שיעור 6 הבעיית הפירוק של מספירם וצופן רבין

- 6.1 הבעיית פירוק מספרים
 - 8.2 צופן רבין

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

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

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

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

לכן

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

מכאן

$$x^{ab-1}x^{tq'(p-1)}=y^{p-1}\stackrel{\mathsf{ergn}}{\equiv} 1\mod p$$

כאשר אפיכך מספר שני. לפיכך מתקיים בגלל ש- $y=x^{tq^\prime}$ והשוויון השני. לפיכך

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

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

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

לכן

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

מכאן

$$x^{ab-1}x^{tp'(q-1)}=z^{q-1}\stackrel{\mathsf{ergn}}{\equiv} 1\mod q$$

כאשר מספר q-שוני. לפיכך מתקיים השני והשוויון ב $z=x^{tp^\prime}$

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

שלב 6) מכיוון ש- p,q ראשוניים אז

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

לפיכד

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

כנדרש.