

Opgaver til Kapitel 1.

- U1 **1.** Möbius-funktionen $\mu(n)$ har værdien 1 for $n = 1$, værdien $(-1)^r$ når n er et produkt af r forskellige primtal, og værdien 0 ellers. Vis, at Möbius-funktionen $\mu(n)$ kan karakteriseres som den eneste funktion $\mu: \mathbb{N} \rightarrow \mathbb{C}$ som opfylder: $\mu(1) = 1$ og $\sum_{d|n} \mu(d) = 0$ for $n > 1$.
- H1 **2.** Bevis formelen $\pi(n) = \sum_k (\mu(k)/k) \Pi(\sqrt[k]{n})$, hvor $\Pi(n)$ er defineret i (1.12).
- H1 **3.** Vis, at de tre asymptotiske formler, $\pi(n) \sim \text{Li}(n)$, $\Pi(n) \sim \text{Li}(n)$, $\pi(n) \sim R(n)$, alle er ækvivalente med Primtalsætningen. Her fortolker vi $R(n)$ som den (endelige) sum der fremkommer af højresiden i (1.12.3), når logaritme-integralet sættes til 0 for $1 < x < 2$.
- H1 **4.** Tegn på millimeterpapir graferne for funktionerne $300\pi(x)$ og $300\nu(x)$ på intervallet $0 \leq x \leq N$, hvor $N := 10^{130}$, idet interval-endepunkterne på x -aksen anbringes med en afstand på 10 cm. Du må gerne antage, at $\pi(x) = x/\log x$ for $x > 2$ (og $\nu(x)$ er antallet af kvadrattal, der højst er x), og du må gerne tegne med en blyant, hvis spids er ca 1mm tyk. Men du skal kunne forsvare din tegning. [Vink: $300 \approx \log 10^{130}$.]
- H1 **5.** Vis, at $(3, 5, 7)$ er det eneste sæt primtalstrillinger.
- 6.** Bestem, med $A(n)$ fra (1.12), $A(10^{18})$ med 2 decimaler. Værdien $\pi(10^{18})$ er givet i (1.13).
- U1 **7.** Fermat-primtallene er (ulige) primtal af formen $p = 2^k + 1$. Vis, at hvis $2^k + 1$ (med $k > 0$) er et primtal, så er k nødvendigvis en potens af 2. Fermat-primtallene er altså af formen $F_n = 2^{2^n} + 1$. De første 5 Fermat-primtal er følgende

n	0	1	2	3	4
F_n	3	5	17	257	65.537

Man kender ikke andre Fermat-primtal. Euler beviste, at 641 går op i F_5 . Check lige udregningen: Det er let at se, at $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$. Modulo 641 gælder derfor, at

$$2^{32} = 2^4 \cdot 2^{28} \equiv -5^4 \cdot (2^7)^4 \equiv -(-1)^4 = -1, \text{ altså er } F_5 = 2^{32} + 1 \equiv 0 \pmod{641}.$$

- U2 **8.** Mersenne-primtallene er primtal af formen $M_p = 2^p - 1$. Vis, at hvis M_p er et primtal, så er p et primtal. Vis, at det omvendte ikke gælder. Her er de første Mersenne-primtal:

p	2	3	5	7	13	17	19	31
M_p	3	7	31	127	8.191	131.071	524.287	2.147.483.647

Der kendes med sikkerhed 39 Mersenne-primtal. Det største, svarende til $p = 13.466.917$, har 4.053.946 cifre.

- 9.** Vis, at et lige tal n er perfekt, dvs lig med summen af sine ægte divisorer (incl. 1), hvis (ifølge Euklid) og kun hvis (ifølge Euler) $n = 2^{q-1}(2^q - 1)$, hvor $2^q - 1$ er et primtal.
- 10.** Check lige, at definitionen i (1.15), $\text{Li}(x) = \text{Ei}(\log x)$, harmonerer med, at logaritme-integralet er en stamfunktion til $1/\log x$, jfr (1.12.2).
- 11.** Vis, at rækkerne (1.14.1) og (1.14.3) er „hinandens reciprokke“.

12. Vis ligningen (1.14.4). [Vink: funktionen $\Pi(x)$ i (1.12) er givet ved

$$\Pi(x) = \sum_{p,m} \frac{1}{m} 1_{[p^m, \infty)}(x),$$

hvor $1_I(x)$ betegner den karakteristiske funktion for intervallet I .]

13. Det er vel klart, at eksponential-integralet $Ei(x)$ er reelt, når x er reel og positiv? Og at $Ei(x) = \lim_{\varepsilon \rightarrow 0} (\int_{-\infty}^{-\varepsilon} + \int_{\varepsilon}^x) e^t t^{-1} dt$.

Opgaver til Kapitel 2.

- U3 1. Vis, at 561 er det mindste Carmichael-tal.
- U3 2. Vis, at et sammensat tal $n > 1$ er et Carmichael-tal, hvis og kun hvis der for alle hele tal a gælder $a^n \equiv a \pmod{n}$.
- U3 3. Vis, at et tal $n > 1$ er et primtal, hvis og kun hvis der for alle a med $1 \leq a < n$ gælder $a^{n-1} \equiv 1 \pmod{n}$.
- H2 4. Bestem alle Carmichael-tal af formen $5p_1p_2$, hvor p_1 og p_2 er primtal.
- U3 5. Vis, at $(\mathbb{Z}/n)^*$ er en 2-gruppe, hvis og kun hvis $n = 2^v p_1 \cdots p_r$, hvor p_1, \dots, p_r er indbyrdes forskellige Fermat-primtal.
- U3 6. Gruppen $(\mathbb{Z}/11^4)^*$ er cyklisk af orden 13.310. Vis, at restklassen af 2 er en frembringer. [Vink: Anvend (2.2)(*) med $1 + kp = 2^{10}$.]
- H2 7. Lad p være et ulige primtal, og lad z være et helt tal således, at $[z]_p$, dvs z 's restklasse modulo p , frembringer gruppen $(\mathbb{Z}/p)^*$. Betragt de p tal, $z_i := z + ip$ for $0 \leq i < p$; de har alle den samme restklasse modulo p , men restklasserne $[z_i]_{p^2}$ er forskellige.
- (i) Vis, at af de p restklasser $[z_i]_{p^2}$ er der $p - 1$, som frembringer den cykliske gruppe $(\mathbb{Z}/p^2)^*$.
- (ii) Vis, at hvis restklassen $[z]_{p^2}$ frembringer gruppen $(\mathbb{Z}/p^2)^*$, så vil restklassen $[z]_{p^v}$ frembringe gruppen $(\mathbb{Z}/p^v)^*$ for alle v .
- [Vink: Ifølge Fermat findes en fremstilling $z^{p-1} = 1 + kp$. Vis, at $[z]_{p^2}$ frembringer $(\mathbb{Z}/p^2)^*$, hvis og kun hvis $p \nmid k$. Bestem den tilsvarende fremstilling for z_i . For at vise (ii) kan man udnytte kongruensen $(1 + kp)^{p^{\mu-1}} \equiv 1 + kp^\mu \pmod{p^{\mu+1}}$, jfr (2.2)(*.)]

Opgaver til Kapitel 3.

- H2 1. Vis, at konstantleddet i Φ_n , for $n > 1$, er lig med 1. Vis, at koefficienterne i Φ_n ikke altid er ± 1 eller 0. [Vink: bestem nogle koefficienter i Φ_{105} .]
- U4 2. Vis for $\zeta \in \mathbb{C}$ og et ulige tal u , at ζ har orden $2u$, hvis og kun hvis $-\zeta$ har orden u . Slut heraf, at $\Phi_{2u}(X) = \Phi_u(-X)$.

- U4 **3.** For et polynomium f af grad k defineres $c(f) := -f_{k-1}$, hvor f_{k-1} er koefficienten til leddet af næsthøjeste grad. Vis, for normerede polynomier f, g , at $c(fg) = c(f) + c(g)$. Vis, at næsthøjestegrads-koefficienten i Φ_n er lig med $-\mu(n)$, hvor $\mu(n)$ er Möbius-funktionen. [Vink: Brug Opgave AT1: 1.]
- U4 **4.** Vis formelen $\Phi_n = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}$, hvor μ er Möbius-funktionen.
- U4 **5.** Det fremgår af Eksempel (3.15), at i $\mathbb{F}_7[X]$ er $f := X^2 + X - 2$ divisor i Φ_{48} . Bestem kvotienten Φ_{48}/f .
- 6.** Angiv, i $\mathbb{F}_7[X]$, primopløsningen af Φ_{48} (eller i hvert fald nogle af primfaktorerne).
- U5 **7.** For hvilke primtal p er Φ_n irreducibel i $\mathbb{F}_p[X]$.
- Slet! **8.** Vis, for $n > 2$, at der er uendelig mange primtal p med $p \not\equiv 1 \pmod{n}$.
- U4 **9.** Vis, når $p \nmid n$, at $\Phi_{np}(X) = \Phi_n(X^p)/\Phi_n(X)$.
- U4 **10.** Vis, når $p \nmid n$, at i $\mathbb{F}_p[X]$ er $\Phi_{np} = \Phi_n^{p-1}$.
- U5 **11.** Vis, at der for $\mathbb{F}_p[X]$ gælder, at brøkdelen af irreducible polynomier blandt alle polynomier af grad n asymptotisk er lig med $1/n$.
- U9 **12.** *Vis „primtalssætningen“ for $\mathbb{F}_p[X]$: Nummerér polynomierne i $\mathbb{F}_p[X]$, således at først kommer konstanterne, dernæst polynomierne af grad 1, dernæst polynomierne af grad 2, osv; polynomierne af samme grad nummereres tilfældigt. Lad $\pi_p(n)$ være antallet af irreducible blandt de første n polynomier. Da gælder asymptotisk: $\pi_p(n) \sim Cn/\log n$, med konstanten $C = \log p$.
- U4 **13.** Vis, at hvis $q^d - 1$ er divisor i $q^s - 1$, så er $d | s$. [Vink: skriv $s = hd + r$, med $r < d$, og regn modulo $q^d - 1$.]

Opgaver til Kapitel 4.

!

- 1.** Bestem for $n = 12$ tallene $W(b)$, som indgår i Sætning (4.15), dvs tallene $W(1)$, $W(5)$, $W(7)$, og $W(11)$. Vis, at der er fire kvadratiske karakterer $\chi: (\mathbb{Z}/12)^* \rightarrow \{\pm 1\}$, og angiv for hver af dem tallet A_χ .
- 2.** Lad $\chi: (\mathbb{Z}/12)^* \rightarrow \{\pm 1\}$ være den kvadratiske karakter bestemt ved Kronecker-symbolet $\left(\frac{a}{12}\right)$. Bestem værdierne $\chi(1)$, $\chi(5)$, $\chi(7)$, og $\chi(11)$, og værdien A_χ .
- 3.** Legemet $L = \mathbb{F}_{49}$ består af elementer $x + iy$, hvor x, y er restklasser modulo 7, og $i^2 = -1$. Vis, at elementet $\zeta := 2i$ i L har orden 12. Bestem i L den tilhørende Gauss-sum $\tau(\chi, \zeta)$, hvor χ er som i opgave (2). Harmonerer det med resultatet fra (2)?
- U5 **4.** Vis påstanden i (4.11) om entydig faktorisering af diskriminanter.
- 5.** Der var lidt at vise sidst i beviset for (4.15): Hvis elementet ξ har orden d i en cyklisk gruppe af orden n , så gennemløber ξ^a , for primiske restklasser a modulo n , samtlige elementer af orden d lige mange gange.

6. Vis, for et ulige primtal p , formlen $\sum_a \left(\frac{a(a+1)}{p}\right) = -1$, hvor summen er over restklasser a primiske med p . [Vink: Med $ab \equiv 1 \pmod{p}$ er $a(a+1) \equiv a^2(1+b)$.]
- U5 7. For hvilke b er $\left(\frac{a}{b}\right)$ den trivielle karakter $(\mathbb{Z}/b)^* \rightarrow \{\pm 1\}$?
- U5 8. Vis, at følgende algoritme bestemmer symbolet $s = \left(\frac{a}{b}\right)$ uden at faktorisere potenser af 2. Initialiser med $\mathbf{a} := a$, $\mathbf{b} := b$, $\mathbf{s} := 1$.
- (0) Hvis $\mathbf{b} \equiv 3 \pmod{4}$, så sæt $\mathbf{b} := -\mathbf{b}$.
- (1) Hvis $\mathbf{b} = 1$, så STOP.
- (2) Bestem den principale rest r af \mathbf{a} ved division med \mathbf{b} , altså $\mathbf{a} = q\mathbf{b} + r$ med $0 \leq r < |\mathbf{b}|$. Hvis $r = 0$, så sæt $\mathbf{s} := 0$ og STOP. Ellers sættes $\mathbf{a} := r$.
- (3) Hvis $\mathbf{a} \equiv 3 \pmod{4}$, så sæt $\mathbf{a} := -\mathbf{a}$. Hvis $\mathbf{a} \equiv 2 \pmod{4}$: Hvis $\mathbf{b} > 0$, så sæt $\mathbf{a} := \mathbf{a} - \mathbf{b}$ og hvis $\mathbf{b} < 0$, så sæt $\mathbf{s} := -\mathbf{s}$ og $\mathbf{a} := -\mathbf{a} - \mathbf{b}$.
- (4) Ombyt og gentag: Sæt $(\mathbf{a}, \mathbf{b}) := (\mathbf{b}, \mathbf{a})$, og GOTO (1).

Opgaver til Kapitel 5.

- H3 1. Bestem for de første primtal $p = 3, 5, 7, \dots, 31$ ordenen af 2 i $(\mathbb{Z}/p)^*$. [Vink: værdien af Legendre-symbolet $\left(\frac{2}{p}\right)$ fortæller ganske meget om ordenen.] Angiv det mindste sammensatte basis-2 pseudoprimtal; — og basis-2 Euler-pseudoprimtal.
- H3 2. Lad p være et ulige primtal. Vis, at $m = M_p := 2^p - 1$ er et basis-2 stærkt pseudoprimtal. Tallet $M_{11} = 2.047$ er faktisk det mindste sammensatte basis-2 stærke pseudoprimtal.
- H3 3. Antag, at $m - 1 = 2^s u$, hvor u er ulige og $\leq 2^s + 1$. Vis, at hvis der findes et tal b således, at $b^{2^{s-1}} \equiv -1 \pmod{m}$, så er m et primtal. [Vink: kongruensen bevares modulo en primdivisor p i m , og den angiver ordenen af restklassen af b .] Vis omvendt, hvis m er et primtal, så er det „let“ at finde et sådant b .

Opgaver til Kapitel 6.

- U7 1. Antag, for et givet $e > 1$, at $x \mapsto x^e$ er bijektiv modulo n . Vis, at n må være kvadrattfri.
- U7 2. Vis, modulo 95, at afbildningen $x \mapsto x^7$ er bijektiv, og angiv den inverse.
- U7 3. Hvorfor står der, i kommentaren til *simpelhed*, at modtageren skal kunne dekode, „hvis det ønskes“?
- H4 4. Min offentlige RSA-nøgle er $(33, 7)$. Restklasserne $0, \dots, 32$ modulo 33 fortolkes som de 29 danske bogstaver efterfulgt af de 4 specialtegn: ‘.’, ‘;’, ‘!’, ‘?’. En student sender mig *h*-teksten ÅPFLØE. Hvad var klarteksten?

Opgaver til Kapitel 7.

- U9 1. Implementer Pollard's algoritme i et program (Pascal eller C eller ...), der som input skal have to (prim)tal p_1, p_2 , som beregner $n = p_1 p_2$, og som output leverer divisoren q i n , samt skridtantallet. Hvorfor stopper det? Hvad sker, når $p_1 = 23, p_2 = 29$?

- U9 2. „Rent Monte Carlo“ er det naturligtvis, for et givet (sammensat, ulige) n , at undersøge, gentagne gange, om et tilfældigt valgt $q < n$ er divisor i n . Giv en vurdering af det skridt-antal, der er nødvendigt for at denne algoritme med sandsynlighed mindst $\frac{1}{2}$ finder en ikke-triviell divisor i n .
3. Lad n (ulige, sammensat) være givet. I stedet for at undersøge, gentagne gange, om det tilfældigt valgte q er divisor i n , kan man spørge, om q har en ikke-triviell divisor fælles med n . Giver det en forbedring af det forventede skridt-antal?

Opgaver til Kapitel 8.

- H4 1. Vis følgende uligheder (den første kun for $n > 1$):

$$2 \leq \tau(n) < 2\sqrt{n}, \quad n \leq \sigma(n) < 2n\sqrt{n},$$

$$n^2/2 < \varphi(n)\sigma(n) \leq n^2, \quad \sqrt{n}/4 < \varphi(n) \leq n.$$

[Vink (til 3. ulighed): $\varphi(n)\sigma(n)$ er multiplikativ, og for en primtalspotens p^ν finder vi umiddelbart, at $\varphi(p^\nu)\sigma(p^\nu) = (p^\nu - p^{\nu-1})(p^{\nu+1} - 1)/(p - 1) = p^{2\nu}(1 - 1/p^{\nu+1})$. For $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ fås altså

$$\varphi(n)\sigma(n) = n^2(1 - 1/p_1^{\nu_1+1}) \cdots (1 - 1/p_r^{\nu_r+1}).$$

Produktet af parenteserne på højresiden er højst 1, og større end eller lig med

$$(1 - 1/p_1^2) \cdots (1 - 1/p_r^2) > \prod_{q=2}^{\infty} (1 - 1/q^2) = \frac{1}{2}.$$

(Den sidste ligning er jo triviell, ikke?) Du kan også vurdere ned ved $\zeta(2)^{-1} = 6/\pi^2$.]

- H4 2. Vis, at udtrykket i formelen (8.9.1) for $\alpha_p(n)$ er positivt for alle n , også når $p > 1$ ikke er et primtal.
- U9 3. Bestem grænseværdien $\lim a_N/N^2$, hvor a_N er antallet af Farey-brøker af orden N . (Farey-brøkerne af orden N er brøkerne i intervallet mellem 0 og 1 med nævner højst N , altså mængden af brøker af formen a/s , hvor $0 \leq a < s \leq N$.)
- U9 4. Vis, at $\sum_{d|n} \mu(d)^2/\varphi(d) = n/\varphi(n)$.
5. Vis *Brauer–Rademacher’s identitet*:

$$\varphi(r) \sum_{d|r, (d,n)=1} \frac{d}{\varphi(d)} \mu\left(\frac{r}{d}\right) = \mu(r) \sum_{d|(n,r)} d \mu\left(\frac{r}{d}\right).$$

6. *Antag, at $\alpha: \mathbb{N} \rightarrow \mathbb{R}$ er multiplikativ og monoton. Vis, at så er α en potensfunktion, $\alpha(n) = n^c$.

Opgaver til Kapitel 9.

1. Vis, at $I(s)$ er holomorf i hele den komplekse plan, og uafhængig af valget af ε .

2. Vis, at $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.
3. Vis, at $\text{Res}_{s=1} \zeta(s) = 1$.
4. Bestem værdierne $\zeta(2)$ og $\zeta(4)$.
5. Vis, at $\zeta(s)$ er reel for alle reelle værdier af $s \neq 1$.

Ekstra opgaver

- U1 1. Vis, at tallene $l! + 2, l! + 3, \dots, l! + l$ en sekvens af $l - 1$ på hinanden følgende tal, der alle er sammensatte. Kan du, med en betingelse på l , sikre dig, at også $l! + 1$ er sammensat?
- U1,8■ 2. Har kongruensen $23x \equiv 17 \pmod{41}$ en løsning? Har kongruensen $x^2 \equiv -8 \pmod{41}$ en løsning?
- U1 3. Hvordan bestemmer man antallet af cifre i Fermat-tallet $F_5 = 2^{2^5} + 1$?
- U1 4. Gauss beviste, at n -kanten er konstruerbar, hvis og kun hvis n er et produkt, $n = 2^v p_1 \cdots p_r$, af en potens af 2 og forskellige Fermat-primtal p_i . Vis, at n -kanten er konstruerbar, hvis og kun hvis $\varphi(n)$ er en potens af 2.
5. For hvert polynomium $f \in \mathbb{Z}[X]$ betegnes med $\mathcal{R}(f)$ det polynomium, der fremkommer, når hver koefficient i f erstattes med sin principale rest modulo 2. Sæt $R_m := \mathcal{R}((1 + X)^m)$ for $m = 1, 2, \dots$. Fx, for $m = 3$, er $(1 + X)^3 = 1 + 3X + 3X^2 + X^3 \equiv 1 + X + X^2 + X^3$, og R_3 er det sidste polynomium. Bestem tallene $R_m(2)$ for $m = 1, \dots, 6$.
 Følgende er et *bemærkelsesværdigt resultat*. Den ulige n -kant er konstruerbar, hvis og kun hvis n er et af tallene i følgen $R_1(2), R_2(2), R_3(2), R_4(2), \dots$.
 Men resultatet er nu heller ikke helt korrekt! Forklar sammenhængen. [Vink: Det er klart, at $(1 + X)^{l+m} = (1 + X)^l (1 + X)^m$, men deraf følger vel ikke, at $R_{l+m} = R_l R_m$!]
6. Stirling's formel udsiger, at $n! \sim \sqrt{2\pi n} n^{n+\frac{1}{2}} e^{-n}$. Lad b_n betegne den største værdi af binomialkoefficienterne $\binom{n}{k}$. Vis ved hjælp af formlen, at der findes en konstant C således, at $b_n \leq C 2^n / \sqrt{n}$. Vis, at for hvert positivt tal c er $b_n \leq 2^{n-c}$ for $n \gg 0$. Vis, at hvis $b_n \leq 2^{n-c}$ for $n = n_0$, så er $b_n \leq 2^{n-c}$ for alle $n \geq n_0$. [Vink til det sidste spørgsmål: Har intet at gøre med det foregående.]
7. Tilføj til tabellen over $\pi(n)$ nogle af differenserne $\pi(n) - n / \log n$, fx for $n = 10^k$ med $k = 6, 7, 8$. Sammenlign med tabellens andre differenser.
- U2 8. Bestem, med $c = 1$ og $C = 1,3$ et naturligt tal N således, at højresiden i (1.10.1) er positiv for $n \geq N$. Gennemfør et bevis for Bertrand's postulat.
- U1 9. Beskriv for en divisor d i n den naturlige homomorfi $(\mathbb{Z}/n)^* \rightarrow (\mathbb{Z}/d)^*$. Vis, at homomorfien er surjektiv, og bestem ordenen af kernen $U(d)$. Betragt $n = 24$ og $d = 8$ og restklassen $b := [3]_8$ i $(\mathbb{Z}/8)^*$. Bestem en primisk restklasse i $(\mathbb{Z}/24)^*$ som ved homomorfien afbildes på b . Angiv restklasserne i $U(8)$ og i $U(6)$ (stadig med $n = 24$).
- U1 10. Vis, for $n > 1$, at hvis kongruensen $x^{2^k} \equiv -1 \pmod{n}$ kan løses, så er 2^{k+1} divisor i $\varphi(n)$. Vis, at der er uendelig mange primtal p med $p \equiv 1$ modulo 4. [Vink: Antag, at p_1, \dots, p_n er givne, og vælg en primdivisor p i $(2p_1 \cdots p_n)^2 + 1$ som p_{n+1} .] Hvad sker modulo 8? – og modulo 16?

- U2 **11.** Vis, at der er uendelig mange primtal p med $p \equiv 3 \pmod{4}$. [Vink: Antag, at p_1, \dots, p_n er givne. Vis, at tallet $4p_1 \cdots p_n - 1$ må have en primdivisor p med $p \equiv 3 \pmod{4}$, og vælg sådan en som p_{n+1} .]
- H1 **12.** Vis, at der er uendelig mange primtal p med $p \equiv 2 \pmod{3}$. Vis for hvert $n > 2$, at der er uendelig mange primtal p med $p \not\equiv 1 \pmod{n}$. (Dirichlet's sætning udsiger, at der i enhver primisk restklasse findes uendelig mange primtal, altså at for hvert givet a med $(a, n) = 1$ er der uendelig mange primtal p med $p \equiv a \pmod{n}$.)
- U1 **13.** Antag, at n ikke er den k 'te potens af et helt tal. Vis, at tallet $\sqrt[k]{n}$ er irrationalt.
- U1 **14.** Antag, at n ikke er en potens af 10. Vis, at 10-talslogaritmen $\log_{10} n$ er irrationalt. Hvad gælder, hvis grundtallet 10 erstattes med et mere generelt helt grundtal g , $g \geq 2$?
- 15.** Antag, at for naturlige tal x, y gælder ligningen $y^2 = 1 + x + x^2 + x^3 + x^4$. Vis, at $(x, y) = (3, 11)$. [Vink: Det er klart, at $x > 1$. Tænk nu på naturlige tal fremstillet i x -tal-sxstemet. Ligningens højreside er så tallet 11111 (med fem cifre). Overvej, at i x -tal-systemet må y være 3-ciffret, og det ledende ciffer (koefficienten til x^2) må være 1. Bestem så de sidste to cifre (og x og y).]
- 16.** Vis for $Q := X^2 - X + 41$, at alle tallene $Q(1), Q(2), \dots, Q(40)$ er primtal. [Vink: det kræver vist gruppearbejde! – eller en henvisning til Mat2AL/Alg2.]
 Vis, at der ikke findes noget ikke-konstant polynomium $P \in \mathbb{Z}[X]$ således, at følgen $P(1), P(2), P(3), \dots$ består af lutter primtal. [Vink: hvis $p := P(1)$, så er $P(np + 1) \equiv P(1) \equiv 0 \pmod{p}$.]
- U4 **17.** Vis, for $n > 1$, at $\sum_{(a,n)=1} a = \frac{1}{2}n\varphi(n)$, hvor summen er over tal a , med $1 \leq a \leq n$ og primiske med n .
- U1 **18.** For hvilke n er $\varphi(n) = 6$? Og for hvilke k er $\varphi(\varphi(k)) = 6$.
- U2 **19.** Vis for $p \geq 2$, at p er et primtal, hvis og kun hvis p går op i $(p - 1)! + 1$ (Wilson's sætning).
- U2 **20.** Vis for $p \geq 2$, at p er et primtal, hvis og kun hvis $p \mid (p - 2)! - 1$. For hvilke p gælder $p \mid 2(p - 3)! + 1$.
- U2 **21.** Vis for $a \geq 3$, at $a - 1$ og $a + 1$ er primtalstvillinger, hvis og kun hvis $a^2 - 1$ går op i $4(a - 2)! + a + 3$.
- U3 **22.** Angiv den fuldstændige løsning til kongruensen $x^2 \equiv 1 \pmod{p^v}$, hvor p er et primtal. [Vink: Antallet af løsninger er 2 når p er ulige, og 4 når $p = 2$ og $v \geq 3$.]
- U3 **23.** (Gauss's generalisering af Wilson's sætning). Lad w være produktet af alle naturlige tal mindre end n og primiske med n . Antag $n > 2$. Vis, at $w \equiv (-1)^{N/2} \pmod{n}$, hvor N er antallet af løsninger modulo n til kongruensen $x^2 \equiv 1 \pmod{n}$. [Vink: $[w]$ er produktet af samtlige elementer i gruppen $(\mathbb{Z}/n)^*$. Faktorerne a og a^{-1} forekommer i produktet, og de spiser hinanden, når de er forskellige, dvs når $a^2 \not\equiv 1$. Tilbage bliver produktet over alle a med $a^2 \equiv 1$. I det sidste produkt forekommer med a også faktoren $-a$, og den er forskellig fra a .]
 *Vis, at $w \equiv -1 \pmod{n}$, når $n = 4$ eller $n = p^v$ eller $n = 2p^v$ (et ulige primtal p), og at $w \equiv 1$ i alle andre tilfælde.

- U3 **24.** Med $\sigma(n)$ betegnes summen af divisorerne i n , altså $\sigma(n) = \sum_{d|n} d$. Bestem $\sigma(p^\nu)$, når p er et primtal. Vis, at når $n = n_1 n_2$, hvor faktorerne n_1, n_2 er primiske, så er $\sigma(n) = \sigma(n_1)\sigma(n_2)$.
- U2 **25.** Et tal n kaldes *fuldkomment*, hvis det er lig med summen af sine ægte divisorer (divisoren 1 medregnet), altså hvis $\sigma(n) = 2n$. Vis Euklid's resultat: Hvis $2^\nu - 1$ er et primtal, så er tallet $n = 2^{\nu-1}(2^\nu - 1)$ fuldkomment.
 *Vis Euler's resultat: ethvert lige, fuldkomment tal n er af Euklid's slags.
- U2 **26.** Vis, at alle tal af formen $n = 6k$ for $k > 1$ er *abundante* tal, dvs opfylder $\sigma(n) > 2n$.
- U3 **27.** Vis, at alle tal af formen $n = 3^\alpha 5^\beta$ ($n > 1$) er *deficiente* tal, dvs opfylder $\sigma(n) < 2n$.
- U3 **28.** Lad $\alpha(n)$ betegne antallet af løsninger til den diofantiske ligning $n = x^2 - y^2$, dvs løsninger med $x, y \in \mathbb{Z}$. Vis, at når n er ulige, så er $\alpha(n) = 2\tau(n)$, hvor $\tau(n)$ er antallet af divisorer i n (som bekendt kan $\tau(n)$ bestemmes ud fra primopløsningen $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ som $\tau(n) = (\nu_1 + 1) \cdots (\nu_r + 1)$). Find en tilsvarende formel for $\alpha(2^\nu u)$, når u er ulige. [Vink: Pas på, der er noget luske omkring $\nu = 1$.]
- U3 **29.** Bestem en frembringer for gruppen $(\mathbb{Z}/17)^*$. Og for gruppen $(\mathbb{Z}/289)^*$.
- U4 **30.** Vis, for enhedsrødderne $\zeta_5 := e^{2\pi i/5}$ og $\zeta_{10} := e^{2\pi i/10}$, at

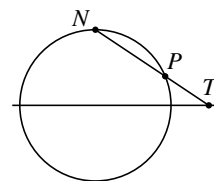
$$\zeta_5 = \frac{\sqrt{5} - 1}{4} + i \frac{\sqrt{10 + 2\sqrt{5}}}{4}, \quad \zeta_{10} = \frac{\sqrt{5} + 1}{4} + i \frac{\sqrt{10 - 2\sqrt{5}}}{4}.$$

[Vink: $\zeta := \zeta_5$ er rod i Φ_5 , så $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$. Efter division med ζ^2 fås $0 = (\zeta + \zeta^{-1})^2 + (\zeta + \zeta^{-1}) - 1$, hvoraf $\zeta + \zeta^{-1} = \frac{-1 \pm \sqrt{5}}{2}$. Tilsvarende er ζ_{10} rod i $\Phi_{10} = X^4 - X^3 + X^2 - X + 1$.]

- U5 **31.** Betragt Jacobi-symbolet $\left(\frac{a}{u}\right)$, hvor u er positiv og ulige, og $(a, u) = 1$. Vis, at hvis kongruensen $x^2 \equiv a \pmod{u}$ kan løses, så er $\left(\frac{a}{u}\right) = 1$. Vis, at det omvendte ikke nødvendigvis gælder.
- U6 **32.** Bestem værdierne af $\left(\frac{3}{D}\right)$ for alle diskriminanter D med $-20 \leq D \leq 20$.
- U5 **33.** Indsæt resten af værdierne i nedenstående tabel over Legendre-symbolet $\chi(a) = \left(\frac{a}{13}\right)$:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\chi(a)$	1			1					1			

- U5 **34.** For et primtal p sættes $S(\mathbb{F}_p) := \{(x, y) \in \mathbb{F}_p^2 \mid x^2 + y^2 = 1\}$; det er „enhedscirklen“ modulo p . Øjensynlig er $|S(\mathbb{F}_2)| = 2$. Vis for $p > 2$, at $|S(\mathbb{F}_p)| = p - (-1)^{(p-1)/2}$. Hvad sker der, når man mere generelt betragter et „keglesnit“ $ax^2 + y^2 = 1$ modulo p , hvor $p \nmid a$?
 [Vink: Punkterne $P = (x, y)$ på den sædvanlige enhedscirkel $S(\mathbb{R})$, fraregnet nordpolen $N = (0, 1)$, parametriseres ved at man lader punktet P svare til skæringspunktet $T = (t, 0)$ mellem linien NP og x -aksen. Beskriv parametriseringen, og overvej, hvordan regningerne forløber, hvis man i stedet regner modulo p .]



U6 35. Lad $v_p(k)$ betegne den eksponent primtallet p forekommer med i primopløsningen af k . Vis, at $v_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \dots$ (det er en endelig sum!). Brug princippet, fx med $p = 2, 3$ og 5 , til at primopløse $100!$.

U6 36. Vis, at et vilkårligt produkt af r på hinanden følgende hele tal altid er deleligt med $r!$.

U8 37. I noterne er det vist, at rækken $\sum \frac{1}{p}$, hvor summen er over primtal p , er divergent. Vis, at divergensen også følger af primtalssætningen $\pi(x) \sim x/\log x$. (*Det kræver lidt mere omhyggelighed at vise, at divergensen alene følger af en vurdering $\pi(x) \geq cx/\log x$.)

Man kan vise, at rækken $\sum \frac{1}{q}$, hvor summen er over primtalstvillinger q (dvs primtal q således, at $q + 2$ eller $q - 2$ også er et primtal), er konvergent. Man formoder, at der for antallet $\pi_2(x)$ af primtalstvillinger mindre end eller lig med x gælder en assymptotisk formel af formen $\pi_2(x) \sim Kx/(\log x)^2$. Vis, at konvergens vil være en følge af formodningen.

H2 38. Bestem for hvert af primtallene $p = 17, 19, 23, 29, 31$ det mindste naturlige tal z således, at $[z]_p$ frembringer gruppen $(\mathbb{Z}/p)^*$.

H2 39. Bestem for hvert af tallene $n = 16, 18, 20, 21, 24, 26, 27, 28, 30$ et element af den maksimale elementorden i $(\mathbb{Z}/n)^*$.

H2 40. Lad $p < q < r$ være ulige primtal. Vis, at tallet $n := pqr$ er et Carmichael-tal, hvis og kun hvis

$$(1) \quad p-1 \mid qr-1, \quad (2) \quad q-1 \mid pr-1, \quad \text{og} \quad (3) \quad r-1 \mid pq-1.$$

Antag, at (3) er opfyldt. Vis, at så er $pq - 1 = d(r - 1)$ med $2 \leq d \leq p - 1$. Vis, at

$$(4) \quad q-1 \mid d(r-1)-p+1,$$

og vis, at hvis også (2) er opfyldt, så er $q - 1$ divisor i $(d + p)(p - 1)$. Slut heraf, at der for et givet primtal p kun er endelig mange Carmichael-tal af formen pqr .

U6 41. Antag om tallet h , at de tre tal $p := 6h + 1, q := 12h + 1$, og $r := 18h + 1$, alle er primtal. Vis, at tallet pqr er et Carmichael-tal.

U6 42. Der er velkendte „pæne“ udtryk for de primitive n 'te enhedsrødder ζ_n for $n = 3, 4$ og 5 . Ud fra et udtryk $\zeta_n = a + ib$ ($b > 0$) får man et udtryk for ζ_{2n} ved at løse andengradsligningen $z^2 = a + ib$; det giver

$$\zeta_{2n} = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} + i\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} = \sqrt{\frac{1+a}{2}} + i\sqrt{\frac{1-a}{2}}.$$

Bestem herved pæne udtryk for $\zeta_6, \zeta_8, \zeta_{10}, \zeta_{12}, \zeta_{16}, \zeta_{20}, \zeta_{24}$. Hvorfor kan man ikke tilsvarende få et udtryk for ζ_9 , og mere generelt for ζ_{3n} , ved at bruge, at $z = \zeta_{3n}$ opfylder $z^3 = a + ib$? – det er jo en simpel trediegradsligning, og Cardano's formel fortæller, hvordan sådan en skal løses.

U6 43. Vis, når p er et primtal og $p \mid m$, at $\Phi_{p^v m}(X) = \Phi_m(X^{p^v})$. Vis, når $p \nmid n$ og $v > 0$, at $\Phi_{p^v n}(X) = \Phi_n(X^{p^v})/\Phi_n(X^{p^{v-1}})$.

- U6 **44.** n 'te enhedrødder kan principielt defineres i en vilkårlig (kommutativ) gruppe G : Det er de elementer $g \in G$, som opfylder, at $g^n = 1$. Lad $\alpha_G(n)$ betegne antallet af n 'te enhedsrødder. Hvordan bestemmer man antallet af elementer af orden n ud fra funktionen α_G ?
- Hvordan bestemmer man $\alpha_G(n)$, når G er cyklisk. Hvordan bestemmes antallet $\alpha_{G \times H}(n)$ for en produktgruppe ud fra α_G og α_H ?
- U8 **45.** Lad K være et endeligt legeme af karakteristisk p . Vis, at elementantallet q i K er en potens $q = p^r$ af p . Vis, at $\alpha^q = \alpha$ for alle $\alpha \in K$.
- 46.** Lad L være et legeme af positiv karakteristisk p . Afbildningen $\sigma(\xi) := \xi^p$ er så en ringhomomorfi $\sigma: L \rightarrow L$, og den inducerer en ringhomomorfi $L[X] \rightarrow L[X]$, hvor billedet σf af et polynomium $f \in L[X]$ fås ved at anvende σ på koefficienterne i f .
- Lad f være et normeret polynomium med koefficienter i \mathbb{F}_p . Vis, at hvis f i L har en rod ξ , så er også ξ^p rod i f .
- Antag, at $f \in \mathbb{F}_p[X]$ er irreducibelt, med roden ξ i L , og at $f \neq X$ (altså at $\xi \neq 0$). Lad r være graden af f og lad n være ordenen af ξ . Da gælder som bekendt, at r er ordenen af restklassen af p modulo n . Vis, at rødderne i f er potenserne ξ^{p^i} for $i = 0, \dots, r-1$.
- U6 **47.** Antag, at $p \equiv 3 \pmod{4}$ er et primtal. Vis, at legemet \mathbb{F}_{p^2} , med p^2 elementer, så kan defineres som kvotienten $\mathbb{F}_p[X]/(X^2+1)$. Idet i betegner restklassen af X , har elementerne α i \mathbb{F}_{p^2} altså fremstillinger $\alpha = a + ib$ med entydigt bestemte koefficienter $a, b \in \mathbb{F}_p$. Regning i \mathbb{F}_{p^2} er bestemt ved $i^2 = -1$.
- Vis, at $\alpha = a + ib$ er rod i polynomiet $(X-a)^2 + b^2 \in \mathbb{F}_p[X]$. Sæt $\bar{\alpha} := a - ib$. Vis, at $\alpha \mapsto \bar{\alpha}$ er en ringhomomorfi $\mathbb{F}_{p^2} \rightarrow \mathbb{F}_{p^2}$. Vis, at $\bar{\alpha} = \alpha^p$ for alle $\alpha \in \mathbb{F}_{p^2}$.
- U6 **48.** Legemet \mathbb{F}_{49} er beskrevet i (3.12): Elementerne har formen $a + ib$, hvor $a, b \in \mathbb{F}_7$ og $i^2 = -1$. For elementet $\xi = 5 + 3i$ er $\xi^2 = 2 + 2i$, og $\xi^4 = i$. Specielt er $\xi^8 = -1$ og ξ har orden 16. Elementet $\zeta = 2\xi = 3 - i$ har så orden 48.
- Bestem de 8 potenser ζ^a for $a = 1, 5, 11, 13, 17, 19, 25, 41$, og de 8 normerede andengradspolynomier i $\mathbb{F}_7[X]$, hvori potenserne er rødder. Hvad kan du sige om disse polynomier i relation til cirkeldelingspolynomiet Φ_{48} .
- U6 **49.** Vis, for et ulige primtal p og $(a, p) = 1$, at a er kvadratisk rest modulo p^v , hvis og kun hvis $\left(\frac{a}{p}\right) = 1$.
- H3 **50.** Vis, at der er uendelig mange primtal p med $p \equiv 3 \pmod{8}$.
- [Vink: Kig, for givne ulige p_1, \dots, p_n på en primdivisor p i $u^2 + 2$, hvor $u := p_1 \cdots p_n$. Vis, at -2 er et kvadrat modulo p , og slut at modulo 8 er $p \equiv 1$ eller $p \equiv 3$. Det sidste må indtræffe for mindst ét p (ja, hvorfor?); vælg sådan et p som p_{n+1} .]
- Vis tilsvarende, at der er uendelig mange primtal p med $p \equiv 7 \pmod{8}$. Hvad med $p \equiv 5 \pmod{8}$? [Vink: Kig på primdivisorer i $(2u)^2 + 1$, hvor u er ulige.] Hvad med $p \equiv 1 \pmod{6}$? [Vink: Kig på $(2u)^2 + 3$.] Og hvad med $p \equiv a \pmod{12}$, for $a = 5, 7, 11$?
- U7 **51.** Hvad betyder „kubisk karakter“? For hvilke primtal p kunne det være af interesse at studere kubiske karakterer modulo p ?
- U7 **52.** Lad D være en diskriminant. Vis, at hvis D er en „kvadratfri“ diskriminant, altså et produkt af parvis primiske primdiskriminanter, så bestemmer Kronecker-symbolet $\left(\frac{a}{D}\right)$ en primitiv

karakter $\chi_D: (\mathbb{Z}/D)^* \rightarrow \{\pm 1\}$. Vis omvendt, at hvis Kronecker-symbolet bestemmer en primitiv karakter, så er D „kvadratifri“.

U7 **53.** Lad p være et ulige primtal. Vis, at for alle $v \geq 1$ er der præcis én ikke-triviel kvadratisk karakter $(\mathbb{Z}/p^v)^* \rightarrow \{\pm 1\}$. Er det karakteren bestemt ved Jacobi-symbolet $(\frac{a}{p^v})$?

54. Vis, modulo et primtal $p > 3$, at summen af de kvadratiske rester er kongruent med 0.

55. *Vis, at for hver primdivisor p i Fermattallet $F_m = 2^{2^m} + 1$ er $p \equiv 1 \pmod{2^{m+2}}$. [Vink: kig på ordenen af 2 modulo p ; det giver i hvert fald umiddelbart $p \equiv 1 \pmod{2^{m+1}}$.]

U7 **56.** Vis, at Fermat-tallet $F_m = 2^{2^m} + 1$ ($m \geq 1$) er et primtal, hvis og kun hvis F_m er divisor i $3^{(F_m-1)/2} + 1$. [Vink. Klart at $F_m \equiv 2 \pmod{3}$. „kun hvis“: Brug Reciprocitetssætningen og „Euler“. „hvis“: Bestem, for $p | F_m$, ordenen af 3 modulo p .]

57. Antag, at $n = n_1 n_2$ er produktet af to primiske faktorer n_1, n_2 . Antag, for $j = 1, 2$, at ζ_j er en n_j 'te enhedsrod og at χ_j er en karakter modulo n_j . Vis, at $\zeta := \zeta_1 \zeta_2$ er en n 'te enhedsrod. Under hvilke omstændigheder bliver ζ en primitiv n 'te enhedsrod? Vis, at enhver n 'te enhedsrod kan skrives på denne form, $\zeta = \zeta_1 \zeta_2$, med passende ζ_j . Vis, at $\chi := \chi_1 \chi_2$, defineret ved $\chi(a) = \chi_1(a) \chi_2(a)$ når $(a, n) = 1$, er en karakter modulo n . Vis for Gauss-summerne, at $\tau(\chi, \zeta) = \tau(\chi_1, \zeta_1) \tau(\chi_2, \zeta_2)$.

U7 **58.** Lad χ være en karakter modulo n , og lad ζ være en n 'te enhedsrod. Vis, når $(b, n) = 1$, at $\chi(b) \tau(\chi, \zeta^b) = \tau(\chi, \zeta)$.

U9 **59.** Betragt Gauss-summen $\tau = \tau(\chi, \zeta)$, hvor $\chi: (\mathbb{Z}/n)^* \rightarrow L^*$ er en karakter og $\zeta \in L$ er en k 'te enhedsrod (hvor $k | n$). Vis, at hvis χ induceres af en karakter $\widehat{\chi}: (\mathbb{Z}/k)^* \rightarrow L^*$, så er $\tau(\chi, \zeta) = (\varphi(n)/\varphi(k)) \tau(\widehat{\chi}, \zeta)$. Vis, at hvis χ ikke er induceret af en karakter modulo k , så er $\tau = 0$.

60. Antag, at $\zeta \in L^*$ er en primitiv n 'te enhedsrod og at $\chi: (\mathbb{Z}/n)^* \rightarrow L^*$ er en primitiv karakter. Sæt $\chi^*(a) = \chi(a)^{-1}$ når $(a, n) = 1$, og giv $\chi(a)$ og $\chi^*(a)$ værdien 0, når a ikke er primisk med n . Specielt er så $\varphi(n) = \sum_{c \pmod n} \chi(c) \chi^*(c)$. Desuden er $\chi^*(a) \tau(\chi, \zeta) = \tau(\chi, \zeta^a)$ for alle a . Betragt Gauss-summerne $\tau = \tau(\chi, \zeta)$ og $\tau^* = \tau(\chi^*, \zeta^{-1})$. Gennemgå de enkelte skridt i følgende udregning (hvor summerne er over alle restklasser modulo n):

$$\begin{aligned} \varphi(n) \tau \tau^* &= \sum_c \chi^*(c) \tau(\chi, \zeta) \chi(c) \tau(\chi^*, \zeta^{-1}) = \sum_c \tau(\chi, \zeta^c) \tau(\chi^*, \zeta^{-c}) \\ &= \sum_{a,b,c} \chi(a) \chi^*(b) \zeta^{ac-bc} = \sum_{a,b} \chi(a) \chi^*(b) \sum_c \zeta^{ac-bc} = \sum_a \chi(a) \chi^*(a) n = \varphi(n) n. \end{aligned}$$

Ved division med $\varphi(n)$ fås $\tau \tau^* = n$. Der er en karakteristisk lille fejl i argumentet. Hvilken?

61. *Antag, at $\zeta \in L^*$ har orden n og at karakteren $\chi: (\mathbb{Z}/n)^* \rightarrow L^*$ induceres af en primitiv karakter modulo f , hvor $f | n$. Vis, at hvis n/f er kvadratifri og $(f, n/f) = 1$, så er $\tau \tau^* = f$. I alle andre tilfælde er $\tau = 0$. [Vink: reducer til tilfældet, hvor f er en primtalspotens.]

62. *Lad $\xi: (\mathbb{Z}/n)^* \rightarrow L^*$ være en karakter modulo n . Vis, at der findes en divisor $f | n$ med følgende egenskab: ξ induceres af en karakter modulo f , og enhver anden divisor $d | n$ således, at ξ induceres af en karakter modulo d , er et multiplum af f . Tallet f kaldes *føreren* for ξ .

23. januar 2006

- 63.** Bestem de komplekse Gauss-summer $\tau(\chi, \zeta_n)$ (hvor $\zeta_n = e^{2\pi i/n}$), når (1) $n = 4$, $\chi = \chi_{-4}$, og (2) $n = 8$, $\chi = \chi_8$, og når (3) $n = 8$, $\chi = \chi_{-8}$.
- 64.** Betragt for et ulige primtal p den komplekse Gauss-sum $\tau_p = \tau(\chi_p, \zeta_p)$, hvor χ_p er Legendre-karakteren og $\zeta_p = e^{2\pi i/p}$. Bestem τ_p for $p = 3, 5, 7$. [Vink: Ifølge resultatet i noterne er det nok at bestemme fortegnet, men for $p = 3$ og $p = 5$ kan du da beregne Gauss-summen direkte.]
- 65.** Betragt legemet $L = \mathbb{F}_{11}$ med 11 elementer. Vis, at restklassen af 2 er en frembringer for gruppen \mathbb{F}_{11}^* . Restklassen $\zeta := [4]$ er derfor en primitiv 5'te enhedsrod i \mathbb{F}_{11} . Lad χ_5 være Legendre-karakteren modulo 5. Bestem, i \mathbb{F}_{11} , Gauss-summen $\tau(\chi_5, \zeta)$. Check lige, at $\tau^2 = 5$.
- 66.** Betragt et element $\xi \neq 0$ i legemet $L = \mathbb{F}_{29}$. Vis, at hvis $\xi^4 \neq 1$, så har ξ^4 orden 7. Vis, at $\zeta := [16]$ har orden 7 i L^* . Bestem, i \mathbb{F}_{29} , Gauss-summen $\tau(\chi_7, \zeta)$. Check lige, at $\tau^2 = -7$.
- 67.** Vis, at der bestemmes en karakter $\chi: (\mathbb{Z}/5)^* \rightarrow \mathbb{C}^*$ ved $\chi(1) = 1$, $\chi(2) = i$, $\chi(3) = -i$, $\chi(4) = -1$. [Vink: $(\mathbb{Z}/5)^*$ er cyklisk, frembragt af restklassen af 2.] Bestem Gauss-summen $\tau = \tau(\chi, \zeta_5)$. Check lige, at $|\tau| = \sqrt{5}$.
- U8 **68.** Lad der være givet et legeme L . Ved en karakter på G , hvor G er en endelig abelsk gruppe, forstås en homomorfi $\chi: G \rightarrow L^*$. Vis, at karaktererne på G udgør en kommutativ gruppe. Vis, at hver værdi $\chi(g)$, for $g \in G$, er en enhedsrod i L .
- 69.** *Lad G være en endelig gruppe og lad l være den maksimale elementorden i G . Antag, at legemet L indeholder en primitiv l 'te enhedsrod. Vis, at gruppen af alle karakterer $\chi: G \rightarrow L^*$ er isomorf med G . (Isomorfien er ikke kanonisk.) [Vink: Vis først påstanden for en cyklisk gruppe; brug struktursætningen i det almindelige tilfælde.]
- 70.** Er karaktererne χ_{12} og χ_{-12} , svarende til Kronecker-symbolerne $\left(\frac{a}{12}\right)$ og $\left(\frac{a}{-12}\right)$, primitive karakterer modulo 12? Vis, at der er 4 karakterer modulo 12. Hvorfor kan de naturligt betegnes $\chi_1, \chi_3, \chi_{-4}$ og χ_{12} ?
- 71.** Vis, at restklassen $\zeta := [2]_{13}$ har orden 12 i \mathbb{F}_{13}^* . Bestem med denne enhedsrod Gauss-summerne i \mathbb{F}_{13} svarende til de 4 karakterer ($\chi_1, \chi_3, \chi_{-4}$ og χ_{12}) modulo 12.
- 72.** Bestem for $n = 5$ de komplekse Gauss-summer $\tau(\chi_5, \zeta_5)$ og $\tau(\chi_1, \zeta_5)$, hvor $\chi_5(a) = \left(\frac{a}{5}\right)$ og χ_1 er den trivielle karakter modulo 5. Lad x_1 og x_2 betegne realdelene af ζ_5 og ζ_5^2 . Udtryk Gauss-summerne ved x_1 og x_2 , og brug resultatet til at bestemme x_1 (og dermed ζ_5).
Besvar de samme spørgsmål for $n = 12$.
- H3 **73.** Legemet \mathbb{F}_{49} er beskrevet i (3.12): Elementerne har formen $a + ib$, hvor $a, b \in \mathbb{F}_7$ og $i^2 = -1$. Vis, at $\zeta := 2i$ er en primitiv 12'te enhedsrod i \mathbb{F}_{49} . Bestem Gauss-summen $\tau = \tau(\chi_{12}, \zeta)$ (hvor $\chi_{12}(a)$ er Kronecker-symbolet $\left(\frac{a}{12}\right)$), og dens kvadrat τ^2 .
- H3 **74.** Legemet \mathbb{F}_{16} er beskrevet i (3.11): Elementerne har formen $a + b\xi + c\xi^2 + d\xi^3$, hvor $a, b, c, d \in \mathbb{F}_2$ og $\xi^4 = 1 + \xi$. Vis, at $\zeta := \xi^3$ er en primitiv 5'te enhedsrod. Bestem Gauss-summen $\tau = \tau(\chi_5, \zeta)$ (hvor $\chi_5(a)$ er Legendre-symbolet $\left(\frac{a}{5}\right)$), og dens kvadrat τ^2 .
- U8 **75.** For hvilke b er tallet 15 et psp_b -tal? Og for hvilke b er tallet 21 et psp_b -tal? Generaliser til tal af formen $3p$, hvor p er et primtal.

- U8 **76.** Antag, at p og $q := 2p - 1$ er primtal, og sæt $m = pq$. Vis, at m er et psp_b -tal, hvis og kun hvis b er primisk med m og en kvadratisk rest modulo q . For hvor stor en del af b 'erne (modulo m) sker det?
- U9 **77.** Antag, at m er ulige og sammensat, at p er en primdivisor i m , og at $(b, m) = 1$.
- (1) Vis, at hvis m er et psp_b -tal, så er $b^{m/p-1} \equiv 1 \pmod{p}$.
 - (2) Vis, at hvis $m = 3p$ (hvor $p > 3$), så er m ikke et psp_b -tal for $b = 2, 5, 7$.
 - (3) Vis, at hvis $m = 5p$ (hvor $p > 5$), så er m ikke et psp_b -tal for $b = 2, 3, 7$.
 - (4) Bestem det mindste sammensatte psp_3 -tal.
- 78.** Betragt antallet af løsninger til den diofantiske ligning $x^2 + y^2 = k$ (dvs løsninger med $x, y \in \mathbb{Z}$). Det er velkendt, at antallet kan bestemmes ud fra primopløsningen af k . Mere præcist: Antag, at $k = 2^l q_1^{n_1} \cdots q_r^{n_r} p_1^{m_1} \cdots p_s^{m_s}$, hvor $q_i \equiv 3 \pmod{4}$ og $p_j \equiv 1 \pmod{4}$. Da er antallet af løsninger lig med $4V(k)$, hvor $V(k) = (m_1 + 1) \cdots (m_s + 1)$ hvis alle eksponenterne n_1, \dots, n_r er lige, og $V(k) = 0$ ellers. Vis, at $V(k) = \sum_{d|k} \chi(d)$, hvor $\chi(d) = 0$ hvis d er lige, og $\chi(d) = (-1)^{(d-1)/2}$ hvis d er ulige. [Vink: χ er multiplikativ.]
- 79.** Vis, at $\sum_{k \leq n} V(k) = \sum_{d \leq n} \chi(d) \lfloor n/d \rfloor$. Vis, at $4 \sum_{k \leq n} V(k) + 1$ er lig med antallet af gitterpunkter i cirkelskiven bestemt ved $x^2 + y^2 \leq n$. Udled, at $\sum_{d \leq n} \chi(d) \lfloor n/d \rfloor \sim \frac{\pi}{4}n$. Vis herved formelen $1 - \frac{1}{3} + \frac{1}{5} - \cdots = \frac{\pi}{4}$.
- H4 **80.** Lad $p > 2$ være et primtal. Vis, at hvis $[a]_p$ frembringer $(\mathbb{Z}/p)^*$, så er $\left(\frac{a}{p}\right) = -1$. Vis, at hvis p er et Fermat-primtal, så gælder også det omvendte. Vis, at hvis p ikke er et Fermat-primtal, så findes et tal a således, at $\left(\frac{a}{p}\right) = -1$ og $[a]_p$ er ikke en frembringer for $(\mathbb{Z}/p)^*$.
- 81.** Vis, at restklassen $g := [2]_{19}$ er en frembringer for $(\mathbb{Z}/19)^*$. Bestem x således, at $[3]_{19} = g^x$.
- U9 **82.** Antag, at $n = pq$ er produkt af to primiske pseudoprimtal p, q . Lad l betegne det mindste fælles multiplum af $p - 1$ og $q - 1$. Vis, at $x \mapsto x^e$ er en bijektiv afbildning $\mathbb{Z}/n \rightarrow \mathbb{Z}/n$, hvis og kun hvis $(e, l) = 1$.
- U8,H4 **83.** Lad \mathcal{E}_n betegne gruppen af de permutationer af \mathbb{Z}/n , der er af formen $x \mapsto x^e$. Antag, at $n = 17 \cdot 19$. Bestem gruppen \mathcal{E}_n . Vis, at den maksimale orden af en permutation i \mathcal{E}_n er 12. Hvilken orden har permutationen $x \mapsto x^5$.
- U8 **84.** Af hvilke grunde er RSA baseret på $n = 31 \cdot 61$ en dårlig ide? Og hvad med $n = 257 \cdot 163$?
- U8 **85.** I (4.14) står der, for en karakter $\chi: (\mathbb{Z}/n)^* \rightarrow L^*$ og en divisor d i n : „Det er let at se, at χ induceres af en karakter modulo d , hvis og kun hvis $\chi(a) = 1$ for alle restklasser $a \in U(d)$ “. (Her består $U(d)$ af de primiske restklasser $[a]_n$, hvor $a \equiv 1 \pmod{d}$.) Hvilken sætning i noterne til Mat2AL/Alg2 giver umiddelbart dette resultat?
- U8 **86.** Herunder er en tabel over logaritmen med grundtal 2 for $\mathbb{Z}/19$. Hvad betyder det?
- | | | | | | | | | | | | | | | | | | |
|---|---|----|---|----|----|---|---|---|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 0 | 1 | 13 | 2 | 16 | 14 | 6 | 3 | 8 | 17 | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 |
- Brug tabellen til at markere, i øverste række, frembringerne for $(\mathbb{Z}/19)^*$, og de kvadratiske rester i $(\mathbb{Z}/19)^*$. Brug tabellen til at bestemme de inverse til restklasserne af 4 og af 6. Løs kongruensen $6(4x + 3)^5 \equiv 8 \pmod{19}$.

87. Er det diskrete logaritme-problem (se (6.24)) trivielt, hvis gruppen E er gruppen C_n af n 'te enhedsrødder i \mathbb{C} ?

H4 88. Lad $p > 2$ være et primtal. Vis, at hvis $[a]_p$ frembringer $(\mathbb{Z}/p)^*$, så er $\left(\frac{a}{p}\right) = -1$. Vis, at hvis p er et Fermat-primtal, så gælder også det omvendte. Vis, at hvis p ikke er et Fermat-primtal, så findes et tal a således, at $\left(\frac{a}{p}\right) = -1$ og $[a]_p$ ikke frembringer $(\mathbb{Z}/p)^*$.

H4 89. Tabellen herunder er uddrag af en tabel med søjler svarende til tallene $n = 2, 3, 4, \dots, 22$. Under n i første række står i anden række primopløsningen af $M_n = 2^n - 1$, og i tredje række de primtal p , for hvilke restklassen $[2]_p$ har orden n i $(\mathbb{Z}/p)^*$. Forklar, hvordan man kan få tredje række ud fra tabellens anden række.

Kompleter tabellen, så den indeholder resultaterne for alle $n = 2, 3, 4, \dots, 21$. Du må gerne overspringe de n , for hvilke M_n er et Mersenne-primtal. Det er nok, at du anfører tabellens tredje række.

2	3	4	5	6	11	21
3	7	3·5	31	3 ² ·7	23·89	
3	7	5	31		23, 89	337

[Vink: Du behøver i hvert fald ikke at beregne potenser af 2 større end 2^{10} . Ultimativt kan du faktorisere $2^n - 1$ ved at bruge, at $2^n - 1 = \prod_{d|n} \Phi_d(2)$, men du kan såmænd nøjes med at bruge, at hvis $n = qd$ er sammensat, så er $2^d - 1$ divisor i $2^{qd} - 1$; ja, faktisk kan du nøjes med at udnytte, at $2^{2d} - 1 = (2^d - 1)(2^d + 1)$.]

Bestem det mindste primtal p , for hvilket der gælder, at $\left(\frac{2}{p}\right) = -1$ og $[2]_p$'s orden er mindre end $p - 1$.