Mårten Wadenbäck

Repetition

Induktionsprincipen lyder:

> Antag att $P(n)$ är ett predikat med universum $\mathbb{N}$.
>
> Om i) $P(0)$ är sann (basfallet), och
>
> ii) $P(n) \Rightarrow P(n+1)$ (induktionssteget)
>
> så är $P(n)$ sann för alla n.

I andra induktionsprincipen byter vi ut ii) mot

ii') $P(0) \wedge P(1) \wedge \ldots \wedge P(n) \Rightarrow P(n+1)$.

I bland behövs flera basfall samtidigt, och det gör bra att börja på ett annat heltal än noll.

Induktionsprincipen används i induktionsbevis.

Välordningsprincipen är ekvivalent med induktionsprincipen, och lyder

> Varje icketom delmängd av $\mathbb{N}$ har ett minsta element.

En talföljd $f(1), f(2), \ldots$ är *rekursivt definierad* om

i) $f(1), \ldots, f(a)$ är givna (begynnelsevärden), och

ii) $f(n)$ är uttryckt som en funktion av $f(1), \ldots, f(n-1)$ (rekursionsekvationen).

Exempel: Fibonaccitalen definieras rekursivt av

$$\begin{cases} F(0)=0 \\ F(1)=1 \\ F(n)=F(n-1)+F(n-2) \quad \text{om} \quad n \geq 2, \end{cases}$$

och vi kan med induktion visa att $\sum_{j=1}^{n} F(2j-1) = F(2n)$.

Rekursion är ett mycket allmänt begrepp och kan gälla talföljder, geometriska figurer, funktioner, ...

Ett heltal b *delar* heltalet a om det finns ett heltal m så att $a=bm$. Detta skrivs $b \mid a$, och om b inte delar a skriver vi $b \nmid a$.

Sats: Delbarhet uppfyller

i) $a \mid 0 \quad \forall a \in \mathbb{Z}$

ii) reflexivitet

iii) transitivitet

iv) $a|b \wedge a|c \iff \forall m,n : a|mb+nc$

v) $a|b \Rightarrow a \leq b$ om $a,b \in \mathbb{Z}_+$

Sats (Divisionsalgoritmen): Om $a,b \in \mathbb{Z}_+$ så finns entydiga heltal q (kvoten) och r (resten) så att

$$a = qb + r \quad \text{och} \quad 0 \leq r < b.$$

Resten blir noll precis då $b|a$.

Om $c|a$ och $c|b$ är c en gemensam delare till a och b, och det största talet bland de gemensamma delarna kallas största gemensamma delaren, $sgd(a,b)$.

Sats: Det gäller att

i) $\forall a \in \mathbb{N}: sgd(a,0) = a$

ii) $\forall a,b,n \in \mathbb{Z}: sgd(a+nb, b) = sgd(a,b)$

iii) $c|a \wedge c|b \Rightarrow c | sgd(a,b)$.

Framförallt ii) leder till

Sats (Euklides algoritm): Om $a, b \in \mathbb{Z}_+$ och $a \geq b$ ger divisionsalgoritmen

$$a = q_1 b + r_1 \quad \text{med} \quad 0 \leq r_1 < b$$
$$b = q_2 r_1 + r_2 \quad \text{med} \quad 0 \leq r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3 \quad \text{med} \quad 0 \leq r_3 < r_2$$
$$\vdots \qquad\qquad \vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n \quad \text{med} \quad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = q_{n+1} r_n \quad \text{(utan rest)},$$

och då är $\text{sgd}(a,b) = r_n$.

Vi kan "gå baklänges" i Euklides algoritm, vilket ger

Sats (Bezouts identitet): Om $a, b \in \mathbb{Z}$ så finns det heltal u och v så att

$$\text{sgd}(a,b) = au + bv.$$

Exempel: Euklides algoritm ger

$$900 = 1 \cdot 684 + 216$$
$$684 = 3 \cdot 216 + 36$$
$$216 = 6 \cdot 36,$$

så $\text{sgd}(900, 684) = 36$.

Baklänges: $36 = 684 - 3\cdot 216 = 684 - 3\cdot(900 - 1\cdot 684) = -3\cdot 900 + 4\cdot 684.$

Vi kan ta $u=-3$ och $v=4$ i Bezouts identitet,

så $\text{sgd}(900, 684) = \underbrace{-3}_{u}\cdot 900 + \underbrace{4}_{v}\cdot 684.$

Ett heltal $a>1$ är ett primtal om de enda positiva delarna är a och 1, och i annat fall kallas a sammansatt.

Om a är ett primtal och $a \nmid b$ är $\text{sgd}(a,b)=1$.

Sats: Om $\text{sgd}(a,b)=1$ gäller $a \mid bc \Rightarrow a \mid c$.

Följdsats: Om p är ett primtal gäller det att

$$p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

Ytterligare följdsatser...

Sats (Aritmetikens fundamentalsats) Varje heltal har en entydig primfaktorisering.

För stora tal finns det inga bra sätt att hitta primfaktoriseringen.

Sats: Om $\text{sgd}(a,b)=1$ har den diofantiska ekvationen

$ax+by=c$ den allmänna lösningen

$$\begin{cases} x = cu - bn \\ y = cv + an \end{cases}, \quad n \in \mathbb{Z}.$$

Om $\text{sgd}(a,b) \mid c$ kan vi dela $a, b,$ och c med $\text{sgd}(a,b)$ och använda satsen, och om $\text{sgd}(a,b) \nmid c$ saknas lösningar.

Om $n \geq 2$ och $a, b \in \mathbb{Z}$ säger vi att a och b är kongruenta modulo n då $n \mid a-b$, och detta skrivs $a \equiv b \mod n$.

Kongruens är en ekvivalensrelation, och ger upphov till $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$.

Sats: $$\begin{cases} a \equiv b \mod n \\ c \equiv d \mod n \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d \mod n \\ ac \equiv bd \mod n \end{cases}$$

Vi låter $[a]+[b]=[a+b]$ och $[a]\cdot[b]=[ab]$.

Sats: Det finns ett unikt $[c] \in \mathbb{Z}_n$ så att $[b][c] = [1]$ precis då $\text{sgd}(b, n) = 1$.

Detta hittas med Euklides algoritm: $1 = bu + nv$, tag u.

Sats (Kinesiska restsatsen): Om m_1 och m_2 är större än 1 och $\text{sgd}(m_1, m_2) = 1$ har ekvationssystemet

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \end{cases}$$

en lösning $x = x_0$, och allmänna lösningen

$$x = x_0 + m_1 m_2.$$

Om $m_1 u + m_2 v = 1$ kan vi välja $x_0 = a_2 m_1 u + a_1 m_2 v$.

Vi kan ha fler kongruenser. Vi kan lösa en kongruens i taget.