Prinsippet om matematisk induksjon: anta du har en påstand som er avhengig av et positivt heltall n. Om du kan vise to ting, nemlig at påstanden er sann for $n = 1$ og at om påstanden er sann for $n = k$, så er den også sann for $n = k+1$, så er den sann for alle positive heltall n.

Dette brukte vi f.eks. til å bevise binomialteoremet

$$(a+b)^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) a^i b^{n-i}$$

Euklids algoritme

Teorem 1 *La a og b være positive heltall. Divider gjentatte ganger, inntil en rest blir null:*

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
&\vdots \\
r_{k-2} &= q_k r_{k-1} + r_k \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Da er $r_n = gcd(a, b)$.

Baklengs gjennom Euklids algoritme for å uttrykke $gcd(a, b)$ som en kombinasjon av a og b, vi fjerner en rest for hver likning. Men først:

$$r_n = r_{n-2} - q_n r_{n-1}$$

Eliminer r_{n-1} fra nest siste likning:

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$$

Sett inn i den første:

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2})$$

Eliminer r_{n-2} fra tredje siste likning, osv. Til slutt står det

$$r_n = noe.b + noe.r_1 = noe.b + noe(a - qb)$$

så den første likningen brukes til å eliminere r_1. Til slutt finner vi altså

$$d = gcd(a, b) = ax + by$$

for passe heltall x og y.

Likningen $ax + by = c$, der a, b, c er heltall, kalles en *lineær diofantisk likning.* Vi er interessert i heltallsløsninger. Da har vi dette resultatet:

Teorem 2 *$ax + by = c$ har en løsning hvis og bare hvis $d = gcd(a, b)$ deler c. Hvis $x = x_0, y = y_0$ er en løsning, er alle løsninger gitt ved*

$$x = x_0 + \frac{b}{d}t,\ y = y_0 - \frac{a}{d}t$$

der parameteren t gjennomløper alle hele tall.

For å finne den første løsningen x_0, y_0, utfør Euklids algoritme for a og b, gå baklengs gjennom den for å uttrykke d som en kombinasjon av a og b, og gang med c/d.

Teorem 3 (Aritmetikkens fundamentalteorem) *Ethvert positivt heltall kan skrives entydig som et produkt av primtall.*

Husk at et *primtall* er et heltall > 1 som bare kan deles på seg selv og på 1.

Teorem 4 *Det finnes uendelig mange forskjellige primtall.*

Teorem 5 (Dirichlet) *Anta a og b er positive heltall med $gcd(a, b) = 1$. Da inneholder følgen*

$$a, a + b, a + 2b, a + 3b, a + 4b, \cdots$$

uendelig mange primtall.

Vi har vist dette for $b = 4, a = 3$.

Delingsegenskaper kan vi også uttrykke ved hjelp av kongruenstegnet.

$$a \equiv b\,(mod\,n) \text{ betyr } n|(a-b)$$

altså at n deler differansen mellom a og b. Dette tegnet (kongruens modulo n) likner på et likhetstegn, dette er ikke tilfeldig. Se på noen egenskaper:

- $a \equiv b(mod\,n) \Leftrightarrow b \equiv a(mod\,n)$
- $a \equiv b(mod\,n) \Rightarrow ka \equiv kb(mod\,n)$
- $a \equiv b(mod\,n)$ og $a' \equiv b'(mod\,n)$ gir $a + a' \equiv b + b'(mod\,n)$.
- $a \equiv b(mod\,n)$ og $a' \equiv b'(mod\,n)$ gir $aa' \equiv bb'(mod\,n)$.

NB: Vanskelig å dele, $ab \equiv ac\,(mod\,n)$ gir bare $b \equiv c\,(mod\,\frac{n}{d})$, der $d = gcd(a,n)$.

En kongruenslikning $ax \equiv b\,(mod\,n)$ har løsning hvis og bare hvis $d = gcd(a,n)|b$, se Teorem 2. Om det finnes en løsning, vil det finnes d inkongruente løsninger $(mod\,n)$. Det kan også formuleres som at det finnes en entydig løsning $(mod\,\frac{n}{d})$.

Eksempel: $3x \equiv 6(mod\,9)$ har løsningene $x \equiv 2,5,8\,(mod\,9)$ (eller $x \equiv 2\,(mod\,3)$ eller $x = 2 + 3t$, det parameteren t gjennomløper alle hele tall).

Hvis $gcd(a,n) = 1$ finnes det bare *en* løsning.

For å finne en løsning bruker vi Euklids algoritme, og den igjen baklengs, til å uttrykke d ved hjelp av a og n, gang med b/d, og vi har funnet den første, x_0. Alle er gitt ved $x \equiv x_0 + \frac{n}{d}t\,(mod\,n)$, der $t = 0,1,2,\cdots,n-1$.

I dette kurset har vi to forskjellige (kongruens)likningssystemer som kan løses ved reduksjon til løsning av lineære kongruenslikninger i en variabel. Først: det kinesiske restklasseteoremet. Se på

$$\begin{aligned} x &\equiv a_1 \,(mod\, n_1) \\ x &\equiv a_2 \,(mod\, n_2) \\ &\vdots \\ x &\equiv a_r \,(mod\, n_r) \end{aligned}$$

Anta $gcd(n_i, n_j) = 1$ for alle par $i \neq j$. La $N_i = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_r$ (produktet av alle n-ene bortsett fra den i-te). Da kan likningene $N_i x \equiv 1 \,(mod\, n_i)$ løses entydig modulo n_i; kall løsningen x_i. Da er

$$x \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_R \,(mod\, N)$$

løsning på det opprinnelige systemet ($N = n_1 n_2 \cdots n_r$). Merk at vi her trenger å bruke Euklid r ganger, fram og tilbake, for å løse de r hjelpelikningene.

Det andre likningstypen vi har med er

$$ax + by \equiv r \,(mod\, n)$$
$$cx + dy \equiv s \,(mod\, n)$$

Den har entydig løsning, modulo n, hvis og bare hvis

$$gcd(ad - bc, n) = 1$$

I så fall kan vi finne løsningen først ved å gange den øverste likningen med c, den andre med a, og så ta differansen. Det gir en likning med bare y som vi kan løse. Deretter ganger vi den første med d, den andre med b, tar differansen, og står igjen med en løsbar likning bare med x. Her må vi bruke Euklids algoritme, men det viser seg at vi bare trenger å gjøre det en gang, for i begge tilfellene blir koeffisienten foran den ukjente $ad - bc$.

Fermats teorem: La p være et primtall, a et heltall slik at p ikke deler a. Da er $a^{p-1} \equiv 1\,(mod\, p)$.

Eulers ϕ-funksjon: La $n \geq 1$ være et heltall. Da er $\phi(n)$ definert som antallet heltall a med $1 \leq a \leq n$ og $gcd(a, n) = 1$.

Eulers teorem. La $n \geq 1$ og a et heltall slik at $gcd(a, n) = 1$. Da er $a^{\phi(n)} \equiv 1\, mod\, n$.

Wilsons teorem. La p være et primtall. Da er

$$(p-1)! \equiv -1\,(mod\, p).$$

Ordenen til et heltall a modulo et heltall $n \geq 1$ er definert når $gcd(a, n) = 1$. Se på mengden av alle tall $k \geq 1$ som er slik at $a^k \equiv 1\,(mod\, n)$. Det finnes slike tall, for ved Eulers teorem er $a^{\phi(n)} \equiv 1\,(mod\, n)$. Ordenen til a er det minste tallet ≥ 1 med denne egenskapen.

Om ordenen er k, vil $a^i \equiv a^j\,(mod\, n)$ hvis og bare hvis $i \equiv j\,(mod\, k)$. Om ordenen k er $\phi(n)$ (den kan aldri være større) sier vi at a er en primitiv rot modulo n. Da er alle tall b med $gcd(b, n) = 1$ kongruente til en potens av a, og vi kan uttrykke multiplikasjon modulo n ved addisjon modulo $\phi(n)$ (i eksponenten til a^i).

Noen moduler har primitive røtter, andre ikke. Men vi vet at alle *primtall* har primitive røtter, og det er alltid $\phi(p-1)$ av dem.

RSA-kryprografi: den som ønsker å motta hemmelige meldinger velger to primtall p og q, og danner $n = pq$. Nå er $\phi(n) = (p-1)(q-1)$. Velg i tillegg d slik at $gcd(\phi(n), d) = 1$ (og $1 \leq d < \phi(n)$). Da finnes det et entydig tall e med $1 \leq e \leq \phi(n)$ og $de \equiv 1\,(mod\,\phi(n))$. Tallene $\{n, e\}$ kalles den offentlige krypteringsnøkkel, og offentliggjøres. Paret $\{n, d\}$ kalles den hemmelige dekypteringsnøkkel, og hemmeligholdes. Den som sender meldingen uttrykt ved tallet M, der $0 \leq M \leq n-1$ beregner $N \equiv M^e\,(mod\,n)$ (minste positive rest), og sender det til den som skal motta melding. Denne beregner $N^d\,(mod\,n)$ (minste positive rest), og dette er den opprinnelige meldingen M. Dette er fordi $a^{\phi(n)+1} \equiv a\,(mod\,n)$ holder for kvadratfrie tall n.

For den som kjenner $\phi(n)$ og enten e eller d, kan den andre av disse beregnes ved hjelp av Euklids algoritme, og denne baklengs.

Heltallslikninger av høyere grad, eksemplet er $x^n + y^n = z^n$. For $n = 2$ har vi

Teorem Anta $x^2 + y^2 = z^2$ for positive heltall x, y, z slik at $gcd(x, y, z) = 1$ og $2|x$. Da finnes heltall $s > t > 0$, $gcd(s, t) = 1$, $s \not\equiv t\,(mod\,2)$ slik at

$$x = 2st,\ y = s^2 - t^2,\ z = s^2 + t^2$$

Omvendt bestemmer alle slike par s, t en løsning av problemet.

Teorem Det finnes ingen positive heltallsløsninger for $x^n + y^n = z^n$ for $n \geq 3$.

Det siste er Wiles-Fermat-teoremet. Vi har bevist det for $n = 4$.

Noen generelle råd om eksamen og eksamenslesing.

- Lær definisjoner! Det er viktig å kunne definere de begrepene vi har med i kurset, og dette gir gratispoeng til eksamen. Husk betingelsene for at ting skal være definert (eksempel: Eulers ϕ-funksjon er definert for heltall $n \geq 1$).

- Lær utsagnene i teoremene! Husk betingelsene, og forstå hva de forskjellige ordene som inngår betyr. Det er alltid spørsmål etter utsagnet i noen av de sentrale resultatene på eksamen, så det er billige poeng for de som kan definisjonene og teoremene.

- Behersk metodene for utregninger! Mange av resultatene i boken gir oss metoder for å regne ut svaret på forskjellige problemer. F.eks. forklarer det kinesiske restklasseteoremet hvordan vi kan løse samtidige konguenslikninger ved hjelp av Euklids algoritme.

- Lær beviser! De sentrale teoremene i boken skal kunne bevises på eksamen. Men husk allikevel at det å kunne gjengi en enkel definisjon ofte kan gi like mye uttelling som å kunne gjennomføre et komplisert bevis.