Tentamen i Elementär talteori, 5p **20 aug 2007 8.30 – 13.30**

Lösningar

1. Hur många inkongruenta lösningar finns det till $x^2 \equiv 11 \pmod{79}$? **(3p)**

Lösning: Enligt kvadratiska reciprocitetssatsen är $\left(\frac{11}{79}\right)\cdot\left(\frac{79}{11}\right) = -1$ *och* $\left(\frac{79}{11}\right) = \left(\frac{2}{11}\right) = -1$ *varför* $\left(\frac{11}{79}\right) = +1$. *Kongruensen har alltså* ***<u>två</u>*** *lösningar.*

2. Låt n vara ett positivt heltal. Visa att $n = 2\Phi(n) \quad \Rightarrow \quad n = 2^i$ där i är ett positivt heltal . **(3p)**

Lösning: Eftersom $\Phi(n) = n\Pi\frac{p_i - 1}{p_i}$ *där produkten löper över alla primtalsfaktorer i n kan den givna förutsättningen skrivas* $\Pi\frac{p_i}{p_i - 1} = 2$.
Genom att till exempel betrakta den största av primtalsfaktorerna ser vi att denna måste vara $= 2$ *(ingen faktor i nämnaren kan dela den största primtalsfaktorn) och följaktligen är* $n = 2^i$

3. Visa att om p är ett primtal > 3 är $2(p-3)! + 1 \equiv 0 \pmod{p}$ **(3p)**

Lösning: Enligt Wilsons sats är $(p-1)! \equiv -1 \pmod{p}$ *om p primtal så*
$-1 \equiv (p-1)! = (p-3)!(p-2)(p-1) \equiv (p-3)!(-2)(-1) = 2(p-3)! \pmod{p}$

4. Sonja har fått i uppdrag att faktorisera talet 703425623. Hon beslutar sig för att använda den metod som kallas Pollard p-1 och hittar så småningom primtalsfaktorn 12601.
Hur många iterationer krävs för att hitta faktorn 12601? **(3p)**
Ledning: utför inte iterationerna!

Lösning: Vi söker det minsta k sådant att k! är delbart med $p-1$. *Och* $p - 1 = 12600 = 2^3 3^2 5^2 7$ *varför* $k = 10$

5. Bestäm alla inkongruenta lösningar till $3x^9 \equiv 11 \pmod{13}$ **(3p)**

Ledning: 2 är en primitiv rot modulo 13

Lösning: "Logaritmering" ger $ind3 + 9indx \equiv ind11 \pmod{12}$ *det vill säga* $4 + 9indx \equiv 7 \pmod{12}$ *som leder till att* $indx \equiv 3, 7, 11 \pmod{12}$. *De inkongruenta lösningarna är följaktligen* $x = 7, 8, 11$

6. Bestäm alla positiva heltal x och y sådana att

a) $x^2 + y^2 = 967$

b) $x^2 - y^2 = 15$ **(2p)**

Lösning: $x^2 + y^2 = 967 \Rightarrow x^2 + y^2 \equiv 3 \pmod 4$ *vilket är orimligt eftersom en kvadrat är kongruent med antingen 0 eller 1.*

$x^2 - y^2 = 15 \Rightarrow (x-y)(x+y) = 15 = 5 \cdot 3$ *Eftersom* $x + y > x - y$ *får vi två fall:* $\begin{cases} x+y=5 \\ x-y=3 \end{cases} \Leftrightarrow \begin{cases} x=4 \\ y=1 \end{cases}$ *eller* $\begin{cases} x+y=15 \\ x-y=1 \end{cases} \Leftrightarrow \begin{cases} x=8 \\ y=7 \end{cases}$

7. Låt n vara ett heltal >1 och ej delbart med 5.

Visa att $n^4 + 4^n$ är sammansatt. **(4p)**

Ledning: för $n = 3, 4, 6, 7$ *är uttrycket* $= 145, 512, 5392, 18785$

Lösning: Påståendet är trivialt om n är jämnt. Betrakta alltså n udda och ej delbart med 5. Då är $4^n + 1^n$ *delbart med* $4 + 1 = 5$. *Vidare är enligt Fermats lilla sats* $n^4 \equiv 1 \pmod 5$. *Alltså är* $n^4 + 4^n \equiv 1 - 1 = 0 \pmod 5$.

Så $n^4 + 4^n$ *är delbart med 2 eller 5 och följaktligen sammansatt.*

8. Låt p och q vara udda primtal.

Visa att $\sum_{i=1}^{p} \left[q - \frac{iq}{p} \right] = \sum_{i=1}^{q} \left[p - \frac{ip}{q} \right]$

$[x]$ betecknar som vanligt heltalsdelen av x. **(4p)**

Ledning: imitera slutfasen av beviset för kvadratiska reciprocitetssatsen.

Lösning: Bägge summor uttrycker antalet av de gitterpunkter i första kvadranten som ligger under linjen $y = q - \frac{q}{p}x \Leftrightarrow x = p - \frac{p}{q}y$