Løysingsforslag til eksamen i MA1301-Talteori, 30/11-2005.

Oppgåve 1

a) Rekn ut $\gcd(788, 116)$. Finn alle løysingane i heile tal til likninga

$$788x + 116y = \gcd(788, 116).$$

b) Ein antikvar sel ein dag nokre bøker for 116 kroner stykket, og kjøper nokre bøker for 788 kroner stykket. Når dagen er over har ho 24 kroner meir enn ho hadde om morgonen. Kva er det minste antallet bøker ho kan ha selt denne dagen? Og kva er det minste antallet bøker ho kan ha kjøpt?

Svar a) Euklids algoritme:

$$\begin{aligned} 788 &= 6.116 + 92 \\ 116 &= 1.92 + 24 \\ 92 &= 3.24 + 20 \\ 24 &= 1.20 + 4 \\ 20 &= 5.4 + 0 \end{aligned}$$

Største felles divisor finn vi som den siste resten som ikkje er null: $\gcd(788, 116) = 4$.

For å løyse likninga går vi attende gjennom Euklids algoritme:

$$\begin{aligned} 4 = \; & 24 - 20 = 24 - (92 - 3.24) = 4.24 - 92 \\ & = 4.(116 - 92) - 92 = 4.116 - 5.92 = 4.116 - 5.(788 - 6.116) \\ & = 34.116 - 5.788 \end{aligned}$$

Dermed har vi funne ei spesiell løysing, $x_0 = -5, y_0 = 34$. Generell løysing:

$$\begin{aligned} x &= x_0 + \tfrac{b}{d}t = -5 + \tfrac{116}{4}t = -5 + 29t \\ y &= y_0 - \tfrac{a}{d}t = 34 - \tfrac{788}{34}t = 34 - 197t \end{aligned}$$

Her er t eit vilkårleg heiltal.

b) Vi skal sjå på likninga $788x + 116y = 24$. Her er x *minus* antall bøker ho har kjøpt, og y er antall bøker ho har selt. Vi veit at ei likning av typen $ax + by = c$ har løysing akkurat når $d|c$, der $d = gcd(a, b)$. Frå a) veit vi at $d = 4$, og $4|24 = 6.4$, så likninga har løysing. Vi finn ei løysing ved å multiplisere løysinga frå a) med $\frac{c}{d} = 6$, og den generelle løysinga er gitt frå denne spesielle på same måten som i a). Vi finn

$$\begin{aligned} x &= x_0 + \tfrac{b}{d}t = -30 + 29t \\ y &= y_0 - \tfrac{a}{d}t = 204 - 197t \end{aligned}$$

Sidan x er eit negativt tal, og y eit positivt tal, får vi krava

$$0 > x = -30 + 29t \quad \Leftrightarrow \quad t < 2$$
$$0 < y = 204 - 197t \quad \Leftrightarrow \quad t < 2$$

(hugs at t er eit heiltal); Vi ser at det minste antallet bøker ho kan ha kjøpt er ei (med $t = 1$), og det gir òg det minste antallet ho kan ha selt, 7 bøker.

Oppgåve 2

a) Finn alle løysingane til dei samtidige kongruensane

$$x \equiv 3 \,(\mathrm{mod}\ 5)$$
$$x \equiv 2 \,(\mathrm{mod}\ 6)$$
$$x \equiv 6 \,(\mathrm{mod}\ 7).$$

b) Forklar kvifor likningssystemet

$$3x + 7y \equiv 2 \,(\mathrm{mod}\ 8)$$
$$4x + 5y \equiv 7 \,(\mathrm{mod}\ 8)$$

har ei og berre ei løysing modulo 8. Løys systemet.

Svar a) Sidan $\gcd(5, 6) = \gcd(5, 7) = \gcd(6, 7) = 1$ kan vi løyse desse samtidige kongruensane ved det kinesiske restklasseteoremet. Vi skal da løyse tre hjelpelikningar:

$$N_1 x_1 = 42x_1 \equiv 2x_1 \equiv 1 \,(\mathrm{mod}\ 5)$$

$$N_2 x_2 = 35x_2 \equiv -x_2 \equiv 1 \,(\mathrm{mod}\ 6)$$

$$N_3 x_3 = 30x_3 \equiv 2x_3 \equiv 1 \,(\mathrm{mod}\ 7)$$

Vi kan finne løysingane ved å bruke Euklids algoritme; t.d. for x_1: $5 = 2.2 + 1$ gir $1 = 5 - 2.2$ eller $1 \equiv -2.2 \equiv 3.2 \,(\mathrm{mod}\ 5)$, så $x_1 \equiv 3 \,(\mathrm{mod}\, 5)$. På same måten får vi $x_2 \equiv -1 \,(\mathrm{mod}\ 6)$ og $x_3 \equiv 4 \,(\mathrm{mod}\ 7)$. Frå teoremet får vi løysinga på dei samtidige kongruensane som

$$x \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \,(\mathrm{mod}\ N)$$
$$x \equiv 3.42.3 + 2.35.(-1) + 6.30.4 \equiv 1028 \equiv 188 \,(\mathrm{mod}\ 210)$$

b) Likningssystemet har ei og berre ei løysing om og berre om determinanten er relativt primisk til modulus 8. Determinanten er $ad - bc = 3.5 - 7.4 = -13$ som er eit oddetal, så $\gcd(-13, 8) = 1$ og vi har ei og berre ei løysing. For å finne x, ta 5 gonger den første likninga, og trekk frå 7 gonger den andre. Det gir

$$-13x \equiv 10 - 49 \equiv -39 \,(\mathrm{mod}\, 8)$$

som har løysinga $x \equiv 3 \,(\mathrm{mod}\ 8)$ (Euklids algoritme). For å finne y, ta tre gonger den andre likninga og trekk frå 4 gonger den første. Det gir

$$-13y \equiv 21 - 8 \equiv 13 \,(\mathrm{mod}\ 8)$$

som har løysinga $y \equiv -1 \equiv 7 \,(\mathrm{mod}\ 8)$.

Oppgåve 3

a) Du skal setje opp eit RSA-system for å motta hemmelege meldingar. Den hemmelege nøkkelen vel du til å vere $\{n, d\} = \{91, 29\}$. Kva vert den offentlege nøkkelen $\{n, e\}$?

b) Den første hemmelege meldinga du får er 9. Dekrypter denne meldinga.

Svar: a) Samanhengen mellom den hemmelege og den offentlege nøkkelen er at $de \equiv 1 \,(\mathrm{mod}\ \phi(n))$. Vi må altså løyse $29e \equiv 1 \,(\mathrm{mod}\ 72)$ ($\phi(91) = \phi(7.13) = (7-1)(13-1) = 72$). Euklids algoritme: $72 = 2.29 + 14$, $29 = 2.14 + 1$. Vi ser at $\gcd(72, 29) = 1$, så den hemmelege koden er i orden, og vi kan løyse likninga! $1 = 29 - 2.14 = 29 - 2(72 - 2.29) = 5.29 - 2.72$, så $1 \equiv 5.29 \,(\mathrm{mod}\ 72)$. Vi må velje den minste positive resten, og får $e = 5$. Den offentlege nøkkelen er altså $\{n, e\} = \{91, 5\}$.

b) Når vi skal dekryptere, må vi rekne ut $9^{29} (\mathrm{mod}\ 91)$ (altså bruke den hemmelege nøkkelen, og finne den minste positive resten). Vi får:

$$\begin{aligned} 9^2 &\equiv 81 \equiv -10 \,(\mathrm{mod}\ 91) \\ 9^3 &\equiv -90 \equiv 1 \,(\mathrm{mod}\ 91) \\ 9^{27} &\equiv 9^{3^9} \equiv 1^9 \equiv 1 \,(\mathrm{mod}\ 91) \\ 9^{29} &= 9^{27}.9^2 \equiv 1.81 \equiv 81 \,(\mathrm{mod}\ 91), \end{aligned}$$

så den dekrypterte meldinga er 81.

Oppgåve 4

a) Formuler Eulers teorem (du treng ikkje vise det).

b) La a vere eit heiltal med $\gcd(a, 5) = 1$. Vis at

$$a^{61} \equiv a \,(\mathrm{mod}\ 8525).$$

Hint: $8525 = 5^2.11.31$.

c) La $n \geq 2$ og a vere heile tal. Når er ordenen til a modulo n definert? Kva er definisjonen? Kva er ordenen til 8 modulo 19?

Svar a) La $n \geq 1$ og a vere heile tal som er relativt primiske ($\gcd(a, n) = 1$). Da er $a^{\phi(n)} \equiv 1 \,(\mathrm{mod}\ n)$. Her er $\phi(n)$ Eulers $\phi-$funksjon (antall tal a, $1 \leq a \leq n$, og $\gcd(a, n) = 1$).

b) Vi bruker Eulers teorem eller Fermats teorem for kvart primtal (eller primtalspotens) i faktoriseringa.

Først 25. Sidan $\gcd(a,5) = 1$ er $\gcd(5^2, a) = 1$ og vi kan bruke Eulers teorem: $a^{20} \equiv 1 \pmod{25}$ ($\phi(5^2) = 5^2 - 5^1 = 20$) som gir

$$a^{61} \equiv (a^{20})^3.a \equiv 1^3.a \equiv a \pmod{25}$$

Så 11. Om $11|a$ er $a^n \equiv 0 \equiv a \pmod{11}$ for alle positive heiltal n, t.d. for $n = 61$. Om $11 \not| a$ seier Fermat (eller Euler) at $a^{10} \equiv 1 \,(\,mod\, 11)$, så

$$a^{61} \equiv (a^{10})^6.a \equiv 1^6.a \equiv a \pmod{11}$$

Til slutt 31. Om $31|a$ er $a^{61} \equiv 0 \equiv a \pmod{31}$. Om $31 \not| a$ er $a^{30} \equiv 1 \pmod{31}$, og derfor

$$a^{61} \equiv (a^{30})^2.a \equiv 1^2.a \equiv a \pmod{31}$$

Vi ser altså at $a^{61} \equiv a \pmod{n}$ for $n = 5^2, 11, 31$. Sidan modulane er relativt primiske, vil dette òg helde for produktet;

$$a^{61} \equiv a \pmod{5^2.11.31 = 8525}$$

c) Ordenen til a modulo n er definert om $\gcd(a,n) = 1$. Ordenen er da det minste talet $k \geq 1$ slik at $a^k \equiv 1 \pmod{n}$ (dette talet finst; Eulers teorem seier at det ikkje kan vere større enn $\phi(n)$).

Vi har at $\phi(19) = 18 = 2.3^2$. Ordenen er alltid ein divisor i $\phi(n)$, så vi må sjekke divisorane til 18 $(1, 2, 3, 6, 9, 18)$.

$$\begin{aligned} 8^2 &\equiv 64 \equiv 7 \pmod{19} \\ 8^3 &\equiv 7.8 \equiv 56 \equiv -1 \pmod{19} \\ 8^6 &\equiv (-1)^2 \equiv 1 \pmod{19} \end{aligned}$$

Så ordenen til 8 modulo 19 er 6.

Oppgåve 5
Wilsons teorem seier at $(p-1)! \equiv -1 \pmod{p}$ for alle primtal p. Vis Wilsons teorem.

Svar For $p = 2$ er $1! \equiv 1 \equiv -1 \pmod{2}$, og for $p = 3$ er $2! \equiv 2 \equiv -1 \pmod{3}$, så resulatet held for desse to tala. La no $p > 3$, og se på eit tal a med $1 \leq a \leq p-1$. Vi kan løyse likninga $ax \equiv 1 \pmod{p}$ sidan $gcd(a,p) = 1$, og vel løysinga a' som det einaste talet mellom 1 og $p-1$ som løyser ho. Da er òg a løysinga på likninga $a'x \equiv 1 \pmod{p}$. Om $a = a'$ er a ei løysing på likninga $x^2 \equiv 1 \pmod{p}$. Vi veit at ei likning av grad 2 (modulo eit primtal) ikkje kan ha meir enn 2 løysingar, og 1 og $p - 1 \equiv -1 \pmod{p}$ er to klare løysingar. Alle dei andre tala $(2, 3, \cdots, p-2)$ kan vi derfor setje i par a, a' slik at $aa' \equiv 1 \pmod{p}$. Det er altså $\frac{p-3}{2}$ slike par, og vi får

$$2.3.\cdots.(p-2) \equiv 1^{\frac{p-3}{2}} \equiv 1 \pmod{p}$$

Multipliser med $p-1$:

$$(p-1)! \equiv 1.(2.3.\cdots.(p-2)).(p-1) \equiv 1.1.(p-1) \equiv -1 \,(\text{mod } p)$$

Det var dette vi skulle vise!

Oppgåve 6

La (x, y, z) vere eit primitivt pytagoreisk trippel (altså er $x^2+y^2 = z^2$ og $\gcd(x, y, z) = 1$). Vis at akkurat eitt av tala x, y, z kan delast på 5. Finn eit døme der $5|x$, og eit døme der $5|z$.

Svar Vi ser først på dei ulike moglege verdiene av kvadrattal modulo 5:

$$\begin{aligned} a \equiv 0 &\Rightarrow a^2 \equiv 0 \,(\text{mod } 5) \\ a \equiv 1 &\Rightarrow a^2 \equiv 1 \,(\text{mod } 5) \\ a \equiv 2 &\Rightarrow a^2 \equiv 4 \,(\text{mod } 5) \\ a \equiv 3 &\Rightarrow a^2 \equiv 9 \equiv 4 \,(\text{mod } 5) \\ a \equiv 4 &\Rightarrow a^2 \equiv 16 \equiv 1 \,(\text{mod } 5) \end{aligned}$$

Særskilt har vi at a kan delast på 5 om og berre om $a^2 \equiv 0 \,(\text{mod } 5)$.

La x, y, z vere eit primitivt pytagoreisk trippel. Om z kan delast på 5 er $z^2 \equiv 0 \equiv x^2 + y^2 \,(\text{mod } 5)$, så ein av x^2 og y^2 må vere kongruent med 1, den andre med 4. Altså kan korkje x eller y delast på 5 (det at både x og y er kongruent med 0, kan ikkje skje sidan trippelet er *primitivt*). Om $z^2 \equiv 1 \equiv x^2 + y^2 \,(\text{mod } 5)$, må ein av x^2 og y^2 vere kongruent med 1, den andre med 0. Altså må akkurat ein av x og y kunne delast på 5. I det siste tilfellet, $z^2 \equiv 4 \equiv x^2 + y^2 \,(\text{mod } 5)$, må ein av x^2 og y^2 vere kongruent med 4, den andre med 0. Altså må akkurat ein av x og y kunne delast på 5.

I alle tilfella er det altså akkurat eitt av tala x, y, z som kan delast på 5.

Døme: $3^2 + 4^4 = 5^2$, $5^2 + 12^2 = 13^2$.

Jon Eivind Vatne