Kapitel 5 Modulär aritmetik och egenskaper hos heltalen

5.1 Kongruenser och Z_n

Division kan ibland lämna rester. Vi vet att $3 \nmid 28$, men vi kan ändå utföra divisionen 28/3. Vi får kvoten 9 och resten 1. Med divisionsalgoritmen kan vi uttrycka oss så här: $28 = 9 \cdot 3 + 1$. Talet 3 är divisor, talet 9 kallas kvot och talet 1 kallas rest och vi säger att 28 ger kvoten 9 och resten 1 vid division med 3. Vart tredje tal ger resten 1 vid division med 3. Dessa tal bildar en hel följd av tal:

$$\ldots, -8, -5, -2, 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, \ldots$$

Punkterna i början och i slutet symboliserar att följden av tal fortsätter i all oändlighet. Vi kan rada upp de tal som ger resten 2 vid division med 3. De är $\ldots, -4, -1, 2, 5, 8, \ldots$. De tal som ger resten 0 vid division med 3 är de tal som är delbara med 3 och de bildar också en följd. Dessa tre följder av tal utgör tillsammans alla heltal och vi illustrerar dem i figur 5.1.

Rest 0:	…	−9			−6			−3			0			3			6			9			12	…						
	Alla tal i denna rad ↑ kan skrivas som 3*k* för olika *k*																													
Rest 1:	…		−8			−5			−2			1			4			7			10			13	…					
	Alla tal i denna rad ↑ kan skrivas som 3*k* + 1 för olika *k*																													
Rest 2:	…			−7			−4			−1			2			5			8			11			14	…				
	Alla tal i denna rad ↑ kan skrivas som 3*k* + 2 för olika *k*																													

Figur 5.1 Restklasser Modulo 3.

Vi säger att talen $\ldots, -9, -6, -3, 0, 3, 6, 9, 12, \ldots$ tillhör en och samma *restklass*. Ordet ”klass” betyder i det här fallet mängd av tal och vi klassificerar dessa tal genom att de ger resten 0 vid division med 3, det vill säga de är alla delbara med 3. För att betona att det är 3 det är frågan om brukar man säga *restklass modulo 3*.

Vi säger på så sätt att talen $\ldots, -8, -5, -2, 1, 4, 7, \ldots$ tillhör samma restklass *modulo* 3. Liknande gäller för den undre talföljden.

Med mängdnotation kan restklassen hörande till resten 0 skrivas så här: $\{d \in Z \mid \exists k \in Z : d = 3 \cdot k\}$. På liknande sätt kan vi beskriva de andra två restklasserna med $\{d \in Z \mid \exists k \in Z : d = 3 \cdot k + 1\}$ och $\{d \in Z \mid \exists k \in Z : d = 3 \cdot k + 2\}$.

Vi inför nu beteckningssättet $x \equiv 1 (\mathrm{mod}\, 3)$ (utläses ”*x* är kongruent med 1 *modulo* 3”) som betyder att x ger resten 1 vid division med 3. (Med mängdnotation har vi $x \in \{d \in Z \mid \exists k \in Z : d = 3 \cdot k + 1\}$.) På liknande sätt betyder $x \equiv 2 (\mathrm{mod}\, 3)$ att x ger resten 2 vid division med 3 och $x \equiv 0 (\mathrm{mod}\, 3)$ betyder att x ger resten 0 vid division med 3, det vill säga att x är delbart med 3.

Om $x \equiv 1 (\mathrm{mod}\, 3)$ betyder alltså detta att x är ett steg större än en multipel av 3. Det betyder i sin tur att talet $x - 1$ är *precis* en multipel av 3, det vill säga talet $x - 1$ är delbart med 3 som vi också kan skriva som $x - 1 \equiv 0 (\mathrm{mod}\, 3)$. Resonemanget går i båda riktningar så vi har alltså:

$$x \equiv 1 (\mathrm{mod}\, 3) \;\Leftrightarrow\; x - 1 \equiv 0 (\mathrm{mod}\, 3)$$

Detta kan vi tolka som att vi subtraherat 1 från båda sidor om kongruenstecknet (≡) och det leder oss till att utvidga skrivsättet $x \equiv tal (\mathrm{mod}\, 3)$ till att innefatta andra tal än 0, 1 och 2. Vi skriver $x \equiv y (\mathrm{mod}\, 3)$ om och endast om skillnaden mellan *x* och *y* är jämnt delbar med 3. Det vill säga

$$x \equiv y (\mathrm{mod}\, 3) \Leftrightarrow x - y \equiv 0 (\mathrm{mod}\, 3) \Leftrightarrow 3 \mid x - y$$

Vi har alltså $x \equiv y (\mathrm{mod}\, 3) \Leftrightarrow x - y \equiv 0 (\mathrm{mod}\, 3) \Leftrightarrow 3 \mid x - y$, men att $3 \mid x - y$ betyder att det finns ett tal *k* sådant att $x - y = 3k \Leftrightarrow x = y + 3k$. För att komma från *x* till *y* lägger vi alltså på *k* stycken 3:or. Det nya skrivsättet innebär att vi anser att tal *x* och *y* är kongruenta med varandra *modulo* 3 om vi kan komma från det ena talet *x* till det andra talet *y* genom att lägga på lämpligt antal 3:or. I figur 2.1 har varje rad av tal just den egenskapen att vi kan komma fån varje tal i en rad till varje annat tal i samma rad genom att lägga på (eller dra ifrån) lämpligt antal 3:or.

Exempel:

- $8 \equiv -4 (\mathrm{mod}\, 3)$ för $-4 + 4 \cdot 3 = 8$, här behövs alltså 4 stycken 3:or för att komma från -4 till 8.
- $2 \equiv 5 (\mathrm{mod}\, 3)$ för $5 = 2 + 1 \cdot 3$, här behövs 1 stycken 3:a.
- $5 \equiv 2 (\mathrm{mod}\, 3)$ för $2 = 5 - 1 \cdot 3$, och här behövs –1 stycken 3:a.

Vi kan även införa flera räknesätt på kongruenstecknet. Vi kan addera (och därmed subtrahera) andra tal på båda sidor om kongruenstecknet, så här:

Om $x \equiv y (\mathrm{mod}\, 3)$ gäller för alla tal *a* att $x + a \equiv y + a (\mathrm{mod}\, 3)$. Till exempel har vi $5 \equiv 2 (\mathrm{mod}\, 3)$, efter addition av 4 till båda sidor fås $5 + 4 \equiv 2 + 4 (\mathrm{mod}\, 3) \Leftrightarrow 9 \equiv 6 (\mathrm{mod}\, 3)$. Att verkligen 9 är kongruent med 6 *modulo* 3 kan vi inse genom att studera figur 2.1 eller genom att observera att vi kan lägga en 3:a till 6, då får vi 9. ($9 = 6 + 1 \cdot 3$.) På samma sätta kan vi multiplicera båda sidor med ett tal *c*: Om $x \equiv y (\mathrm{mod}\, 3)$ gäller för alla tal c att $cx \equiv cy (\mathrm{mod}\, 3)$. Vi har följande användbara sats:

Sats 4.1: 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: Bevis av (i) och (ii) lämnas som övning till läsaren. Vi visar endast första delen av (iii): Vi ska visa att $x^2 \equiv y^2 (\mathrm{mod}\, n)$, det vill säga vi ska visa att $n \mid x^2 - y^2$. Vi har som förutsättning att $x \equiv y (\mathrm{mod}\, n)$, det vill säga att $n \mid x - y$. Studera alltså talet $x^2 - y^2$. Enligt konjugatregeln vet vi att $x^2 - y^2 = (x - y)(x + y)$, men $n \mid x - y$ så det finns ett *k* sådant att

$x - y = k \cdot n$. Nu kan vi skriva $x^2 - y^2 = (x-y)(x+y) = k \cdot n \cdot (x+y) = n \cdot heltal$. Vi har alltså visat att $n \mid x^2 - y^2$ vilket är ekvivalent med $x^2 \equiv y^2 (\mathrm{mod}\, n)$ vilket skulle visas.

Exempel: Vi studerar ett par exempel på konsekvenser av sats 4.1.

- $121^{1000} = (120+1)^{1000} = (40 \cdot 3 + 1)^{1000} \equiv 1^{1000} (\mathrm{mod}\, 3) \equiv 1 (\mathrm{mod}\, 3)$. Här har vi observerat att 121 är kongruent med 1 *modulo* 3. Det betyder att 121^{1000} måste vara kongruent med 1 *modulo* 3 enligt sats 4.1 (iii) (med *m* = 1000).

- $98^{99} = (99-1)^{99} = ((33 \cdot 3) - 1)^{99} \equiv (-1)^{99} (\mathrm{mod}\, 3) \equiv -1 (\mathrm{mod}\, 3)$. Här har vi återigen använt samma sats på samma sätt. Vi har också observerat att $-1^{99} = -1^{uddatal} = -1$.

- Om vi nu använder första delen av stas 1 får vi $121^{1000} + 98^{99} \equiv 1 - 1 \equiv 0 (\mathrm{mod}\, 3)$. Vi har alltså funnit att $3 \mid 121^{1000} + 98^{99}$.

Man brukar kalla detta sätt att räkna för *kongruensräkning* vilket innebär att vi kastar alla multiplar av 3. (Eller något annat *n*.) Kongruensräkning är en viktig del av talteorin och har stor betydelse i kryptering och vilket vi kommer att studera senare.

Vi kan uttrycka detta på ett annat sätt, kongruensräkning *modulo* 3 betyder att vi samlar alla tal kongruenta med 0 *modulo* 3 (alltså alla tal delbara med 3) och räknar med dem som om de alla vore 0. På samma sätt samlar vi alla tal kongruenta med 1 *modulo* 3 och räknar med dem som om de alla vore 1. Slutligen samlar vi alla tal som är kongruenta med 2 *modulo* 3 och räknar med dem som om alla de vore 2. Alla tal delbara med 3 representeras alltså av 0, alla tal kongruenta med 1 representeras av 1 och alla tal kongruenta med 2 representeras av 2. Men det riktigt eleganta är att vi faktiskt har friheten att välja representant. I exemplet ovan räknade vi så här $98^{99} = (99-1)^{99} = ((33 \cdot 3) - 1)^{99} \equiv (-1)^{99} (\mathrm{mod}\, 3) \equiv -1 (\mathrm{mod}\, 3)$, vi låter alltså det stora ohanterliga talet 98^{99} ersättas av den lätthanterliga representanten –1. Saken är den att vi faktiskt kan räkna med alla tal kongruenta med 0 i en klump och symbolisera allihop med **0** (0 i fetstil alltså.) På samma sätt symboliserar **1** och **2** alla tal kongruenta med 1 respektive 2 *modulo* 3.

Vi inför ett notationssätt enligt tabell 5.1

Symbol	Exempel på tal	Beskrivning av talen	Mängdnotation
0	$0, \pm 3, \pm 6, \pm 9, \ldots$	alla multiplar av 3	$\{d \mid \exists k \in Z : d = 3 \cdot k\}$
1	$1, 1 \pm 3, 1 \pm 6, 1 \pm 9,$	alla tal som ger rest 1	$\{d \mid \exists k \in Z : d = 3 \cdot k + 1\}$
2	$2, 2 \pm 3, 2 \pm 6, 2 \pm 9,$	alla tal som ger rest 1	$\{d \mid \exists k \in Z : d = 3 \cdot k + 2\}$

Tabell 5.1 Notationssätt för restklasser.

Symbolen **0** betecknar alltså inte ett tal utan en hel klass av tal. En så kallad *restklass*. Det är nu möjligt att definiera räkneoperationer mellan restklasser. Vi illustrerar detta för tal kongruenta *modulo* 3 i följande exempel:

Exempel: Studera figur 2.1 igen.

- Välj $x = 1$ ur rad 2 och $y = 2$ ur rad 3. Addera dessa tal, det ger $x + y = 1 + 2 = 3 = z$, $z = 3$ ligger i rad 1.
- Välj $x = 4$ ur rad 2 och $y = 8$ ur rad 3. Addera dessa tal, det ger $x + y = 4 + 8 = 12 = z$, $z = 12$ ligger i rad 1.
- Välj $x = 7$ ur rad 2 och $y = -1$ ur rad 3. Addera dessa tal, det ger $x + y = 7 + -1 = 6 = z$, $z = 6$ ligger i rad 1.

Det gäller alltså *alltid* (bevisa detta!) att tal ur rad 2 adderade till rad 3 alltid ger tal i rad 1! Talen i rad 2 är restklassen **1** och talen i rad 3 är restklassen **2** och talen i rad 1 är restklassen **0**. Vi kan därför anse att vi kan addera hela rader (eller restklasser) till varandra, rad 1 adderad till rad 2 ger rad 1 vilket tolkas som att restklassen **1** adderad till restklassen **2** ger restklassen **0**. Vi har alltså **1** + **2** = **0**. De tre restklasserna **0**, **1** och **2** brukar man sammantagna kalla Z_3 som alltså är en ny mängd matematiska objekt. Nu kan vi skapa en additionstabell för Z_3. Den återges i tabell 5.2.

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

Tabell 5.2 Additionstabell för Z_3

Tabell 5.2 är alltså en tabell över *modulo*-3 addition i Z_3. Vi kan även skapa en multiplikationstabell på samma sätt (genomför beräkningarna i exemplet ovan, men byt ordet ”addera” mot ”multiplicera” för att se att detta går att genomföra även för multiplikation). Vi åteyrger den i tabell 5.3.

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

Tabell 5.3 Multiplikationstabell för Z_3.

Z_3 betecknar alltså {**0**, **1**, **2**} = mängden av de tre restklasserna *modulo* 3. Vi kan göra detta för andra tal än 3, till exempel har additionstabellen för Z_4 återgiven i tabell 5.4

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

Tabell 5.4 Additionstabellen för Z_4.

Multiplikationstabellen för Z_4 återges i tabell 5.5.

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

Tabell 5.5 Multiplikationstabellen för Z_4.

Vi studerar multiplikationstabellerna för Z_5, Z_7 och Z_{10} i tabellerna 5.6, 5.7 och 5.8.

*	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**

Tabell 5.6. Multiplikationstabellen för Z_5.

*	0	1	2	3	4	5	6
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**	**6**
2	**0**	**2**	**4**	**6**	**1**	**3**	**5**
3	**0**	**3**	**6**	**2**	**5**	**1**	**4**
4	**0**	**4**	**1**	**5**	**2**	**6**	**3**
5	**0**	**5**	**3**	**1**	**6**	**4**	**2**
6	**0**	**6**	**5**	**4**	**3**	**2**	**1**

Tabell 5.7. Multiplikationstabellen för Z_7.

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

Tabell 5.8. Multiplikationstabellen för Z_{10}.

Någonting som är ganska spännande att lägga märke till är att raderna i multiplikationstabellen hörande till Z_7 (tabell 5.7) innehåller, på varje rad, varje element ur Z_7 och varje element förekommer exakt en gång. Till exempel innehåller rad 3 i multiplikationstabellen för Z_7 elementen **0**, **3**, **6**, **2**, **5**, **1**, **4** vilket är alla element i Z_7 fast i en omkastad ordning. Detta är fallet för alla rader. Varje rad i multiplikationstabellen för Z_7 ger

oss alltså en omordning av alla element i Z_7. Detta är något som utnyttjas i kryptering, fast i en annan form som vi senare ska se. Motsvarande gäller *inte* för Z_{10}, till exempel består rad 5 i tabell 5.8 bara av elementen **0** och **5**. Nyckelegenskapen är att 7 är ett primtal och 10 är inte ett primtal.

5.2 Egenskaper hos heltalen

Med kongruenser, delbarhet och bevismetoder som studerat i kapitel 1 och 2 har vi nu en del verktyg som kan använda för att göra olika utredningar och insikter om de hela talen. Vi ska ta ett par exempel.

Exempel:

- Visa att alla tal som är på formen $n^2 - n$ alltid är delbara med 2.
  Lösning: Alla tal *n* kan enligt divisionsalgoritmen skrivas på formen $n = 2 \cdot q + r$ där r = 0 eller 1. Vi får således 2 fall:

  Fall 1: $n = 2k$. Då får vi $n^2 - n = (2k)^3 - (2k) = 4k^2 - 2k = 2 \cdot (2k^2 - k)$. Detta är ett tal som är delbart med 2 och vi har alltså visa att $2 | n^3 - n$ då $n = 2k$.

  Fall 2: $n = 2k + 1$. Då får vi $n^2 - n = (2k+1)^2 - (2k+1) = 4k^2 + 4k + 1 - 2k - 1 = 4k^2 + 2k = 2 \cdot (2k^2 + k)$ vilket också är delbart med 2. Således har vi visat att $2 | n^3 - n$ då $n = 2k + 1$.

  Eftersom de enda två fallen som kan inträffa är $n = 2k$ och $n = 2k + 1$ och uttrycket $n^2 - n$ visade sig vara delbart med 2 i båda dessa fallen saken klar.

  Anmärkning: Vi skulle kunna löst detta med kongruenser också. Vi studerar ett liknande exempel där vi löser en uppgift av detta slag med kongruenser.

- Visa att alla tal som är på formen $n^3 - n$ alltid är delbara med 3.
  Lösning: Vi ska alltså visa att $\forall n \in Z : 3 \mid n^3 - n$. Ett tal är delbart med 3 om och endast om det är kongruent med 0 modulo 3. Det betyder att om vi kan visa att $\forall n \in Z : n^3 - n \equiv 0 (\mathrm{mod}\, 3)$ så är vi klara. Alla tal *n* ligger i någon av de tre restklasserna 0, 1 eller 2 av Z_3 så vi behöver bara kontrollera att $n^3 - n \equiv 0$ för **0**, **1** och **2** (elementen ur Z_3). Vi beräknar således

  $0^3 - 0 = 0 \equiv (\mathrm{mod}\, 3)$ och $1^3 - 1 = 1 - 1 = 0 \equiv (\mathrm{mod}\, 3)$ och $2^3 - 2 = 8 - 2 = 6 \equiv 0 (\mathrm{mod}\, 3)$.

  Eftersom vi fann att alla kongruenser blev noll är saken klar. Vi har visat att $\forall n \in Z : n^3 - n \equiv 0 (\mathrm{mod}\, 3)$.

Övning 5.1. Gör en egen figur liknande figur 1.1, men basera figuren på restklasser *modulo* 5. Hur många rader (restklasser) blir det i din figur?

Övning 5.2.

a. Vilken rest fås då 411*821 + 376*297 divideras med 7?

b. Vilken rest fås då 207^{61} divideras med 13? Vilken rest fås då 207^{6100} divideras med 13?

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

d. Visa att $3^{2n+1} + 5^{2n}$ är delbart med 4 men inte med 8 för n>=0.