6.4 Eksempel. Vi skal se på et eksempel på bruk av kongruensregning. Alle som bor i Norge har et 11-sifret personnummer. Personnummeret består av et 6-sifret fødselsnummer, et 3-sifret individnummer og 2 kontrollsiffer. La

$$(a_1, \ldots, a_9)$$

være de 9 første sifrene. Det tiende sifferet er gitt ved $a_{10} = \overline{(-a)}$ i $\mathbf{Z}/(11)$ hvor a er beregnet ved skalarproduktet

$$a = (3, 7, 6, 1, 8, 9, 4, 5, 2) \cdot (a_1, \ldots, a_9)$$

Det siste sifferet er gitt på tilsvarende måte ved at $a_{11} = \overline{(-b)}$ i $\mathbf{Z}/(11)$ hvor

$$b = (5, 4, 3, 2, 7, 6, 5, 4, 3, 2) \cdot (a_1, \ldots, a_{10})$$

Vi betegner vekt-vektorene med F og G. Anta nå at vi har oppgitt et 11-sifret personnummer

$$(b_1, b_2, \ldots, b_{11})$$

hvor det er en feil i ett av de 9 første sifferene. Vi lar feilen være i siffer i og av størrelse x, som betyr at det korrekte personnummeret er $(a_1, a_2, \ldots, a_{11})$ hvor $a_j = b_j$ for $j \neq i$ og $a_i = b_i + x$. La $(A, B) = (a_{10}, a_{11}) = (b_{10}, b_{11})$ være de to kontrollsifrene. La (A', B') være de beregnede kontrollsifrene fra de ikke-korrekte personnummeret, dvs.

$$A' \equiv -\sum_{k=1}^{9} F_k b_k \equiv -\sum_{k=1}^{9} F_k a_k + F_i x \equiv A + F_i x \qquad (mod\, 11)$$

og

$$\begin{aligned} B' &\equiv -\sum_{k=1}^{9} G_k b_k - G_{10} A' \equiv -\sum_{k=1}^{10} G_k a_k + G_i x + G_{10}(a_{10} - A') \\ &\equiv B + G_i x + G_{10}(A - A') \equiv B + G_i x + 2(A - A') \qquad (mod\, 11) \end{aligned}$$

Sett $\alpha \equiv A' - A \equiv F_i x$ $(mod\, 11)$ og $\beta \equiv B' - B + 2\alpha \equiv G_i x$ $(mod\, 11)$. En feil x i siffer i måles ved $(\alpha, \beta) = (F_i x, G_i x)$. Løser vi ut x av disse to likningene og setter uttrykkene lik hverandre får vi

$$\beta \bar{G}_i^{-1} = \alpha \bar{F}_i^{-1}$$

eller

$$\alpha^{-1} \beta = \bar{F}_i^{-1} \bar{G}_i$$

Vi kaller høyresiden for H og beregner den for hver i. Dette gir

$$H = (H_1, \ldots, H_9) = (\bar{9}, \bar{10}, \bar{6}, \bar{2}, \bar{5}, \bar{8}, \bar{4}, \bar{3}, \bar{7})$$

Dermed kan vi finne ut hvilken i feilen sitter i. Deretter bruker vi funksjonen

$$\bar{F}^{-1} = (\bar{F}_1^{-1}, \ldots, \bar{F}_9^{-1}) = (\bar{4}, \bar{8}, \bar{2}, \bar{1}, \bar{7}, \bar{5}, \bar{3}, \bar{9}, \bar{6})$$

som kombinert med formelen $\bar{x} = \alpha \cdot \bar{F}_i^{-1}$ gir oss avviket.

Vi skal illustrere hele prossessen med et konkret eksempel. Anta at vi har fått oppgitt personnummeret 260482-08697. Vi skal sjekke nummeret for feil og (forhåpentligvis) rette feilen (hvis det bare er en). De beregnede kontrollsifferene (fra de gitte 9) er $1, 3$. Det gir $\alpha = \bar{3}$ og $\beta = \bar{2}$ og dermed $\alpha^{-1} = \bar{4}$ og $H = \bar{8}$ Dette gir oss $i = 6$ i henhold til lista over. Størrelsen på feilen er gitt ved $\bar{x} = \bar{3} \cdot \bar{5} = \bar{4}$. Siden observert siffer er $b_6 = 2$ får vi $a_6 = \bar{2} + \bar{4} = \bar{6}$. Korrekt fødselsnummer er derfor 26048**6**-08697.