# אלגוריתמים - תרגיל 13

20 בינואר 2004

תאריך אחרון להגשה: יום ה' 29.1.2004

1. פתרון משוואות מודולריות
אנו מעוניינים לפתור את המשוואה $ax \equiv b(mod\, n)$.
הגדרה: תהי $\mathbb{Z}_n$ החבורה הציקלית מסדר $n$, ויהי $a \in \mathbb{Z}_n$ איבר כלשהו בה. נגדיר את הקבוצה $S = \{ka | k = 0, \ldots, n-1\}$. בתרגיל הקודם הוכחתם כי $S$ היא תת חבורה של $\mathbb{Z}_n$. $S$ נקראת תת החבורה הנוצרת על ידי $a$, אומרים ש-$a$ הוא היוצר של $S$, ומסמנים $S =< a >$.
א. יהי $d = \gcd(a, n)$. הוכיחו כי $< a >=< d >= \{0, d, 2d, \ldots, (\frac{n}{d} - 1)d\}$.
רמז: הוכיחו הכלה בשני הכיוונים. השתמשו באלגוריתם $Extended - Euclid$ שנלמד בכיתה.
ב. הסיקו מכך שלמשוואה $ax \equiv b(mod\, n)$ יש פתרון אם ורק אם $\gcd(a, n)|b$.
רמז: בשביל כיוון אחד השתמשו בכך שאם יש פתרון למשוואה, משמעות הדבר שיש $y$ כך ש-$ax + ny = b$. בשביל הכיוון השני השתמשו בסעיף א'.
ג. הוכיחו כי הסדרה $ak(mod\, n)$ עבור $k = 1, \ldots, n-1$ היא מחזורית עם מחזור $\frac{n}{d}$.
ד. הסיקו מכך שלמשוואה המודולרית $ax \equiv b(mod\, n)$ יש או $0$ פתרונות או $d$ פתרונות.
ה. נניח ש-$d|b$ וש-$d = ax' + ny'$ עבור $x', y'$ שלמים. הוכיחו כי $x'\frac{b}{d}$ הוא פתרון של המשוואה המודולרית הנתונה.
ו. מצאו את $d - 1$ הפתרונות הנוספים של המשוואה.
ז. תארו אלגוריתם המקבל כקלט $a, b, n$ ומחזיר את כל פתרונות המשוואה $ax \equiv b(mod\, n)$ (או מודיע שאין פתרון). מהו זמן הריצה של האלגוריתם?

2. ב-$RSA$ המפתח הפומבי הוא $(e, n)$ כאשר $n = pq$ $p, q$ ראשוניים גדולים), ו-$e$ הוא מספר אי זוגי זר ל-$(p-1)(q-1)$. המפתח הסודי הוא $(d, n)$ כאשר $d$ הוא ההפכי של $e$ מודולו $(p-1)(q-1)$. כיצד ניתן למצוא את $d$ בהינתן $e, p, q$?