שיעור 7
הבעיית הפירוק של מספירם וצופן רבין

7.1 הבעיית פירוק מספרים

7.2 צופן רבין

$$\lambda(n) \overset{(\#1)}{=} \frac{(p-1)(q-1)}{\left(\frac{p-1}{p'}\right)} = p'(q-1) \ . \quad \Leftrightarrow \quad d = \frac{p-1}{p'} \ . \tag{1*}$$

$$\lambda(n) \overset{(\#2)}{=} \frac{(p-1)(q-1)}{\left(\frac{q-1}{q'}\right)} = q'(p-1) \ . \quad \Leftrightarrow \quad d = \frac{p-1}{p'} \ . \tag{2*}$$

שלב 4) $ab \equiv 1 \mod \lambda(n)$ (נתון) לכן קיים t שלם כך ש-

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

לכן

$$ab - 1 = t(p-1)q' \ .$$

מכאן

$$x^{ab-1}x^{tq'(p-1)} = y^{p-1} \overset{\text{פרמה}}{\equiv} 1 \mod p$$

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

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

שלב 5) $ab \equiv 1 \mod \lambda(n)$ (נתון) לכן קיים t שלם כך ש-

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

לכן

$$ab - 1 = t(q-1)p' \ .$$

מכאן

$$x^{ab-1}x^{tp'(q-1)} = z^{q-1} \overset{\text{פרמה}}{\equiv} 1 \mod q$$

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

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

שלב 6) מכיוון ש- p, q ראשוניים אז

$$\left.\begin{array}{ll} x^{ab-1} & \equiv 1 \mod q \\ x^{ab-1} & \equiv 1 \mod q \end{array}\right\} \quad \Rightarrow \quad x^{ab-1} \equiv 1 \mod pq$$

לפיכך

$$x^{ab-1} \equiv 1 \mod n \quad \Rightarrow \quad \left(x^b\right)^a \equiv x \mod n$$

כנדרש.

■