LÖSNINGAR

till övningsuppgifter i

Grundkurs i talteori

av

Boris Sjöberg

§ 1. Tals delbarhet och upplösning i faktorer

Uppgift 1.1 a) $q = 13$, $r = 16$, b) $q = -23$, $r = 13$.

Uppgift 1.2 Då $a \mid b$ fås att $b = an$, där n är ett heltal $\neq 0$. Alltså är $|n| \geq 1$. Ekvationen $b = an$ ger nu $|b| = a|n| \geq a$, dvs. $a \leq |b|$.

Uppgift 1.3 Enligt divisionsalgoritmen existerar hela tal q och r, sådana att $a = nq + r$ och $0 \leq r < n$. Sätt $\nu = n - r$. Då är $1 \leq \nu \leq n$ och $a + \nu = nq + r + \nu = n(q + 1)$. Talet $a + \nu$ är alltså jämnt divisibelt med n. Något annat tal av formen $a + \nu$ med $1 \leq \nu \leq n$, som skulle vara divisibelt med n, existerar ej. Antag nämligen att vi skulle ha: $a + \nu = bn$ och $a + \nu' = b'n$, där $1 \leq \nu \leq n$ och $1 \leq \nu' \leq n$. Då vore $\nu - \nu' = n(b - b')$, dvs. $\nu - \nu'$ vore delbart med n. Å andra sidan är $|\nu - \nu'| \leq n - 1$. Detta ger $\nu = \nu'$, dvs. talet ν är entydigt bestämt.

Uppgift 1.4 $a^3 - a = a(a-1)(a+1)$. Talen $a - 1$, a och $a + 1$ är tre på varandra följande heltal. Enligt föregående uppgift är ett av dem delbart med 3. Då är även $a^3 - a$ delbart med 3.

Uppgift 1.5 (a) Ur $[x] \leq x$, $[y] \leq y$ fås $[x] + [y] \leq x + y$, där $[x] + [y]$ är ett heltal. Eftersom $[x + y]$ är det största heltalet $\leq x + y$, fås $[x + y] \geq [x] + [y]$.

(b) Olikheterna $[x] \leq x$, $[y] \leq y$ ger (då alla ingående tal är icke-negativa): $[x][y] \leq xy$, där $[x][y]$ är ett heltal. Eftersom $[xy]$ är det största heltalet $\leq xy$, fås $[xy] \geq [x][y]$.

Uppgift 1.6 För heltaligt x är $[x] + [-x] = 0$, för icke-heltaligt x är $[x] + [-x] = -1$.

Uppgift 1.7 Sätt $H = \{a - bq : q \in Z\}$. I mängden H finns alltid tal ≥ 0. För $q = [a/b]$ gäller nämligen $q \leq a/b$, som ger $a - bq \geq 0$. Låt nu P vara den delmängd av H, som består av icke-negativa tal. Enligt välordningsprincipen har P ett minsta tal $r = a - bq \geq 0$. För detta r och q gäller alltså $a = bq + r$ med $r \geq 0$. Återstår att visa att $r < b$. Enligt r:s definition gäller att $r - b \notin P$. Å andra sidan gäller att $r - b \in H$, eftersom $r - b = a - b(q + 1)$. Härav fås $r - b < 0$, dvs. $r < b$. Att talen r och q är entydigt bestämda av a och b, bevisas på samma sätt som i sats 1.6.

Uppgift 1.8 Sätt $n = [a/b]$. Då gäller enligt formel (1.1): $(a/b) - 1 < n \leq a/b$. Vi särskiljer nu två fall:

(a) $$(a/b) - \frac{1}{2} \leq n \leq a/b$$

(b) $$(a/b) - 1 < n < (a/b) - \frac{1}{2}.$$

I fallet (a) sättes $q = n$, i fallet (b) sätter vi $q = n + 1$. I bägge fallen sättes $r = a - bq$, varvid $a = bq + r$. I fallet (a) fås genom multiplikation med b: $a - \frac{b}{2} \leq bq \leq a$. Följaktligen är $0 \leq a - bq \leq \frac{b}{2}$, dvs. $0 \leq r \leq \frac{b}{2}$. I fallet (b) fås: $a - b < b(q-1) < a - \frac{b}{2}$, som ger $a < bq < a + \frac{b}{2}$. I detta fall gäller alltså: $-\frac{b}{2} < a - bq < 0$, dvs. $|r| < \frac{b}{2}$. I bägge fallen har vi sålunda $a = bq + r$, där q och r är hela tal med $|r| \leq \frac{b}{2}$.

Uppgift 1.9 Antag som antites att $n/p = ab$, där a och b är hela tal med $1 < a < n/p$, $1 < b < n/p$. Då är $n = abp$. Eftersom p är den minsta primfaktorn i n, fås: $a \geq p$, $b \geq p$. Detta ger $n \geq p^3$, vilket strider mot att $p > \sqrt[3]{n}$. Alltså är n/p ett primtal.

Uppgift 1.10 Vi har att i intervallet $[100,200]$ stryka alla heltaliga multipler av de primtal, som är $\leq \sqrt{200}$, således primtalen 2, 3, 5, 7, 11 och 13. Vi kan börja med att stryka alla jämna tal och alla tal, som slutar på 0 eller 5. Talet 102 är delbart med 3. Alltså skall vi stryka talen 102, 105, 108,... (såvida de ej redan är strukna). Då vi fortsätter på detta sätt t.o.m. multiplerna av talet 13, återstår slutligen primtalen i intervallet $[100,200]$. Dessa är: 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199.

§ 2. Primtalens fördelning

Uppgift 2.1 Primtalssatsen ger:

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = \lim_{x\to\infty} \frac{\pi(x)\log x}{x\log x} = \lim_{x\to\infty} \left(\pi(x) : \frac{x}{\log x}\right) \lim_{x\to\infty} \frac{1}{\log x} = 1 \cdot 0 = 0.$$

Uppgift 2.2 De givna uppskattningarna ger till en början:

(a) $$\pi(x) - \frac{x}{\log x} < \frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right) - \frac{x}{\log x} = \frac{3x}{2(\log x)^2}$$

(b) $$\pi(x) - \frac{x}{\log x} > \frac{x}{\log x}\left(1 + \frac{1}{2\log x}\right) - \frac{x}{\log x} = \frac{x}{2(\log x)^2}.$$

Genom att ånyo utnyttja de givna uppskattningarna får vi ur (a) och (b):

$$\frac{\pi(x) - \frac{x}{\log x}}{\pi(x)} < \frac{3x}{2(\log x)^2} : \left[\frac{x}{\log x}\left(1 + \frac{1}{2\log x}\right)\right] = \frac{3}{1 + 2\log x}$$

$$\frac{\pi(x) - \frac{x}{\log x}}{\pi(x)} > \frac{x}{2(\log x)^2} : \left[\frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right)\right] = \frac{1}{3 + 2\log x}.$$

Vi får således följande uppskattningar av det relativa felet:

$$\frac{1}{3 + 2\log x} < \frac{\pi(x) - \frac{x}{\log x}}{\pi(x)} < \frac{3}{1 + 2\log x}.$$

Eftersom bägge gränserna går mot noll när $x \to \infty$, så gäller detsamma även för det relativa felet.

Uppgift 2.3 Varje positivt heltal m kan skrivas i formen $m = 6q + r$, där q och r är heltal med $q \geq 0$ och $0 \leq r < 6$. Detta följer omedelbart ur divisionsalgoritmen. För $r = 0,2,3,4$ kan m uppenbarligen inte vara ett primtal, såvida ej $m = 2$ eller $m = 3$. Återstår endast möjligheterna $6q + 1$ och $6q + 5$ för primtal > 3. Nu är $6q + 5 = 6(q + 1) - 1$. Primtal > 3 kan alltså endast vara av formen $6n \pm 1$ med $n = 1, 2, 3, \ldots$

Uppgift 2.4 Låt $p\,(>3)$ vara ett primtal av formen $p=6n-1$. Vi bildar talet $N=(2\cdot3\cdot5\cdot7\cdots p)-1$, där talet inom parentes utgör produkten av alla primtal till och med p. Talet N är ej divisibelt med något av primtalen 2, 3, 5, 7,..., p (sats 1.5). Således innehåller N någon primfaktor $q>p$ (sats 1.7). Vi skall nu visa att det även finns någon primfaktor q av formen $q=6m-1$ $(m\in Z_+)$. Vi vet enligt föregående uppgift att q är antingen av formen $q=6m-1$ eller av formen $q=6m+1$ (då ju $q>3$). Produkten av två tal av formen $6m+1$ är av denna form, ty $(6a+1)(6b+1)=6(6ab+a+b)+1$. Vore nu alla primfaktorerna i N av formen $6m+1$, så vore alltså även N av formen $6m+1$. Men N är uppenbarligen av formen $N=6m-1$. Alltså måste någon primfaktor q i talet N vara av formen $q=6m-1$. Till varje primtal $p\,(>3)$ av formen $p=6n-1$ hör alltså ett annat primtal $q>p$ av samma form, vilket betyder att det finns oändligt många primtal av formen $6n-1$ $(n=1,2,3,\ldots)$.

Uppgift 2.5 Antag att 2^n-1 är ett primtal för något heltal $n\geq 2$. Antites: n är av formen $n=ab$ med $1<a<n,\ 1<b<n$. Då är

$$2^n-1=(2^a)^b-1=(2^a-1)((2^a)^{b-1}+(2^a)^{b-2}+\cdots+1).$$

Eftersom a och b är >1, är $M\equiv 2^a-1>1$ och $N\equiv(2^a)^{b-1}+\cdots+1>1$. Talet 2^n-1 är alltså av formen $2^n-1=MN$, där M och N är hela tal >1. Men detta strider mot att 2^n-1 är ett primtal. Alltså är även n ett primtal.

Uppgift 2.6 I en primtalstrilling $(p,p+2,p+4)\neq(3,5,7)$ måste vi ha $p\geq 5$. Antag alltså att p är ett primtal ≥ 5. Då är p antingen av formen $p=6n+1$ eller av formen $p=6n-1$ (uppgift 2.3). I det förra fallet är $p+2$, i det senare är fallet är $p+4$ av formen $6n+3$. Alltså är antingen $p+2$ eller $p+4$ divisibelt med 3. Vartdera talet kan således inte vara primtal. Härav följer att det inte existerar någon primtalstrilling $(p,p+2,p+4)$ med $p\geq 5$.

§ 3. Största gemensamma divisorn. Talteorins fundamentalsats

Uppgift 3.1 a) Man har (6,10,15) = 1. Ekvationen $6m+10n+15p=1$ satisfieras t.ex. av $m=1$, $n=1$, $p=-1$.

b) (70,98,105) = 7. Ekvationen $70m+98n+105p=7$ satisfieras t.ex. av $m=0$, $n=-1$, $p=1$. I bägge fallen existerar oändligt många linjärkombinationer, som uppfyller villkoren ifråga.

Uppgift 3.2 Antag först att $d=(a,b)$. Då d är en divisor i a och b, så existerar hela tal m och n, sådana att $a=md$, $b=nd$. Således är $m=a/d$, $n=b/d$. Av sats 3.4 (formel (3.7)) följer nu att $(m,n)=1$. Antag omvänt att det existerar hela tal m och n med de angivna egenskaperna. Då är $(a,b)=(md,nd)=d(m,n)=d$ enligt formel (3.6).

Uppgift 3.3 a) 26, b) 59.

Uppgift 3.4 Vi tillämpar Euklides algoritm på talen $5k+3$ och $3k+2$. Då fås:

$$\begin{aligned} 5k+3 &= 1\cdot(3k+2)+(2k+1)\\ 3k+2 &= 1\cdot(2k+1)+(k+1)\\ 2k+1 &= 1\cdot(k+1)+k\\ k+1 &= 1\cdot k+1\\ k &= k\cdot 1. \end{aligned}$$

Den sista från noll skilda resten är alltså $= 1$. Detta betyder att $(5k+3, 3k+2) = 1$.

Uppgift 3.5 Vi kan anta att $m \geq n$. Då man tillämpar divisionsalgoritmen på m och n, får man $m = nq + r$, där q och r är hela tal med $0 \leq r < n$. Detta ger oss följande identitet:

$$a^m - 1 = (a^n - 1)(a^{m-n} + a^{m-2n} + a^{m-3n} + \cdots + a^{m-qn}) + a^r - 1,$$

varvid $0 \leq a^r - 1 < a^n - 1$. Således gäller följande

Lemma. *Om r är den minsta positiva resten, när m divideras med n, så är $a^r - 1$ den minsta positiva resten, när $a^m - 1$ divideras med $a^n - 1$.*

Vi utför nu Euklides algoritm på talen $m = r_0$ och $n = r_1$. Vi får då följande schema:

$$\begin{aligned} r_0 &= r_1q_1 + r_2 && (0 < r_2 < r_1)\\ r_1 &= r_2q_2 + r_3 && (0 < r_3 < r_2)\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ r_{n-2} &= r_{n-1}q_{n-1} + r_n && (0 < r_n < r_{n-1})\\ r_{n-1} &= r_nq_n. \end{aligned}$$

Således är $(m,n) = r_n$. Vi tillämpar nu Euklides algoritm på talen $R_0 = a^m - 1$ och $R_1 = a^n - 1$. Då får vi med beaktande av lemmat och ovanstående schema:

$$\begin{aligned} R_0 &= R_1Q_1 + R_2, && R_2 = a^{r_2} - 1\\ R_1 &= R_2Q_2 + R_3, && R_3 = a^{r_3} - 1\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ R_{n-2} &= R_{n-1}Q_{n-1} + R_n, && R_n = a^{r_n} - 1\\ R_{n-1} &= R_nQ_n. \end{aligned}$$

Den sista från noll skilda resten är alltså $R_n = a^{r_n} - 1 = a^{(m,n)} - 1$, vilket representerar största gemensamma divisorn till talen $a^m - 1$ och $a^n - 1$.

Uppgift 3.6 T.ex. $m = -876$, $n = 401$. Ekvationen satisfieras av oändligt många värdepar m, n.

Uppgift 3.7 Sätt $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 5$, $a_5 = 8$, ... Enligt definitionen på Fibonacci-följden är $a_{\nu+2} = a_{\nu+1} + a_\nu$. Genom att i tur och ordning insätta $\nu = 1, 2, 3, \ldots, n$ och beakta att $a_2 = 2a_1$ får vi följande schema:

$$\begin{aligned} a_{n+2} &= a_{n+1} + a_n \\ a_{n+1} &= a_n + a_{n-1} \\ &\cdots\cdots\cdots\cdots \\ a_4 &= a_3 + a_2 \\ a_3 &= a_2 + a_1 \\ a_2 &= 2a_1. \end{aligned}$$

Men detta schema är ingenting annat än Euklides algoritm tillämpad på talen a_{n+2} och a_{n+1}. Då den sista från noll skilda resten $= a_1 = 1$, ser vi att $(a_{n+2}, a_{n+1}) = 1$. Eftersom detta gäller för godtyckligt n, är påståendet därmed bevisat.

Uppgift 3.8 Enligt formel (3.5) är $(a,b) = (a+b,b)$ och $(a,b) = (b,a) = (a+b,a)$. Härav följer att talen $a+b$ och a samt talen $a+b$ och b är relativt prima. Kor. 3.9 ger nu att talen $a+b$ och ab är relativt prima.

Uppgift 3.9 a) $2^3 5^2 7 \cdot 11^2$, b) $3^2 11 \cdot 101$, c) $7^2 13^2 17$.

Uppgift 3.10 a) $3^3 7 \cdot 11 \cdot 13 \cdot 37$, b) $3^2 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$, c) $2^3 7 \cdot 13 \cdot 19 \cdot 37 \cdot 757$.

Uppgift 3.11 Betrakta talräckan 1, 2, 3, ..., n. Av dessa tal är talen p, $2p$, $3p$, ..., $[n/p]p$ delbara med p, således $[n/p]$ stycken. Dessa tal bidrar alltså med $[n/p]$ faktorer p i $n!$ Av talen p, $2p$, $3p$, ..., $[n/p]p$ är talen p^2, $2p^2$, $3p^2$, ..., $[n/p^2]p^2$ dessutom delbara med p^2. Dessa ger ytterligare $[n/p^2]$ faktorer p i $n!$ Då vi fortsätter på detta sätt, får vi slutligen den sökta formeln. Eftersom $[n/p^k] = 0$ för tillräckligt stort k, blir endast ett ändligt antal termer i summan $\neq 0$. Genom att tillämpa formeln ifråga för $n = 20$ samt $p = 2, 3, 5, 7, 11, 13, 17, 19$ får vi $20! = 2^{18} 3^8 5^4 7^2 11 \cdot 13 \cdot 17 \cdot 19$.

Uppgift 3.12 a) 153153, b) 999999.

Uppgift 3.13 12068509.

Uppgift 3.14 Fyra lösningar: 1) $a = 18$, $b = 540$, 2) $a = 90$, $b = 108$, 3) $a = 54$, $b = 180$, 4) $a = 36$, $b = 270$. Dessutom fås ytterligare fyra lösningar med talen a och b omkastade.

Uppgift 3.15 Sätt $d = (a,b)$. Då är $a = md$, $b = nd$, där talen m och n är relativt prima (uppgift 3.2). Enligt sats 3.13 är $[a,b] = ab/d = mnd$. Således gäller enligt sats 3.4 (formel (3.6)):

$$(*) \qquad (a+b, [a,b]) = (d(m+n), mnd) = d(m+n, mn).$$

Enligt uppgift 3.8 är talen $m+n$ och mn relativt prima, dvs. $(m+n, mn) = 1$. Alltså gäller enligt $(*)$: $(a+b, [a,b]) = d = (a,b)$.

Uppgift 3.16 Talen är 308 och 490.

Uppgift 3.17 Låt x, y, z vara godtyckliga reella tal. Utan inskränkning av allmängiltigheten kan vi anta att $x \leq y \leq z$. Man ser då lätt att

(a) $$\max(x,y,z) - \min(x,y,z) = x + y + z - \min(x,y) - \min(x,z) - \min(y,z).$$

Vi antar att a, b och c har primfaktoriseringarna:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}, \qquad c = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}.$$

Sätt $M_i = \max(a_i, b_i, c_i)$, $m_i = \min(a_i, b_i, c_i)$, $u_i = \min(a_i, b_i)$, $v_i = \min(a_i, c_i)$, $w_i = \min(b_i, c_i)$ för $i = 1, 2, \ldots, n$. Då gäller enligt (a):

(b) $$M_i - m_i = a_i + b_i + c_i - u_i - v_i - w_i.$$

Enligt formlerna (3.17) och (3.20) gäller:

$$(a,b,c) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}, \qquad [a,b,c] = p_1^{M_1} p_2^{M_2} \cdots p_n^{M_n},$$

$$(a,b) = p_1^{u_1} p_2^{u_2} \cdots p_n^{u_n}, \qquad (a,c) = p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n}, \qquad (b,c) = p_1^{w_1} p_2^{w_2} \cdots p_n^{w_n}.$$

Detta ger, då vi dessutom beaktar formel (b):

$$\begin{aligned}
\frac{[a,b,c]}{(a,b,c)} &= p_1^{M_1 - m_1} p_2^{M_2 - m_2} \cdots p_n^{M_n - m_n} \\
&= \frac{p_1^{a_1+b_1+c_1} p_2^{a_2+b_2+c_2} \cdots p_n^{a_n+b_n+c_n}}{p_1^{u_1+v_1+w_1} p_2^{u_2+v_2+w_2} \cdots p_n^{u_n+v_n+w_n}} \\
&= \frac{(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})(p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n})(p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n})}{(p_1^{u_1} p_2^{u_2} \cdots p_n^{u_n})(p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n})(p_1^{w_1} p_2^{w_2} \cdots p_n^{w_n})} \\
&= \frac{abc}{(a,b)(a,c)(b,c)}.
\end{aligned}$$

Därmed är formel (3.23) bevisad.

Uppgift 3.18 a) $x = 21 + 14t$, $y = -21 - 21t$ $(t \in Z)$, b) ingen lösning, c) $x = 889 - 1969t$, $y = 633 - 1420t$ $(t \in Z)$.

Uppgift 3.19 5, 15 resp. 10 personer.

Uppgift 3.20 Antag att man vill köpa resechecker för $n \cdot 100$ mk. Man får då ekvationen $2x + 5y = n$. Den allmänna lösningen är i detta fall: $x = -2n + 5t$, $y = n - 2t$, där $t \in Z$. Villkoren $x \geq 0$, $y \geq 0$ ger: $2n/5 \leq t \leq n/2$. För $n = 1$ och $n = 3$ finns det inga heltaliga t, som satisfierar dessa olikheter. För $n = 2$ och $n \geq 4$ satisfieras olikheterna däremot alltid av något heltaligt t.

§ 4. Representation av tal

Uppgift 4.1 4783.

Uppgift 4.2 $(215252)_7$.

Uppgift 4.3 $(1334141)_5$.

Uppgift 4.4 $(54271)_9$.

Uppgift 4.5 Multiplikationstabellen lyder som följer:

	1	2	3	4
1	1	2	3	4
2	2	4	11	13
3	3	11	14	22
4	4	13	22	31

Multiplikationen ser ut på följande sätt (minnessiffrorna är utelämnade):

$$
\begin{array}{r}
3\,4\,0\,1 \\
2\,3\,1\,4 \\
\hline
3\,0\,1\,0\,4 \\
3\,4\,0\,1 \\
2\,1\,2\,0\,3 \\
1\,2\,3\,0\,2 \\
\hline
2\,0\,0\,4\,1\,4\,1\,4
\end{array}
$$

Uppgift 4.6 $(16674)_{16}$.

Uppgift 4.7 $(10010110110)_2$.

Uppgift 4.8 $(111110111)_2$.

Uppgift 4.9 Multiplikationstabellen lyder: $0 \cdot 0 = 0$, $0 \cdot 1 = 0$, $1 \cdot 0 = 0$, $1 \cdot 1 = 1$. Med stöd härav utföres multiplikationen på samma sätt som i uppgift 4.5 med beaktande av att basen = 2. Resultatet blir då $(10110001101)_2$.

Uppgift 4.10 Man delar in det binära talets siffror i grupper om 4 siffror i varje grupp börjande från slutet. Varje grupp representerar då en siffra i det hexadecimala systemet.

§ 5. Kongruenser

Uppgift 5.1 a) $m = 1, 2, 11, 22$, b) $m = 1, 3, 9, 27, 37, 111, 333, 999$, c) $m = 1, 11, 121, 1331$.

Uppgift 5.2 Ur $a \equiv b \pmod{c}$ fås $a = b + kc$, där k är ett heltal. Härav följer med stöd av sats 3.4: $(a, c) = (b + kc, c) = (b, c)$.

Uppgift 5.3 Kongruensen $a^2 \equiv b^2 \pmod{p}$ innebär att $a^2 - b^2 = (a-b)(a+b)$ är delbart med p. Då p är ett primtal, följer härav att $a - b$ eller $a + b$ (eventuellt vardera) är delbart med p (kor. 3.8). Detta ger: $a \equiv \pm b \pmod{p}$.

Uppgift 5.4 Att $n \equiv 3 \pmod{4}$ innebär att n är av formen $n = 4k + 3$, där k är ett heltal. För summan $a^2 + b^2$ av två heltalskvadrater kan tre fall inträffa: 1) a och b är vardera jämna tal. Då är $a^2 + b^2$ delbart med 4. 2) a är jämnt och b är udda (eller tvärtom). Då är $a^2 + b^2$ av formen $4m + 1$. 3) a och b är vardera udda. Då är $a^2 + b^2$ av formen $4m + 2$. I inget av de tre fallen är $a^2 + b^2$ av formen $4k + 3$. Således kan n inte vara summan av två heltalskvadrater.

Uppgift 5.5 a) 12, b) 1, c) 0.

Uppgift 5.6 a) –2, b) 2, c) 6.

Uppgift 5.7 a) 18, b) 1.

Uppgift 5.8 17.

Uppgift 5.9 Vi visar först att $2^{5^k} \equiv 32 \pmod{100}$ för alla heltaliga $k \geq 1$. Påståendet gäller för $k = 1$, emedan $2^5 = 32$. Antag nu att påståendet gäller för ett visst $k \geq 1$. Då är

$$2^{5^{k+1}} = (2^{5^k})^5 \equiv 32^5 \pmod{100}.$$

Vidare är

$$32^2 = 1024 \equiv 24 \pmod{100}$$
$$32^4 \equiv 24^2 = 576 \equiv 76 \pmod{100}$$
$$32^5 = 32 \cdot 32^4 \equiv 32 \cdot 76 = 2432 \equiv 32 \pmod{100}.$$

Således är $2^{5^{k+1}} \equiv 32 \pmod{100}$, om $2^{5^k} \equiv 32 \pmod{100}$. Påståendet följer nu av induktionsprincipen. Varje term i den givna summan är alltså kongruent med 32 modulo 100. Då är summan kongruent med $1991 \cdot 32 = 63712$ modulo 100. De två sista siffrorna i summan är således $= 12$.

Uppgift 5.10 a) $x \equiv 3 \pmod{7}$, b) $x \equiv 2 \pmod{3}$.

Uppgift 5.11 a) lösning saknas, b) $x \equiv -1 \pmod{1597}$.

Uppgift 5.12 De positiva inverserna ≤ 10 är: 1, 6, 4, 3, 9, 2, 8, 7, 5, 10. Alla övriga inverser är kongruenta med dessa modulo 11. Den sökta resten = –1.

Uppgift 5.13 a) Vi behöver uppenbarligen endast söka lösningar, som är inkongruenta modulo 7. Eftersom $(3,7) = 1$, så har kongruensen $3y \equiv 1 - 2x \pmod 7$ säkert en entydig lösning y modulo 7 för varje heltalsvärde på x. Vi insätter fördenskull $x = 0,1,2,3,4,5,6$ och löser de så erhållna kongruenserna med avseende på y. Då fås $(x,y) \equiv (0,5)$, $(1,2)$, $(2,6)$, $(3,3)$, $(4,0)$, $(5,4)$, $(6,1) \pmod 7$.

b) Vi skriver kongruensen i formen $4y \equiv 6 - 2x \pmod 8$. Eftersom $(4,8) = 4$, så har denna kongruens lösningar endast för sådana värden på x, för vilka $6 - 2x$ är delbart med 4. Dessa x-värden är $x = 1,3,5,7$. (Endast värden, som är sinsemellan inkongruenta modulo 8, behöver beaktas). För vart och ett av ovannämnda x-värden har kongruensen $4y \equiv 6 - 2x \pmod 8$ enligt sats 5.9 fyra sinsemellan inkongruenta lösningar modulo 8. Efter insättning av $x = 1,3,5,7$ fås följande lösningspar: $(x,y) \equiv (1,1)$, (1,3), (1,5), (1,7), (3,0), (3,2), (3,4), (3,6), (5,1), (5,3), (5,5), (5,7), (7,0), (7,2), (7,4), $(7,6) \pmod 8$.

Uppgift 5.14 Om vi betecknar den genomsnittliga varvtiden i sekunder med x, får vi kongruensen $25x \equiv 15 \pmod{60}$. Då $(25,60) = 5$ och $5 \mid 15$, så är kongruensen lösbar. Man ser lätt att $x_0 = 3$ är en partikulär lösning. Den allmänna lösningen är då enligt sats 5.9: $x = 3 + 12t$ $(t \in Z)$. Detta ger löptiden $25x = 75 + 300t$. För $t = 6$ fås tiden 31 min 15 sek, vilket är den mest sannolika. ($t = 5$ och $t = 7$ skulle ge en 5 min kortare resp. längre löptid). Den mot $t = 6$ svarande varvtiden är 75 sek.

Uppgift 5.15 $x \equiv 23 \pmod{30}$.

Uppgift 5.16 $x \equiv 28 \pmod{30}$. Använd substitutionsmetoden!

Uppgift 5.17 Ingen lösning.

Uppgift 5.18 Kongruensen innebär att $(x-1)(2x-1)$ bör vara divisibelt med 6. Detta kan apriori inträffa på fyra olika sätt: a) $x-1$ är delbart med 2 och $2x-1$ är delbart med 3, b) $x-1$ är delbart med 3 och $2x-1$ är delbart med 2, c) $x-1$ är delbart med 6, d) $2x-1$ är delbart med 6. Dessa fyra fall ger upphov till följande kongruenser:

a) $x \equiv 1 \pmod 2$ $\quad 2x \equiv 1 \pmod 3$ $\qquad$ b) $x \equiv 1 \pmod 3$ $\quad 2x \equiv 1 \pmod 2$ $\qquad$ c) $x \equiv 1 \pmod 6$ $\qquad$ d) $2x \equiv 1 \pmod 6$

Man ser genast att kongruenserna $2x \equiv 1 \pmod 2$ och $2x \equiv 1 \pmod 6$ saknar lösning. Fallen b) och d) kan alltså inte inträffa. Återstår fallen a) och c). Fallet a) har lösningen $x \equiv 5 \pmod 6$. Detta jämte c) ger den fullständiga lösningen till den givna kongruensen.

Uppgift 5.19 a) Vi använder ett fjärdedels dygn som tidsenhet. Om x betecknar antalet förflutna tidsenheter, när alla cyklerna samtidigt uppnår sitt maximum, så skall x satisfiera följande kongruenssystem:

$$\text{(a)} \qquad \begin{aligned} x &\equiv 23 \pmod{92} \\ x &\equiv 28 \pmod{112} \\ x &\equiv 33 \pmod{132}. \end{aligned}$$

Den första kongruensen ger $x = 23 + 92t$ $(t \in Z)$. När vi insätter detta värde på x i den andra kongruensen, får vi $92t \equiv 5 \pmod{112}$. Denna kongruens saknar lösning, emedan $(92,112) = 4$ och $4 \nmid 5$. Kongruenssystemet (a) har alltså ingen lösning, dvs. de tre cyklerna uppnår aldrig sitt maximum samtidigt.

b) Om x betecknar antalet förflutna dagar, när den ifrågavarande händelsen inträffar, så skall x satisfiera följande kongruenssystem:

$$\text{(b)} \qquad \begin{aligned} x &\equiv 0 \pmod{23} \\ x &\equiv 0 \pmod{28} \\ x &\equiv 0 \pmod{33}. \end{aligned}$$

Eftersom talen 23, 28 och 33 är parvis relativt prima, har systemet (b) enligt sats 5.10 en entydig lösning modulo $23 \cdot 28 \cdot 33 = 21252$. En partikulär lösning är uppenbarligen $x = 0$. Den allmänna lösningen är alltså: $x \equiv 0 \pmod{21252}$. Det går alltså 21252 dagar mellan varje gång, som de tre cyklerna passerar noll från minus till plus. Då $21252 \approx 58 \cdot 365$, så kan detta inträffa högst en gång (bortsett från födelseögonblicket) i en människas liv.

Uppgift 5.20 a) 2^8, b) 2^4, c) 2^{10}.

Uppgift 5.21 a) delbart, b) delbart, c) ej delbart.

Uppgift 5.22 a) ej delbart, b) delbart.

Uppgift 5.23 Talet ifråga må vara $n = a_p \cdot 10^p + a_{p-1} \cdot 10^{p-1} + \cdots + a_1 \cdot 10 + a_0$. Antag att $p = 3q + r$, där $0 \leq r \leq 2$. Då kan n skrivas i formen

$$\begin{aligned} n = {} & (a_0 + a_1 \cdot 10 + a_2 \cdot 10^2) \\ & + 10^3(a_3 + a_4 \cdot 10 + a_5 \cdot 10^2) \\ & + 10^6(a_6 + a_7 \cdot 10 + a_8 \cdot 10^2) \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & + 10^{3q}(a_{3q} + a_{3q+1} \cdot 10 + a_{3q+2} \cdot 10^2). \end{aligned}$$

Härvid är $a_{3q+2} = 0$, om $r \leq 1$. Om $r = 0$ är dessutom $a_{3q+1} = 0$. Då $10^3 \equiv -1 \pmod{7}$, $\pmod{11}$ och $\pmod{13}$, så är

$$
\begin{aligned}
n \equiv\ & (a_0 + a_1 \cdot 10 + a_2 \cdot 10^2) \\
& - (a_3 + a_4 \cdot 10 + a_5 \cdot 10^2) \\
& + (a_6 + a_7 \cdot 10 + a_8 \cdot 10^2) \\
& \ldots\ldots\ldots\ldots\ldots\ldots \\
& + (-1)^q (a_{3q} + a_{3q+1} \cdot 10 + a_{3q+2} \cdot 10^2) \pmod 7, \pmod{11}, \pmod{13}.
\end{aligned}
$$

Regeln för delbarhet med 7, 11 och 13 framgår nu omedelbart av kongruensen ovan.

Uppgift 5.24 a) Sätt $m = 875961$, $n = 2753$, $p = 24105520633$. Då är $s(m) = 9$, $s(n) = 8$, $s(p) = 4$. Härav fås $s(s(m) \cdot s(n)) = 9 \neq 4 = s(p)$. Multiplikationen är alltså inte korrekt utförd.

b) Sätt $m = 24789$, $n = 43717$, $p = 1092700713$. Då är $s(m) = 3$, $s(n) = 4$, $s(p) = 3$. Härav fås $s(s(m) \cdot s(n)) = 3 = s(p)$. Nioprovet stämmer alltså. Härav kan man emellertid *inte* sluta att multiplikationen är rätt utförd. I själva verket är den felaktig. Det rätta svaret är 1083700713.

Uppgift 5.25 Sätt $m = 89878$, $n = 58965$, $p = 5299?56270$. Härav fås $s(m) = 4$, $s(n) = 6$, $S(p) = 45 + x$, då den obekanta siffran betecknas med x. Således är $s(s(m) \cdot s(n)) = 6$. Genom att successivt insätta $x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ och beräkna $s(p)$ finner vi att endast $x = 6$ satisfierar ekvationen $s(p) = 6$. Den sökta siffran är alltså 6.

Uppgift 5.26 Lördag.

Uppgift 5.27 Svaret på den första frågan är individuellt och kan inte ges här. Beträffande den andra frågan kan följande utredning göras. Antag att personen ifråga är född den d:te dagen i m:te månaden år $1900 + Y$. (Härvid gäller samma modifikationer för m och Y som i teorin, för den händelse att födelsedagen ligger i januari – februari). Veckodagen W_0 för födelsedagen fås nu enligt formel (5.31), då vi beaktar att $C = 19$:

$$W_0 \equiv d + [2{,}6(m+1)] + Y + [Y/4] \pmod 7.$$

Härvid har vi även beaktat att $-35 \equiv 0 \pmod 7$. Låt nu W beteckna veckodagen den dag personen fyller x år. Då gäller:

$$W \equiv d + [2{,}6(m+1)] + Y + x + [(Y+x)/4] \pmod 7.$$

Observera att ingen justering ifråga om C behöver göras i det fall att $Y + x \geq 100$, eftersom år 2000 är ett skottår. Sättes nu $W \equiv W_0 \pmod 7$, fås följande villkorskongruens för x:

$$\text{(a)} \qquad x + [(Y+x)/4] - [Y/4] \equiv 0 \pmod 7.$$

Denna kongruens kan ytterligare förenklas. Antag nämligen att $Y = 4q + r$ med $0 \leq r \leq 3$. Då är $[(Y+x)/4] = q + [(r+x)/4]$ och $[Y/4] = q$. Kongruensen (a) övergår då i kongruensen

$$\text{(b)} \qquad x + [(r+x)/4] \equiv 0 \pmod 7.$$

Denna kongruens har nu olika lösningar beroende på r:s värde. Allmänt gäller att om x_0 är en lösning, så är varje x med $x \equiv x_0 \pmod{28}$ även en lösning. För varje värde på $r = 0, 1, 2, 3$ har kongruensen (b) 4 lösningar, som är sinsemellan inkongruenta modulo 28. Alla övriga lösningar är då kongruenta med dessa modulo 28. Genom att i tur och ordning insätta $r = 0, 1, 2, 3$ kan man för varje r bestämma de fyra inkongruenta lösningarna. Man får då följande tabell över x-värden ≤ 50, som satisfierar (b):

r	x						
0	6	17	23	28	34	45	
1	6	11	17	28	34	39	45
2	11	17	22	28	39	45	50
3	5	11	22	28	33	39	50

Uppgift 5.28 De sökta åren bör vara skottår, där 1 februari infaller en lördag. Om vi betecknar årtalet med $1900 + x$, så har vi att i formel (5.31) insätta $W = 6$, $d = 1$, $m = 14$, $Y = x - 1$ och $C = 19$. Vi får då efter diverse förenklingar:

(a) $$x + [(x-1)/4] \equiv 2 \pmod{7}.$$

Då året är ett skottår, sätter vi $x = 4y$, där y är en ny obekant. Då är $[(x-1)/4] = y - 1$, varför kongruensen (a) övergår i

$$5y \equiv 3 \pmod{7}.$$

Denna kongruens har enligt kor. 5.9 en entydig lösning modulo 7. Lösningen är $y \equiv 2 \pmod{7}$. Härur fås $y = 2, 9, 16, 23$, som ger $x = 8, 36, 64, 92$. De sökta årtalen är alltså: 1908, 1936, 1964 och 1992.

Uppgift 5.29 Härledningen följer samma riktlinjer som härledningen av formel (5.31). Vi använder samma beteckningar som vid denna härledning. Eftersom alla med 4 delbara delbara årtal var skottår i den julianska kalendern, får vi $S = [N/4]$ skottår under perioden från år 0 till år N. Sättes här $N = 100C + Y$, fås $S = 25C + [Y/4]$. För veckodagen d_N den 1 mars år N får vi alltså $d_N = d_0 + N + S$, då d_0 betecknar veckodagen den 1 mars år 0 i den julianska kalendern. Insättning av uttrycken för N och S ger:

(a) $$\begin{aligned} d_N &= d_0 + 125C + Y + [Y/4] \\ &\equiv d_0 + Y - C + [Y/4] \pmod{7}. \end{aligned}$$

Enligt uppgiften var den 1 mars 1582 en torsdag. Således är $d_N \equiv 4 \pmod{7}$ för $C = 15, Y = 82$. Insättning i (a) ger: $d_0 \equiv 1 \pmod{7}$. Den 1 mars år 0 var alltså en måndag. Härav fås

(b) $$d_N \equiv 1 + Y - C + [Y/4] \pmod{7}.$$

För att få veckodagen W för den d:te i den m:te månaden år N har vi nu att till d_N addera $d-1+t_m$, där t_m betecknar "månadstillägget" (5.30). Vi får då efter smärre förenklingar slutresultatet:

(c) $$W \equiv (d+4) + [2{,}6(m+1)] + (Y - C) + [Y/4] \pmod 7.$$

Uppgift 5.30 Om man med hjälp av formel (5.31) beräknar veckodagen för den 13:de i månaden för alla månader under åren 1600–1999, får man följande antal för de olika veckodagarna: 687 söndagar, 685 måndagar, 685 tisdagar, 687 onsdagar, 684 torsdagar, 688 fredagar och 684 lördagar. Då dessa tal divideras med deras summa 4800, får vi följande sannolikheter (i växande storleksordning) för att den 13:de i månaden skall infalla på angiven veckodag:

$$p(\text{torsdag}) = p(\text{lördag}) = 0{,}1425$$
$$p(\text{måndag}) = p(\text{tisdag}) = 0{,}1427$$
$$p(\text{söndag}) = p(\text{onsdag}) = 0{,}1431$$
$$p(\text{fredag}) = 0{,}1433$$

Sannolikheten är alltså störst för att den 13:de i månaden infaller på en fredag. Det finns m.a.o. ett visst fog för påståendet att den 13:de oftare infaller på en fredag än på någon annan veckodag. Därav följer dock inte att fredagen den 13:de är en olycksdag.

§ 6. Några speciella kongruenser

Uppgift 6.1 $25!/13! = 14 \cdot 15 \cdot 16 \cdots 25 \equiv 1 \cdot 2 \cdot 3 \cdots 12 = 12! \equiv -1 \pmod{13}$ enligt Wilsons sats. Huvudresten modulo 13 är alltså 12.

Uppgift 6.2 Formeln är trivial i fallet $p = 2$, $k = 1$. Vi kan därför i fortsättningen anta att p är udda. Vi skriver Wilsons sats i formen

$$(k-1)!k(k+1)(k+2)\cdots(p-1) \equiv -1 \pmod p.$$

Talen k, $k+1$, $k+2$,..., $p-1$ utbytes nu mot de därmed kongruenta talen $k-p$, $k+1-p$, $k+2-p$,..., (-1). Produkten av dessa tal kan skrivas i formen $(p-k)!(-1)^{p-k}$. Således är

$$(k-1)!(p-k)!(-1)^{p-k} \equiv -1 \pmod p.$$

Multiplikation med $(-1)^k$ ger:

$$(k-1)!(p-k)!(-1)^p \equiv -(-1)^k \pmod p.$$

Då p är udda, är $(-1)^p = -1$, varför vi får $(k-1)!(p-k)! \equiv (-1)^k \pmod p$.

Uppgift 6.3 Då $10^6 = 12 \cdot 83333 + 4$, fås med stöd av Fermat's lilla sats:

$$2^{10^6} = (2^{12})^{83333}2^4 \equiv 2^4 = 16 \equiv 3 \pmod{13}.$$

Således är $2^{10^6} \bmod 13 = 3$.

Uppgift 6.4 Sista siffran i talet 3^{100}, skrivet i 7-systemet, är $3^{100} \bmod 7$. (Jfr. algoritmen (4.2)). Nu är $100 = 6 \cdot 16 + 4$, varför Fermat's lilla sats ger:

$$3^{100} = (3^6)^{16}3^4 \equiv 3^4 = 81 \equiv 4 \pmod{7}.$$

Den sökta siffran är alltså 4.

Uppgift 6.5 Då p och q är olika primtal, är ingetdera av dem delbart med det andra. Fermat's lilla sats ger då: $q^{p-1} \equiv 1 \pmod{p}$ och $p^{q-1} \equiv 1 \pmod{q}$. Således är $q^{p-1} - 1$ och $p^{q-1} - 1$ divisibla med p resp. q. Detta medför att produkten

$$(q^{p-1} - 1)(p^{q-1} - 1) = p^{q-1}q^{p-1} - p^{q-1} - q^{p-1} + 1$$

är divisibel med pq. Eftersom termen $p^{q-1}q^{p-1}$ är divisibel med pq, så följer härav att $p^{q-1} + q^{p-1} - 1$ är divisibelt med pq, eller m.a.o. att $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Uppgift 6.6 Med beaktande av att $343 \equiv 2$ och $1024 \equiv 1 \pmod{341}$ fås

$$\begin{aligned} 7^{341} &= (7^3)^{113}7^2 = 343^{113}49 \equiv 2^{113}49 \\ &= (2^{10})^{11}2^3 49 = 1024^{11}8 \cdot 49 \equiv 392 \equiv 51 \not\equiv 7 \pmod{341}. \end{aligned}$$

Således är $7^{341} \not\equiv 7 \pmod{341}$, dvs. 341 är inte ett pseudoprimtal till basen 7.

Uppgift 6.7 Eftersom 2^{161038} är divisibelt med 2, så gäller:

(a) $$2^{161038} \equiv 2 \pmod{2}.$$

Då $161038 = 72 \cdot 2236 + 46$, så följer av Fermat's lilla sats:

$$2^{161038} = (2^{72})^{2236}2^{46} \equiv 2^{46} = (2^9)^5 2 = 512^5 2 \equiv 2 \pmod{73},$$

ty $512 \equiv 1 \pmod{73}$. Alltså gäller:

(b) $$2^{161038} \equiv 2 \pmod{73}.$$

Ur likheten $161038 = 146 \cdot 1102 + 146$ följer enligt Fermat's lilla sats:

$$\begin{aligned} 2^{161038} &= (2^{1102})^{146}2^{146} \equiv 2^{146} = (2^{16})^9 2^2 = 65536^9 4 \equiv 459^9 4 \\ &= (459^2)^4 459 \cdot 4 = 210681^4 1836 \equiv 8^4 1836 = 4096 \cdot 1836 \\ &\equiv 787 \cdot 733 = 576871 \equiv 2 \pmod{1103}. \end{aligned}$$

Således gäller:

(c) $$2^{161038} \equiv 2 \pmod{1103}.$$

Då nu $161038 = 2 \cdot 73 \cdot 1103$ och talen 2, 73 och 1103 är parvis relativt prima, så följer ur kongruenserna (a) – (c) med stöd av kor. 5.7:

$$2^{161038} \equiv 2 \pmod{161038},$$

vilket visar att 161038 är ett pseudoprimtal till basen 2.

Uppgift 6.8 Den sista siffran i talet 7^{1000} är 7^{1000} mod 10. Eftersom $\phi(10) = 4$ och $1000 = 4 \cdot 250$, så följer av Eulers sats:

$$7^{1000} = (7^4)^{250} \equiv 1 \pmod{10}.$$

Den sista siffran i talet 7^{1000} är alltså 1.

Uppgift 6.9 Då a är relativt primiskt till 63, är a även relativt primiskt till 7 och 9. Eftersom $\phi(7) = \phi(9) = 6$, så ger Eulers sats: $a^6 \equiv 1 \pmod{7}$ och $a^6 \equiv 1 \pmod{9}$. Härav följer med beaktande av att 7 och 9 är relativt prima: $a^6 \equiv 1 \pmod{63}$. (Jfr. kor. 5.7).

Uppgift 6.10 Eftersom $\phi(35) = 24$ och $100000 = 24 \cdot 4166 + 16$, så följer av Eulers sats:

$$\begin{aligned} 3^{100000} &= (3^{24})^{4166} 3^{16} \equiv 3^{16} = 81^4 \equiv 11^4 \\ &= 121^2 \equiv 16^2 = 256 \equiv 11 \pmod{35}. \end{aligned}$$

Således: 3^{100000} mod $35 = 11$.

Uppgift 6.11 a) Låt primfaktoriseringen av talet n vara

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

där vi kan anta att $p_1 < p_2 < \cdots < p_k$. Enligt formel (6.9) kan $\phi(n)$ skrivas i formen

(a) $$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_k^{a_k-1} (p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

Härav framgår att

(b) $$\phi(n) \geq (p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

Vi konstaterar först att n kan innehålla högst två olika primfaktorer, då $\phi(n) = 6$. Ty då $p_1 \geq 2$, $p_2 \geq 3$, $p_3 \geq 5$, ..., så skulle vi enligt (b) ha $\phi(n) \geq 1 \cdot 2 \cdot 4 = 8$, ifall antalet faktorer vore minst tre. Av (b) framgår även att ingen primfaktor kan vara > 7. Vidare kan faktorn 5 uteslutas, emedan

$\phi(n)$ då enligt (a) skulle innehålla en faktor 4. Möjliga primfaktorer i talet n är alltså 2, 3 och 7. Antag först att n innehåller två olika primfaktorer p_1 och p_2. Då är

(c) $$\phi(n) = p_1^{a_1-1}p_2^{a_2-1}(p_1-1)(p_2-1).$$

Genom att kombinera talen 2, 3 och 7 två och två och jämföra med (c) ser vi att endast följande fall kan inträffa: $n = 2 \cdot 3^2 = 18$ och $n = 2 \cdot 7 = 14$. Antag nu att n innehåller endast en primfaktor p. Då är n av formen $n = p^a$, varav fås $\phi(n) = p^{a-1}(p-1)$. Insättes här i tur och ordning $p = 2, 3, 7$, ser vi att endast följande två fall kan inträffa: $n = 3^2 = 9$ och $n = 7$. Resultatet blir alltså att $\phi(n) = 6$ för $n = 7, 9, 14$ och 18. *Anmärkning:* Samma resultat fås givetvis, om man beräknar $\phi(n)$ för $n = 1, 2, 3, \ldots, 18$ samt utväljer de n, för vilka $\phi(n) = 6$. Detta förfarande kräver emellertid, att man ytterligare visar att $\phi(n) \neq 6$ för alla $n \geq 19$.

b) Vi antar samma primfaktorisering för n som i moment a). Då $\phi(n) = 14$, måste någon av faktorerna i högra ledet av (a) vara delbar med 7. (Sats 3.9). Denna faktor är antingen 7 eller 14. Inget av talen $p_1 - 1, p_2 - 1, \ldots, p_k - 1$ är emellertid 7 eller 14, eftersom 8 och 15 inte är primtal. Alltså är något $p_i^{a_i-1} = 7$, vilket medför att $p_i = 7$ och $a_i = 2$. Då är $p_i - 1 = 6$ och således $\phi(n) \geq 7 \cdot 6 = 42$. Men detta är omöjligt, då $\phi(n) = 14$. Härav sluter vi att ekvationen $\phi(n) = 14$ saknar lösning i positiva heltal n.

Uppgift 6.12 Antag att m:s olika primfaktorer är $p_1, p_2, \ldots, p_h$. Då gäller enligt formel (6.9):

(a) $$\phi(m) = m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_h}).$$

Eftersom m delar n, innehåller n alla primfaktorerna i m jämte eventuellt ytterligare faktorer. Låt dessa tilläggsfaktorer vara $p_{h+1}, p_{h+2}, \ldots, p_k$. För $\phi(n)$ får vi alltså följande uttryck:

(b) $$\phi(n) = n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_h})(1-\frac{1}{p_{h+1}})\cdots(1-\frac{1}{p_k}).$$

Observera att det inte spelar någon roll i vilka potenser faktorerna $p_1, p_2, \ldots, p_k$ förekommer i primfaktoriseringarna av talen m och n, eftersom deras exponenter inte ingår i (a) resp. (b). Ur dessa formler följer att

(c) $$\frac{\phi(n)}{\phi(m)} = \frac{n}{m}(1-\frac{1}{p_{h+1}})\cdots(1-\frac{1}{p_k}) = \frac{n}{m}\cdot\frac{(p_{h+1}-1)\cdots(p_k-1)}{p_{h+1}\cdots p_k}.$$

Då m delar n, så innehåller heltalskvoten $\frac{n}{m}$ alla faktorerna $p_{h+1}, \ldots, p_k$. Dessa faktorer kan alltså förkortas bort i (c), som därmed representerar ett helt tal. Detta innebär att $\phi(m) \mid \phi(n)$.

Uppgift 6.13 Antag först att n är sammansatt. Om n innehåller en enda primfaktor p, så är n av formen $n = p^a$ med $a \geq 2$. Härvid är $\phi(n) = n(1-\frac{1}{p})$. Nu är $p \leq \sqrt{n}$ med likhet i fallet $a = 2$. Detta ger

(a) $$\phi(n) \leq n(1-\frac{1}{\sqrt{n}}) = n - \sqrt{n}.$$

Om n innehåller k (≥ 2) olika primfaktorer $p_1 < p_2 < \cdots < p_k$, så gäller enligt formel (6.9):

(b) $$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Enligt lemma 1.9 är $p_1 \leq \sqrt{n}$, vilket ger $n(1 - \frac{1}{p_1}) \leq n - \sqrt{n}$. De övriga faktorerna i högra ledet av (b) är alla < 1, varför vi nu får strikt olikhet i (a). Antag slutligen att n är ett primtal. Då är $\phi(n) = n - 1$ och således $\phi(n) > n - \sqrt{n}$. Detta bevisar att (a) medför att n är sammansatt.

Uppgift 6.14 Låt divisorerna i det perfekta talet n vara $d_1 < d_2 < \cdots < d_k$, varvid $d_1 = 1$ och $d_k = n$. Vi betraktar summan

$$s = \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k}.$$

Multiplikation med n ger

$$ns = \frac{n}{d_1} + \frac{n}{d_2} + \cdots + \frac{n}{d_k} = n + d_{k-1} + d_{k-2} + \cdots + 1.$$

Då n är perfekt, är $d_{k-1} + d_{k-2} + \cdots + 1 = n$, varför vi får $ns = 2n$. Alltså är $s = 2$.

§ 7. En tillämpning på kryptografi

Uppgift 7.1 Kryptotexten lyder 11 05 07 02 25 07.

Uppgift 7.2 Klartexten är HJÄLP.

Uppgift 7.3 Då $n = 35$, är $p = 5$, $q = 7$ och således $\phi(n) = 24$. Kalla krypterings- och dekrypteringsexponenterna e resp. d. Då skall gälla: $(e, 24) = 1$ och $ed \equiv 1 \pmod{24}$. Det förstnämnda villkoret innebär att e är ett udda tal, som inte är delbart med 3. Av talen $e-1$ och $e+1$ är alltså det ena delbart med 2, det andra med 4. Produkten $(e-1)(e+1)$ är alltså delbar med 8. Av de tre på varandra följande talen $e-1$, e och $e+1$ är exakt ett delbart med 3. Då e inte är delbart med 3, måste det ena av talen $e-1$ och $e+1$ vara delbart med 3. Alltså är $e^2 - 1 = (e-1)(e+1)$ delbart med 24, eller m.a.o. $e^2 \equiv 1 \pmod{24}$. Detta innebär att kongruensen $ed \equiv 1 \pmod{24}$ satisfieras av $d = e$. Någon annan modulo 24 inkongruent lösning existerar inte, eftersom kongruensen ifråga enligt kor. 5.9 har en entydig lösning d modulo 24.

Uppgift 7.4 Vi har att lösa ekvationssystemet $pq = 4386607$, $(p-1)(q-1) = 4382136$. Eftersom $(p-1)(q-1) = pq - (p+q) + 1$, finner vi att $p + q = 4472$. Talen p och q är alltså rötter till andra grads ekvationen $x^2 - 4472x + 4386607 = 0$. Då denna löses fås $p = 1453$, $q = 3019$.

§ 8. Primitiva rötter

Uppgift 8.1 Exponenterna är i nämnd ordning: 1, 12, 3, 6, 4, 12, 12, 4, 3, 6, 12 och 2.

Uppgift 8.2 a) 4, b) 4, c) 6.

Uppgift 8.3 $a \equiv 2, 7, 8, 13 \pmod{15}$.

Uppgift 8.4 Vi visar först att för varje positivt heltal m gäller:

(a) $$a^m \equiv 1 \pmod{n} \iff \bar{a}^m \equiv 1 \pmod{n}.$$

Antag först att $a^m \equiv 1 \pmod{n}$. Ur kongruensen $a\bar{a} \equiv 1 \pmod{n}$ fås då: $a^m\bar{a}^m = (a\bar{a})^m \equiv 1 \pmod{n}$. Då nu $a^m \equiv 1 \pmod{n}$, fås härur: $\bar{a}^m \equiv 1 \pmod{n}$. Alltså: $a^m \equiv 1 \pmod{n} \Longrightarrow \bar{a}^m \equiv 1 \pmod{n}$. Omvändningen visas analogt. Formel (a) ger nu omedelbart att $\mathrm{ord}_n a = \mathrm{ord}_n \bar{a}$.

Uppgift 8.5 Låt m vara ett positivt heltal med egenskapen

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

Då denna kongruens upphöjes till potenserna d resp. e, fås

$$1 \equiv (ab)^{md} = (a^d)^m b^{dm} \equiv b^{dm} \pmod{n}$$

resp.

$$1 \equiv (ab)^{me} = a^{em}(b^e)^m \equiv a^{em} \pmod{n}.$$

Vi har således: $a^{em} \equiv 1$ och $b^{dm} \equiv 1 \pmod{n}$. Härav följer med stöd av sats 8.1: $d \mid em$ och $e \mid dm$, vilket i sin tur ger $d \mid m$ och $e \mid m$, eftersom d och e är relativt primiska (jfr. sats 3.8). Talet m är således en gemensam multipel till d och e. Nu är emellertid $\mathrm{ord}_n(ab)$ det minsta positiva heltalet m, för vilket (a) gäller. Alltså är $\mathrm{ord}_n(ab) = [d, e] = de$, när d och e är relativt prima (jfr. sats 3.12).

Uppgift 8.6 Antag som antites att n är sammansatt. Då gäller enligt uppgift 6.13: $\phi(n) \leq n - \sqrt{n} \leq n - 2$, ty $n \geq 4$. Enligt sats 8.1 bör vi ha: $(n-1) \mid \phi(n)$. Men detta är omöjligt, då $\phi(n) \leq n - 2$. Alltså är n ett primtal.

Uppgift 8.7 a) 7, 13, 17, 19. b) Talet 12 saknar primitiva rötter enligt sats 8.10.

Uppgift 8.8 Eftersom $\phi(23) = 22$, så kan talet 5 endast höra till någon av exponenterna 1, 2, 11, 22 (kor. 8.1). Man finner följande kongruenser modulo 23: $5^1 \equiv 5$, $5^2 \equiv 2$, $5^{11} \equiv -1$. Talet 5 hör alltså inte till någon av exponenterna 1, 2 eller 11. Alltså måste 5 höra till exponenten 22, dvs. 5 är en primitiv rot modulo 23. Enligt sats 8.9 representeras alla primitiva rötter till 23 av de tal 5^m $(1 \leq m \leq 22)$, för vilka $(m, 22) = 1$, dvs. av talen $5^1, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}$. Då dessa tal reduceras modulo 23, fås talen 5, 10, 20, 17, 11, 21, 19, 15, 7, 14.

Uppgift 8.9 Av antagandet framgår att $4 \mid (p-1)$. Det existerar alltså enligt sats 8.8 exakt två tal, vilka hör till exponenten 4 modulo p. Låt a vara det ena av dem. Då är $a^4 \equiv 1 \pmod{p}$. Detta ger: $p \mid (a^2-1)(a^2+1)$, och då p är ett primtal, måste vi ha antingen $p \mid (a^2-1)$ eller $p \mid (a^2+1)$ (kor. 3.8). Vi kan inte ha $p \mid (a^2-1)$, ty då vore $a^2 \equiv 1 \pmod{p}$, vilket strider mot att a hör till exponenten 4 modulo p. Alltså gäller $p \mid (a^2+1)$, dvs. $a^2 \equiv -1 \pmod{p}$.

Uppgift 8.10 Index skall bestämmas endast för de positiva heltal ≤ 18, som är relativt primiska till 18, dvs. för talen 1, 5, 7, 11, 13, 17. Genom att bilda 5^i mod 18 för $i = 1,2,3,4,5,6$ finner vi följande kongruenser modulo 18:

$$5^1 \equiv 5, \quad 5^2 \equiv 7, \quad 5^3 \equiv 17, \quad 5^4 \equiv 13, \quad 5^5 \equiv 11, \quad 5^6 \equiv 1.$$

Härav fås: $\text{ind}_5 1 = 6$, $\text{ind}_5 5 = 1$, $\text{ind}_5 7 = 2$, $\text{ind}_5 11 = 5$, $\text{ind}_5 13 = 4$, $\text{ind}_5 17 = 3$.

Uppgift 8.11 a) $x \equiv 9 \pmod{13}$, b) $x \equiv 7, 8, 11 \pmod{13}$.

Uppgift 8.12 Kongruensen saknar lösning.

Uppgift 8.13 Kongruensen är lösbar för $a \equiv 2, 5, 6 \pmod{13}$. För $a = 2$ fås lösningarna $x \equiv 1, 5, 8, 12 \pmod{13}$. För $a = 5$ fås $x \equiv 2, 3, 10, 11 \pmod{13}$ och för $a = 6$ lösningarna $x \equiv 4, 6, 7, 9 \pmod{13}$.

Uppgift 8.14 Enligt definitionen på index gäller:

(a) $$s^{\text{ind}_s a} \equiv a \pmod{n}$$

samt

(b) $$s^{\text{ind}_s r \cdot \text{ind}_r a} = \left(s^{\text{ind}_s r}\right)^{\text{ind}_r a} \equiv r^{\text{ind}_r a} \equiv a \pmod{n}.$$

Då (a) och (b) jämföres, finner vi att

$$s^{\text{ind}_s a} \equiv s^{\text{ind}_s r \cdot \text{ind}_r a} \pmod{n}.$$

Härur följer $\text{ind}_s a \equiv \text{ind}_s r \cdot \text{ind}_r a \pmod{\phi(n)}$, då vi tillämpar sats 8.2 och beaktar att $d = \phi(n)$. Därmed är moment a) påvisat. Moment b) följer ur moment a), då vi sätter $a = s$ och beaktar att $\text{ind}_s s \equiv 1 \pmod{\phi(n)}$.

Uppgift 8.15 Då r är en primitiv rot till p, så är $r^{p-1} \equiv 1 \pmod{p}$. Talet

$$r^{p-1} - 1 = (r^{(p-1)/2} - 1)(r^{(p-1)/2} + 1)$$

är alltså delbart med p. Talet $r^{(p-1)/2} - 1$ kan ej vara delbart med p, ty detta skulle innebära att $r^{(p-1)/2} \equiv 1 \pmod{p}$, vilket strider mot att r är en primitiv rot till p. Alltså är $r^{(p-1)/2} + 1$ delbart med p (kor. 3.8), dvs. $r^{(p-1)/2} \equiv -1 \pmod{p}$. Detta bevisar påståendet.

§ 9. Kvadratiska rester

Uppgift 9.1 De kvadratiska resterna är 1, 2, 4, 8, 9, 13, 15 och 16.

Uppgift 9.2 $\left(\frac{a}{7}\right) = 1$ för $a = 1, 2, 4$. $\left(\frac{a}{7}\right) = -1$ för $a = 3, 5, 6$.

Uppgift 9.3 a) Eulers kriterium ger: $\left(\frac{7}{13}\right) \equiv 7^6 \pmod{13}$. Nu är $7^2 \equiv 10$ och $7^4 \equiv 100 \equiv 9 \pmod{13}$. Härav fås $7^6 \equiv 90 \equiv -1 \pmod{13}$. Alltså är $\left(\frac{7}{13}\right) = -1$.

b) Vi betraktar talföljden 7, 14, 21, 28, 35, 42. Talens huvudrester modulo 13 är: 7, 1, 8, 2, 9, 3. Av dessa är 7, 8 och $9 > 6{,}5$, dvs. 3 stycken. Då är $\left(\frac{7}{13}\right) = (-1)^3 = -1$.

Uppgift 9.4 Problemet är ekvivalent med att bestämma $\left(\frac{-2}{p}\right)$, då p är ett *udda* primtal. Varje udda primtal kan skrivas i någon av formerna $p = 8n \pm 1$ eller $p = 8n \pm 3$, där $n \in Z_+$. Det är alltså tillräckligt att undersöka $\left(\frac{-2}{p}\right)$ för dessa värden på p. Enligt formlerna (9.9) och (9.12) är

$$\left(\frac{-2}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8} = (-1)^{(p^2+4p-5)/8}.$$

Genom direkt insättning finner man lätt att $(p^2+4p-5)/8$ är jämnt för $p = 8n+1$ och $p = 8n+3$ samt udda för $p = 8n-1$ och $p = 8n-3$. Således gäller:

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{för } p = 8n+1 \text{ och } p = 8n+3 \\ -1 & \text{för } p = 8n-1 \text{ och } p = 8n-3. \end{cases}$$

Därmed är uppgiften löst.

Uppgift 9.5 a) -1, b) -1.

Uppgift 9.6 Vi konstaterar först att $371 = 7 \cdot 53$ och att 1367 är ett primtal. Vi får således enligt sats 9.4:

(a) $$\left(\frac{371}{1367}\right) = \left(\frac{7}{1367}\right)\left(\frac{53}{1367}\right).$$

Reciprocitetssatsen samt satserna 9.2 och 9.7 ger:

(b) $$\left(\frac{7}{1367}\right) = -\left(\frac{1367}{7}\right) = -\left(\frac{2}{7}\right) = -1.$$

Vidare fås med stöd av reciprocitetssatsen samt satserna 9.2, 9.4, 9.5 och formel (9.7):

(c) $$\left(\frac{53}{1367}\right) = \left(\frac{1357}{53}\right) = \left(\frac{-11}{53}\right) = \left(\frac{-1}{53}\right)\left(\frac{11}{53}\right) = \left(\frac{11}{53}\right) = \left(\frac{53}{11}\right) = \left(\frac{9}{11}\right) = \left(\frac{3^2}{11}\right) = 1.$$

Då resultaten (a), (b) och (c) sammanställes, fås

$$\left(\frac{371}{1367}\right) = -1.$$

Uppgift 9.7 Enligt reciprocitetssatsen är

(a) $$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

Varje primtal $p > 3$ är av formen $p = 6m \pm 1$ (se övningsuppgift 2.3). I fallet $p = 6m + 1$ fås med beaktande av (a), sats 9.2 och formel (9.7):

$$\left(\frac{3}{p}\right) = (-1)^{3m}\left(\frac{p}{3}\right) = (-1)^{3m}\left(\frac{1}{3}\right) = (-1)^{3m}.$$

I fallet $p = 6m - 1$ fås med stöd av (a) samt satserna 9.2 och 9.5:

$$\left(\frac{3}{p}\right) = (-1)^{3m-1}\left(\frac{p}{3}\right) = (-1)^{3m-1}\left(\frac{-1}{3}\right) = (-1)^{3m}.$$

I bägge fallen gäller således: $\left(\frac{3}{p}\right) = (-1)^{3m}$. Uttrycket $(-1)^{3m}$ är $+1$ eller -1, beroende på om m är jämnt eller udda. Om m är jämnt, så är p av formen $p = 12n \pm 1$, om m är udda, så är p av formen $p = 12n \pm 5$. Alltså är $\left(\frac{3}{p}\right) = 1$ för $p = 12n \pm 1$ och $\left(\frac{3}{p}\right) = -1$ för $p = 12n \pm 5$.

Uppgift 9.8 Talen a, $2a$, $3a$, ..., $(p-1)a$ bildar ett reducerat restsystem modulo p (sats 6.6). De är således i någon ordning kongruenta med talen 1, 2, 3,..., $p - 1$ modulo p. Av de sistnämnda talen är den ena hälften kvadratiska rester och den andra hälften kvadratiska ickerester modulo p (sats 9.1). Således är

$$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = 0.$$

På grund av sats 9.2 är dessa Legendre-symboler i någon ordning = Legendre-symbolerna $\left(\frac{a}{p}\right)$, $\left(\frac{2a}{p}\right)$, $\left(\frac{3a}{p}\right)$,..., $\left(\frac{(p-1)a}{p}\right)$, varför de sistnämndas summa = 0.

Uppgift 9.9 Vi betraktar Legendre-symbolen $\left(\frac{5}{p}\right)$ och söker de värden på p, för vilka $\left(\frac{5}{p}\right) = 1$ resp. -1. Härvid kan vi anta att det udda primtalet $p \neq 5$ i enlighet med Legendre-symbolens definition. Då 5 är av formen $4n + 1$, så är $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ enligt kor. 9.8. Eftersom $\left(\frac{a}{5}\right) = \left(\frac{p}{5}\right)$ för $a \equiv p \pmod 5$, behöver vi beräkna $\left(\frac{a}{5}\right)$ endast för $a = 1, 2, 3, 4$. Man finner med stöd av formel (9.7) att $\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1$. Då är $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$ på grund av sats 9.1. Således är 5 en kvadratisk rest till alla udda primtal p av formen $p = 5m \pm 1$ och en kvadratisk ickerest till alla udda primtal p av formen $p = 5m \pm 2$. I det första fallet måste m vara ett jämnt tal, för att p skall bli udda, således $m = 2n$. I det senare fallet måste m vara udda, således $m = 2n + 1$. Svaret kan därför även skrivas i den naturligare formen: 5 är en kvadratisk rest till alla primtal av formen $p = 10n \pm 1$ och en ickerest till alla primtal av formen $p = 10n \pm 3$.

Uppgift 9.10 a) $x \equiv 2$ och $x \equiv 4 \pmod 7$, b) $x \equiv 1 \pmod 7$, c) ingen rot.

§ 10. Pytagoreiska tal och Fermat's stora sats

Uppgift 10.1 a) (3,4,5), (5,12,13), (8,15,17), (7,24,25), (20,21,29), (12,35,37), (9,40,41).
b) Utgående från de primitiva tripplerna (x,y,z) bildas alla trippler av formen (kx,ky,kz) $(k \geq 1)$, för vilka $kz \leq 50$. Då fås (3,4,5), (6,8,10), (5,12,13), (9,12,15), (8,15,17), (12,16,20), (7,24,25), (15,20,25), (10,24,26), (20,21,29), (18,24,30), (16,30,34), (21,28,35), (12,35,37), (15,36,39), (24,32,40), (9,40,41), (27,36,45), (30,40,50), (14,48,50).

Uppgift 10.2 Då $z = y+1$, måste trippeln vara primitiv. I en primitiv pytagoreisk trippel är z alltid udda. Alltså är $y = z-1$ ett jämnt tal. Trippeln är alltså av formen $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$. (Se sats 10.4 jämte anmärkning). Villkoret $z = y+1$ ger $m - n = 1$. Insättes nu $m = n+1$ i uttrycken för x,y,z fås $x = 2n+1$, $y = 2n(n+1)$, $z = 2n(n+1)+1$. Villkoret $z < 100$ ger $n \leq 6$. Insättes nu $n = 1,2,3,4,5,6$ i de sistnämnda uttrycken för x,y,z fås tripplerna (3,4,5), (5,12,13), (7,24,25), (9,40,41), (11,60,61), (13,84,85).

Uppgift 10.3 Av talen x och y är det ena av formen $2mn$, det andra av formen $m^2 - n^2$. (Sats 10.4 jämte anmärkning). Om m eller n är delbart med 3, så är $2mn$ delbart med 3. Antag nu att varken m eller n är delbart med 3. Då gäller: $m \equiv \pm 1$ och $n \equiv \pm 1 \pmod 3$. Detta ger: $m^2 \equiv n^2 \equiv 1 \pmod 3$ och således $m^2 - n^2 \equiv 0 \pmod 3$. Talet $m^2 - n^2$ är alltså i detta fall delbart med 3. Således är antingen x eller y delbart med 3.

Uppgift 10.4 Vi kan anta att talen x,y,z är av formen $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$. Om m eller n är delbart med 5, så är x delbart med 5. Antag nu att varken m eller n är delbart med 5. Då är m och n kongruenta med något av talen ± 1 eller ± 2 modulo 5. Om m och n vardera är kongruenta med antingen ± 1 eller ± 2, så är $m^2 - n^2 \equiv 0 \pmod 5$. I detta fall är y delbart med 5. Antag nu att $m \equiv \pm 1$ och $n \equiv \pm 2$ eller $m \equiv \pm 2$ och $n \equiv \pm 1 \pmod 5$. I bägge fallen fås: $m^2 + n^2 \equiv 5 \pmod 5$, dvs. z är delbart med 5. Således är åtminstone ett av talen x,y,z delbart med 5. Två av dessa tal kan inte vara delbara med 5, då x,y,z är en primitiv trippel (Lemma 10.1).

Uppgift 10.5 Antag som antites att vi skulle ha $x^4 + y^4 = z^4$ för någon heltalstrippel x,y,z. Sätt $a = y^4$, $b = 2x^2z^2$, $c = x^4 + z^4$ och $d = xy^2z$. Då fås

$$a^2 + b^2 = (z^4 - x^4)^2 + 4x^4z^4 = (x^4 + z^4)^2 = c^2.$$

Vidare gäller: $ab/2 = x^2y^4z^2 = (xy^2z)^2 = d^2$. Talen a,b,c är alltså sidor i en rätvinklig triangel, vars yta $ab/2$ är en jämn kvadrat. Men detta är omöjligt enligt Fermat. Alltså saknar ekvationen $x^4 + y^4 = z^4$ positiva heltalslösningar.

Uppgift 10.6 Låt x,y,z vara en pytagoreisk trippel och antag att $n \geq 3$. Då är

$$z^n = z^{n-2} \cdot z^2 = z^{n-2}(x^2 + y^2) = z^{n-2} \cdot x^2 + z^{n-2} \cdot y^2.$$

Eftersom $z > x$ och $z > y$, så är $z^{n-2} > x^{n-2}$ och $z^{n-2} > y^{n-2}$. Då dessa olikheter insättes i uttrycket för z^n, fås $z^n > x^n + y^n$.