Georg Mohr-vinderseminar 2004

Træning, talteori

Sætning A

Lad $x = x_0$, $y = y_0$ være en løsning til $ax + by = c$, hvor $(a, b) = 1$. Så er samtlige løsninger givet ved $x = x_0 - bt$, $y = y_0 + at$, hvor t er et helt tal.

[x_0, y_0 kan ofte gættes. En systematisk metode til at løse ligningen er først at benytte Euklids algoritme til at bestemme x_1 og y_1 så $ax_1 + by_1 = 1$. Så er $x = cx_1$, $y = cy_1$ en løsning til $ax + by = c$.]

Øvelse. Løs $35x - 60y = 165$.

Sætning B

Om kongruensen $mx \equiv a \pmod{n}$ med $d = (m, n) = sm + tn$ gælder:

1. Der er en løsning med hensyn til x hvis og kun hvis $d \mid a$.
2. Løsningen er så $x \equiv sa/d \pmod{n/d}$.

[d, s og t kan findes med Euklids algoritme.]

Øvelse. Løs $56x - 3 \equiv 133 \pmod{1324}$.

Sætning C (Den kinesiske restklassesætning)

Lad $n_1, n_2, \ldots, n_k$ være parvis primiske. For ethvert sæt $a_1, a_2, \ldots, a_k$ af hele tal har systemet af kongruenser $x \equiv a_1 \pmod{n_1}$, $\ldots$, $x \equiv a_k \pmod{n_k}$ så løsninger med hensyn til x, og de udgør en restklasse modulo $n_1 n_2 \cdots n_k$.

Øvelse. Bestem de hele tal x som opfylder $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{6}$, $x \equiv 4 \pmod{7}$.

Sætning D

$(a)_n{}^{-1}$ findes hvis og kun hvis $(a, n) = 1$. $(a)_n{}^{-1}$ kan så bestemmes ved mindst tre forskellige metoder:

1. Prøve sig frem.
2. Løse kongruensen $ax \equiv 1 \pmod{n}$.
3. Benytte Euler-Fermats sætning: $(a)_n{}^{-1} = (a)_n{}^{\phi(n)-1}$.

Øvelse. Bestem $(5)_{21}{}^{-1}$ på hver af disse måder.