Talteori 6hp, Kurskod TATA54, Provkod TEN1
19 Augusti 2021
LINKÖPINGS UNIVERSITET
Matematiska Institutionen
Examinator: Jan Snellman

1) Är kongruensen

$$x^2 \equiv 97 \mod 157$$

lösbar?

Lösning:

$$\left(\frac{97}{157}\right) = \left(\frac{157}{97}\right) = \left(\frac{60}{97}\right) = \left(\frac{2}{97}\right)^2 \left(\frac{3}{97}\right)\left(\frac{5}{97}\right) = \left(\frac{97}{3}\right)\left(\frac{97}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = -1$$

så kongruensen är ej lösbar.

2) Är kongruensen

$$x^2 + y^2 \equiv 97 \mod 167$$

lösbar?

Lösning: 97 är ett primtal och $97 \equiv 1 \mod 4$, så 97 är en summa av två kvadrater, $97 = 4^2 + 9^2$. Denna likhet gäller förstås även modulo 167.

3) Är kongruensen

$$x^5 + x + 1 \equiv 0 \mod 25$$

lösbar? Ange i så fall alla lösningar. **Lösning:** Prövning ger att $x \equiv 2 \mod 5$ är den unika lösningen modulo 5. Eftersom $5 * 2^4 + 2 \neq 0 \mod 5$ så lyfter denna lösning unikt till en lösning modulo 25; man får att $x \equiv 2 + 3 * 5 \equiv 17 \mod 25$ är den unika lösningen.

4) Ge en rationell approximation till $\sqrt{11} - 3$ med ett fel mindre än $5 * 10^{-5}$.

Lösning: $\sqrt{11} - 3 = [0; \overline{3, 6}]$, med partiella konvergenter

$$0, 1/3, 6/19, 19/60, 120/379.$$

Vi ser att

$$19/60 - 120/379 = 1/22740 < 5 * 10^{-5}$$

5) Primtalsfaktorisera $5^{12} - 1$.

Lösning: Från en tidigare tenta.

6) Låt a vara ett heltal. Kan a^2 vara en primitiv rot modulo ett udda primtal p?

Lösning: Sätt $d = o(a)$, multiplikativa ordnigen av a modulo p. Då är $p-1$ jämnt, och $d|p-1$. Vidare så är $o(a^2) = d/\mathrm{sgd}(2,d)$.

Om d jämnt så är $\mathrm{sgd}(2,d) = 2$ och $o(a^2) = d/2 < d \leq p-1$, så a^2 ej primitiv rot.

Om d udda så är $\mathrm{sgd}(2,d) = 1$ och $o(a^2) = d < p-1$, ty $p-1$ jämnt, så a^2 ej primitiv rot.

7) Visa att för varje positivt heltal n så gäller att

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{\substack{p|n \\ p \text{ primtal}}} \left(1 - \frac{1}{p}\right)$$

Lösning: μ är multiplikativ, liksom $d \mapsto 1/d$, så räcker kontrollera för primpotenser.