MA1301 TALLTEORI, HØST 2012
LØSNINGSSKISSE – EKSAMEN

Oppgave 1. Vi skal løse likningssystemet

$$\begin{aligned} 2x &\equiv 4 \pmod 6 \\ x &\equiv 2 \pmod 7 \\ x &\equiv 1 \pmod{11}. \end{aligned}$$

Ettersom $\gcd(2,6) = 2$ og $2|4$ får vi at den første kongruensen er ekvivalent med $x \equiv 2 \pmod 3$. Anvender kinesiske restklasseteorem og finner x_1, x_2 og x_3 slik at $77x_1 \equiv 1 \pmod 3$, $33x_2 \equiv 1 \pmod 7$ og $21x_3 \equiv 1 \pmod{11}$. Dette gir $x_1 \equiv 2 \pmod 3$, $x_2 \equiv 3 \pmod 7$ og $x_3 \equiv 10 \pmod{11}$ og unik løsning

$$x \equiv 2 \cdot 77 \cdot 2 + 2 \cdot 33 \cdot 3 + 1 \cdot 21 \cdot 10 \equiv 23 \pmod{231}$$

Oppgave 2. For $m = 3$ og $m = 9$ får vi $10 \equiv 1 \pmod m$. Dermed følger det at

$$n = a_0 + a_1 \cdot 10 + \cdots + a_k \cdot 10^k \equiv a_0 + a_1 + \cdots + a_k = T(n) \pmod m.$$

Motsatt ser vi at $m = 3$ og $m = 9$ er de eneste mulighetene: hvis $m \geq 10$ er $m > T(m)$ så $m|m$, men $m \nmid T(m)$. For $m < 10$ ser vi at $T(9 + m) = m$, så det følger at m må dele $9 + m$ som igjen gir at $m = 3$ eller $m = 9$.

Oppgave 3. For definisjon av ϕ-funksjonen: se boka. La $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ og benytt at ϕ-funksjonen er multiplikativ: $\phi(n) = \phi(p_1^{k_1}) \cdot \phi(p_2^{k_2}) \cdots \phi(p_r^{k_r})$. Ettersom $\phi(n) = 8$ må $\phi(p_i) \in \{1, 2, 4, 8\}$. Vi skriver opp mulighetene: $\phi(2) = 1, \phi(3) = 2$ og $\phi(5) = 4$. Vi merker oss at for alle odde primtall p_i må $k_i \leq 1$ ellers vil $p_i|\phi(n)$, og at $\phi(2^k) > 8$ for $k > 4$. Vi må dermed sjekke tilfellene $n = 2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3}$ for $0 \leq k_1 \leq 4$, $0 \leq k_2 \leq 1$ og $0 \leq k_3 \leq 1$. Anta først $k_2 = k_3 = 0$ da må $k_1 = 4$ og $n = 2^4 = 16$. Videre får vi: $k_2 = 1, k_3 = 0$ gir $k_1 = 3$ og $n = 2^3 \cdot 3 = 24$, $k_2 = 0, k_3 = 1$ gir $k_1 = 2$ og $n = 2^2 \cdot 5 = 20$, $k_2 = k_3 = 1$ gir $k_1 = 0$ eller $k_1 = 1$ og $n = 3 \cdot 5 = 15$ eller $n = 2 \cdot 3 \cdot 5$. Oppsummert har vi at $n \in \{15, 16, 20, 24, 30\}$.

Oppgave 4.

a. Vi skal løse $13x \equiv 1 \pmod{60}$. Ettersom $\gcd(13, 60) = 1$ har denne kongruensen unik løsning. Denne kan vi finne enten ved å benytte divisjonsalgoritmen eller å prøve oss frem. Vi ser at $8 \cdot 60 = 480$ og at $13 \cdot 37 = 481$. Alle løsninger er dermed på formen $x \equiv 37 + 60t$ for $t \in \mathbb{Z}$.

b. Vi får oppgitt at den hemmelige dekrypteringsnøkkelen er $\{n, d\} = \{7 \cdot 11, 13\}$. Vi vet at e velges slik at $ed \equiv 1 \pmod{\phi(n)}$ som gir $13e \equiv 1 \pmod{60}$. Fra forrige oppgave ser vi at dette gir $\{n, e\} = \{77, 37\}$.

c. Beskjeden finner vi ved: $m \equiv N^d \equiv 20^{13} \equiv 69 \pmod{77}$.

Oppgave 5.

a. Se bok.

b. Ettersom $\phi(17) = 16$ søker vi a slik at $k = 16$ er den minste k som gir $a^k \equiv 1 \pmod{17}$. Vi husker at det er nok å prøve alle k slik at $k|16$. For $a = 2$ har vi $2^8 \equiv 1 \pmod{17}$ mens $3^k \not\equiv 1 \pmod{17}$ for $k = 1, 2, 4, 8$. Dermed må $3^{16} \equiv 1 \pmod{17}$ og 3 er en primitiv rot modulo 17. Alle andre primitive røtter er da på formen 3^m for $m < \phi(n) = 16$ med $\gcd(m, \phi(n)) = \gcd(m, 16) = 1$.

c. Vi merker oss at $4^q = 2^{2q} = 2^{p-1} \equiv 1 \pmod p$, der den siste likheten følger fra Fermats teorem. Siden $\phi(p) = p - 1 = q$ og q er primtall, kan det ikke finnes $1 < k < q$ slik at $4^k \equiv 1 \pmod p$, og vi konkluderer med at 4 er en primitiv rot modulo p.

Oppgave 6. Vi bruker hintet og løser likningen modulo 5. Modulo 5 gir Fermats teorem at $m^5 \equiv m$ og vi sitter igjen med $n^2 \equiv -2 \equiv 3 \pmod 5$. Ettersom $n^2 \not\equiv 3 \pmod 5$ for $n = 0, 1, 2, 3, 4$ følger det at likningen ikke har noen løsninger.

Date: 16. desember 2012.

Oppgave 7. Merk at $311 \equiv 7 \pmod{19}$ og at $64 = 7 + 3 \cdot 19$. Dermed er $x^2 \equiv 7 \pmod{19}$ for $x \equiv 8 \pmod{19}$. For del b) bruker vi teoremet om kvadratisk resiprositet: $(19/311) \cdot (311/19) = (19/311) \cdot 1 = (-1)^{(310/2)\cdot(18/2)} = -1$. Det finnes altså ikke x slik at $x^2 \equiv 19 \pmod{311}$.