

## Algebra II: Provtena

1. Låt  $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$  vara Eulers  $\varphi$ -funktion. Bestäm alla  $n \in \mathbb{N}$  med  $\varphi(n) = 32$ .
2. Hitta en primitiv rot för enhetsgruppen  $\mathbb{Z}_{49}^*$ .
3. Given den offentliga nyckeln  $(91, 53)$  avkoda  $\overline{41} \in \mathbb{Z}_{91}$ .
4. Ange alla idempotenta och alla nilpotenta element i restklassringen  $\mathbb{Z}_{693}$ .
5. För vilka primtal  $p$  har polynomet  $X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}_p[X]$  ett nollställe i  $\mathbb{Z}_p$ ? Kan det då faktoriseras som produkt av linjära polynom? Gör det ifall  $p = 11$ .
6. Visa: Ett ändligt integritetsområde är en kropp!
7. Faktorisera det Gaußiska heltalet  $70+i$  som produkt av Gaußiska primtal!
8. Är ringen  $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$  ett principalidealområde? Bevis eller motbevis!