Övningar till kapitel 5 Modulär aritmetik

5.1. Kongruenser och Z_n.

5.1.1. Gör en egen figur liknande figur 5.1 men basera figuren på restklasser *modulo* 5. Hur många rader (restklasser) blir det i din figur?

5.1.2. Skriv restklasserna hörande till figur 5.1 med mängdnotation. (Klamrar osv.) Vad blir unionen av alla dessa restklasser? Vad blir snittet mellan två av dessa restklasser? Motivera dina påståenden.

5.1.3. Avgör vilka av följande påståenden som är sanna och vilka som är falska:

$2 \equiv 5 (\mathrm{mod}\, 3)$ $\quad$ $2 \equiv 5 (\mathrm{mod}\, 4)$ $\quad$ $2 \equiv -5 (\mathrm{mod}\, 6)$

$2 \equiv -5 (\mathrm{mod}\, 7)$ $\quad$ $-8 \equiv 4 (\mathrm{mod}\, 12)$ $\quad$ $-8 \equiv 4 (\mathrm{mod}\, 4)$

$-8 \equiv 4 (\mathrm{mod}\, 3)$ $\quad$ $-8 \equiv 4 (\mathrm{mod}\, 5)$ $\quad$ $23 \equiv 72 (\mathrm{mod}\, 7)$

$23 \equiv 72 (\mathrm{mod}\, 7)$

Motivera dina påståenden.

5.1.4. Bevisa del (i) och (ii) av sats 5.1. (Om $x \equiv y (\mathrm{mod}\, n)$ så gäller...) Välj från din egen figur från övning 5.1.1 ett antal tal för att se att satsen stämmer.

5.1.5. Bevisa följande räkneregler för kongruenser och ge ett par exempel på tal från din egen tabell från övning 5.1.1 för att se att reglerna stämmer:

$x_1 \equiv x_2 (\mathrm{mod}\, n)$ och $y_1 \equiv y_2 (\mathrm{mod}\, n) \Rightarrow x_1 + y_1 \equiv x_2 + y_2 (\mathrm{mod}\, n)$ samt $x_1 x_2 \equiv y_1 y_2 (\mathrm{mod}\, n)$.

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

5.1.7. Vilken rest får då 207^{61} divideras med 13. Vilken rest får då 207^{6100} divideras med 13.

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

5.1.9. Studera följande additionstabell och multiplikationstabbeller för Z_3:

+	**0**	**1**	**2**
0	**0**	**1**	**2**
1	**1**	**2**	**0**
2	**2**	**0**	**1**

*	**0**	**1**	**2**
0	**0**	**0**	**0**
1	**0**	**1**	**2**
2	**0**	**2**	**1**

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

5.1.10. Gör om övning 5.1.9 fast med dessa tabeller för Z_4 respektive Z_5.

+	**0**	**1**	**2**	**3**
0	**0**	**1**	**2**	**3**
1	**1**	**2**	**3**	**0**
2	**2**	**3**	**0**	**1**
3	**3**	**0**	**1**	**2**

*	**0**	**1**	**2**	**3**	**4**
0	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**
2	**0**	**2**	**4**	**1**	**3**
3	**0**	**3**	**1**	**4**	**2**
4	**0**	**4**	**3**	**2**	**1**

5.1.11. Konstruera additions- och multiplikationstabeller för Z_9.

5.1.12. Konstruera additions- och multiplikationstabeller för Z_{11}.

5.1.13. Kan Du se någon intressant skillnad mellan multiplikationstabellerna från 5.1.11 och 5.1.12? Kan Du förklara denna skillnad?

5.2. Egenskaper hos heltalen

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

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

5.2.3. Visa att $5 \mid n^5 - n$ för alla positiva heltal *n*.

5.2.4. Gäller $6 \mid n^6 - n$ för alla positiva heltal *n*? Gäller det för något heltal alls förutom 0 och 1?

Blandade övningar

(Blandade övningar är av tentamenskaraktär.)

5.1. Visa att $3^{2n+1}+5^{2n}$ är delbart med 4 men inte med 8 för alla $n \geq 0$.

5.2. Visa att $3 \mid n \cdot (2n+1) \cdot (4n+1)$ för alla $n \geq 0$. *(Ledning: Studera de tre fall som kan uppkomma med kongruenser modulo 3.)*
Från tentamen i diskret matematik den 13 januari 2004.

5.3. Visa att $n \cdot (n^2-1)$ är delbart med 6 för alla heltal *n*. (*Ledning: 6 delfall uppkommer vid kongruenser modulo 6.*)

Anmärkning: Uppgifterna 5.2, 5.3 och 5.4 är direkta omformuleringar av uppgifter från kapitel 3 vilket visar att kongruensräkning ibland kan vara ett bra hjälpmedel vid undersökning av delbarhetsförhållanden rörande heltal.

5.4. Visa att $3 \mid 7^n - 4^n$ för alla heltal $n \geq 0$.

5.5. Visa att $4 \mid 5^n - 1$ för alla heltal $n \geq 0$.

5.6. Visa att $n^4 - 1$ är delbart med 5 om *n inte* är delbart med 5.
(Sistauppgift på gammal tenta.)

5.7. Visa att $14 \mid 13^{2n} + 13$ för alla positiva heltal *n*.

5.8. Visa att $12 \mid 17^{2n} - 13^n$ för alla positiva heltal *n*.

5.9. Visa att $16 \mid 15 \cdot 17^n + 3^{4n}$ för alla positiva heltal *n*.

Facit till övningar till kapitel 5 Modulär aritmetik

5.1.1.

	Rest 0		-10					-5					0					5					10	
	Rest 1			-9					-4					1					6					11
	Rest 2				-8					-3					2					7				
	Rest 3					-7					-2					3					8			
	Rest 4	-11					-6					-1					4					9		

Det blir 5 restklasser modulo 5.

5.1.2. Restklasserna modulo 5 är:

{..., -10, -5, 0, 5, 10, ...} = $\{5 \cdot k \mid k \in Z\}$. (Rad 1, uppifrån i tabellen i övning 5.1.1.)
{..., -9, -4, 1, 6, 11, ...} = $\{5 \cdot k + 1 \mid k \in Z\}$. (Rad 2, uppifrån i tabellen i övning 5.1.1.)
{..., -8, -3, 2, 7, 12, ...} = $\{5 \cdot k + 2 \mid k \in Z\}$. (Rad 3, uppifrån i tabellen i övning 5.1.1.)
{..., -7, -2, 3, 8, 13, ...} = $\{5 \cdot k + 3 \mid k \in Z\}$. (Rad 4, uppifrån i tabellen i övning 5.1.1.)
{..., -11, -6, -1, 4, 9, ...} = $\{5 \cdot k + 4 \mid k \in Z\}$. (Rad 5, uppifrån i tabellen i övning 5.1.1.)

5.1.3.

$2 \equiv 5 (\mathrm{mod}\, 3)$, sant ty $2 + 3 \cdot 1 = 5$, således skiljer det en multipel av 3 mellan 2 och 5.

$2 \equiv 5 (\mathrm{mod}\, 4)$, falskt ty $2 \equiv 5 (\mathrm{mod}\, 4) \Leftrightarrow 2 - 5 \equiv 0 (\mathrm{mod}\, 4) \Leftrightarrow -3 \equiv 0 (\mathrm{mod}\, 4) \Leftrightarrow 4 \mid -3$, men 4 kan inte absolut inte dela -3 eftersom 4 är större än 3.

$2 \equiv -5 (\mathrm{mod}\, 6)$, falsk ty $2 \equiv -5 (\mathrm{mod}\, 6) \Leftrightarrow 2 - (-5) \equiv 0 (\mathrm{mod}\, 6) \Leftrightarrow 7 \equiv 0 (\mathrm{mod}\, 6) \Leftrightarrow 6 \mid 7$, men 6 delar inte 7 ty 7 är ett primtal och har således bara sig själv (och 1) som delare.

$2 \equiv -5 (\mathrm{mod}\, 7)$, sant ty $2 = -5 + 1 \cdot 7$, 2 och -5 skiljer sig således med en multipel av 7 vilket innebär att de är kongruenta *modulo* 7.

$-8 \equiv 4 (\mathrm{mod}\, 12)$, sant ty $-8 \equiv 4 + -1 \cdot 12$ -8 och 4 skiljer sig således med en multipel av 12 vilket innebär att de är kongruenta *modulo* 12.

$-8 \equiv 4 (\mathrm{mod}\, 4)$, sant ty $-8 \equiv 4 + -3 \cdot 4$, -8 och 4 skiljer sig således med en multipel av 4 vilket innebär att de är kongruenta *modulo* 4.

$-8 \equiv 4 (\mathrm{mod}\, 3)$, sant ty $-8 \equiv 4 + -4 \cdot 3$, -8 och 4 skiljer sig således med en multipel av 3 vilket innebär att de är kongruenta *modulo* 3.

$-8 \equiv 4 (\mathrm{mod}\, 5)$, falskt ty $-8 \equiv 4 (\mathrm{mod}\, 5) \Leftrightarrow -4 - 8 \equiv 0 (\mathrm{mod}\, 5) \Leftrightarrow -12 \equiv 0 (\mathrm{mod}\, 5) \Leftrightarrow 5 \mid 12$, men 5 delar inte 12, ty $12 = 3 \cdot 4 = 2^2 \cdot 3$ och det förekommer inga 5:or i primtalsfaktoriseringen av 12. (Vilket det måste göra om 5 | 12.)

$23 \equiv 72 (\mathrm{mod}\, 7)$, sant ty $23 \equiv 72 (\mathrm{mod}\, 7) \Leftrightarrow 72 - 23 \equiv 0 (\mathrm{mod}\, 7) \Leftrightarrow 49 \equiv 0 (\mathrm{mod}\, 7) \Leftrightarrow 7 \mid 49$, vilket är sant.

$23 \equiv 72 (\mathrm{mod}\, 7)$, sant av samma skäl som $23 \equiv 72 (\mathrm{mod}\, 7)$, vi får bara ett teckenbyte.

5.1.4.

Sats 5.1: Om $x \equiv y(\mathrm{mod}\, n)$ så gäller
(i) $x + a \equiv y + a(\mathrm{mod}\, n)$ för alla tal *a*.
(ii) $cx \equiv cy(\mathrm{mod}\, n)$ för alla tal c.
(iii) $x^2 \equiv y^2(\mathrm{mod}\, n)$ och $x^3 \equiv y^3(\mathrm{mod}\, n)$, …, $x^m \equiv y^m(\mathrm{mod}\, n)$ för alla tal *m*.

Bevis av (i) och (ii): Antag att $x \equiv y(\mathrm{mod}\, n)$.
(i): Vi ska visa att $x + a \equiv y + a(\mathrm{mod}\, n)$. Studera differensen mellan leden på var sida om kongruenstecknet: $(x + a) - (y + a) = x + a - y - a = x - y + a - a = x - y$. Så differensen mellan de båda leden blir $x - y$. Enligt förutsättningen gäller $x \equiv y(\mathrm{mod}\, n) \Leftrightarrow x - y \equiv 0(\mathrm{mod}\, n)$ så vi har således $(x + a) - (y + a) = x - y \equiv 0(\mathrm{mod}\, n)$. Men detta är samma sak som $x + a \equiv y + a(\mathrm{mod}\, n)$, vilket skulle bevisas.
(ii): Vi ska visa att $cx \equiv cy(\mathrm{mod}\, n)$ för alla heltal *c*. Studera återigen differensen mellan leden på var sida om kongruenstecknet: $cx - cy = c(x - y)$. Eftersom $x \equiv y(\mathrm{mod}\, n)$ så gäller att $n \mid x - y \Leftrightarrow \exists k \in Z : n - y = k \cdot n$. Detta använt på $cx - cy = c(x - y)$ ger oss $\boldsymbol{cx \equiv cy(\mathrm{mod}\, n)}$. Men detta innebär att vi visat att $cx - cy = c(x - y) = ett\ heltal \cdot n$, det vill säga $n \mid cx - cy$. Detta är samma sak som att vilket skulle visas.
Beviset är klart.

5.1.5.

Bevis av $x_1 \equiv x_2(\mathrm{mod}\, n)$ och $y_1 \equiv y_2(\mathrm{mod}\, n) \Rightarrow x_1 + y_1 \equiv x_2 + y_2(\mathrm{mod}\, n)$ samt $x_1 y_1 \equiv x_2 y_2(\mathrm{mod}\, n)$: Antag att $x_1 \equiv x_2(\mathrm{mod}\, n)$ och $y_1 \equiv y_2(\mathrm{mod}\, n)$. Detta är ekvivalent med att det finns tal *h* och *k* sådana att $x_1 - x_2 = h \cdot n$ och $cx \equiv cy(\mathrm{mod}\, n)$ Vi studerar skillnaden mellan leden på var sida om kongruenstecknet i $x_1 + y_1 \equiv x_2 + y_2(\mathrm{mod}\, n)$. Den skillnaden är $(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2)$. Vi använder nu likheterna med *h* och *k* för att skriva om detta som $(x_1 - x_2) + (y_1 - y_2) = h \cdot n + k \cdot n = (h + k) \cdot n = ett\ heltal \cdot n$. Vi har nu visat att $n \mid (x_1 + y_1) - (x_2 + y_2)$ vilket är samma sak som att $x_1 + y_1 \equiv x_2 + y_2(\mathrm{mod}\, n)$ vilket var det första som skulle bevisas. Vi visar nu $x_1 y_1 \equiv x_2 y_2(\mathrm{mod}\, n)$. Fördenskull skriver vi om $x_1 - x_2 = h \cdot n$ och $y_1 - y_2 = k \cdot n$ till $x_1 = x_2 + h \cdot n$ och $y_1 = y_2 + k \cdot n$. Vi studerar produkten mellan x_1 och y_1: $x_1 \cdot y_1 = (x_2 + h \cdot n)(y_2 + k \cdot n) = x_2 y_2 + x_2 kn + y_2 hn + hkn^2$. Vi bryter ut *n* ur de sista tre termerna i sista uttrycket och får $x_1 \cdot y_1 = x_2 y_2 + (x_2 k + y_2 h + hkn) \cdot n = x_2 y_2 + ett\ heltal \cdot n$. Det vill säga vi har visat att $x_1 y_1$ och $x_2 y_2$ skiljer sig åt med en multipel av *n*. Detta betyder att $n \mid x_1 y_1 - x_2 y_2$ vilket innebär att $x_1 y_1 \equiv x_2 y_2(\mathrm{mod}\, n)$ vilket skulle bevisas.

Vi väljer $x_1 = 3$ och $x_2 = 8$ från restklassen **3** och $y_1 = 2$ och $y_2 = 7$ från restklassen **2**. Vi studerar nu $x_1 y_1$ och $x_2 y_2$: $x_1 y_1 = 3 \cdot 2 = 6$, $x_2 y_2 = 8 \cdot 7 = 56$. Som vi ser skiljer sig 56 och 6 med 50, och det är en multipel av 5. Således är $x_1 y_1$ och $x_2 y_2$ kongruenta *modulo* 5 vilket indikerar att satsen stämmer.

5.1.6. Vi börjar kasta multiplar av 7. Vi vet att $98 = 14 \cdot 7 \equiv 0(mod\, 7)$ så
$411 \cdot 821 + 376 \cdot 297 = (400 + 11) \cdot (800 + 21) + (300 + 76) \cdot (200 + 97) =$

$411 \cdot 821 + 376 \cdot 297 = (4 \cdot 100 + 11) \cdot (8 \cdot 100 + 21) + (3 \cdot 100 + 76) \cdot (2 \cdot 100 + 97) \equiv$

$411\cdot 821+376\cdot 297=(4\cdot 2+11)\cdot(\mathbf{8}\cdot 2+\mathbf{21})+(3\cdot 2+\mathbf{7}6)\cdot(2\cdot 2+97)(mod 7)$. Detta kan ytterligare reduceras modulo 7, de fetmarkerade siffrorna och talen försvinner, 21 blir 0, 7 blir 0, 8 blir 1. Således har vi att det blir lika med $(4\cdot 2+11)\cdot(\mathbf{1}\cdot 2)+(3\cdot 2+6)\cdot(2\cdot 2+97)(mod 7)$. Vidare gäller $91=13\cdot 7$ och $4\cdot 2=8\equiv 1(mod 7)$ så uttrycket är kongruent med $(1+11)\cdot 2+(3\cdot 2+6)\cdot(2\cdot 2+6)(mod 7)\equiv 24+12\cdot 10\equiv 3+5\cdot 3\equiv 3+15\equiv 3+1\equiv 4(\mathrm{mod}\,7)$. Således ger talet $411\cdot 821+376\cdot 297$ resten 4 då det divideras med 7.

5.1.7. $207^{61}=(16\cdot 13-1)^{61}\equiv(-1)^{61}\equiv -1\equiv 12(mod 13)$. Således ger 207^{61} resten 12 då det divideras med 13. $207^{6100}=(207^{61})^{100}\equiv(-1)^{100}\equiv 1(mod 13)$. Således ger 207^{6100} resten 1 då det divideras med 13.

5.1.8. Vi observerar att $4^6=(4^2)^3=16^3\equiv 3^3=27\equiv 1(mod 13)$. Detta använder vi successivt och skriver
$(17^{47}+2^{12})^{14}-4\equiv(4^{47}+4^6)^{14}-4=(4^5\cdot(4^6)^7+4^6)^{14}-4\equiv(4^5\cdot(1)^7+1)^{14}-4=(16\cdot 16\cdot 4+1)^{14}-4\equiv$
$(3\cdot 3\cdot 4+1)^{14}-4\equiv(27+9+1)^{14}-4\equiv 11^{14}-4\equiv 121^7-4\equiv 30^7-4\equiv 4^7-4\equiv 4\cdot 4^6-4\equiv 4\cdot 1-4=0$

Eftersom $(17^{47}+2^{12})^{14}-4\equiv 0(mod 13)$ måste $13\,|\,(17^{47}+2^{12})^{14}-4$.

Facit är under utveckling och kommer att fortsätta här snart.

5.1.9. Additionstabell och multiplikationstabell för Z_3:

+	**0**	**1**	**2**
0	**0**	**1**	**2**
1	**1**	**2**	**0**
2	**2**	**0**	**1**

*	**0**	**1**	**2**
0	**0**	**0**	**0**
1	**0**	**1**	**2**
2	**0**	**2**	**1**

Vi väljer 29 från **2** och 35 också från **2**: Summan av 29 och 35 är 64 vilket tillhör **1**. Detta indikerar att **2** + **2** = **1** som vi också ser i additionstabellen. Vi studerar produkten av 29 och 35. Den är 1015. Vid en undersökning av vilken restklass som 1015 ligger i finner vi att $1015=338*3+1$. Det vill säga 1015 ger resten 1 vid division med 3 vilket innebär att 1015 ligger i **1**. Detta indikerar att **2** * **2** = **1** vilket också framgår av multiplikationstabellen ovan.

Vi väljer ett par till exempel:

30 ligger i **0**, 10 ligger i **1**. 30 + 10 = 40 som ligger i **1**. Detta indikerar att **0** + **1** = **1**.
30 ligger i **0**, 10 ligger i **1**. 30 * 10 = 300 som ligger i **0**. Detta indikerar att **0** * **1** = **0**.

31 ligger i **1**, 11 ligger i **2**. 31 + 11 = 42 som ligger i **0**. Detta indikerar att **1** + **2** = **0**.
31 ligger i **1**, 11 ligger i **2**. 31 * 11 = 341 som ligger i **2**. Detta indikerar att **1** * **2** = **2**.

5.1.10.

Additionstabell för Z_4.

+	0	1	2	3
0	**0**	**1**	**2**	**3**
1	**1**	**2**	**3**	**0**
2	**2**	**3**	**0**	**1**
3	**3**	**0**	**1**	**2**

För att illustrera additionstabellen ovan ser vi till exempel:

22 i **2** och 19 i **3**: 22 + 19 = 41 ligger i **1**. Detta indikerar **2** + **3** = **1**.

20 i **0** och 9 i **1**: 20 + 9 = 29 ligger i **1**. Detta indikerar **0** + **1** = **1**.

Multiplikationstabell för Z_5.

*	0	1	2	3	4
0	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**
2	**0**	**2**	**4**	**1**	**3**
3	**0**	**3**	**1**	**4**	**2**
4	**0**	**4**	**3**	**2**	**1**

För att illustrera additionstabellen ovan ser vi till exempel:

22 i **2** och 19 i **4**: 22 * 19 = 418. En undersökning ger att 418 = 83*5 + 3. Detta ligger i **3** och indikerar således att **2** * **4** = **3**.

20 i **0** och 9 i **4**: 20 * 9 = 180 som är delbart med 5. Således ligger det i **0** och detta indikerar att **0** * **1** = **0**.

5.1.11.

Additionstabell för Z_9:

+	0	1	2	3	4	5	6	7	8
0	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**0**
2	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**0**	**1**
3	**3**	**4**	**5**	**6**	**7**	**8**	**0**	**1**	**2**
4	**4**	**5**	**6**	**7**	**8**	**0**	**1**	**2**	**3**
5	**5**	**6**	**7**	**8**	**0**	**1**	**2**	**3**	**4**
6	**6**	**7**	**8**	**0**	**1**	**2**	**3**	**4**	**5**
7	**7**	**8**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
8	**8**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**

Multiplikationstabell för Z_9:

+	0	1	2	3	4	5	6	7	8
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
2	**0**	**2**	**4**	**6**	**8**	**1**	**3**	**5**	**7**
3	**0**	**3**	**6**	**0**	**3**	**6**	**0**	**3**	**6**
4	**0**	**4**	**8**	**3**	**7**	**2**	**6**	**1**	**5**
5	**0**	**5**	**1**	**6**	**2**	**7**	**3**	**8**	**4**
6	**0**	**6**	**3**	**0**	**6**	**3**	**0**	**6**	**3**
7	**0**	**7**	**5**	**3**	**1**	**8**	**6**	**4**	**2**
8	**0**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**

5.1.12.

Additionstabell för Z_{11}:

+	0	1	2	3	4	5	6	7	8	9	10
0	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**0**
2	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**0**	**1**
3	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**0**	**1**	**2**
4	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**0**	**1**	**2**	**3**
5	**5**	**6**	**7**	**8**	**9**	**10**	**0**	**1**	**2**	**3**	**4**
6	**6**	**7**	**8**	**9**	**10**	**0**	**1**	**2**	**3**	**4**	**5**
7	**7**	**8**	**9**	**10**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
8	**8**	**9**	**10**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
9	**9**	**10**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
10	**10**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

Multiplikationstabell för Z_{11}:

*	0	1	2	3	4	5	6	7	8	9	10
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2	**0**	**2**	**4**	**6**	**8**	**10**	**1**	**3**	**5**	**7**	**9**
3	**0**	**3**	**6**	**9**	**1**	**4**	**7**	**10**	**2**	**5**	**8**
4	**0**	**4**	**8**	**1**	**5**	**9**	**2**	**6**	**10**	**3**	**7**
5	**0**	**5**	**10**	**4**	**9**	**3**	**8**	**2**	**7**	**1**	**6**
6	**0**	**6**	**1**	**7**	**2**	**8**	**3**	**9**	**4**	**10**	**5**
7	**0**	**7**	**3**	**10**	**6**	**2**	**9**	**5**	**1**	**8**	**4**
8	**0**	**8**	**5**	**2**	**10**	**7**	**4**	**1**	**9**	**6**	**3**
9	**0**	**9**	**7**	**5**	**3**	**1**	**10**	**8**	**6**	**4**	**2**
10	**0**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**

5.1.13. Skillnaden mellan multiplikationstabellerna för Z_9 och Z_{11} är att den för Z_9 innehåller flera nollor på några av raderna. Dessa rader innehåller vidare inte alla tal. Varje rad i multiplikationstabellen för Z_{11} innehåller varje element ur Z_{11}. Exempelvis innehåller rad 7 ur multiplikationstabellen för Z_{11} elementen **0**, **7**, **3**, **10**, **6**, **2**, **9**, **5**, **1**, **8** och **4**. Detta är också alla element ur Z_{11} fast i en annan ordning. Om vi jämför med rad 3 ur multiplikationstabellen för Z_9 ser vi att denna rad innehåller elementen **0**, **3**, **6**, **0**, **3**, **6**, **0**, **3**, **6**. Anledningen till att tabellen för Z_9 på denna rad inte innehåller alla element är att raden har nummer **3** och att elementet **3** är en faktor i **9**. Då **3** (på tredje raden) således multipliceras med olika element ur Z_9 produceras bara element delbara med **3**, vilket sorterar bort **1**, **2**, **4**, **5**, **7** och **8** som alltås inte är delbara med **3**. Istället förekommer bara multiplarna av **3** vilket alltså utgörs av elementen **0**, **3**, **6**, **0**, **3**, **6**, **0**, **3**, **6**.

5.2.1. Visa att om ett tal inte är delbart med 3 så är kvadraten på talet kongruent med 1 *modulo* 3.
Bevis: Låt n vara ett tal som inte är delbart med 3. Då gäller antingen $n \equiv 1(mod\ 3)$ eller $n \equiv 2(mod\ 3)$. Vi studerar båda dessa fall:
$n \equiv 1(mod\ 3) \Rightarrow n^2 \equiv 1^2(mod\ 3) \equiv 1(mod\ 3)$ så här är kvadraten på talet kongruent med 1 *modulo* 3.
$n \equiv 2(mod\ 3) \Rightarrow n^2 \equiv 2^2(mod\ 3) \equiv 4(mod\ 3) \equiv 4-3(mod\ 3) \equiv 1(mod\ 3)$. Även i andra fallet gäller således att kvadraten på talet kongruent med 1 *modulo* 3. I båda de fall som kan inträffa gäller att kvadraten på talet kongruent med 1 *modulo* 3 vilket skulle visas.

5.2.2. Visa att kvadraten på varje heltal antingen är kongruent med 0 eller 1 *modulo* 4.
Bevis: Kalla heltalet för n. Då vi räknar modulo 4 finns det 4 fall: $n \equiv 0(mod\ 4)$, $n \equiv 1(mod\ 4)$, $n \equiv 2(mod\ 4)$ och $n \equiv 3(mod\ 4)$. Vi studerar vad kvadraten på n är kongruent med i dessa fyra fall:
$n \equiv 0(mod\ 4) \Rightarrow n^2 \equiv 0^2(mod\ 4)$ så här gäller $n^2 \equiv 0(mod\ 4)$.
$n \equiv 1(mod\ 4) \Rightarrow n^2 \equiv 1^2(mod\ 4)$ så här gäller $n^2 \equiv 1(mod\ 4)$.
$n \equiv 2(mod\ 4) \Rightarrow n^2 \equiv 2^2(mod\ 4) \equiv 4(mod\ 4) \equiv 0(mod\ 4)$ så här gäller $n^2 \equiv 0(mod\ 4)$.
$n \equiv 3(mod\ 4) \Rightarrow n^2 \equiv 3^2(mod\ 4) \equiv 9(mod\ 4) \equiv 1(mod\ 4)$ så här gäller $n^2 \equiv 1(mod\ 4)$.
I alla fall gäller endera att kvadraten på n är kongruent med 0 eller 1 modulo. Detta skulle bevisas.

5.2.3. Visa att $5 \mid n^5 - n$ för alla positiva heltal n.

Bevis: Vi räknar *modulo* 5 och det finns då 5 fall: $n \equiv 0(mod\ 5)$, $n \equiv 1(mod\ 5)$, $n \equiv 2(mod\ 5)$, $n \equiv 3(mod\ 5)$ och $n \equiv 4(mod\ 5)$. Vi studerar hur vad uttrycket $n^5 - n$ blir kongruent med i dessa 5 fall:

$n \equiv 0(mod\ 5) \Rightarrow n^5 - n \equiv 0^5 - 0 \equiv 0 - 0 \equiv 0(mod\ 5)$.

$n \equiv 1(mod\ 5) \Rightarrow n^5 - n \equiv 1^5 - 1 \equiv 1 - 1 \equiv 0(mod\ 5)$

$n \equiv 2(mod\ 5) \Rightarrow n^5 - n \equiv 2^5 - 2 \equiv 32 - 2 \equiv 30 \equiv 6 \cdot 5 \equiv \{delbart\ med\ 5\} \equiv 0(mod\ 5)$

$n \equiv 3(mod\ 5) \Rightarrow n^5 - n \equiv 3^5 - 3 \equiv 243 - 3 \equiv 240 \equiv 48 \cdot 5 \equiv 0(mod\ 5)$

$n \equiv 4(mod\ 5) \Rightarrow n^5 - n \equiv 4^5 - 4 \equiv 1024 - 4 \equiv 1020 \equiv 204 \cdot 5 \equiv 0(mod\ 5)$

I samtliga fall ser vi att uttrycket $n^5 - n$ blir kongruent med 0 modulo 5. Detta innebär att uttrycket alltid måste vara delbart med 5 vilket skulle bevisas.

5.2.4. Gäller $6 \mid n^6 - n$ för alla positiva heltal n?

Nej, till exempel gäller $2^6 - 2 = 64 - 2 = 62$ och 62 är inte delbart med 6. Det finns en sats som heter Fermats lilla sats som säger att om p är ett primtal så gäller alltid att $n^p - n \equiv 0(mod\ p)$. Denna sats har exemplifierats i övning 5.2.3 och 5.2.4.

Blandade övningar

5.1. Visa att $3^{2n+1} + 5^{2n}$ är delbart med 4 men inte med 8 för alla $n \geq 0$.

Bevis: Då vi räknar modulo 4 gäller

$3^{2n+1} + 5^{2n} \equiv (4-1)^{2n+1} + (4+1)^{2n} \equiv (-1)^{2n+1} + 1^{2n} \equiv (-1)^{udda\ tal} + 1 \equiv -1 + 1(mod\ 4) \equiv 0(mod\ 4)$.

Eftersom uttrycket är kongruent med 0 modulo 4 innebär detta att uttrycket är delbart med 4 för alla heltal $n \geq 0$.

Vi räknar nu modulo 8 och får

$3^{2n+1} + 5^{2n} \equiv 3 \cdot (3^2)^n + (5^2)^n \equiv 3 \cdot 9^n + 25^n = 3 \cdot (1+8)^n + (1+3 \cdot 8)^n \equiv 3 \cdot (1+0)^n + (1+0)^n \equiv 3 \cdot 1^n + 1^n \equiv 3 + 1 \equiv 4(mod\ 8)$

Av denna uträkning ser vi att uttrycket $3^{2n+1} + 5^{2n}$ inte är kongruent med 0 *modulo* 8 (det är alltid kongruent med 4 *modulo* 8) vilket innebär att det inte är delbart med 8 för något heltal $n \geq 0$.

5.2. Visa att $3 \mid n \cdot (2n+1) \cdot (4n+1)$ för alla $n \geq 0$.

Bevis: För alla $n \geq 0$ gäller ett av tre fall: $n \equiv 0(mod\ 3)$, $n \equiv 1(mod\ 3)$ eller $n \equiv 2(mod\ 3)$. Vi studerar nu uttrycket $n \cdot (2n+1) \cdot (4n+1)$ för dessa tre fall:

$n \equiv 0(mod\ 3) \Rightarrow n \cdot (2n+1) \cdot (4n+1) \equiv 0 \cdot (2 \cdot 0 + 1) \cdot (4 \cdot 0 + 1) \equiv 0(mod\ 3)$.

$n \equiv 1(mod\ 3) \Rightarrow n \cdot (2n+1) \cdot (4n+1) \equiv 1 \cdot (2 \cdot 1 + 1) \cdot (4 \cdot 1 + 1) \equiv 1 \cdot 3 \cdot 5 \equiv 3 \cdot 5 \equiv 0(mod\ 3)$.

$n \equiv 2(mod\ 3) \Rightarrow n \cdot (2n+1) \cdot (4n+1) \equiv 2 \cdot (2 \cdot 2 + 1) \cdot (4 \cdot 2 + 1) \equiv 2 \cdot 5 \cdot 9 \equiv 2 \cdot 5 \cdot 3 \cdot 3 \equiv 3 \cdot 30 \equiv 0(mod\ 3)$.

I samtliga fall som kan inträffa ser vi att uttrycket $n \cdot (2n+1) \cdot (4n+1)$ är kongruent med 0 modulo 3. Detta betyder att $n \cdot (2n+1) \cdot (4n+1)$ således alltid måste vara delbart med 3, det vill säga $3 \mid n \cdot (2n+1) \cdot (4n+1)$ för alla $n \geq 0$ vilket skulle bevisas.

5.3. Visa att $n\cdot(n^2-1)$ är delbart med 6 för alla heltal *n*.
Bevis: Vid räkning *modulo* 6 uppkommer 6 delfall: $n\equiv 0(mod\ 6)$, $n\equiv 1(mod\ 6)$, $n\equiv 2(mod\ 6)$, $n\equiv 3(mod\ 6)$, $n\equiv 4(mod\ 6)$ och $n\equiv 5(mod\ 6)$. Vi studerar uttrycket $n\cdot(n^2-1)$ i dessa fall.

$n\equiv 0(mod\ 6)\Rightarrow n\cdot(n^2-1)\equiv 0\cdot(0^2-1)\equiv 0(mod\ 6)$.
$n\equiv 1(mod\ 6)\Rightarrow n\cdot(n^2-1)\equiv 1\cdot(1^2-1)\equiv 1\cdot 0\equiv 0(mod\ 6)$.
$n\equiv 2(mod\ 6)\Rightarrow n\cdot(n^2-1)\equiv 2\cdot(2^2-1)\equiv 2\cdot 3\equiv 6\equiv 0(mod\ 6)$.
$n\equiv 3(mod\ 6)\Rightarrow n\cdot(n^2-1)\equiv 3\cdot(3^2-1)\equiv 3\cdot 8\equiv 3\cdot 2\cdot 4\equiv 6\cdot 4\equiv 0(mod\ 6)$.
$n\equiv 4(mod\ 6)\Rightarrow n\cdot(n^2-1)\equiv 4\cdot(4^2-1)\equiv 4\cdot 15\equiv 60\equiv 6\cdot 10\equiv 0(mod\ 6)$.
$n\equiv 5(mod\ 6)\Rightarrow n\cdot(n^2-1)\equiv 5\cdot(5^2-1)\equiv 5\cdot 24\equiv 5\cdot 6\cdot 4\equiv 6\cdot 20\equiv 0(mod\ 6)$.

I alla fall som kan uppkomma, för alla heltal *n*, ser vi att uttrycket $n\cdot(n^2-1)$ alltid är kongruent med 0 *modulo* 6. Detta betyder att $n\cdot(n^2-1)$ är delbart med 6 för alla heltal vilket skulle bevisas.

5.4. Visa att $3\,|\,7^n-4^n$ för alla heltal $n\geq 0$.
Bevis: Med räkning *modulo* 3 erhålles $7^n-4^n\equiv(2\cdot 3+1)^n-(3+1)^n\equiv 1^n-1^n\equiv 0(mod\ 3)$. Att uttrycket 7^n-4^n är kongruent med 0 *modulo* 3 bevisar att det är delbart med 3 för alla heltal vilket skulle bevisas.

5.5. Visa att $4\,|\,5^n-1$ för alla heltal $n\geq 0$.
Bevis: Med räkning *modulo* 4 erhålles $5^n-1\equiv(4+1)^n-1\equiv 1^n-1\equiv 0(mod\ 4)$. Detta visar att $4\,|\,5^n-1$ för alla heltal $n\geq 0$ vilket skulle bevisas.

5.6. Visa att n^4-1 är delbart med 5 om *n inte* är delbart med 5.
Bevis: Om *n* inte är delbart med 5 kan det vara på 4 sätt:
$n\equiv 1(mod\ 5)$, $n\equiv 2(mod\ 5)$, $n\equiv 3(mod\ 5)$ och $n\equiv 4(mod\ 5)$. Vi undersöker nu uttrycket n^4-1 för dessa fyra fall:
$n\equiv 1(mod\ 5)\Rightarrow n^4-1\equiv 1^4-1\equiv 1-1\equiv 0(mod\ 5)$
$n\equiv 2(mod\ 5)\Rightarrow n^4-1\equiv 2^4-1\equiv 16-1\equiv 15\equiv 3\cdot 5\equiv 0(mod\ 5)$
$n\equiv 3(mod\ 5)\Rightarrow n^4-1\equiv 3^4-1\equiv 81-1\equiv 80\equiv 16\cdot 5\equiv 0(mod\ 5)$
$n\equiv 4(mod\ 5)\Rightarrow n^4-1\equiv 4^4-1\equiv 256-1\equiv 255\equiv 5\cdot 51\equiv 0(mod\ 5)$

I alla möjliga fall där *n* inte är delbart med 5 ser vi att det uttryck vi studerar (n^4-1) är kongruent med 0 modulo 5. Således kan vi dra slutsatsen att n^4-1 är delbart med 5 då *n* inte är det. Detta skulle bevisas.

5.7. Visa att $14\,|\,13^{2n}+13$ för alla positiva heltal *n*.
Bevis: $13^{2n}+13\equiv(13-14)^{2n}+13\equiv(-1)^{2n}+13\equiv(-1)^{jämnt\ tal}+13\equiv 1+13\equiv 14\equiv 0(mod\ 14)$. Att $13^{2n}+13$ är kongruent med 0 modulo 14 för alla positiva heltal *n* visar att $14\,|\,13^{2n}+13$ för alla positiva heltal *n* vilket skulle bevisas.

5.8. Visa att $12 \mid 17^{2n} - 13^n$ för alla positiva heltal *n*.
Bevis:
$17^{2n} - 13^n \equiv (12+5)^{2n} - (12+1)^n \equiv 5^{2n} - 1 \equiv (5^2)^n - 1 \equiv 25^n - 1 \equiv (2 \cdot 12 + 1)^n - 1 \equiv 1^n - 1 \equiv 1 - 1 \equiv 0 (mod\ 12)$
Uträkningen visar att $17^{2n} - 13^n$ är kongruent med 0 *modulo* 12 för alla positiva heltal *n*. Detta betyder att $12 \mid 17^{2n} - 13^n$ för alla positiva heltal *n* vilket skulle bevisas.

5.9. Visa att $16 \mid 15 \cdot 17^n + 3^{4n}$ för alla positiva heltal *n*.
Bevis: $15 \cdot 17^n + 3^{4n} \equiv 15 \cdot (16+1)^n + 81^n \equiv 15 \cdot 1^n + (5 \cdot 16 + 1)^n \equiv 15 + (0+1)^n \equiv 15 + 1 \equiv 16 \equiv 0 (mod\ 16)$

Uträkningen visar att $15 \cdot 17^n + 3^{4n}$ är kongruent med 0 *modulo* 16 för alla positiva heltal *n*. Detta betyder att $16 \mid 15 \cdot 17^n + 3^{4n}$ för alla positiva heltal *n* vilket skulle bevisas.