MA1301 TALLTEORI, HØST 2011
LØSNINGSFORSLAG – MIDTSEMESTERPRØVE

Oppgave 1. Vi skal løse den diofantiske ligninga $630x - 144y = 108$.

Ligninga har løsninger hvis og bare hvis $d = \gcd(630, 144) \mid 108$. Vi finner $d = 18$:

$$\begin{aligned}
630 &= 4 \cdot 144 + 54\\
144 &= 2 \cdot 54 + 36\\
54 &= 1 \cdot 36 + 18\\
36 &= 2 \cdot \underline{18} + 0
\end{aligned}$$

Siden $18 \mid 108$, har ligninga løsninger.

Tilbakesubstitusjon gir

$$18 = 54 - 36 = 3 \cdot 54 - 144 = 3 \cdot 630 - 13 \cdot 144,$$

og multiplikasjon med $108/18 = 6$ gir en løsning av ligninga,

$$108 = 6 \cdot 18 = 6 \cdot (3 \cdot 630 - 13 \cdot 144) = 18 \cdot 630 - 78 \cdot 144,$$

så med andre ord er en spesiell løsning av ligninga gitt ved $x_0 = 18$, $y_0 = 78$.

Da gir Teorem 2.9 alle løsninger av ligninga, parametrisert over $t \in \mathbb{Z}$:

$$\begin{aligned}
x &= 18 + (-144)/18 \cdot t = 18 - 8t\\
y &= 78 - 630/18 \cdot t = 78 - 35t
\end{aligned}$$

Her kan man oppgi svaret på mange, ekvivalente, måter. For eksempel ved å bytte ut t med $2 - s$, får man alle løsninger for $s \in \mathbb{Z}$:

$$\begin{aligned}
x &= 18 - 8(2 - s) = 2 + 8s\\
y &= 78 - 35(2 - s) = 8 + 35s
\end{aligned}$$

Oppgave 2. At a er et tall som gir rest 2 eller 3 når det deles på 4 betyr at det er på form $4k + 2$ eller $4k + 3$.

Nå lar vi b være et vilkårlig tall, så b er enten på form $2l$ eller $2l + 1$. Da er enten $b^2 = 4(l^2)$ eller $b^2 = (2l + 1)^2 = 4(l^2 + l) + 1$. Så alle kvadrattall er på formen $4k$ eller $4k + 1$. Dette viser at a umulig kan være et kvadrattall.

Alternativt kan vi bruke kongruenser. La b være et vilkårlig tall. Dette betyr at b er kongruent 0, 1, 2 eller 3 modulo 4. Det betyr at b^2 er kongruent med en av:

$$0^2 \equiv 0 \pmod 4, \quad 1^2 \equiv 1 \pmod 4, \quad 2^2 \equiv 0 \pmod 4, \quad 3^2 \equiv 1 \pmod 4.$$

Men $a \equiv 2 \pmod 4$ eller $a \equiv 3 \pmod 4$ ved antagelse, så a kan ikke være et kvadrattall.

Oppgave 3. Vi skal løse systemet

$$\begin{aligned}
x &\equiv -2 \pmod 4\\
2x &\equiv -4 \pmod 7\\
4x &\equiv 2 \pmod 9,
\end{aligned}$$

og deretter finne den minste positive løsningen.

Vi ønsker å bruke det kinesiske restteoremet, så vi skriver om ligningene slik at hver venstre side er x. Fra andre ligning får vi, ved å gange med 4,

$$x \equiv 8x \equiv -16 \equiv 5 \pmod 7,$$

og fra tredje får vi (ved å gange med -2)

$$x \equiv -8x \equiv -4 \equiv 5 \pmod 9.$$

Date: 11. oktober 2011.

Så det opprinnelige systemet har samme løsninger som

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 5 \pmod 7 \\ x &\equiv 5 \pmod 9. \end{aligned}$$

Siden alle moduliene er relativt primiske kan vi benytte det kinesiske restteoremet. Det garanterer at det finnes en entydig løsning av systemet modulo $4 \cdot 7 \cdot 9$. Sett $N = 4 \cdot 7 \cdot 9 = 252$. Vi løser ligningene

$$\frac{N}{4}x_1 \equiv 1 \pmod 4, \quad \frac{N}{7}x_2 \equiv 1 \pmod 7, \quad \frac{N}{9}x_3 \equiv 1 \pmod 9.$$

Vi finner x_1:

$$1 \equiv \frac{N}{4}x_1 \equiv 63x_1 \equiv -x_1 \pmod 4,$$

så $x_1 = -1$ løser kongruensen. Likedan får vi spesielle løsninger $x_2 = 1$ og $x_3 = 1$.

Alle løsninger av systemet er dermed gitt ved

$$x \equiv 2 \cdot \frac{N}{4}x_1 + 5 \cdot \frac{N}{7}x_2 + 5 \cdot \frac{N}{9}x_3 \equiv 194 \pmod{252},$$

så minste positive løsning er 194.

Alternativt kan vi starte med det opprinnelige systemet. Fra første ligning har vi at $x = 4k + 2$, for en k. Dette gir, innsatt i andre ligning at $-4 \equiv 2(4k + 2) \equiv k + 4 \pmod 7$, altså $k \equiv 6 \pmod 7$, så $k = 7l + 6$, for en l. Da er $x = 4k + 2 = 4(7l + 6) + 2 = 28l + 26$ løsningene av de to første ligningene. Innsatt i tredje ligning får vi

$$2 \equiv 4x \equiv 4(28l + 26) \equiv 112l + 104 \equiv 4l + 5 \pmod 9,$$

så $4l \equiv 6 \pmod 9$. Multiplikasjon med -2 gir da at $l \equiv -8l \equiv -12 \equiv 6 \pmod 9$, så $l = 9m + 6$, for en m.

Dette betyr at løsningene for systemet er gitt ved

$$x = 28l + 26 = 28(9m + 6) + 26 = 252m + 194,$$

og dermed at minste positive løsning er 194.

Oppgave 4. Hvis p er et primtall, og $p \nmid a$, så sier Fermat at

$$a^{p-1} \equiv 1 \pmod p.$$

Ekvivalent har vi at $p \mid (a^{p-1} - 1)$. Siden p er odde, så er $\frac{p-1}{2}$ et heltall. Det betyr at vi ved konjugatsetningen (tredje kvadratsetning) kan skrive

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right).$$

Siden p er et primtall, må p dele minst én av faktorene (Teorem 3.1). Vi har at

$$p \mid \left(a^{\frac{p-1}{2}} - 1\right) \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

og

$$p \mid \left(a^{\frac{p-1}{2}} + 1\right) \iff a^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

så minst én av kongruensene må holde.

Hvis p er et odde primtall, så holder kun én av disse samtidig. For å se dette beviser vi det kontrapositive: La p være et primtall. Hvis begge holder, så er $p = 2$.

Anta at begge holder. Da er sammensetningen av kongruensene

$$1 \equiv a^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

så $p \mid 2$. Dette medfører at $p = 2$, siden p er et primtall.