ELEMENTR̈ TALTEORI

6. RÄKNEÖVNINGARNA

(1) Hur många primitiva rötter finns det i modulo 13? Beräkna primitiva rötter modulo 13.
(2) Presentera det reducerade restsystemet med hjälp av den primitiva roten som du valde (i övning 1).
(3) Lös ekvationen $x^2 \equiv 12 \pmod{13}$. (Tips: Skriv talet 12 med hjälp av en primitiv rot, berätta varför du kan använda kvadratrot i ekvationen och använd Lagrange sats.)
(4) Låt $n = 47 \cdot 53$. Välj något tal e som du kan använda i den offentliga nyckeln i RSA (välj inte talet 1...), och beräkna de andra talen som behövs om du vill använda RSA. Slutligen, välj något tal och krypta talet och sen dekrypta.
(5) Låt $n = 16637$. Hitta primtalsfaktorer p och q.
(6) Låt $(n, e) = (16637, 11)$ vara en offentlig nyckel i RSA-systemet. Hitta den hemliga nyckeln.