Svar eller lösningar till tentamen i Elementär talteori, MMG100

Fredag 21 augusti 2015

1. Systemet som skall lösas är $\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 1 \mod 7. \\ x \equiv 4 \mod 8 \end{cases}$
   Man får att $x \equiv 1 \cdot 56 \cdot 3 + 3 \cdot 40 \cdot 1 + 3 \cdot 35 \cdot 4 = 708 \ (mod\ 280)$

   Svar: $x = 148 + 280n$ där $n \geq 0$

2. Enligt Fermats lilla sats gäller $0 = a^p + b^p - c^p \equiv a + b - c \ \ (mod\ p)$.
   Det följer att $a + b - c$ är delbart med p.

3. Enligt Wilson gäller $-1 \equiv 22! = 19! \cdot 20 \cdot 21 \cdot 22 \equiv 19! \cdot (-6) \ (mod\ 23)$

   Och eftersom $6 \cdot 4 \equiv 1 \ (mod\ 23)$ får vi att $19! \equiv 4 \ (mod\ 23)$

4. Vi har $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$

   $\left(\frac{-1}{p}\right) = \begin{cases} 1 \ om\ p \equiv 1 \ (mod\ 4) \\ -1\ om\ p \equiv 3 \ (mod\ 4 \end{cases}$ och $\left(\frac{2}{p}\right) = \begin{cases} 1 \ \ om \ \ p \equiv \pm 1 \ (mod\ 8) \\ -1\ annars \end{cases}$

   Det följer att $\left(\frac{-2}{p}\right) = 1$ om $p \equiv 1\ eller\ 3 \ (mod\ 8)$

5. Om $\Phi(n) = n - 2$ kan *n* inte vara primtal. Om $n = a \cdot b$ där $a \neq b$ blir $\Phi(n) \leq n - 3$.
   Så $n = p^a$ med *p* primtal. Eftersom $\Phi(p^a) = p^a - p^{a-1}$ blir $p = a = 2$.

   Svar: $n = 4$

6. Vi vet att $x^3 \equiv a \ (mod\ p)$ är lösbar precis när $a^{\frac{p-1}{d}} \equiv 1\ (mod\ p)$
där $d = (p-1,3)$.

   Antag nu att $p \equiv 1 \ (mod\ 3)$. Då är $d = 3$ och kongruensen
   lösbar om $a^{\frac{p-1}{3}} \equiv 1 \ (mod\ p)$.

   Men detta kan inte gälla för alla $a < p$ ty då skulle vi inte ha några primitiva rötter.

   Antag i stället att $p \equiv 2 \ (mod\ 3)$. Då blir $d = 1$ och kongruensen lösbar om $a^{p-1} \equiv 1 \ (mod\ p)$. Detta är förvisso sant för alla $a < p$.

   Svar: Alla *p* med $p \equiv 2 \ (mod\ 3)$

7. Enligt förutsättningarna är $n-1$ delbart med $ord(x)$, ordningen för *x* modulo *n*.
   Låt $n - 1 = ord(x) \cdot k$. Om $k > 1$ finns ett primtal *q* sådant att *q* delar *k*.

   Då är $x^{\frac{n-1}{q}} = \left(x^{ord(x)}\right)^{\frac{k}{q}} \equiv 1\ (mod\ n)$, vilket strider mot förutsättningarna.
   Alltså är $k = 1$ och $ord(x) = n - 1$.

   Eftersom $ord(x) \leq \Phi(n) \leq n - 1$ måste $\Phi(n) = n - 1$ och *n* är följaktligen ett primtal.