

4 ארבעה

13.6.2010, אש"ם, גרמון

1. בשיעור הוכחנו שקיימים קבועים $C_1, C_2 > 0$ כך שלכל $x \geq 2$ מתקיים $C_1 x < \theta(x) < C_2 x$, כאשר $\theta(x) = \sum_{p \leq x} p$.

אסקו מצה, גלא יוגר ממה שורג, קירסה חמה של הפוסטולט של ברטונז: קיים $B > 0$ כך שלכל $x > B$ מתקיים $x < p \leq Bx$.
 הפוסטולט של ברטונז טוען שאפשר לקחת $(B=2)$.

2. איכותו (אפשר להשתמש בכך מה שסיניו בייצור) כי לכל $0 < \delta < 1$ ולכל $x \geq 2$ מתקיים $1 \leq \frac{\pi(x) \ln x}{\theta(x)} \leq \frac{x^{1-\delta} \ln x}{\theta(x)} + \frac{1}{1-\delta}$.

אסקו כי

$$\lim_{x \rightarrow \infty} \frac{\frac{\pi(x)}{\ln x}}{\frac{\theta(x)}{\ln x}} = 1$$

3. להוכיח כי אכן ראשוני אב ורק אב בחבורה $(\mathbb{Z}/n\mathbb{Z})^\times$ יש אבר מסדר $n-1$.

4. יהי p ראשוני. להוכיח כי $n = 2p + 1$ הן ראשוני אב ורק אב $(n \text{ מסדר } 1 \equiv 2^{n-1})$.

5. הן עזר אלגוריתם להזיק ראשוני. בהינתן n אב זיקי, זגל, בוחרים $n-1$ קבועים $(a_1, \dots, a_{n-1}) \in ((\mathbb{Z}/n\mathbb{Z})^\times)^{n-1}$.

לכל $n \equiv 1 \pmod{2}$, יהי $b_i = a_i^{\frac{n-1}{2}}$ אב $(b_1, \dots, b_{n-1}) = (\pm 1, \pm 1, \dots, \pm 1)$.

אך $(1, \dots, 1, 0, \dots, 0) \neq (1, \dots, 1, 0, \dots, 0)$, עוציב "כן". אחר כך עוציב "לא".
 להראות שהאלקטרויקה של בזמן פולינומיאל, שאם n ראשוני אזי
 הוא עוציב "כן" בהסתברות $1 - \frac{1}{2^n}$, ואם n לא ראשוני
 אזי הוא עוציב "לא" בהסתברות $1 - \frac{1}{2^n}$.

6. אמצאו בגזיקה מיסדר-רביע כגוי להוכיח שהמספר $2^{32} + 1$
 אינו ראשוני.

7. יהי $n=22$. כמה איברים $\in (\mathbb{Z}/n\mathbb{Z})^*$ = $\{1, 2, 3, \dots, 22\}$
 יש שזו אג הקטובה "כן" באלקטרויקה של מיסדר-רביע,
 אחר כך שהמספר n אינו ראשוני? האם זה סוגי אג החסם
 שהוכחנו בשיעור?

8. להוכיח כי n ראשוני אם ורק אם $(n-1) \equiv 1 \pmod{n}$ לכל $a \in \mathbb{Z}$
 כך $a^{n-1} \equiv 1 \pmod{n}$.