

**ARBEJDSDAG FOR 2G FRA LANGKÆR GYMNASIUM
MATEMATIKKEN BAG KRYPTERING OG SIGNERING V.HJ.A. RSA
ET OFFENTLIG NØGLE KRYPTERINGSSYTEM**

JOHAN P. HANSEN

INDHOLD

| | |
|--|---|
| 1. Dagens Program | 1 |
| 2. Indbyrdes primiske hele tal | 1 |
| 3. Regning med rester | 2 |
| 4. Kryptering og signering ved hjælp af et offentligt nøgle kryptosystem RSA | 4 |

1. DAGENS PROGRAM

Foredrag og øvelser finder sted i Aud. F.

- 9:15 -10 Forelæsning, afsnit 2 og 3
- 10:15-11:30 Øvelser
- 11:30-12:15 Frokostpause
- 12:15-13 Forelæsning, afsnit 4
- 13:15-14 Øvelser

2. INDBYRDES PRIMISKE HELE TAL

Definition 1. To hele tal m, n kaldes indbyrdes primiske, hvis de ingen fælles divisorer har, når vi ser bort fra 1 og -1. Med $\phi(m)$ betegner vi antallet af positive hele tal mindre end m , der er indbyrdes primiske med m (Euler's ϕ funktion).

Øvelse 2. Vis, at

$$\phi(12) = 4$$

Lad p, q være forskellige primtal. Vis at

$$\phi(p) = p - 1$$

$$\phi(pq) = (p - 1)(q - 1).$$

I opgaven har vi set at det er let at bestemme $\phi(n)$, hvis vi kender faktoriseringen af n i primfaktorer. Kendes faktorisering af n ikke, er det imidlertid MEGET tidskrævende at bestemme $\phi(n)$. Har n for eksempel 100 cifre vil det, at forsøge sig frem med et tal $1, 2, 3, \dots, n$ ad gangen tage

$$\frac{10^{100}}{10^{12}} \text{ sekunder} \sim 10^{61} \text{ år}$$

Document version: 14. januar 2000.

på en maskine, der i 1 sekund kan foretage 10^{12} (en million million) undersøgelser af om et tal er primisk med n . (Universets alder anslås til $15 \cdot 10^{12}$ år).

Det er det store tidsforbrug, der fordres til bestemmelse af $\phi(n)$, der er sikkerheden i RSA kryptosystemet, som vi vender tilbage til senere.

Lemma 3. *Lad m, n være indbyrdes primiske hele tal. Der findes hele tal f, g således at*

$$1 = mf + ng$$

Bevis. Lad d være det mindste positive hele tal på formen

$$d = mf + ng$$

Påstanden er nu, at $d = 1$.

Antag det modsatte og lav heltalsdivision med rest:

$$m = qd + r, \quad 0 \leq r < d,$$

heri indsætter vi udtrykker for d og får:

$$m = q(mf + ng) + r \Rightarrow r = m(1 - qf) - nqg = mf' + ng',$$

som er et mindre positivt helt tal på den angivne form i strid med minimalitet af d . \square

Korollar 4. *Lad k, m være indbyrdes primiske hele tal. Så gælder, at*

$$k \mid am \rightarrow k \mid a$$

Bevis. Da k, m en indbyrdes primiske findes der hele tal f, g således at

$$1 = mf + kg \Rightarrow a = amf + akng.$$

Da $k \mid amf + akng$ følger påstanden. \square

Øvelse 5. Find hele tal f, g , så

$$1 = 7f + 9g$$

Øvelse 6. Find hele tal f, g , så

$$1 = 71f + 8448g$$

3. REGNING MED RESTER

Gauss indførte en bemærkelsesværdig notation, som letter omgangen med heltalsdivision med rest.

Definition 7. Givet hele tal a, b og $m > 0$. Vi siger, at a er kongruent med b modulo m og skriver

$$a \equiv b \pmod{m},$$

hvis a og b har samme rest ved division med m , altså hvis m går op i forskellen $a - b$. Når m fremgår af sammenhængen skriver vi blot $a \equiv b$.

For eksempel er $19 \equiv 7 \pmod{12}$, $1 \equiv -1 \pmod{2}$, $3^2 \equiv -1 \pmod{5}$.

Lemma 8. *Lad $m > 0$ være givet. Hvis $a_1 \equiv b_1$ og $a_2 \equiv b_2$, så er $a_1 + a_2 \equiv b_1 + b_2$ og $a_1 a_2 \equiv b_1 b_2$.*

Endvidere gælder, at hvis k er indbyrdes primisk med m , så kan der forkortes med k :

$$ka \equiv kb \Rightarrow a \equiv b.$$

Bevis. Følger af definitionen og ved anvendelse af Korollar 4:

$$ka \equiv kb \Rightarrow m \mid k(a - b) \Rightarrow m \mid a - b \Rightarrow a \equiv b.$$

□

Øvelse 9. Modular exponentiering. Lad $m = 7$. Vis, at

$$2^3 \equiv 1$$

$$2^4 \equiv 2$$

$$2^5 \equiv 4$$

$$2^6 \equiv 1$$

$$2^7 \equiv 2$$

Bestem $r, 0 \leq r < 7$, så

$$2^{100} \equiv r$$

Definition 10. Lad $m > 0$ være givet. Med $[a]$ betegner vi mængden af alle hele tal x , der er kongruent med a modulo m . Mængden $[a]$ kaldes restklassen af a .

Et *fuldstændigt sæt af rester modulo m* består af m hele tal, en fra hver restklasse.

Et *reduceret sæt af rester modulo m* består af $\phi(m)$ hele tal, en fra hver restklasse, og hver for sig indbyrdes primisk med m .

For $m = 6$ er $[3] = \{\dots - 9, -3, 3, 9, 15, \dots\}$, tallene $0, 1, 2, 3, 4, 5$ er et fuldstændigt sæt af rester, mens tallene $6, 14, 13, -2, 27, 35$ er et andet fuldstændigt sæt af rester. De tilsvarende reducerede sæt af rester har hver $\phi(6) = 2$ elementer og er $1, 5$ og $13, 35$

Sætning 11. Lad $a_1, \dots, a_{\phi(m)}$ være et reduceret sæt af rester modulo m og lad k være et helt tal primisk med m . Så er $ka_1, \dots, ka_{\phi(m)}$ også et reduceret sæt af rester modulo m .

Bevis. Ifølge Lemma 8 kan vi slutte, at

$$ka_i \equiv ka_j \Rightarrow a_i \equiv a_j.$$

Derfor ligger $ka_1, \dots, ka_{\phi(m)}$ i hver sin restklasse. Tilsvarende er $ka_1, \dots, ka_{\phi(m)}$ hver for sig primiske med m , idet Lemma 8 anvendt på en fælles divisor n i m og ka_i , der naturligvis også er primisk med k , giver

$$n \mid (ka_i) \Rightarrow n \mid a_i$$

i modstrid med at a_i er primisk med m . □

Øvelse 12. Bestem et komplet sæt af reducerede rester modulo 12 (der skal være 4 ialt). Multipliser hver af de 4 elementer i sættet med 5 og vis, at det nye sæt også er et komplet sæt af reducerede rester.

Sætning 13. (Euler-Fermat) *Antag at k, m er indbyrdes primiske. Så er*

$$k^{\phi(m)} \equiv 1 \pmod{m}.$$

Bevis. Lad $a_1, \dots, a_{\phi(m)}$ være et reduceret sæt af rester modulo m , ifølge sætningen ovenfor ved vi, at $ka_1, \dots, ka_{\phi(m)}$ også er et reduceret sæt af rester. Anvender vi nu Lemma 8, har vi

$$a_1 \cdot \dots \cdot a_{\phi(m)} \equiv k^{\phi(m)} a_1 \cdot \dots \cdot a_{\phi(m)} \pmod{m}.$$

Da a_i alle er indbyrdes primisk med m giver gentagne anvendelser af forkortningsdelen af Lemma 8, det ønskede. □

Øvelse 14. Eftersvis, at

$$k^{\phi(12)} \equiv 1 \pmod{12}.$$

for alle k , der er primiske med 12.

4. KRYPTERING OG SIGNERING VED HJÆLP AF ET OFFENTLIGT NØGLE KRYPTOSYSTEM RSA

En person A, der ønsker at lave et kryptosystem med henblik på modtagelse gør følgende:

- vælger 2 store primtal p, q og beregner $n = pq$
- beregner $\phi(n)$, jvf. Øvelse 2. (Sikkerheden beror på, at det er tidskrævende at bestemme $\phi(n)$ alene ud fra kendskabet til n).
- vælger et e primisk med $\phi(n)$
- beregner f (og g), så $1 = ef + \phi(n)g$, jvf. Lemma 3
- offentligør n, e

En vilkårlig person B ønsker at sende tallet k til personen A. B indkoder tallet k ved brug af den offentlige nøgle n, e , nemlig ved at beregne og sende:

$$h = k^e$$

modulo n . Personen A modtager h og beregner ved hjælp af sin hemmelige viden om $\phi(n)$ og f

$$h^f \equiv (k^e)^f \equiv k^{ef} \equiv k^{1-\phi(n)g} \equiv k \cdot (k^{\phi(n)})^{-g} \equiv k$$

ifølge Sætning 13, idet alle beregninger er foretaget modulo m .

Øvelse 15. Lad $p = 89$ og $q = 97$. Bestem n og $\phi(n)$. Lad $e=71$. Bestem f, g så

$$1 = ef + \phi(n)g$$

Indkod $k = 3$ ved at beregne $h = 3^e$ og dekrypter ved at beregne $(3^e)^f$.

Krypteringssystemet har n, e er som offentlige nøgler og $\phi(n)$ og f som hemmelige nøgler.

Signering (underkrift, digital signatur) foretages ved at personen A indkoder f.eks. sit "navn" k med sin hemmelige nøgle f, n . Modtageren kan afkode med A's offentlige nøgle e, n . Giver afkodningen "navnet" k , er der overfor modtageren godtgjort, at afsenderen har den hemmelige nøgle, der passer til den offentlige nøgle.

Øvelse 16. Lav endnu et nøglesæt og vis ved et eksempel, hvordan man laver *digital signatur*.

E-mail address: matjph@mi.aau.dk

DEPARTMENT OF MATHEMATICS, NY MUNKEGADE, 8000 AARHUS C, DENMARK