sætning: Hvis a og b er heltal da findes heltal s og t så

$$gcd(a, b) = sa + tb.$$

lemma: Hvis a, b og c er heltal så $gcd(a, b) = 1$ og $a|bc$ da vil $a|c$.

lemma: Hvis p er et primtal og $p|a_1a_2 \cdots a_n$ hvor hvert a_j er et heltal da findes et indeks i så $p|a_i$.

Fra denne sætning kan der vises entydighed af primfaktorering af heltal.

def (Invers modulo et heltal): Hvis a og m er heltal og $m > 1$ da siges at $\overline{a}$ er en invers modulo m for a hvis $a\overline{a} \equiv 1 (\text{mod } m)$.

sætning: Hvis a og m er indbyrdes primske og $m > 1$ da har a en invers modulo m.

Fra denne sætning kan der derved findes løsninger til ligninger af følgende form $ax \equiv b (\text{mod } m)$ hvis $gcd(a, m) = 1$ (Denne slags ligninger kaldes lineære kongurens-ligninger).

Den kinesiske restklassesætning: Lad $m_1, \ldots, m_n$ være indbyrdes primske heltal. Da findes en entydig løsning x (modulo $m = m_1 m_2 \cdots m_n$) til følgende ligningssystem :

$$\begin{aligned} x &\equiv a_1 (\text{mod } m_1) \\ x &\equiv a_2 (\text{mod } m_2) \\ &\vdots \\ x &\equiv a_n (\text{mod } m_n). \end{aligned}$$

Hvis $M_i := \frac{m}{m_i}$ da følger det at m_i og M_i er indbyrdes primske da alle faktorerne i M_i er indbyrdes primske med m_i. Lad s_i være en invers til M_i modulo m_i for $i \in \{1, \ldots, n\}$ Det følger da at

$$x = M_1 \cdot a_1 \cdot s_1 + M_2 \cdot a_2 \cdot s_2 + \cdots + M_n \cdot a_n \cdot s_n \text{ mod } m$$

er en løsning til ligningssystemt fra den kinesiske restklassesætning.

Anvendelse af den kinesiske restklassesætning til aritmetik med store tal:

Lad $m_1, \ldots, m_n$ være indbyrdes primske heltal. Fra den kinesiske restklassesætning følger det at ethvert tal a hvor $0 \leq a < m$ kan repræsenteres entydigt ved (a mod m_1,a mod m_2, $\ldots$, a mod m_n).

Dette benyttes ved følgende eksempel:

Lad $m_1 = 99$, $m_2 = 98$, $m_3 = 97$ og $m_4 = 95$.

Tallet 123684 kan da repræsenteres ved (33,8,9,89) mens 413456 kan repræsenteres ved (32,92,42,16).

Det følger nu at 123684+413456 kan repræsenteres ved

$$(33 + 32 \bmod 99, 8 + 92 \bmod 98, 9 + 42 \bmod 97, 89 + 16 \bmod 95)$$

$$= (65, 2, 51, 10).$$

Ved at løse det tilsvarende ligningssystemet ses at dette svarer til tallet 537140=413456+123684.

sætning (Fermats lille): Hvis p er et primtal og p ikke er en divisor i a, da er $a^{p-1} \equiv 1 (\text{mod } p)$.

kryptering

Simpelt privat key krypteringssystem : (shift cipher).

Der skal sendes en besked mellem nogle folk, således andre ikke kan læse beskeden. Ved et private key krypteringssystem benyttes ved kryptering en "krypterings-nøgle" som kun disse folk kender og til dekrytering benyttes en "nøgle" som let kan fås fra krypteringsnøglen.

p : tegn der ønskes sendt (repræsenteret ved et tal mellem 0 og 25).

k : nøglen som i dette tilfælde er et heltal mellem 0 og 25.

p krypteres da til det entydige heltal c mellem 0 og 25 så

$$c = (p + k) \bmod 26.$$

Fra kendskab til k er det let at gendanne p fra c da

$$p = (c - k) \bmod 26.$$

Public key kryptering

Ide : Der ønskes sendt en besked mellem to personer, således kun modtager kan læse beskeden. Derfor krypteres beskeden inden den sendes med en offentlig nøgle som alle må kende. Det er da meningen at modtageren kender en "privat nøgle" til at dekryptere med og man ikke kan finde denne private nøgle ud fra de offentlige nøgler.

eksempel: RSA

Ved dette private key krypteringssystem dannes (af modtager) nøgler til kryptering og dekryptering på følgende vis :

1. Lad p og q være to store primtal som er forskellige og lad $n = pq$.
2. Lad e være et heltal der opfylder at $gcd(e, (p-1)(q-1)) = 1$.
3. Lad d betegne en invers til e modulo $(p-1)(q-1)$.
4. e og n benyttes da som offentlige nøgler mens d benyttes som den private nøgle.

Ideen er da at der kan sendes "tal" med værdi højst $n-1$ (Dette skal svare til en del af strengen der ønskes sendt).

Eksempel på RSA: Der ønskes sendt beskeden HELP. Denne omdannes til talfølgen 07041115. For at danne nøglen vælges $p = 43$ og $q = 59$ hvorved $n = 43 \cdot 59 = 2537$. Det ses at e kan vælges til at være 13 da der da gælder at

$$gcd(e, (p-1)(q-1)) = gcd(13, 42 \cdot 58) = 1.$$

Da 937 er en invers til e modulo $(p-1)(q-1)$ vælges $d = 937$.

$(937 \cdot 13 = 12181 = 5(p-1)(q-1) + 1 = 5 \cdot 2436 + 1)$

Da $n > 2525$ kan vi sende 2 tegn af gangen (britisk alfabet). Derfor skal der først sendes 0704 som svarer til tegnene HE og derefter 1115 som svarer til LP.

Kryptering og dekryptering ved RSA:

Lad M være tallet der skal sendes da krypteres M til $C = M^e \bmod n$. For at dekryptere C og derved finde M benyttes at $M = C^d \bmod n$. (Det skal bemærkes at der skal gælde at $gcd(M, n) = 1$)

Eksempel på RSA fortsat: 0704 krypteres til

$$704^{13} \bmod 2537 = 981$$

og 1115 krypteres til

$$1115^{13} \bmod 2537 = 0461.$$

Derved bliver den krypterede tekst til 0981 efterfulgt af 0461. Til dekryptering findes $981^{937} \bmod 2537 = 0704$ og
$461^{937} \bmod 2537 = 1115$.