

שיעור 7

הבעית הפירוק של מספרים וצופן רבין

7.1 הבעית פירוק מספרים

7.2 צופן רבין

שלב 3

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} = \frac{(p-1)(q-1)}{d}.$$

$$\lambda(n) \stackrel{(\#2)}{=} \frac{(p-1)(q-1)}{\binom{p-1}{p'}} = p'(q-1). \Leftrightarrow d = \frac{p-1}{p'}.$$
(1*)

$$\lambda(n) \stackrel{(\#2)}{=} \frac{(p-1)(q-1)}{\binom{q-1}{q'}} = q'(p-1). \Leftrightarrow d = \frac{p-1}{p'}.$$
(2*)

שלב 4) מכיוון $ab \equiv 1 \pmod{\lambda(n)}$ ניתן למצוא t שולם כך ש-

$$ab = 1 + t\lambda(n) \stackrel{(2*)}{=} 1 + t(p-1)q'.$$

לכן
 $ab - 1 = t(p-1)q'.$

מכאן
 $x^{ab-1}x^{tq'(p-1)} = y^{p-1} \stackrel{\text{פרמה}}{\equiv} 1 \pmod{p}$

כאשר $y = x^{tq'}$ והשוינו השני מתקיים בಗלל ש- p מספר ראשוני. לפיכך

$$x^{ab-1} \equiv 1 \pmod{p}.$$

שלב 5) מכיוון $ab \equiv 1 \pmod{\lambda(n)}$ ניתן למצוא t שולם כך ש-

$$ab = 1 + t\lambda(n) \stackrel{(1*)}{=} 1 + t(q-1)p'.$$

לכן
 $ab - 1 = t(q-1)p'.$

מכאן
 $x^{ab-1}x^{tp'(q-1)} = z^{q-1} \stackrel{\text{פרמה}}{\equiv} 1 \pmod{q}$

כאשר $z = x^{tp'}$ והשוינו השני מתקיים בगלל ש- q מספר ראשוני. לפיכך

$$x^{ab-1} \equiv 1 \pmod{q}.$$

שלב 6) מכיוון ש- q, p ראשוניים אז

$$\left. \begin{array}{l} x^{ab-1} \equiv 1 \pmod{q} \\ x^{ab-1} \equiv 1 \pmod{p} \end{array} \right\} \Rightarrow x^{ab-1} \equiv 1 \pmod{pq}$$

לפיכך
 $x^{ab-1} \equiv 1 \pmod{n} \Rightarrow (x^b)^a \equiv x \pmod{n}$
 כנדרש.

