MMG100 Elementär talteori
Kortfattade lösningar till tentamen 23: augusti 2019

1. Kinesiska restsatsen ger
   $x = 3 \cdot 35 \cdot 3 + 2 \cdot 28 \cdot 4 + 6 \cdot 20 \cdot 6 = 1259 \equiv 139 \ (mod\ 140)$

2. Vi har $-1 \equiv 88! \equiv 84!\,(-4)(-3)(-2)(-1) \equiv 24 \cdot 84! \ (mod\ 89)$
   Vi söker alltså inversen till $-24 \equiv 65 \ (mod\ 89)$ som man till exempel med hjälp av Euklides bestämmer till 63.
   Svar: $84! \equiv 63 \ (mod\ 89)$

3. Genom att bilda index får vi $ind8 + 7indx \equiv ind5 \ (mod 12)$, dvs
   $3 + 7indx \equiv 9 \ (mod\ 12)$ så att $indx \equiv 6 \ (mod 12)$
   Alltså blir $x \equiv 2^6 \equiv 12 \ (mod\ 13)$

4. Eftersom $\Phi(n) = \prod \ (p^a - p^{a-1})$ där produkten bildas över alla primtal *p* som delar *n* och varje faktor är jämn om $p > 2$ är det klart att n bara kan innehålla högst ett udda primtal, dvs $n = 2^a p^b$ och $\Phi(n) = 2^{a-1}p^{b-1}(p-1)$.
   Vi får följande lösningar:
   $n = 1, n = 2, n = 4, n = p^a, n = 2p^a$, där *p* är ett udda primtal med $p \equiv 3 \ (mod\ 4)$

5. Enligt sats är $ord(2^i) = \frac{ord(2)}{(ord(2),i)}$ som alltså skall vara =9. Eftersom 2 är en primitiv

   rot är $ord(2) = 36$ och vi söker *i* med $(36, i) = 4$, dvs *i* delbart med 4 men inte med 3. Alltså $i = 4, 8, 16, 20, 28, 32$, och de tal vi söker är $\equiv 2^4$ osv.
   Svar: 16, 34, 9, 33, 12 och 7.

6. Det är klart att A är sammansatt om n är jämnt. Om n är udda och ej delbart med 5 gäller $n^4 + 4^n \equiv 1 + (-1)^n \equiv 0 \ (mod\ 5)$
   Alltså finns bara ett $n, n = 1$, som gör att A blir primtal.

7. Låt $P(n)$ vara påståendet att $k^{(2^n)} - 1 = C2^{n+2}$ med C heltal.
   Eftersom både $k-1$ och $k+1$ är jämna och en av dem delbar med 4 följer att $k^2 - 1$ är delbart med 8 och således är $P(1)$ sant.
   Vidare gäller att $k^{(2^{n+1})} - 1 = \left(k^{(2^n)} - 1\right)\left(k^{(2^n)} + 1\right) = C2^{n+2} \cdot 2D = C_1 2^{n+3}$ för några heltal D och C_1, således att $P(n) \Longrightarrow P(n+1)$