Tentamen i Elementär talteori, 5p **15 jan 2008 8.30 – 13.30**

Examinator: Johan Berglind

Telefonvakt: Micke Persson 076 – 272 18 61

Tillåtna hjälpmedel: typgodkänd räknedosa

Motivera lösningarna noggrant.

1. Bestäm alla primtal p sådana att kongruensen $x^2 + 3 \equiv 0 \pmod{p}$ är lösbar. **(4p)**

2. En grupp apor samlar sina bananer i 11 lika stora högar, var och en med fler än en banan; det blir då 6 bananer över. Därefter gör de om uppdelningen och får då 17 lika stora högar; denna gång blir det ingen banan över. Vilket är det minsta antalet bananer aporna kan ha? **(3p)**

3. Låt a vara ett positivt heltal och p ett primtal. Visa att p delar $a^p + a(p-1)$ **(3p)**

4. Rut måste på något sätt faktorisera talet 703425623. Hon försöker hitta en primfaktor med Pollard p-1 och finner till sin lättnad att 14081 delar det givna talet.
Hur många iterationer krävs för att hitta faktorn 14081? **(3p)**

Ledning: utför inte iterationerna!

5. Bestäm alla inkongruenta lösningar till $8x^7 \equiv 5 \pmod{13}$ **(4p)**

Ledning: 2 är en primitiv rot modulo 13

6. Låt m och n vara positiva heltal med $(m,n) = p$ där p är ett primtal.
Visa att $\Phi(mn) = \Phi(m)\Phi(n)\dfrac{p}{p-1}$ **(4p)**

7. Låt a, b, c och m vara positiva heltal med b och m relativt prima.
Antag att $b^a \equiv 1 \pmod{m}$ och $b^c \equiv 1 \pmod{m}$
Visa att $b^d \equiv 1 \pmod{m}$ där $d = (a,c)$ **(4p)**