

Matematiska Institutionen
KTH

Lösning till lappskrivning nummer 2A till kursen Diskret matematik för D2 och F, SF1631 och SF1630, den 24 februari 2010, kl 15.15-15.40.

Namn:

Resultat:

Bonuspoäng till tentan från denna lappskrivning är antalet godkända uppgifter nedan.

OBS Lösningarna skall motiveras väl och skrivas på detta pappers fram- och baksida. Inga hjälpmedel är tillåtna.

1. Bestäm den minsta positiva resten vid division av talet 68^{73} med talet 37.

LÖSNING: Vi observerar att 37 är ett primtal och kommer då att använda Fermats lilla sats:

$$68^{73} \equiv_{37} (68^{36})^2 \cdot 68 \equiv_{37} 1^2 \cdot 68 \equiv_{37} 37 + 31 \equiv_{37} 31$$

Svar: 31.

2. Bestäm *antalet* lösningar till ekvationen $x^2 - 4x + 3 = 0$ i ringen Z_{770} .

LÖSNING: En kvadratkomplettering ger ekvationen

$$(x - 2)^2 = 1 ,$$

så antalet lösningar blir lika med antalet lösningar till en ekvation $z^2 = 1$ i den givna ringen.

Vi observerar att $770 = 2 \cdot 5 \cdot 7 \cdot 11$, och att talen 2, 5, 7, och 11 är parvis relativt prima. Vi kan då enligt kinesiska restsatsen transformera våra räkningar till räkningar i den direkta produkten $Z_2 \times Z_5 \times Z_7 \times Z_{11}$ genom sambandet

$$z^2 = 1 \iff (z_1^2, z_2^2, z_3^2, z_4^2) = (1, 1, 1, 1) ,$$

där $z_1 = z \pmod{2}$, $z_2 = z \pmod{5}$, $z_3 = z \pmod{7}$ och $z_4 = z \pmod{11}$.

Det är lätt att kontrollera att i var och en av ringarna Z_5 , Z_7 och Z_{11} finns precis två rötter till ekvationen $y^2 = 1$ men att i ringen Z_2 finns bara en. Totalt har alltså ekvationen

$$(z_1^2, z_2^2, z_3^2, z_4^2) = (1, 1, 1, 1) ,$$

precis åtta lösningar vilket också blir vårt svar.