MA1301 TALLTEORI, HØST 2011
LØSNINGSFORSLAG – EKSAMEN

Oppgave 1. Vi skal finne resten til 1301^{338} ved divisjon på 98. Vi skal altså finne $0 \leq r < 98$ slik at $1301^{338} \equiv r \pmod{98}$. Eulers teorem sier at hvis $\gcd(a, 98) = 1$, så er $a^{\varphi(98)} \equiv 1 \pmod{98}$. Nå er $98 = 2 \cdot 7^2$, så $\varphi(98) = (2-1)(7^2 - 7) = 42$. Nå bruker vi at $1301 = 13 \cdot 98 + 27$, $338 = 8 \cdot 42 + 2$ og at $\gcd(27, 98) = 1$ for å få at

$$1301^{338} \equiv 27^{338} \equiv 27^{8 \cdot 42+2} \equiv \left(27^{42}\right)^8 \cdot 27^2 \overset{\mathsf{E}}{\equiv} 1^8 \cdot 27^2 \equiv 27^2 \equiv 43 \pmod{98}.$$

Resten er altså 43.

Oppgave 2. Vi skal løse systemet

$$\begin{aligned} 8x &\equiv 6 \pmod{7} \\ x &\equiv -3 \pmod{9} \\ 4x &\equiv -1 \pmod{13}. \end{aligned}$$

Først ser vi kan bytte ut første ligning med $x \equiv 6 \pmod{7}$ og andre ligning med $x \equiv 6 \pmod{9}$. Tredje ligning sier at $4x \equiv 12 \pmod{13}$, og siden $\gcd(4, 13) = 1$ kan vi forkorte 4 på begge sider og står igjen med $x \equiv 3 \pmod{13}$.

Vi har derfor følgende ekvivalente ligningssystem:

$$\begin{aligned} x &\equiv 6 \pmod{7} \\ x &\equiv 6 \pmod{9} \\ x &\equiv 3 \pmod{13}. \end{aligned}$$

Det kinesiske restteoremet forteller oss at siden 7, 9 og 13 er parvis relativt primiske, så har dette systemet en entydig løsning modulo $7 \cdot 9 \cdot 13 = 819$. Før vi finner løsningene merker vi at ligningssystemet er ekvivalent med

$$\begin{aligned} x &\equiv 6 \pmod{63} \\ x &\equiv 3 \pmod{13}, \end{aligned}$$

siden x er kongruent med 6 både modulo 7 og 9 hvis og bare hvis x er kongruent med 6 modulo $7 \cdot 9 = 63$.

De x som løser første kongruens er altså på form $x = 63k + 6$. Ved å sette inn i andre kongruens får vi da

$$3 \equiv x \equiv 63k + 6 \equiv -2k + 6 \pmod{13}.$$

Vi flytter over og får $2k \equiv 3 \equiv 16 \pmod{13}$. Siden $\gcd(2, 13) = 1$ kan vi stryke 2 på begge sider og har dermed at $k \equiv 8 \pmod{13}$. Altså er $k = 13l + 8$ for en eller annen l.

Totalt har vi fått at $x = 63k + 6 = 63(13l + 8) + 6 = 819l + 510$, for en l. Dette betyr at løsningene av systemet er $x \equiv 510 \pmod{819}$.

Oppgave 3. Vi har gitt at $\{n, e\} = \{187, 21\}$ og skal finne $\{n, d\}$. Vi skal altså finne en d slik at $de \equiv 1 \pmod{\varphi(n)}$. Første steg er å faktorisere tallet $187 = 11 \cdot 17$. Da finner vi at $\varphi(187) = (11-1)(17-1) = 160$. For å finne en invers til $e = 21$ modulo 160 benytter vi Euklids algoritme:

$$\begin{aligned} 160 &= 7 \cdot 21 + 13 \\ 21 &= 13 + 8 \\ 13 &= 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + \underline{1} \end{aligned}$$

(Dette viser spesielt at e *har* en invers modulo 160.) Ved tilbakesubstitusjon får vi

$$1 = 3 - 2 = 2 \cdot 3 - 5 = \cdots = 61 \cdot 21 - 8 \cdot 160.$$

Date: 5. desember 2011.

Modulo 160 gir dette

$$61 \cdot 21 \equiv 1 \pmod{160},$$

så en invers til $e = 21$ modulo 160 er $d = 61$. Det hemmelige nøkkelparet er altså $\{n, d\} = \{187, 61\}$.

Vi skal kryptere $M = 20$ med krypteringsnøkkelen, dvs. regne ut resten til M^e modulo 187. Vi regner ut at $20^2 \equiv 26$, $20^4 \equiv 26^2 \equiv 115$, $20^8 \equiv 115^2 \equiv 135$ og $20^{16} \equiv 86$ modulo 187. Dermed har vi at

$$M^e \equiv 20^{21} \equiv 20^{16} \cdot 20^4 \cdot 20 \equiv 86 \cdot 115 \cdot 20 \equiv 141 \pmod{187}.$$

Den krypterte meldinga er derfor 141.

Oppgave 4. Vi skal finne et tall $1 < d < a$ slik at $d \mid a$ hvor $a = 77! - 1$.

Det eneste resultatet vi kjenner fra pensum som dette kan minne om er Wilsons teorem som sier at for primtall p, så er $(p-1)! \equiv -1 \pmod{p}$. Fra Wilson følger at $(p-2)! \equiv 1 \pmod{p}$. [1] Nå er 79 et primtall, så resultatet over forteller oss at $77! \equiv 1 \pmod{79}$. Ekvivalent har vi at $79 \mid (77! - 1)$. Dermed oppfyller $d = 79$ kravet at $d \mid a$.

Oppgave 5. Vi skal vise at for oddetall n så har vi $31 \mid (n^8 - 1)$. Vi bruker konjugatsetningen og skriver

$$n^8 - 1 = (n^4+1)(n^4-1) = (n^4+1)(n^2+1)(n^2-1) = (n^4+1)(n^2+1)(n+1)(n-1).$$

Siden n er et oddetall er også n^2 og n^4 det. Dette betyr at $2 \mid (n^4+1)$ og $2 \mid (n^2+1)$. Videre er n enten på form $4k+1$ eller $4k+3$. Dermed er nøyaktig én av $n+1$ og $n-1$ delelig på 4 og den andre på 2. (Nøyaktig ett av to etterfølgende partall er delelig på 4.) Totalt har vi at $n^8 - 1$ deles av (minst) $2 \cdot 2 \cdot 2 \cdot 4 = 32$.

Oppgave 6. Vi definerer følgen (f_n) ved $f_1 = f_2 = 1$ og $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$, og skal vise at da er $\sum_{i=1}^n f_i^2 = f_n f_{n+1}$ for alle $n \geq 1$. Vi viser dette ved induksjon.

For $n = 1$ er dette ok, siden $f_1^2 = 1 = f_1 f_2$. Anta så at $\sum_{i=1}^n f_i^2 \overset{\text{ih}}{=} f_n f_{n+1}$ for en $n \geq 1$. Da er $n+2 \geq 3$, så det følger at

$$f_{n+1}f_{n+2} = f_{n+1}(f_{n+1} + f_n) = f_{n+1}^2 + f_{n+1}f_n \overset{\text{ih}}{=} f_{n+1}^2 + \sum_{i=1}^n f_i^2 = \sum_{i=1}^{n+1} f_i^2.$$

Dette viser at da holder likhet for $n+1$ også. Ved induksjon har vi vist at likhet holder for alle $n \geq 1$.

Oppgave 7. La k være ordenen til tallet a modulo n. Vi viser at $a^t \equiv 1 \pmod{n}$ hvis og bare hvis $k \mid t$.

Anta først at $k \mid t$, dvs. $t = kq$ for et heltall q. Da har vi at

$$a^t \equiv a^{kq} \equiv (a^k)^q \equiv 1^q \equiv 1 \pmod{n}.$$

Dette viser implikasjonen mot venstre.

For å vise implikasjonen mot høyre, skriv $t = kq + r$, $0 \leq r < k$, ved hjelp av divisjonsalgoritmen. Ved antagelsen har vi at

$$1 \equiv a^t \equiv a^{kq+r} \equiv (a^k)^q a^r \equiv 1^q a^r \equiv a^r \pmod{n}.$$

Siden ordenen til et tall er det minste positive heltallet k med $a^k \equiv 1 \pmod{n}$ og $r < k$, følger det at $r = 0$. Dermed har vi $t = kq$, så $k \mid t$.

Oppgave 8a. Eulers kriterium sier at kongruensen $x^2 \equiv -1 \pmod{p}$ har en løsning hvis og bare hvis $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$. Her er venstre side ± 1, så siden p er odde, er dette tilfelle hvis og bare hvis $(p-1)/2$ er et partall. Da følger at kongruensen er løsbar hvis og bare hvis $(p-1)/2 = 2k$, for et heltall k, som igjen er ekvivalent med at $p = 4k+1$, for et heltall k.

[1] $(p-1) \cdot (p-2)! \equiv (p-1)! \overset{\text{W}}{\equiv} -1 \equiv p-1 \pmod{p}$. Siden $\gcd(p-1, p) = 1$ kan vi stryke $p-1$ på begge sider, og resultatet følger.

Oppgave 8b. Anta at tallene $p_1, p_2, \ldots, p_t$ er forskjellige primtall av form $4k+1$. Vi viser at da finnes et primtall p på samme form, forskjellig fra alle p_i. Konsekvensen av dette er at det finnes uendelig mange primtall på form $4k+1$.

Dann tallet $N = (2p_1 \cdots p_t)^2 + 1$. Velg deretter en primtallsdivisor p av N. Siden $p \mid \big((2p_1 \cdots p_t)^2 + 1\big)$ har vi at $p \nmid (2p_1 \cdots p_t)^2$, så p er en odde primtallsdivisor som er forskjellig fra p_i for alle i. (p er altså ikke i den opprinnelige listen av primtall på form $4k+1$.)

Men siden $p \mid N$ får vi at

$$(2p_1 \cdots p_t)^2 \equiv -1 \pmod{p},$$

så kongruensen $x^2 \equiv -1 \pmod{p}$ er løsbar. Fra del (a) vet vi at da er p på form $4k+1$.

Vi har dermed funnet et primtall p på form $4k+1$ som ikke er i den opprinnelige listen. Dette viser at det finnes uendelig mange primtall på form $4k+1$.

Oppgave 9. Vi skal avgjøre om kongruensen $x^2 + 4x \equiv 30 \pmod{31}$ er løsbar. Vi fullfører kvadratet på venstre side ved å legge til 4:

$$(x+2)^2 \equiv x^2 + 4x + 4 \equiv 34 \equiv 3 \pmod{31}$$

Denne kongruensen er løsbar hvis og bare hvis Legendresymbolet $(3/31) = 1$.

Fra kvadratisk resiprositet får vi at $(3/31)(31/3) = (-1)^{(3-1)/2(31-1)/2} = (-1)^{15} = -1$. Det følger at

$$(3/31) = -(31/3) = -(1/3) = -1,$$

hvor vi har brukt at $31 \equiv 1 \pmod{3}$ og at $(1/3) = 1$ (1 er en kvadratisk rest av 3).

Kongruensen er derfor ikke løsbar.

Denne oppgaven kan også løses uten å referere til kvadratisk resiprositet, men heller bruke Eulers kriterium. Da finner man at $3^{(31-1)/2} \equiv -1 \pmod{31}$ som gir samme konklusjon.