# תרגיל רשות בקריפטוגרפיה paillier cryptosystem & naïve electronic Voting

מגישים:

* איקה בר-מנחם, ת.ז. 040176901, דוא"ל: [ikabar@cs.bgu.ac.il](mailto:ikabar@cs.bgu.ac.il)
* ניר חמד, ת.ז.

## הגדרות מושגים במערכת ההצפנה

1. מספר z יקרא **השארית הn-ית מודולו n^2** אם קיים מספר כך שמתקיים