LØSNINGSFORSLAG EKSAMEN MA1301 HØST 2010

Oppgave 1. Kinesiske restteorem: setter

$$N_1 = 11 \cdot 7 = 77, \qquad N_2 = 8 \cdot 7 = 56, \qquad N_3 = 8 \cdot 11 = 88$$

og finner tre spesielle løsninger av kongruensene

$$N_1 x_1 \equiv 1 \pmod 8 \rightsquigarrow 77x_1 \equiv 1 \pmod 8 \rightsquigarrow x_1 = -3$$

$$N_2 x_2 \equiv 1 \pmod{11} \rightsquigarrow 56x_2 \equiv 1 \pmod{11} \rightsquigarrow x_2 = 1$$

$$N_3 x_3 \equiv 1 \pmod 7 \rightsquigarrow 88x_3 \equiv 1 \pmod 7 \rightsquigarrow x_3 = 2$$

Så setter vi

$$\overline{x} = 3N_1x_1 + 9N_2x_2 + 4N_3x_3 = 3 \cdot 77 \cdot (-3) + 9 \cdot 56 \cdot 1 + 4 \cdot 88 \cdot 2 = 515.$$

Siden $8 \cdot 11 \cdot 7 = 616$ blir løsningen på systemet

$$x \equiv 515 \pmod{616},$$

og den minste positive løsningen er $x_0 = 515$.

Oppgave 2. Siden 67 er et primtall gir Wilsons teorem at $66! \equiv -1 \pmod{67}$, og sammen med kongruensen $-1 \equiv 66 \pmod{67}$ gir dette at

$$66! \equiv 66 \pmod{67}.$$

Vi kan dele ut 66 fordi $\gcd(66, 67) = 1$, og da får vi

$$65! \equiv 1 \pmod{67}.$$

Derfor:

$$65! + 70 \equiv 1 + 70 = 71 \equiv 4 \pmod{67}.$$

Vi får en rest på 4.

Oppgave 3. Anta at det bare finnes endelig mange slike primtall, og kall dem $p_1, p_2, \ldots, p_t$. Se deretter på tallet

$$n = 4p_1p_2 \cdots p_t - 1.$$

Siden

$$n \equiv -1 \equiv 3 \pmod 4$$

må n være et oddetall (et partall er enten kongruent med 0 eller 2 modulo 4). Derfor må enhver primtallsdivisor av n være et oddetall. La $q_1, \ldots, q_s$ være primtallsdivisorene i n, dvs at

$$n = q_1q_2 \cdots q_s.$$

Hver q_i er et oddetall, så derfor gjelder enten $q_i \equiv 1 \pmod 4$ eller $q_i \equiv 3 \pmod 4$. Hvis $q_i \equiv 1 \pmod 4$ for alle $1 \leq i \leq s$, så kan vi gange sammen alle kongruensene

$$\begin{aligned} q_1 &\equiv 1 \pmod 4 \\ q_2 &\equiv 1 \pmod 4 \\ &\vdots \\ q_2 &\equiv 1 \pmod 4 \end{aligned}$$

og få $n \equiv 1 \pmod 4$. Men n er ikke kongruent med 1 modulo 4, så for minst en i må vi ha $q_i \equiv 3 \pmod 4$. Men $p_1, p_2, \ldots, p_t$ er jo alle primtallene som er kongruent med 3 modulo 4, så derfor må q_i finnes blant $p_1, p_2, \ldots, p_t$. Dette betyr at n er delelig med minst ett av primtallene $p_1, p_2, \ldots, p_t$, noe som er umulig siden n gir rest -1 når vi deler på hvert av de tallene.

Oppgave 4. (a) Har at $\phi(161) = \phi(7 \cdot 23) = (7-1) \cdot (23-1) = 132$. Tallet d er det unike tallet som tilfredsstiller

$$ed \equiv 1 \pmod{\phi(161)}, \qquad 1 < d < \phi(161),$$

det vil si

$$25d \equiv 1 \pmod{132}, \qquad 1 < d < 132.$$

Bruker Euklids algoritme:

$$\begin{aligned} 132 &= 5 \cdot 25 + 7 \\ 25 &= 3 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1, \end{aligned}$$

og når vi jobber oss bakover får vi $25 \cdot 37 - 1 = 7 \cdot 132$, dvs

$$25 \cdot 37 \equiv 1 \pmod{132}, \qquad 1 < 37 < 132.$$

Derfor er $d = 37$, og den hemmelige nøkkelen er da $\{n, d\} = \{161, 37\}$.

(b) For å kryptere en melding M må man regne ut hva M^e er kongruent med modulo n, så vi må finne 2^{25} modulo 161. Vi har

$$2^8 = 256 \equiv 95 \pmod{161},$$

som gir

$$2^{24} \equiv 95^3 = 857375 \equiv 50 \pmod{161}.$$

Dette gir

$$2^{25} \equiv 50 \cdot 2 = 100 \pmod{161},$$

så den krypterte meldingen er $C = 100$.

Oppgave 5. Anta at $\sqrt{pq}$ er et rasjonalt tall. Da finnes to heltall a, b slik at $\sqrt{pq} = a/b$ og $\gcd(a, b) = 1$. Kvadrering gir

$$pqb^2 = a^2.$$

Da må p dele a^2, som igjen medfører at p deler a siden p er et primtall. Dette betyr at $a = pn$ for et tall n, og når vi setter inn i ligningen over får vi

$$pqb^2 = a^2 = p^2n^2.$$

Vi deler så ut p og får

$$qb^2 = pn^2.$$

Da må p dele qb^2, og siden $\gcd(p, q) = 1$ (husk at p og q er ulike primtall) må p da dele b^2, og dette igjen medfører at p deler b. Vi har nå vist at p deler både a og b, men dette er umulig siden $\gcd(a, b) = 1$. Med andre ord har vi en motsigelse, så $\sqrt{pq}$ kan ikke være et rasjonalt tall.

Merk at vi også kunne ha argumentert på samme måte med rollene til p og q byttet om.

Oppgave 6. (a) La x være antall medlemmer og y være antall ikke-medlemmer. Den totale inngangssummen s er da gitt ved

$$34x + 85y = s.$$

Dette betyr at $\gcd(34, 85)$ må dele s, altså at 17 må dele s. Derfor må s tilfredsstille

$$38100 < s < 38130, \qquad 17 \mid s,$$

så eneste mulighet er $s = 38114$.

(b) Vi løser først den diofantiske ligningen

$$34x + 85y = 38114.$$

Først må vi skrive $\gcd(34, 85)$, altså 17, som en lineærkombinasjon av 34 og 85. En mulighet er å bruke Euklids algoritme, men man kan kanskje også se direkte at

$$34 \cdot (-2) + 85 \cdot 1 = 17.$$

Dette git

$$38114 = 17 \cdot 2242 = 34 \cdot (-4484) + 85 \cdot 2242,$$

så $x_0 = -4484$ og $y_0 = 2242$. Alle løsningene er da gitt ved

$$\begin{array}{rclcl} x & = & x_0 + (85/17)t & = & 5t - 4484 \\ y & = & y_0 - (34/17)t & = & 2242 - 2t \end{array}$$

for heltall t. Vi vet at x må tilfredsstille $900 \leq x \leq 905$, med andre ord at

$$900 \leq 5t - 4484 \leq 905.$$

Dette gir

$$1076.8 \leq t \leq 1077.8,$$

så siden t er et heltall må vi ha $t = 1077$. Derfor:

$$\begin{array}{rclcl} x & = & 5 \cdot 1077 - 4484 & = & 901 \\ y & = & 2242 - 2 \cdot 1077 & = & 88, \end{array}$$

så det var 901 medlemmer og 88 ikke-medlemmer på konserten.

Oppgave 7. Vi splitter opp tallet 2010 i primtall: $2010 = 2 \cdot 3 \cdot 5 \cdot 67$. Da ser vi at $\gcd(2010, 13) = 1$, så Eulers teorem gir

$$13^{\phi(2010)} \equiv 1 \pmod{2010}.$$

Siden

$$\phi(2010) = \phi(2 \cdot 3 \cdot 5 \cdot 67) = (2-1) \cdot (3-1) \cdot (5-1) \cdot (67-1) = 528$$

får vi altså kongruensen

$$13^{528} \equiv 1 \pmod{2010}.$$

For hver $n \geq 1$ kan vi opphøye begge sider i n og få

$$13^{528n} \equiv 1^n = 1 \pmod{2010},$$

som nettopp betyr at 2010 deler $13^{528n} - 1$.

Oppgave 8. Tvillingprimtall er odde primtall som ligger så nær hverandre som mulig, altså er avstanden mellom dem 2. Det betyr at enten er $p = q + 2$ eller så er $p = q - 2$. Siden begge primtallene er odde sier loven om kvadratisk resiprositet at

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

hvor (p/q) og (q/p) er Legendre-symbol. Siden p og q er tvillingprimtall, så er ett av dem på formen $4k+1$ og det andre på formen $4k+3$. Hvis p er på formen $4k+1$ så er $\frac{p-1}{2}$ et partall, mens hvis q er på formen $4k+1$ så er $\frac{q-1}{2}$ et partall. Uansett er $\frac{p-1}{2} \cdot \frac{q-1}{2}$ et partall, så høyresiden i ligningen må være 1, dvs

$$(p/q)(q/p) = 1.$$

Dette betyr at $(p/q) = (q/p)$, siden et Legendre-symbol har verdien ± 1. Med andre ord: kongruensen

$$x^2 \equiv p \pmod{q}$$

er løsbar hvis og bare hvis kongruensen

$$x^2 \equiv q \pmod{p}$$

er løsbar.