1. Ge en explicit bijektion från de naturliga talen till mängden av alla udda heltal,

$$M = \{\ldots, -3, -1, 1, 3, \ldots\}.$$

Lösning: Låt $f : \mathbf{N} \to M$ definieras som $f(n) = n$ om n är udda och $f(n) = -n + 1$ om n är jämnt. Observera att udda tal avbildas på positiva tal medan jämna tal avbildas på negativa. Funktionen f är injektiv för givet två naturliga tal, n, m, så ger $f(n) = f(m)$ antingen $n = m$ om talen är udda och $-n + 1 = -m + 1$ om talen är jämna, men det senare ger också $n = m$. Vi ska nu visa att funktionen är surjektiv. Varje positivt udda heltal är bilden av sig själv och ett negativt heltal, n, fås som bilden av $-(n-1)$, så f är surjektiv. Då f är både injektiv och surjektiv så är den en bijektion.

2. Finn ett alternativt uttryck för den booleska funktionen

$$f(x, y, z, w) = \bar{x}\bar{y}\bar{z}w + \bar{x}\bar{y}zw + \bar{x}y\bar{z}\bar{w} + \bar{x}y\bar{z}w + \bar{x}yzw + \bar{x}yz\bar{w} + xy\bar{z}w + x\bar{y}\bar{z}w + x\bar{y}zw$$

med så få termer som möjligt.
Lösning: Vi använder ett Karnaughdiagram.

$xy\backslash zw$	00	01	11	10
00	0	1	1	0
01	1	1	1	1
11	0	1	0	0
10	0	1	1	0

De markerade grupperna ger oss: $\bar{x}y + \bar{z}w + \bar{y}w$. Vi kan inte täcka 1:orna med färre cirklar så detta är ett minimalt uttryck.

3. Ett 9-spel består av en platta med 8 bitar och en tom plats och det är tillåtet att skjuta biten närmast till höger om, vänster om, ovanför eller nedanför tomrummet till den tomma platsen. T ex kan vi som första steg, i den vänstra figuren nedan, flytta Y eller T till den tomma platsen. Visa att det inte går, med tillåtna drag, att ändra uppställningen till vänster så att den blir den till höger.

A	E	I
O	U	Y
R	T	

A	Y	I
R	O	T
E	U	

.

Lösning: Permutationen som tar den första uppställningen till den andra är:

$$(A)(EYTUOR)(I)(\square).$$

Så den är udda eftersom den innehåller en cykel med jämn längd. Men för att den tomma platsen ska kunna komma tillbaka till utgångspunkten måste antalet förflyttningar uppåt vara lika med dem nedåt och de åt höger lika med de åt vänster, vilket betyder att permutationen måste vara jämn eftersom en förflyttning sker via en transposition. Udda permutationer är således omöjliga att uppnå. Se också exempel 5.6 i boken.

4. Finn polynom $\mu(x)$ och $\lambda(x)$ i $\mathbf{Z}_5[x]$ sådana att

$$\mu(x)(x^2 + 3x + 2) + \lambda(x)(x^3 + 2x^2 + 3x) = 1.$$

Lösning: Euklides algoritm ger

$$\begin{aligned} x^3+2x^2+3x &= (x+4)(x^2+3x+2)+(4x+2) \\ x^2+3x+2 &= 4x(4x+2)+2. \end{aligned}$$

Går vi baklänges får vi

$$\begin{aligned} 2 &= (x^2+3x+2)-4x(4x+2) \\ 2 &= (x^2+3x+2)-4x((x^3+2x^2+3x)-(x+4)(x^2+3x+2)) \\ &= (1+4x(x+4))(x^2+3x+2)-4x(x^3+2x^2+3x) \\ &= (4x^2+x+1)(x^2+3x+2)+x(x^3+2x^2+3x). \end{aligned}$$

Vi har nu löst motsvarande ekvation med en tvåa som högerled. För att få en 1:a multiplicerar vi med 3, som är invers till 2 modulo 5. Det ger

$$1=(2x^2+3x+3)(x^2+3x+2)+3x(x^3+2x^2+3x),$$

dvs $\mu(x)=2x^2+3x+3$ och $\lambda(x)=3x$ är en lösning.

5. Förklara hur man med hjälp av kantfärgning kan utvidga nedanstående latinska rektangel till en latinsk kvadrat.

A	D	E	B	C
C	B	A	D	E
E	C	B	A	D

Lösning: Se boken avsnitt 10.3.

6. Visa att det inte kan finnas någon perfekt binär kod med längd 6 som rättar ett fel. Ge exempel på en linjär kod med längd 6, som rättar ett fel och som är maximal med avseende på antalet kodord.
Lösning: Om koden ska kunna rätta ett fel måste mängderna av ord, som man kan få genom att göra högst ett fel utgående från ett kodord, vara disjunkta. Om C betecknar mängden av kodord, betyder det att vi har olikheten: $|C|\cdot(1+\binom{6}{1}) \leq 2^6 = 64$. Eftersom $7 \nmid 64$ så kan det inte finnas någon perfekt binär kod som rättar ett fel. Om koden är linjär så är $|C|=2^k$ för något k, och det största värdet på k som passar in i olikheten ovan är $k=3$, dvs $|C|=8$. Ett exempel på en sådan kod är t ex $\{000000, 011001, 101010, 110011, 110100, 101101, 011110, 000111\}$.

7. Finn samtliga delgrupper till $U(\mathbf{Z}_{24})$, dvs den multiplikativa gruppen av inverterbara element i $\mathbf{Z}_{24}$.
Lösning: Gruppen har ordning $\phi(24)=8$ och Lagranges sats säger att ordningen hos delgrupperna ska dela gruppens ordning. Delgrupperna har därför ordning 1, 2, 4 eller 8. Delgruppen med ordning 1 är helt enkelt $\{1\}$ och den enda delgruppen med ordning åtta är gruppen själv. Elementen i gruppen är de som saknar gemensam delare med 24, dvs $\{1,5,7,11,13,17,19,23\}$. En enkel räkning modulo 24 visar att alla elementen utom 1 har ordning 2. Det ger att delgrupperna med ordning 2 blir $\{1,5\}$, $\{1,7\}$, $\{1,11\}$, $\{1,13\}$, $\{1,17\}$, $\{1,19\}$, $\{1,23\}$. Delgrupperna med ordning 4 fås genom att ta två element ur mängden $\{5,7,11,13,17,19,23\}$ och sedan lägga till element så den blir multiplikativt sluten, dvs 1 och produkten av de två elementen. Vi får $\{1,5,7,11\}$, $\{1,5,13,17\}$, $\{1,5,19,23\}$, $\{1,7,13,19\}$, $\{1,7,17,23\}$, $\{1,11,13,23\}$, $\{1,11,17,19\}$.

8. Bevisa med ett kombinatoriskt argument identiteten

$$\binom{n}{4} = \sum_{k=0}^{n-4} \binom{n-1-k}{3},$$

för alla $n \geq 4$.
Lösning: Vi ska välja 4 element ur en mängd med n element. Givet ett element z i mängden kan vi dela upp valen i två fall: de där z ingår och de där z inte ingår. Om z ingår återstår det att välja 3 element bland övriga vilket är en mängd med $n-1$ element. Det ger summanden $\binom{n-1}{3}$. Om z inte ingår så ska vi välja 4 element bland övriga. Välj ett nytt element, z', i den mängden. Vi får då igen två fall: att z' ingår eller inte ingår. Det första alternativet ger summanden $\binom{n-1-1}{3}$. Proceduren kan upprepas ända tills vi har kvar en mängd med bara 4 element då vi måste välja samtliga.

9. Den underliggande mängden i den booleska algebran $\mathcal{B}_n$ är mängden av alla binära ord med längd n, V^n. I $\mathcal{B}_n$ har vi de tre operationerna $+, \cdot$ och $^-$. Vi har också, i samband med felrättande koder, definierat en annan addition på V^n, som vi kan beteckna $\oplus$, genom att addera komponentvis modulo 2. Uttryck operationen $\oplus$ med $+, \cdot$ och $^-$. Visa också att $(V^n, \oplus, \cdot)$ är en ring.
Lösning: Eftersom alla operationerna räknas komponentvis räcker det att betrakta fallet $n = 1$ för att komma fram till hur $\oplus$ kan uttryckas i $+, \cdot, ^-$. Funktionen $(x, y) \mapsto x \oplus y$ är 1 precis då en av variablerna är 1 och den andra 0. Funktionens disjunktiva normalform blir därför $x\bar{y} + \bar{x}y$. Så $x \oplus y = x\bar{y} + \bar{x}y$. Vi ska nu visa att $(V^n, \oplus, \cdot)$ är en ring. Per definition är $(V^n, \oplus)$ isomorf med $\mathbf{Z}_2^n$. Vi får därmed att $(V^n, \oplus)$ är en abelsk grupp, vilket visar att axiom R1 är uppfyllt. Att operationen $\cdot$ är sluten, associativ och har ett identitetselement följer direkt från definitionen. Det återstår att verifiera de två distributiva lagarna

$$\begin{aligned} z \cdot (x \oplus y) &= z \cdot x \oplus z \cdot y \\ (x \oplus y) \cdot z &= x \cdot z \oplus y \cdot z. \end{aligned}$$

Eftersom multiplikationen är kommutativ räcker det att visa den första. Vi har

$$\begin{aligned} z \cdot x \oplus z \cdot y = z \cdot x \cdot \bar{z} \cdot \bar{y} + \bar{z} \cdot \bar{x} \cdot z \cdot y = z \cdot x \cdot (\bar{z} + \bar{y}) + (\bar{z} + \bar{x}) \cdot z \cdot y = \\ z \cdot x \cdot \bar{y} + \bar{x} \cdot z \cdot y = z \cdot (x \cdot \bar{y} + \bar{x} \cdot y) = z \cdot (x \oplus y). \end{aligned}$$

10. RSA-kryptering fungerar tack vare identiteten

$$x^{k(p-1)(q-1)+1} \equiv x \pmod{pq},$$

som gäller då p, q är två olika primtal och k, x är två heltal. Bevisa identiteten.
Lösning: Om $\mathrm{SGD}(x, p) = 1$ så ger Fermats lilla sats att $x^{p-1} \equiv 1 \pmod{p}$ vilket i sin tur ger $x^{k(p-1)(q-1)+1} \equiv x \pmod{p}$ och den senare identiteten är uppenbart sann även om $p|x$ för då står det $0 \equiv 0 \pmod{p}$. Vi har alltså $p|x^{k(p-1)(q-1)+1} - x$ och på samma sätt får vi $q|x^{k(p-1)(q-1)+1} - x$. Då $\mathrm{SGD}(p, q) = 1$ betyder det att $pq|x^{k(p-1)(q-1)+1} - x$, dvs $x^{k(p-1)(q-1)+1} \equiv x \pmod{pq}$.