

שיעור 7

הבעיית הפירוק של מספירם וצופן רבין

7.1 הבעיית פירוק מספרים

7.2 צופן רבין

שלב 6 מכיוון ש- p, q ראשוניים אז

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

לפיכך

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

כנדרש.

