Avsnitt 19

11) Vi vil løse ligningen $x^3 - 2x^2 - 3x = 0$ i $\mathbb{Z}_{12}$.

Vi faktoriserer:

$$x(x^2-2x-3) = x(x-3)(x+1) \equiv (x-0)(x-3)(x-11) \pmod{12}$$ m

Så løsningene er $12\mathbb{Z}$, $3+12\mathbb{Z}$ og $11+12\mathbb{Z}$, i tillegg til $5+12\mathbb{Z}$, $8+12\mathbb{Z}$ og $9+12\mathbb{Z}$. $(5-3)(5-11)$, $(8-0)(8-11)$, $(9-3)(9-11)$.

2) Vi vil løse $3x = 2$ i $\mathbb{Z}_7$ og i $\mathbb{Z}_{23}$. I $\mathbb{Z}_7$ ser vi $x = 3+7\mathbb{Z}$ er løsningen, og i $\mathbb{Z}_{23}$ har vi $x = 16 + 23\mathbb{Z}$. d

11) Vi lar R være en kommutativ ring med karakteristikk 4. Da R er kommutativ holder binomialteoremet.

$$(a+b)^4 = \sum_{n=0}^{4} \binom{4}{n} a^n b^{4-n} = a^4 + 4ab^3 + 6a^2b^2 + 4a^3b + b^4$$

$$= a^4 + 2a^2b^2 + b^4 = (a^2+b^2)^2.$$

(Her lar vi $n \cdot x = \underbrace{x + x + x + \cdots + x}_{n \text{ ganger}}$.) dk

23) Vi lar R være en divisjonsring og vil finne elementer som oppfyller $a^2 = a$. Dersom $a \neq 0$ har vi a^{-1} s.a. $a^{-1}a^2 = a^{-1}a \Rightarrow a = 1$. Videre, om $a = 0$ har vi $a^2 = a$, så de eneste to mulighetene er $a = 0$ og $a = 1$ (multiplikativ og additiv identitet.) de □

26) La R vare en ring som inneholder minst to elementer. Anta for hver $a \neq 0$ $\exists! b \in R$ s.a. $aba = a$.

(a) Vi vil vise at R ikke har noen nulldivisorer. La $a \neq 0$ og anta $ax = 0$. La b vare unik s.a. $aba = a$. Her da

$$b + x = k$$
$$a(b+x) = ak$$
$$ab + ax = ak$$
$$ab = ak$$
$$aba = aka$$
$$a = aka,$$

men da må $b = b$, da dette var unik i å ha $aba = a$. Følgelig er $b + x = b$, og $x = 0$. Altså har vi ingen nulldivisorer i R.

(b) Av (a) og teorem 19.5 holder forkortningslovene. Nå har vi

$$aba = a \implies abab = ab \implies bab = b.$$

(c) Vi nominer ab til enhet. Se at

$$xab = y \implies xabba = ya \implies xa = ya$$
$$\implies x = y.$$

Tilsvarende er ab venstreidentitet.

$$abx = y \implies babx = by \implies bx = by$$
$$\implies x = y, \text{ ved (b).}$$

Følgelig er $ab = 1$ for $a \neq 0$ og b s.a. $aba = a$.

(d) La $x \neq 0$. Nominer $y \in R$ s.a. $xyx = 1$ som invers. Ved forkortningslover og (c) får vi $yx = 1$ og $xy = 1$. Følgelig er R en divisjonsring. de

□

29) La D være et integritetsområde. En mulighet er at D har karakteristikk 0, fx $\mathbb{Z}$. Anta så at karakteristikken er $k > 0$, og $k = m \cdot n$, der $m, n > 1$. Har da at

Er $m \cdot n = m + n - 1$

$$(mn \cdot 1) = (m \cdot 1)(n \cdot 1) \stackrel{?}{=} \underbrace{([m+n-1] \cdot 1)}_{a} \cdot \underbrace{1}_{b} = 0.$$

La $a = m \cdot 1$, $b = n \cdot 1$ $\Rightarrow$ lut. omr. $\Rightarrow a = 0 \vee b = 0$ $\Rightarrow \operatorname{char} R \leq m \cdot n$

Men da vi er i et integritetsområde vil dette implisere $ab = 0$, og følgelig må a eller b være 0, som åpenbart er galt. Altså må karakteristikken $k = p$, primtall p. □

30) Vi lar R være en ring med karakteristikk k, og definer $S = R \times \mathbb{Z}$ om $k = 0$ og $S = R \times \mathbb{Z}_n$ om $k = n$. La addisjon være definert komponentvis som vanlig, og definer multiplikasjon ved

$$(r_1, n_1)(r_2, n_2) = (r_1 r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1 n_2)$$

hvor nr tolkes som i seksjon 18.

(a) Vi vil vise at S er en ring.

(R_1) Da R og $\mathbb{Z}$ ($\mathbb{Z}_n$) er abelske grupper under addisjon, er $R \times \mathbb{Z}$ ($R \times \mathbb{Z}_n$) også abelske grupper under koordinatvis addisjon.

(R_2) La $a = (r_1, n_1)$, $b = (r_2, n_2)$ og $c = (r_3, n_3)$. Da har vi

$$a(bc) = (r_1, n_1)(r_2 r_3 + n_2 \circ r_3 + n_3 \circ r_2, n_2 n_3)$$

$$= (r_1 (r_2 r_3 + n_2 \circ r_3 + n_3 \circ r_2) + n_1 \circ (r_2 r_3 + n_2 \circ r_3 + n_3 \circ r_2) + (n_2 n_3)(r_1), n_1 n_2 n_3)$$

$$= (r_1 r_2 r_3 + r_1 \circ (n_2 n_3) + r_2 \circ (n_1 n_3) + r_3 \circ (n_1 n_2) + n_1 (r_2 r_3) + n_2 (r_1 r_3) + n_3 (r_1 r_2), n_1 n_2 n_3)$$

$$= ((r_1 r_2 + n_1 \circ r_2 + n_2 \circ r_1) r_3 + n_3 (r_1 r_2 + n_1 \circ r_2 + n_2 \circ r_1) + (n_1 n_2) \circ r_3)$$

$$= (r_1 r_2 + n_1 \circ r_2 + n_2 \circ r_1, n_1 n_2)(r_3, n_3)$$

$$= (ab)(c),$$

Så multiplikasjon er assosiativ.

(R_3) La a, b, c være som i (R_3). Her har vi

$$a(b+c) = (r_1, n_1)(r_2 + r_3, n_2 + n_3)$$

$$= (r_1 (r_2 + r_3) + n_1 (r_2 + r_3) + (n_2 + n_3) \circ r_1, n_1 n_2 + n_1 n_3)$$

$$= (r_1 r_2 + n_1 r_2 + n_2 r_1 + r_1 r_3 + n_1 r_3 + n_3 r_1, n_1 n_2 + n_1 n_3)$$

$$= (r_1 r_2 + n_1 \circ r_2 + n_2 \circ r_1, n_1 n_2) + (r_1 r_3 + n_1 \circ r_3 + n_3 \circ r_1, n_1 n_3)$$

$= ab + ac.$

Tilsvarende følger $(a+b)c = ac + bc$, men dette bokstaveringsarbeid på denne kjøp jeg meg ikke.

Følgelig er S en ring.

(b) Vi lar 0 betegne additiv identitet i R. Vi ser da at $(0,1) = 1_S$. La $a = (r,n)$. Vi får da

$$a \cdot 1_S = (r,n)(0,1) = (r\cdot 0 + n\cdot 0 + 1\cdot r, n\cdot 1) = (r,n) = a$$
$$1_S \cdot a = (0,1)(r,n) = (0\cdot r + 1\cdot r + n\cdot 0, 1\cdot n) = (r,n) = a$$

(c) Dersom R har karakteristikk 0, dvs. $n \cdot x \neq 0$ om $n \neq 0$ ser vi dette vil holde for $S = R \times \mathbb{Z}$, spesielt da $\mathbb{Z}$ har karakteristikk 0 og i $\mathbb{Z}$-koordinatet er operasjonen definert som i $\mathbb{Z}$.

La derfor karakteristikken til R være n. Dette betyr $n \cdot r = 0$, $\forall r \in R$. La $a \in R \times \mathbb{Z}$. $a = (r,k)$. Her da:

Nok å se på $r \cdot (0,1)$.

$$n \cdot a = \underbrace{(r,k) + (r,k) + \cdots + (r,k)}_{n \text{ ganger}}$$
$$= (r + r + \cdots k, nk) = (nr, nk)$$
$$= (0, nk) = (0,0),$$

da $nk \equiv 0 \pmod n$, $\forall k \in \mathbb{Z}_n$. Følgelig har vi at karakteristikken til S er lik karakteristikken til R.

og $\operatorname{char} \mathbb{Z}_n = n$

$\square$

merk:

$n \cdot a = 0 \ \forall a \in S$
$\Updownarrow$
$n \cdot 1_S = 0$

Bevis: $\Downarrow$: opplagt.
$\Uparrow$: $n \cdot a = (a + \cdots + a)$
$= (1 \cdot a + \cdots + 1 \cdot a)$
$= (1 + \cdots + 1) a$
$= (n \cdot 1) \cdot a$
$n \cdot 1 = 0 \Rightarrow n \cdot a = 0 \ \forall a \in S$

(d) Vi definerer $\phi: R \to S$ ved $\phi(r) = (r,0)$. Vil vise at dette er en isomorfi til en underring av S.

Vi viser først at ϕ er en homomorfi av ringer:

$$\phi(r+s) = (r+s, 0+0) = (r,0) + (s,0) = \phi(r) + \phi(s).$$

$$\phi(rs) = (rs, 0) = (r,0)(s,0) = \phi(r)\phi(s).$$

$$\phi(1) = \phi(1) = (1,0),$$

som vi i (5) ikke var enhet i S. Nei! $(0,1) = 1_S$ men $\operatorname{Im}\phi \cong R$ der $1_{\operatorname{Im}\phi} = (1,0)$

Vi definerer $U = \{(a,b) \in R \times \mathbb{Z}_{(n)} \mid b = 0\}$. Vi ser at ϕ er bijektiv $\phi: R \to U$ åpenbart, hvis vi viser at U er en underring av S.

(1) Vi ser at $0_S = (0,0) \in U$.

(2) La $a \in U$. $a = (r,0)$. Da er $-a = (-r,0) \in U$ og $a + (-a) = (r+(-r), 0+0) = (0,0)$, så inverser er med.

(3) Assosiativitet arves fra S.

(4) Distributivitet arves fra S.

(5) Vi viser at U er lukket. La $a = (r,0)$ og $b = (s,0)$ være med i U:

$$a + b = (r+s, 0) \in U$$

$$a \cdot b = (ab + 0a + 0b, 0^2) = (ab, 0) \in U.$$

Følgelig er U en underring, og ϕ er isomorfi: $\phi: R \to U$. □

Avsnitt 20

1) Vi vil finne en generator for $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$. Ser at 5 er en slik generator:

$$5 \equiv 5 \pmod 7$$
$$5^2 \equiv 4 \pmod 7$$
$$5^3 \equiv 6 \pmod 7$$
$$5^4 \equiv 2 \pmod 7$$
$$5^5 \equiv 3 \pmod 7$$

og åpenbart $5^6 \equiv 5^{7-1} \equiv 1$ ved Fermats teorem. Altså er 5 en generator, og $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$ er syklisk.

Ja

2) Vi vil finne en generator for $G = (\mathbb{Z}_{11} \setminus \{0\}, \cdot)$. Vi ser at 2 er en generator:

$$2, 4, 8, 5, 10, 9, 7, 3, 6, 1.$$

Altså er $G = \langle 2 \rangle$ og syklisk.

Ja

4) Vi bruker Fermats teorem og får

$$3^{47} \equiv (3^{22})^2 \cdot 3^3 \equiv 1^2 \cdot 27 \equiv 27 \equiv 4 \pmod{23},$$

så rest blir 4.

Ja

6) Vi vil beregne resten til $2^{(2^{17})}+1$ når vi deler ved 19. Ved Fermats teorem vet vi at $2^{18} \equiv 1 \pmod{19}$. Vi vil altså skrive

$$2^{17} = 18q + r,$$

for dette vil gi

$$\left(2^{(2^{17})}+1\right) \equiv 2^{18q+r} + 1 \equiv 2^r + 1 \pmod{19}$$

Vi må altså beregne resten til 2^{17} når vi deler på 18. Vi har $\varphi(18) = 8$, som gir ved Eulers teorem: Eulers gjelder kun dersom $\gcd(2,18)=1$!!?

$$r \equiv 2^{17} \equiv 2 \cdot (2^8)^2 \equiv 2 \pmod{18}$$

Følgelig har vi

$$2^2 + 1 \equiv 5 \pmod{19},$$

Som blir resten om vi deler $2^{(2^{17})}+1$ på 19.

8) La p være et primtall. Vi vil beregne

$$\varphi(p^2) = |\{x \mid 1 \le x \le p \wedge \gcd(x,p) \neq 1\}| = p^2 - |\{kp \mid k = 0,1,2,3,\ldots,p\}| = p^2 - p = p(p-1).$$

de

9) Vi lar $p \neq q$ og vil beregne $\varphi(p)\varphi(q) = \varphi(pq)$, da φ er multiplikativ. Nå vi vet at $\varphi(p) = (p-1)$ og $\varphi(q) = (q-1)$, så $\varphi(pq) = (p-1)(q-1)$.

ok

10) Vi vil bruke Eulers teorem til å beregne resten til 7^{1000} når vi deler på 24.
Vi har at

$$\varphi(24) = \varphi(3 \cdot 2^3) = \varphi(3) \cdot \varphi(2^3) = (3-1)(2-1)\cdot 2^{3-1} = 8.$$

Følgelig er

$$7^{1000} \equiv (7^8)^{125} \equiv 1^{125} \equiv 1 \pmod{24}.$$

ok

24) Vi har $\mathbb{Z}_{12}$, og finner $U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$.
Multiplikasjonstabellen blir:

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Notem at alle elementer er s.a. $x^2 = 1$, så
$U(\mathbb{Z}_{12}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ – Klein-4-gruppen.

ok

27) Vi vil finne alle elementer som er sin egen invers i kroppen $\mathbb{Z}_p$. Dette gir

$$x^2 \equiv 1 \pmod{p}$$

Men dette gir likningen

$$x^2 - 1 \equiv 0 \pmod{p}$$

Da $\mathbb{Z}_p$ er kommutativ kan vi skrive

$$(x-1)(x+1) \equiv 0 \pmod{p}$$

Da $\mathbb{Z}_p$ er en kropp, er den også et integritetsområde, dvs. $ab = 0 \iff a = 0 \vee b = 0$. Altså har vi kun mulighetene

$$\begin{cases} x - 1 \equiv 0 \pmod{p} \\ x + 1 \equiv 0 \pmod{p} \end{cases}$$

Som gir løsningene

$$\begin{cases} x \equiv 1 \pmod{p} \\ x \equiv p - 1 \pmod{p}. \end{cases}$$

Følgelig er 1 og $p-1$ de eneste elementene med multiplikativ selvinvers. □

28) Vi vil vise at dersom p er et primtall vil

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

Vi ser at det stemmer for $p=2$. Anta $p \geq 3$. Av forrige oppgave vet vi at kun 1 og $p-1$ er sin egen invers. Videre vet vi at inversen er unik, så for de $p-3$ elementa

$$2, 3, 4, \ldots, p-2$$

vil hver av disse ha en annen som sin invers. Da $\mathbb{Z}_p$ er kommutativ, kan vi skrive om på disse så

$$2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1^{\frac{p-3}{2}} \pmod{p}.$$

Følgelig er

$$(p-1)! \equiv 1 \cdot 1^{\frac{p-3}{2}} \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}$$

hvilket vi skulle vise. □

[Vi noterer at dersom n ikke er primtall vil $n = a \cdot b$ der $a, b < n$. Følgelig vil $ab \mid (n-1)!$ og $(n-1)! \equiv 0 \pmod{n}$.]