ב״ה

תורת המספרים (89-256)

תרגיל 1

להגשה עד כ״ח באדר תשע״ב (22.3.2012).

1. יהיו $m,n\in\mathbb{N}$ ונניח שהפירוקים שלהם לגורמים ראשוניים ידועים: $m=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, $n=q_1^{a_1}q_2^{a_2}\cdots q_s^{a_s}$, כאשר $p_j\neq p_i$, $q_j\neq q_i$ עבור $j\neq i$. מהו הפירוק של (m,n), ומהו הפירוק של המכפלה המשותפת המינימלית $\operatorname{lcm}(m,n)$ של m,n? הוכח כי

$$(m,n)\cdot \operatorname{lcm}(m,n)=mn.$$

2. יהיו $a,b\in\mathbb{Z}$. האלגוריתם הבא מחשב את (a,b) בלי לדעת את הפירוקים של a,b. הוכח שהאלגוריתם רץ בזמן סופי (כלומר, שהוא לא ירוץ עד אינסוף) ושהוא תמיד מוציא בסוף את התשובה הנכונה.
הערה: האלגוריתם אפילו רץ בזמן פולינומיאלי, אך אינך נדרש להוכיח את זה.

א) נגדיר $a_0=a$, $b_0=b$.

ב) נחליף את a_n, b_n ב-$|a_n|,|b_n|$ אם צריך, ונוכל להניח בלי הגבלת הכלליות כי $a_n,b_n\geq 0$. אם $a_n=b_n$, מוציאים תשובה $(a,b)=(a_n,b_n)=a_n$ ומסיימים.
אחרת, נניח $a_n>b_n\geq 0$ (ונחליף את a_n ו-b_n אם צריך) ונעבור לצעד הבא.

ג) נפעיל את האלגוריתם האוקלידי לחילוק ארוך ונמצא $q_n,r_n\in\mathbb{Z}$ כך ש- $a_n=b_nq+r_n$, כאשר $0\leq r_n<b_n$.

ד) אם $r_n=0$, אז $(a,b)=b_n$ וסיימנו.

ה) אם $r_n\neq 0$, נגדיר $a_{n+1}=b_n$, $b_{n+1}=r_n$, ונריץ את ב) עם a_{n+1},b_{n+1}.

3. תשתמש באלגוריתם מן השאלה הקודמת כדי לחשב $(455, 1235)$.

4. יהיו $\alpha,\beta\in\mathbb{Z}[i]$. הוכח כי $\beta|\alpha$ אם ורק אם לכל $\gamma,\delta\in\mathbb{Z}[i]$ שמקיים $\alpha=\beta\gamma+\delta$ וגם $N(\delta)<N(\beta)$, מתקיים $\delta=0$.

5. יהיו $\alpha=3+4i$, $\beta=1+2i$. האם $\beta|\alpha$?

6. למצוא פירוק לגורמים ראשוניים של $6\in\mathbb{Z}[i]$

7. תשים לב כי $65=1^2+8^2=4^2+7^2$. לכן,

$$65=(1+8i)(1-8i)=(4+7i)(4-7i)$$

האם זה סותר את היחידות של הפריקה של 65 לגורמים ראשוניים? תמצא את הפריקה.

8. תשתמש ברעיון של השאלה הקודמת כדי למצוא מספר טבעי שניתן להציג אותו כסכום של ריבועים בשלוש דרכים שונות.
כלומר, תמצא $n\in\mathbb{N}$ כך ש-

$$n=a^2+b^2=c^2+d^2=e^2+f^2$$

כאשר הקבוצות $\{a,b\},\{c,d\},\{e,f\}$ שונות.