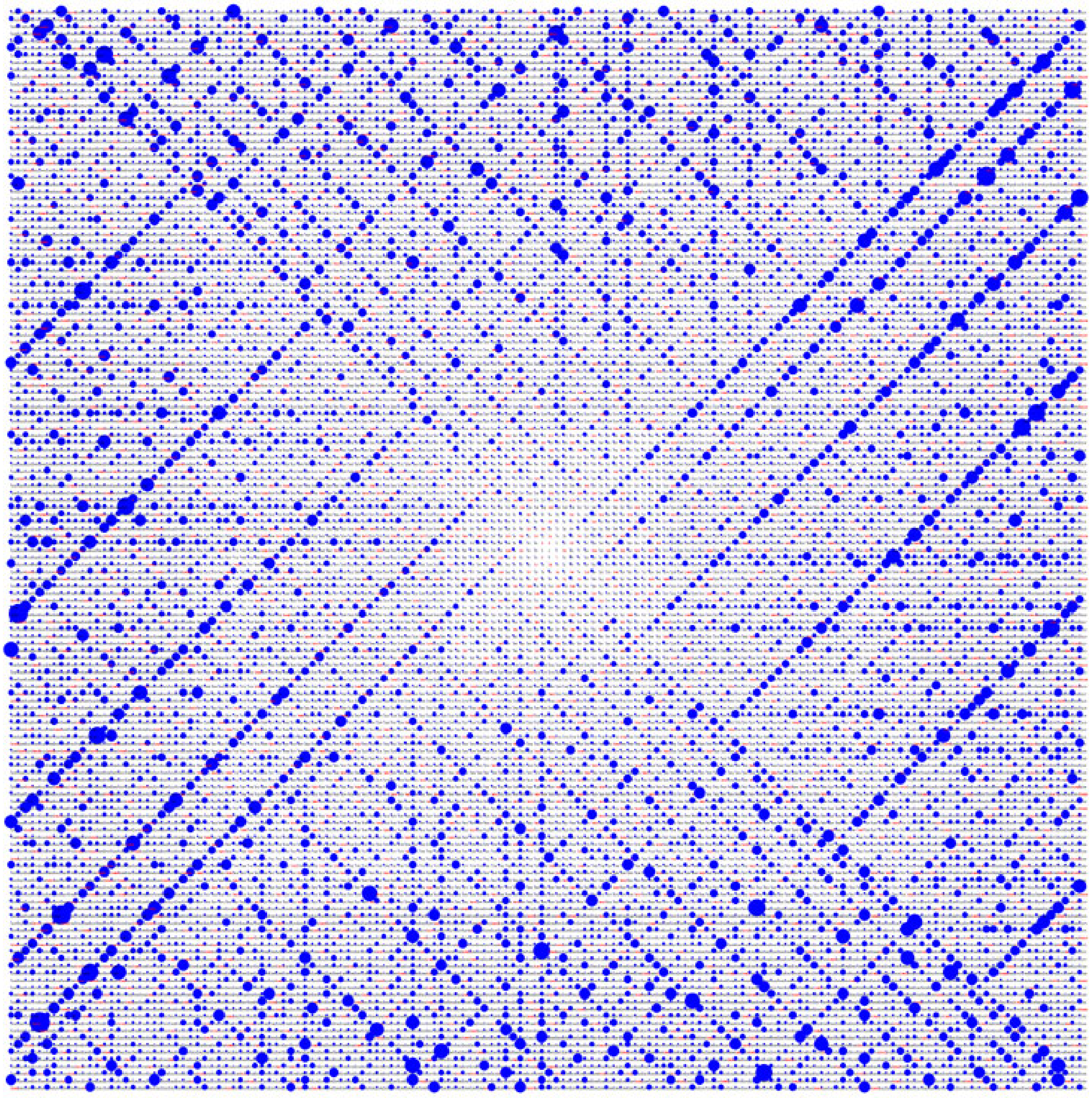

מבוא לתורת המספרים (104157)
אביב 2024
רשימות תרגולים

אלן סורני

הרשימות עודכנו לאחרונה בתאריך ה־23 ביוני 2024

תוכן העניינים

סימונים

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ אוסף המספרים הטבעיים.
- $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$ אוסף המספרים הטבעיים החיוביים (כלומר, לא כולל אפס).
- $[n] = \{1, \ldots, n\}$.
- $\lfloor x \rfloor$ המספר הכי גדול שקטן או שווה ל-$x \in \mathbb{R}$.
- $\lceil x \rceil$ המספר הכי קטן שגדול או שווה ל-x.
-

$$\gcd(a_1, \ldots, a_n)$$
$$\operatorname{lcm}(a_1, \ldots, a_n)$$

בהתאמה, המחלק המשותף הגדול ביותר של המספרים $a_1, \ldots, a_n$, והכפולה המשותפת המינימלית שלהם.

פרק 1

תרגול 3 - שימושים בפריקות יחידה

1.1 תזכורת

הגדרה 1.1.1. יהי $n \in \mathbb{N}_+$. נגדיר

1. $\nu(n) := \sum_{d|n} 1$. זה מספר המחלקים של n.
2. $\sigma(n) := \sum_{d|n} d$. זה סכום המחלקים של n.
3.

$$\varphi(n) := \sum_{\substack{\gcd(d,n)=1 \\ 1<d<n}} 1.$$

זה מספר המספרים הטבעיים שקטנים מ־n וזרים לו. זאת נקראת **פונקציית אוילר** (**Euer totient function**).

4. $\pi(n)$ מספר האיברים הראשוניים הקטנים או שווים ל־n. זאת נקראת **פונקציית המספרים הראשוניים** (**prime-counting function**).
5.

$$\mu(n) = \begin{cases} (-1)^{\ell} & \forall p \text{ prime} : p^2 \nmid n \\ 0 & \text{otherwise} \end{cases}$$

כאשר ℓ מספר הראשוניים שמחלקים את n. זאת נקראת **פונקציית מביוס** (**Möbius function**).

1.2 תרגילים

תרגיל 1.1 (פרק 2, תרגיל 7). הסיקו מתרגיל 6 כי

$$\operatorname{ord}_p(n!) \leq \frac{n}{p-1}$$

וכי

$$\sqrt[n]{n!} \leq \prod_{p|n!} p^{1/(p-1)}.$$

פתרון. לפי תרגיל 6 מהתרגול הקודם,

$$\operatorname{ord}_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

נקבל כי

$$\begin{aligned} \operatorname{ord}_p(n!) &\leq \sum_{k=1}^{\infty} \frac{n}{p^k} \\ &= n \sum_{k=1}^{\infty} \left(\frac{1}{p}\right)^k \end{aligned}$$

וכיוון ש־$p \in \mathbb{N}_+$ ראשוני מתקיים $\left|\frac{1}{p}\right| < 1$. מסכום סדרה הנדסית נקבל כי

$$\begin{aligned}\sum_{k=1}^{\infty}\left(\frac{1}{p}\right)^k \\ &= \frac{1-\left(1-\frac{1}{p}\right)}{1-\frac{1}{p}}-1 \\ &= \frac{\frac{1}{p}}{1-\frac{1}{p}} \\ &= \frac{1}{p-1}\end{aligned}$$

ולכן

$$\operatorname{ord}_p(n!) \le \frac{n}{p-1}.$$

אז מתקיים גם

$$\begin{aligned}n! &= \prod_{\substack{p\mid n \\ p \text{ prime}}} p^{\operatorname{ord}_p(n!)} \\ &\le \prod_{\substack{p\mid n \\ p \text{ prime}}} p^{\frac{n}{p-1}} \\ &\le \prod_{p\mid n} p^{\frac{n}{p-1}} \\ &= \left(\prod_{p\mid n} p^{\frac{1}{p-1}}\right)^n\end{aligned}$$

ולכן

$$\sqrt[n]{n!} \le \prod_{p\mid n} p^{\frac{1}{p-1}},$$

כנדרש.

תרגיל 1.2 (פרק 2, תרגיל 8). השתמשו בתוצאת התרגיל הקודם כדי להראות שיש אינסוף ראשוניים.
רמז: הראו קודם שמתקיים $(n!)^2 \ge n^n$ לכל $n \in \mathbb{N}_+$.

פתרון. ראשית, נראה כי $(n!)^2 \ge n^n$ לכל $n \in \mathbb{N}_+$.
מתקיים

$$\begin{aligned}n! &= \prod_{k=0}^{n-1}(k+1) \\ n! &= \prod_{k=0}^{n-1}(n-k)\end{aligned}$$

ולכן

$$(n!)^2 = \prod_{k=0}^{n-1}(k+1)(n-k).$$

נראה כי הגורמים הנסכמים גדולים או שווים ל־n. כאשר $k=0$ מתקיים $(k+1)(n-k)=n$. כאשר $0<k\le\frac{n}{2}$ מתקיים $n-k\ge\frac{n}{2}$ ואז

$$(k+1)(n-k) \ge \frac{(k+1)n}{2} \ge \frac{2n}{2} = n.$$

כאשר $\frac{n}{2}<k<n-1$ נקבל כי $n-k\ge 2$ ולכן

$$(k+1)(n-k) > 2\cdot\frac{n}{2} = n.$$

כאשר $k=n-1$ נקבל

$$(k+1)(n-k)=(n-1+1)\cdot(n-n+1)=n\cdot 1=n\,.$$

לכן $(n!)^2\geq\prod_{k=0}^{n-1}n=n^n$, כנדרש.
כעת, מהוכחת הסעיף הקודם ניתן לראות כי

$$\sqrt[n]{n!}\leq\prod_{\substack{p|n!\\ p\text{ prime}}}p^{\frac{1}{p-1}}$$

ואם נראה שאגף שמאל שואף לאינסוף נקבל שגם אגף ימין שואף לאינסוף, ובפרט שיש אינסוף ראשוניים.
אכן, מכך שמתקיים $(n!)^2\geq n^n$ נובע כי $\sqrt[n]{n!}\geq\sqrt{n}$ ולכן $\lim_{n\to\infty}\sqrt[n]{n!}=\infty$.

תרגיל 1.3 (פרק 2, תרגיל 15). הראו כי

(א) לכל $n\in\mathbb{N}_+$ מתקיים

$$\sum_{d|n}\mu(n/d)\,\nu(d)=1\,.$$

(ב) לכל $n\in\mathbb{N}_+$ מתקיים

$$\sum_{d|n}\mu(n/d)\,\sigma(d)=n\,.$$

פתרון. ראשית נזכיר כי

$$(f*g)(n)\coloneqq\sum_{d|n}f(d)\,g\left(\frac{n}{d}\right)$$

לכל $f,g\colon\mathbb{N}_+\to\mathbb{C}$, וכי ראינו שלכל f כנ"ל מתקיים $f=(f*1)*\mu$.

(א) מתקיים

$$\sum_{d|n}\mu(n/d)\,\nu(d)=(\nu*\mu)(n)\,,$$

לכן צריך להראות כי $(\nu*\mu)(n)=1$. כיוון שקונוולוציית דיריכלה הינה קומוטטיבית, די להראות כי $(\mu*\nu)(n)=1$, כלומר כי

$$\sum_{d|n}\mu(d)\,\nu(n/d)=n\,.$$

יהי $n=\prod_{i\in[k]}p_i^{r_i}$ פירוק של n לראשוניים. עבור $d\mid n$ מתקיים כי $\mu(d)\neq 0$ רק עבור d חסר ריבועים. במקרה זה d מהצורה $\prod_{i\in[k]}p_i^{s_i}$ עבור $s_i\in\{0,1\}$ ומתקיים $\mu(d)=|\{i\mid s_i=1\}|$.

נספור את המחלקים של n שאינם מחלקים את n/d במקרה זה. אלו מחלקים $e\mid n$ עבורם קיים $i\in[k]$ כך ש-$s_i=1$ וגם $\operatorname{ord}_{p_i}(e)=r_i$.

(ב)

תרגיל 1.4 (פרק 2, תרגיל 18). הראו כי

$$\forall m,n\in\mathbb{N}_+:\varphi(n)\,\varphi(m)=\varphi(\gcd(n,m))\,\varphi(\operatorname{lcm}(n,m))\,.$$

פתרון. נזכיר כי עבור $x=p_1^{a_1}\cdot\ldots p_\ell^{a_\ell}$ מתקיים באופן כללי

$$\varphi(x)=x\prod_{k\in[\ell]}\left(1-\frac{1}{p_k}\right).$$

יהיו

$$n=\left(\prod_{i\in[k]}p_i^{\alpha_i}\right)\left(\prod_{i\in[\ell]}q_i^{r_i}\right)$$
$$m=\left(\prod_{i\in[k]}p_i^{\beta_i}\right)\left(\prod_{i\in[\tilde{\ell}]}\tilde{q}_i^{s_i}\right)$$

הפירוקים של n, m לראשוניים, כאשר $p_1, \ldots, p_k$ הראשוניים שמחלקים גם את n וגם את m.
אז

$$\varphi(n) = n \left(\prod_{i\in[k]}\left(1-\frac{1}{p_i}\right)\right)\left(\prod_{i\in[\ell]}\left(1-\frac{1}{q_i}\right)\right)$$
$$\varphi(m) = m \left(\prod_{i\in[k]}\left(1-\frac{1}{p_i}\right)\right)\left(\prod_{i\in[\tilde{\ell}]}\left(1-\frac{1}{\tilde{q}_i}\right)\right)$$
$$\varphi(\gcd(n,m)) = \gcd(n,m)\prod_{i\in[k]}\left(1-\frac{1}{p_i}\right)$$
$$\varphi(\mathrm{lcm}(n,m)) = \mathrm{lcm}(n,m)\left(\prod_{i\in[k]}\left(1-\frac{1}{p_i}\right)\right)\left(\prod_{i\in[\ell]}\left(1-\frac{1}{q_i}\right)\right)\left(\prod_{i\in[\tilde{\ell}]}\left(1-\frac{1}{\tilde{q}_i}\right)\right)$$

וכיוון ש-$\gcd(n,m)\,\mathrm{lcm}(n,m) = nm$, נקבל כי

$$\varphi(n)\,\varphi(m) = \varphi(\gcd(n,m))\,\varphi(\mathrm{lcm}(n,m)),$$

כנדרש.

תרגיל 1.5 (פרק 2, תרגיל 19). הראו כי

$$\forall m,n\in\mathbb{N}_+ : \varphi(mn)\,\varphi(\gcd(m,n)) = \gcd(m,n)\,\varphi(m)\,\varphi(n).$$

פתרון. כיוון שראשוני מחלק את mn אם ורק אם הוא מחלק את $\mathrm{lcm}(m,n)$, נקבל כי

$$\begin{aligned}\frac{\varphi(mn)}{mn} &= \prod_{\substack{p\mid mn\\ p\text{ prime}}}\left(1-\frac{1}{p}\right)\\ &= \prod_{\substack{p\mid \mathrm{lcm}(m,n)\\ p\text{ prime}}}\left(1-\frac{1}{p}\right)\\ &= \frac{\varphi(\mathrm{lcm}(m,n))}{\mathrm{lcm}(m,n)}.\end{aligned}$$

נקבל כי

$$\begin{aligned}\varphi(mn) &= \frac{mn}{\mathrm{lcm}(m,n)}\cdot\varphi(\mathrm{lcm}(m,n))\\ &= \gcd(m,n)\,\varphi(\mathrm{lcm}(m,n)).\end{aligned}$$

לכן

$$\begin{aligned}\varphi(mn)\,\varphi(\gcd(m,n)) &= \gcd(m,n)\,\varphi(\mathrm{lcm}(m,n))\,\varphi(\gcd(m,n))\\ &= \gcd(m,n)\,\varphi(m)\,\varphi(n)\end{aligned}$$

כאשר בשוויון השני השתמשנו בתרגיל הקודם.

תרגיל 1.6 (פרק 2, תרגיל 20). הראו כי

$$\prod_{d\mid n} d = n^{\nu(n)/2}.$$

היעזרו בעובדה הבאה: $\nu(n)$ אי־זוגי אם ורק אם n ריבוע.

פתרון. יהי $n = \prod_{i\in[k]} p_i^{r_i}$ פירוק של n לראשוניים.
נניח ראשית כי $n = m^2$ עבור $m\in\mathbb{N}_+$. מתקיים

$$n^{\nu(n)/2} = \left(m^2\right)^{\nu(n)/2} = m^{\nu(n)}.$$

אז

$$\mathrm{ord}_{p_i}\left(n^{\nu(n)/2}\right) = \nu(n)\cdot\mathrm{ord}_{p_i}(m),$$

ולכן די להראות כי

$$\operatorname{ord}_{p_i}\left(\prod_{d\mid n}\right)=\nu\left(n\right)\cdot\operatorname{ord}_{p_i}\left(m\right).$$

כיוון ש-$n=m^2$, מתקיים $\operatorname{ord}_{p_i}\left(n\right)=2\operatorname{ord}_{p_i}\left(m\right)$, לכן $\operatorname{ord}_{p_i}\left(m\right)=\frac{\operatorname{ord}_{p_i}n}{2}$. לכן די להוכיח כי

$$\operatorname{ord}_{p_i}\left(\prod_{d\mid n}d\right)=\frac{\nu\left(n\right)\cdot\operatorname{ord}_{p_i}\left(n\right)}{2}.$$

אם n אינו ריבוע, $\nu\left(n\right)$ זוגי, ואז $\nu\left(n\right)/2$ שלם. נקבל כי במקרה זה

$$\operatorname{ord}_{p_i}\left(n^{\nu(n)/2}\right)=\frac{\nu\left(n\right)\cdot\operatorname{ord}_{p_i}\left(n\right)}{2},$$

ולכן גם במקרה זה די להוכיח כי

$$\operatorname{ord}_{p_i}\left(\prod_{d\mid n}d\right)=\frac{\nu\left(n\right)\cdot\operatorname{ord}_{p_i}\left(n\right)}{2}.$$

נקבע $i\in[k]$. מתקיים

$$\operatorname{ord}_{p_i}\left(\prod_{d\mid n}d\right)=\sum_{d\mid n}\operatorname{ord}_{p_i}\left(d\right).$$

לכל $r\in\{0,\ldots,r_i\}$ נסמן

$$A_r=\left\{d\;\middle|\;\substack{d\mid n\\ \operatorname{ord}_{p_i}(d)=r}\right\},$$

ואז

$$\{d\mid d\mid n\}=\bigcup_{r=0}^{r_i}A_r.$$

כל הקבוצות A_r מאותו גודל, כי עבור בחירת החזקה עבור p_i יש אותו מספר דרכים לבחור את שאר החזקות. מתקיים גם $\left|\bigcup_{r=0}^{r_i}A_r\right|=\nu\left(n\right)$, ולכן

$$\left|A_r\right|=\frac{\nu\left(n\right)}{r_i+1}$$

לכל $r\in\{0,\ldots,r_i\}$. נקבל

$$\begin{aligned}\sum_{d\mid n}\operatorname{ord}_{p_i}\left(d\right)&=\sum_{r\in\{0,\ldots,r_i\}}\sum_{d\in A_r}r\\&=\sum_{r\in\{0,\ldots,r_i\}}\left|A_r\right|r\\&=\frac{\nu\left(n\right)}{r_i+1}\cdot\sum_{r\in\{0,\ldots,r_i\}}r\\&=\frac{\nu\left(n\right)}{r_i+1}\cdot\frac{r_i\left(r_i+1\right)}{2}\\&=\frac{\nu\left(n\right)r_i}{2}\\&=\frac{\nu\left(n\right)\operatorname{ord}_{p_i}\left(n\right)}{2}\end{aligned}$$

כנדרש.

תרגיל 1.7 (פרק 2, תרגיל 23). יהי $f\in\mathbb{Z}\left[x\right]$ ויהי $\psi\left(n\right)$ מספר הערכים $f\left(j\right)$ עבור $j\in[n]$ כך ש-$\gcd\left(f\left(j\right),n\right)=1$.

(א) הראו כי $\psi\left(n\right)$ פונקציה כפלית וכי $\psi\left(p^t\right)=p^{t-1}\psi\left(p\right)$ לכל ראשוני $p\in\mathbb{N}_+$.

(ב) הסיקו כי

$$\psi\left(n\right)=n\prod_{p\mid n}\frac{\psi\left(p\right)}{p}.$$

פתרון.