

## **שיעור 7**

### **הבעיית הפירוק של מספירם וצופן רבין**

#### **7.1 הבעיית פירוק מספרים**

#### **7.2 צופן רבין**

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

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

**שלב 4**  $ab \equiv 1 \pmod{\lambda(n)}$  (נתון) לכן קיים  $t$  שלם 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  $y = x^{tq'}$  והשוויון השני מתקיים בגלל ש- $p$  מספר ראשוני. לפיכך

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

**שלב 5**  $ab \equiv 1 \pmod{\lambda(n)}$  (נתון) לכן קיים  $t$  שלם 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  $z = x^{tp'}$  והשוויון השני מתקיים בגלל ש- $q$  מספר ראשוני. לפיכך

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

**שלב 6** מכיוון ש- $p, q$  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.