MA1301 TALLTEORI, HØST 2015
LØSNINGSFORSLAG – ØVING 10

Avsnitt 8.1

Oppgave 1. Vi finner ordenen til tallene 2, 3 og 5 modulo 17 og 19. Fra Teorem 8.1 vet vi at ordenen deler hhv. $\varphi(17) = 16$ eller $\varphi(19) = 18$. Så modulo 17 er alle mulige ordener divisorer av 16, nemlig 1, 2, 4, 8 eller 16.

Modulo 17 har vi

$$2^2 \equiv 4; \quad 2^4 \equiv 4^2 \equiv -1 \pmod{17},$$

så $2^8 \equiv 1 \pmod{17}$. Videre er

$$3^2 \equiv 9; \quad 3^4 \equiv 9^2 \equiv 13; \quad 3^8 \equiv 13^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17},$$

så $3^{16} \equiv 1 \pmod{17}$. Til slutt har vi

$$5^2 \equiv 8; \quad 5^4 \equiv 8^2 \equiv 13; \quad 5^8 \equiv 13^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17},$$

så $5^{16} \equiv 1 \pmod{17}$. Dette betyr at ordenen til 2, 3 og 5 modulo 17 er hhv. 8, 16 og 16.

Nå gjør vi det samme modulo 19. Her er ordenen en divisor av 18, så den er 1, 2, 3, 6, 9 eller 18.

$$2^2 \equiv 4; \quad 2^3 \equiv 8; \quad 2^6 \equiv 8^2 \equiv 7; \quad 2^9 \equiv 2^3 2^6 \equiv 8 \cdot 7 \equiv -1 \pmod{19},$$

så $2^{18} \equiv 1 \pmod{19}$. Vi har også

$$3^2 \equiv 9; \quad 3^3 \equiv 8; \quad 3^6 \equiv 8^2 \equiv 7; \quad 3^9 \equiv 3^3 3^6 \equiv 8 \cdot 7 \equiv -1 \pmod{19},$$

så $3^{18} \equiv 1 \pmod{19}$. Til slutt har vi

$$5^2 \equiv 6; \quad 5^3 \equiv 5 \cdot 6 \equiv 11; \quad 5^6 \equiv (-8)^2 \equiv 7; \quad 5^9 \equiv 5^3 5^6 \equiv 11 \cdot 7 \equiv 1.$$

Så ordenen til 2, 3 og 5 modulo 19 er hhv. 18, 18 og 9.

Oppgave 2a. Anta at a har orden hk modulo n. Dette betyr at hk er det minste tallet slik at $a^{hk} \equiv 1 \pmod{n}$. Da er $(a^h)^k \equiv a^{hk} \equiv 1 \pmod{n}$. Men k er det minste tallet slik at $(a^h)^k \equiv 1 \pmod{n}$, så k er ordenen til a^h modulo n. For å se dette, anta at $1 \equiv (a^h)^{k'} \equiv a^{hk'} \pmod{n}$. Da er $hk' \geq hk$ (fordi hk er ordenen til a modulo n), så $k' \geq k$.

Oppgave 2b. Anta at a har orden $2k$ modulo p. Da er $0 \equiv a^{2k} - 1 \equiv (a^k - 1)(a^k + 1) \pmod{p}$. Ved definisjon betyr dette at $p \mid (a^k - 1)(a^k + 1)$, så $p \mid (a^k - 1)$ eller $p \mid (a^k + 1)$. Men nå bruker vi at $2k$ er ordenen til a, som betyr at $a^k \not\equiv 1 \pmod{p}$ eller, ekvivalent, at $p \nmid (a^k - 1)$. Dermed har vi at $p \mid (a^k + 1)$, som gir $a^k \equiv -1 \pmod{p}$.

Oppgave 4. Vi har at $a^h \equiv 1 \pmod{n}$ og $b^k \equiv 1 \pmod{n}$. Dermed blir

$$(ab)^{hk} \equiv (a^h)^k (b^k)^h \equiv 1^k 1^h \equiv 1 \pmod{n}.$$

Så hvis l er ordenen til ab, må $l | hk$.

Hvis $\gcd(h, k) = 1$ så kan vi skrive $l = h_1 k_1$ der $h_1 | h$ og $k_1 | k$, dvs $h = h_1 h_2$ og $k = k_1 k_2$. Da har vi (mod n):

$$(ab)^{h_1 k_1} \equiv 1 \implies (ab)^{h_1 k_1 k_2} = (a^k)^{h_1} (b^k)^{h_1} \equiv 1 \implies (a^k)^{h_1} \equiv 1.$$

I følge Thm.8.3 har a^k orden h, altså er $h_1 = h$. Tilsvarende vises at $k_1 = k$. Altså er $l = hk$.

Date: 22. oktober 2015.

Oppgave 5. Vi antar at a har orden 3 modulo p, hvor p er et odde primtall. Dette betyr at $p \mid (a^3-1)$ (siden $a^3 \equiv 1 \pmod{p}$). Nå er $a^3-1 = (a-1)(a^2+a+1)$, så $p \mid (a-1)$ eller $p \mid (a^2+a+1)$. Men $p \mid (a-1)$ vil medføre at a har orden 1 modulo p, så vi må ha at $p \mid (a^2+a+1)$, dvs. $a^2+a+1 \overset{*}{\equiv} 0 \pmod{p}$.

For å vise at $a+1$ har orden 6 må vi vise at $(a+1)^6 \equiv 1 \pmod{p}$ og at det ikke finnes noen eksponent $0 < k < 6$ slik at $(a+1)^k \equiv 1 \pmod{p}$.

Vi har at $(a+1)^2 \equiv a^2+2a+1 \overset{*}{\equiv} a \pmod{p}$, så $(a+1)^6 \equiv a^3 \equiv 1 \pmod{p}$. La k være ordenen til $a+1$ modulo p. Ved teorem 8.1 er $k \mid 6$, altså er ordenen 1, 2, 3 eller 6.

$a+1 \not\equiv 1 \pmod{p}$ siden $a \not\equiv 0 \pmod{p}$. Vi har også $(a+1)^2 \overset{*}{\equiv} a \not\equiv 1 \pmod{p}$. Til slutt er $(a+1)^3 \overset{*}{\equiv} a(a+1) \overset{*}{\equiv} -1 \not\equiv 1 \pmod{p}$. Dette viser at verken 1, 2 eller 3 er ordenen, og dermed er 6 ordenen til $a+1$ modulo p.

Oppgave 6a. Anta $p \mid n^2+1$, hvor p er et odde primtall. Da har vi at $n^2 \equiv -1 \pmod{p}$, så $n^4 \equiv 1 \pmod{p}$. Ved teorem 8.1 er da 4 ordenen til tallet n modulo p (fordi ordenen k oppfyller $k \mid 4$, men verken 1 eller 2 er ordenen). Videre følger det av teorem 8.1 at $4 \mid \varphi(p)$, så det finnes en k slik at $4k = p-1$. Med andre ord er $p = 4k+1$.

Oppgave 11a. Vi skal finne to primitive røtter av 10. Det vil si, vi vil finne to a med orden $\varphi(10) = 4$ modulo 10. For at a skal ha en orden, så må vi ha $\gcd(a, 10) = 1$. Hvis vi krever at $0 \le a < 10$ må a være blant $1, 3, 7, 9$.

Nå har 1 orden 1 og $9 \equiv -1 \pmod{10}$ orden 2, så dersom oppgaven skal være løsbar må både 3 og 7 være de tallene med orden 4, ved korollaret på side 151. La oss sjekke dette:

$$3^2 \equiv -1; \quad 3^4 \equiv (-1)^2 \equiv 1 \pmod{10},$$

$$7^2 \equiv -1; \quad 7^4 \equiv (-1)^2 \equiv 1 \pmod{10},$$

så både 3 og 7 har orden 4. (Alle tall som er kongruente med 3 og 7 modulo 10 har også orden 4, så her er det mange mulige svar!)

Oppgave 11b. Vi har opplyst at $a = 3$ er en primitiv rot av 17, altså at 3 har orden $\varphi(17) = 16$ modulo 17. Ved korollaret på side 151 vet vi da at 17 har $\varphi\big(\varphi(17)\big) = \varphi(16) = 8$ inkongruente primitive røtter modulo 17.

Ved teorem 8.4 er de 8 primitive røttene å finne blant $\{a, a^2, a^3, \ldots, a^{16}\}$. Ved teorem 8.3 har da a^h orden $16/\gcd(h, 16)$. Så for at a^h skal være en primitiv rot (ha orden 16) må vi velge h relativt primisk til 16. Dermed er de primitive røttene:

$$\{a, a^3, a^5, a^7, a^9, a^{11}, a^{13}, a^{15}\}$$

Nå er $a = 3$, så vi kan regne ut tallene a^h modulo 17.

$$3^1 \equiv 3; \quad 3^3 \equiv 10; \quad 3^5 \equiv 5; \quad 3^7 \equiv 11; \quad 3^9 \equiv 14; \quad 3^{11} \equiv 7; \quad 3^{13} \equiv 12; \quad 3^{15} \equiv 6 \pmod{17}$$

er en fullstendig liste av de 8 inkongruente primitive røttene til 17.

Eksamen høst 2003

Oppgave 4a*. Ligninga $7x \equiv 1 \pmod{40}$ har løsninger hvis og bare hvis $d = \gcd(7, 40) \mid 1$. Da har man d inkongruente løsninger. Ved Euklids algoritme finner man at $d = 1$, så ligninga har én inkongruent løsning, og at $1 = 3 \cdot 40 - 17 \cdot 7$. Modulo 40 får vi da

$$1 \equiv -17 \cdot 7 \equiv 23 \cdot 7 \pmod{40},$$

så $x \equiv 23 \pmod{40}$.

Oppgave 4b*. Husk at hvis $\{n, e\} = \{55, 7\}$ så er den hemmelige nøkkelen i RSA gitt ved $\{n, d\}$ hvor $de \equiv 1 \pmod{\varphi(n)}$. Nå er $\varphi(55) = 4 \cdot 10 = 40$, så vi søker en løsning av ligninga

$$7d \equiv 1 \pmod{40}.$$

Denne løste vi i del a, og vi fikk at $d \equiv 23 \pmod{40}$. Dermed er den hemmelige nøkkelen (husk at $0 < d < \varphi(n)$) $\{n, d\} = \{55, 23\}$.

Oppgave 4c*. Nå skal kryptere meldinga $M = 13$. Det betyr å finne resten til M^e modulo n, altså å regne ut 13^7 modulo 55. La oss gjøre noen mellomregninger:

$$13^2 \equiv 4; \quad 13^4 \equiv 4^2 \equiv 16 \pmod{55}.$$

Fra dette får vi at

$$13^7 \equiv 13^4 \cdot 13^2 \cdot 13 \equiv 16 \cdot 4 \cdot 13 \equiv 7 \pmod{55}.$$

Den krypterte meldinga er derfor 7.

Oppgave 5. La p og q være tvillingprimtall. Ett av disse tallene er størst, og vi kan anta at $p < q$, dvs. $q = p + 2$ (hvis ikke bytter vi om navnene på p og q). Siden q er et primtall, sier Wilsons teorem at $(q-1)! \equiv -1 \pmod{q}$. Nå er $-(q-1) \equiv 1 \pmod{q}$, og $(q-2)! = p!$ så vi har at

$$p! \equiv 1 \cdot (q-2)! \equiv -(q-1) \cdot (q-2)! \equiv -(q-1)! \equiv -(-1) \equiv 1 \pmod{q}.$$

Men den andre kongruensen holder ikke, fordi

$$q! \equiv (p+2)! \equiv (p+2)(p+1)p \cdot (p-1)! \equiv 0 \not\equiv 1 \pmod{p}.$$

Dette viser at nøyaktig én av kongruensene holder.

Eksamen høst 2004

Oppgave 7a*. Vi lar a og n være relativt primiske, og k være ordenen til a modulo n. Vi viser at for $t \geq 1$ så er

$$a^t \equiv 1 \pmod{n} \iff k \mid t.$$

Først antar vi at $k \mid t$. Da har vi at $t = kq$, så $a^t \equiv (a^k)^q \equiv 1^q \equiv 1 \pmod{n}$. Dette viser implikasjonen mot venstre.

Nå antar vi at $k \nmid t$. Da er $t = kq + r$, hvor $0 < r < k$. Da er $a^t \equiv a^{kq+r} \equiv (a^k)^q a^r \equiv 1^q a^r \equiv a^r \pmod{n}$. Men siden $0 < r < k$, og k er ordenen til a, så har vi at $a^r \not\equiv 1 \pmod{n}$. Dermed er $a^t \not\equiv 1 \pmod{n}$. Dette viser det kontrapositive utsagnet, altså har vi vist implikasjonen mot høyre.

Oppgave 7b*. 7 er en primitiv rot av 11 hvis 7 har orden 10 modulo 11. Vi vet at ordenen må dele $10 = \varphi(11)$ (teorem 8.1). Så ordenen er 1, 2, 5 eller 10. Den er opplagt ikke 1, siden $7^1 \equiv 7 \pmod{11}$. Den er heller ikke 2 siden $7^2 \equiv 5 \pmod{11}$. Nå er $7^5 \equiv 7 \cdot (7^2)^2 \equiv 7 \cdot 5^2 \equiv -1 \pmod{11}$, så ordenen er heller ikke 5. Dermed kan vi konkludere med at ordenen er 10, og derfor er 7 en primitiv rot av 11.

Siden 37 er et primtall vet vi fra korollaret på side 155 at vi har nøyaktig $\varphi(36) = \varphi(2^2)\varphi(3^2) = 2 \cdot 6 = 12$ inkongruente primitive røtter.