Kongruensregning

Vi kan regne med restklassene vi får ved divisjon på et heltall.

La a, b være heltall, $n \geq 1$ positivt. Vi sier at a er kongruent med b modulo n,

$$a \equiv b\,(mod\,n)$$

om $n|(a-b)$, altså om n deler differansen mellom a og b. For eksempel:

$$12 \equiv 7\,(mod\,5), \;\; -24 \equiv 1\,(mod\,5), \;\; 23 \not\equiv 12\,(mod\,5)$$

Siden 1 deler alle tall, vil $a \equiv b\,(mod\,1)$ være sant for alle tall a og b; derfor antar vi fra nå av at $n \geq 2$.

Dersom $a \equiv b\,(mod\,n)$ finnes det et heltall k slik at $kn = a - b$, og omvendt. Ved divisjonsalgoritmen finnes det alltid tall q, r med $0 \leq r < n$ slik at $a = qn + r$, eller $a - r = qn$. Da er

$$a \equiv r\,(mod\,n),\ 0 \leq r < n$$

På den annen side kan ikke n dele $r - r'$ for to tall mellom 0 og n (differansen er alltid mindre enn n i absoluttverdi) med mindre de er like. Dermed er ethvert tall kongruent modulo n til nøyaktig ett tall r med $0 \leq r < n$. Dette kan formaliseres til

Lemma $a \equiv b\,(mod\,n)$ hvis og bare hvis a og b har samme rest når de deles på n.

Lemma For alle heltall a, b, c og $n \geq 2$ har vi disse egenskapene:

i $a \equiv a\,(mod\,n)$.

ii $a \equiv b\,(mod\,n)$ gir $b \equiv a\,(mod\,n)$.

iii $a \equiv b\,(mod\,n)$ og $b \equiv c\,(mod\,n)$ gir $a \equiv c\,(mod\,n)$.

Dette sier at $\equiv\ (mod\,n)$ er en ekvivalensrelasjon.

Siden $3 \equiv 8\,(mod\,5)$ er også $8 \equiv 3\,(mod\,5)$. Siden $3 \equiv 8\,(mod\,5)$ og $8 \equiv 8008\,(mod\,5)$ er også $3 \equiv 8008,\ (mod\,5)$.

Vi kan også regne:

Lemma a, b, c, d heltall, $n \geq 2$:

iv $a \equiv b\,(mod\, n)$ og $c \equiv d\,(mod\, n)$ gir $a+c \equiv b+d\,(mod\, n)$ og $ac \equiv bd\,(mod\, n)$

v $a \equiv b\,(mod\, n)$ gir $a+c \equiv b+c\,(mod\, n)$ og $ac \equiv bc\,(mod\, n)$.

vi $a \equiv b\,(mod\, n)$ gir $a^f \equiv b^f\,(mod\, n)$ for alle heltall f.

Siden $3 \equiv 8\,(mod\, 5)$ og $7 \equiv 12\,(mod\, 5)$ er også $10 \equiv 20\,(mod\, 5)$ og $21 \equiv 96\,(mod\, 5)$.

NB: Vi kan vanligvis ikke dele! $12 \equiv 18\,(mod\, 6)$ men $4 \not\equiv 6\,(mod\, 6)$.