Tentamen i Elementär talteori, MMG100 17 aug 2009 8.30 – 13.30

Lösningar

1. Bestäm alla heltal x sådana att $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 2 \pmod{12} \\ x \equiv 8 \pmod{13} \end{cases}$ **(3p)**

Lösning: en enkel tillämpning av kinesiska restsatsen ger att
$x \equiv 11786 \equiv 866 \pmod{1092}$

2. Låt p vara ett udda primtal och q den minsta kvadratiska icke-resten modulo p.
Visa att q är ett primtal. **(4p)**

Lösning: Antag q sammansatt, $q = ab$ där både a och b är större än 1 och mindre än q. Men $(-1) = \left(\frac{q}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *så antingen a eller b är en icke-rest, vilket motsäger att q skulle vara den minsta.*

3. Låt p vara ett primtal och a ett positivt heltal.
Bilda $N = a^p + a \cdot (p-1)!$ Visa att N är delbart med p. **(3p)**

Lösning: $N = a^p + a \cdot (p-1)! \equiv a + a \cdot (-1) \equiv 0 \pmod p$ *enligt satser av Fermat och Wilson.*

4. Finns det något heltal x sådant att $x^2 \equiv 14 \pmod{137}$? **(3p)**

Lösning: 137 är primtal och vi söker därför $\left(\frac{14}{137}\right) = \left(\frac{2}{137}\right) \cdot \left(\frac{7}{137}\right)$. *Här är* $\left(\frac{2}{137}\right) = +1$ *eftersom* $137 \equiv 1 \pmod 8$. *Vidare är* $\left(\frac{7}{137}\right) \cdot \left(\frac{137}{7}\right) = 1$ *enligt reciprocitetssatsen och* $\left(\frac{137}{7}\right) = \left(\frac{4}{137}\right) = 1$ *så* $\left(\frac{14}{137}\right) = 1$

5. Visa att det inte existerar några positiva heltal n sådana att $\Phi(n) = \frac{n}{6}$ **(4p)**

Lösning: Om $\frac{\Phi(n)}{n} = \prod_{p \text{ delar } n} \frac{p-1}{p} = \frac{1}{6}$ *måste 3 vara det största primtal som delar n. Men i så fall kan produkten* $\prod_{p \text{ delar } n} \frac{p-1}{p}$ *bara anta värdena 2/3 resp 1/3*

6. Låt p vara ett primtal sådant att $p \equiv 1 \pmod 4$ och låt r vara en primitiv rot modulo p.
Visa att även $p - r$ är en primitiv rot modulo p. **(4p)**

Lösning: p kan skrivas $p = 4k+1$ *med k heltal så att* $\frac{p-1}{2} = 2k$ *och* $r^{2k} \equiv -1$.
Alltså är $-r \equiv r^{2k} r = r^{2k+1}$ *och eftersom* $(2k+1, 4k) = 1$ *är –r en primitiv rot.*

7. Låt p vara ett primtal sådant att $p \equiv 1 \pmod{12}$.
Beräkna $\left(\frac{3}{p}\right)$ med hjälp av Gauss lemma. **(4p)**
Kvadratiska reciprocitetssatsen får alltså inte användas!

Lösning: Vi bildar mängden $U = \left\{3, 6, 9, \ldots, 3\frac{p-1}{2}\right\}$. *Enligt Gauss lemma är* $\left(\frac{3}{p}\right) = (-1)^N$ *där N är det antal minsta positiva rester i U som är större än* $\frac{p}{2}$.
Och eftersom $3\frac{p-1}{2} < 3\frac{p}{2}$ *är det klart att N är antal element i U mellan* $\frac{p}{2}$ *och* $3\frac{p}{2}$.
Eftersom p kan skrivas $p = 12k+1$ *är* $\frac{p}{2} = 6k + \frac{1}{2}$, *och de efterfrågade elementen i U är följaktligen* $6k+3, 6k+6, 6k+9, \ldots 12k$. *De är 2k till antalet och N är därför jämnt. Alltså blir* $\left(\frac{3}{p}\right) = +1$