\cdot(n^2-1)$ är delbart med 6 i de två första fallen. Resten lämnas till läsaren.
$n = 6q$: $n\cdot(n^2-1)=6\cdot q\cdot((6q)^2-1)=6\cdot \textit{ett heltal}$. Saken är klar. $n\cdot(n^2-1)$ är delbart med 6.
$n = 6q + 1$:
$n\cdot(n^2-1)=(6\cdot q+1)\cdot((6q+1)^2-1)=()\cdot(36q^2+12q+1^2-1)=()\cdot 6\cdot(6q^2+2q)=6\cdot \textit{ett heltal}$. Även här är saken klar, $n\cdot(n^2-1)$ är delbart med 6.
Beviset är klart. (Nästan, fallen $n = 6q + 2$, $n = 6q + 3$, $n = 6q + 4$ och $n = 6q + 5$ återstår.)

3.8.
Euklides algoritm tillämpad på 63063 och 2310:

$63063=27\cdot 2310+693$
$2310=3\cdot 693+231$
$693=3\cdot \mathit{231}+\mathbf{0}$

Svar: GCD(63063, 2310) = <u>231</u>.

3.9.

Sats: Låt $n > d > 0$ vara två givna heltal och låt q och r väljas så att villkoren för divisionsalgoritmen är uppfyllda, det vill säga så att $n = q \cdot d + r$ och $0 \leq r < d$. Då är GCD(n, d) = GCD(d, r).

Bevis: Kalla GCD(n, d) för a och GCD(d, r) för b. Vi ska visa att $a = b$. Eftersom $a \mid n$ och $a \mid d$ har vi $n = t_1 \cdot a$ och $d = t_2 \cdot b$ för några tal t_1 och t_2. Detta insatt i ekvationen $n = q \cdot d + r$ ger oss då $t_1 \cdot a = q \cdot t_2 \cdot a + r \Leftrightarrow r = a \cdot (t_1 - q \cdot t_2)$. Detta betyder att $a \mid r$. Så a är en gemensam delare till d och r. Eftersom b är den största gemensamma delaren till d och r måste vi ha olikheten $a \leq b$. Nu gör vi likadant med b. Eftersom b är en gemensam delare till d och r så finns tal s_1 och s_2 sådana att $d = s_1 \cdot b$ och $r = s_2 \cdot b$. Dessa båda likheter insatt i ekvationen $n = q \cdot d + r$ ger oss $n = q \cdot s_1 \cdot b + s_2 \cdot b = b \cdot (q \cdot s_1 + s_2) = b \cdot \mathit{ett\ heltal}$. Vi har visat att b även är en delare till n Och därmed en gemensam delare till n och d. Eftersom a är den största gemensamma delaren till n och d har vi alltså $a \geq b$. Vi har nu visat att både $a \leq b$ och $a \geq b$. Den enda möjligheten är nu att $a = b$ vilket är samma sak som att GCD(n, d) = GCD(d, r) (eftersom a och b bara var alternativa namn på dessa tal.) Beviset är klart.

Anmärkning: Detta var en svårare uppgift.

3.10.

a) Visa att $2 \mid n!+2$ för alla $n \geq 2$.

Bevis: $n!+2 = n \cdot (n-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1 + 2 = 2 \cdot (n \cdot (n-1) \cdot \ldots \cdot 3 \cdot 1 + 1) = 2 \cdot \mathit{ett\ heltal}$. Således gäller $2 \mid n!+2$.

b) Visa att $k \mid n!+k$ för alla $n \geq 2$ och alla $k = 2$, 3, …, n.

Bevis: Låt k vara ett godtyckligt tal mellan 2 och n. Då gäller:

$n!+k = n \cdot (n-1) \cdot \ldots \cdot (k+1) \cdot k \cdot (k-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1 + k = k \cdot (n \cdot (n-1) \cdot \ldots \cdot (k+1) \cdot (k-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1 + 1) =$

$k \cdot \mathit{ett\ heltal}$. Således gäller $k \mid n!+k$ för alla dessa k.

c) Talet 1000! + 1 har egenskapen att inget av de 999 därpå följande talen är primtal eftersom 1000! + 2 är delbart med 2, 1000! + 3 är delbart med 3, 1000! + 4 är delbart med 4 och så vidare upp till och med 1000! + 1000 som är delbart med 1000. Dessa tal, 1000! + 2, 1000! + 3, ..., 1000! + 1000 är 999 stycken.

d) Talet 10000! + 1 har egenskapen att inget av de 9999 därpå följande talen är primtal av samma anledning som förklarades i föregående deluppgift.

e) I analogi med b) och c) bildar vi nu talet (N + 1)! + 1 som således har egenskapen att inget av de N därpå följande talen är primtal. Vi kan välja N hur stort som helst och således skapa hur långa följder av på varandra följande heltal med egenskapen att inget av dem är primtal. Vi har skapat en så kallad *primtalsöken*.