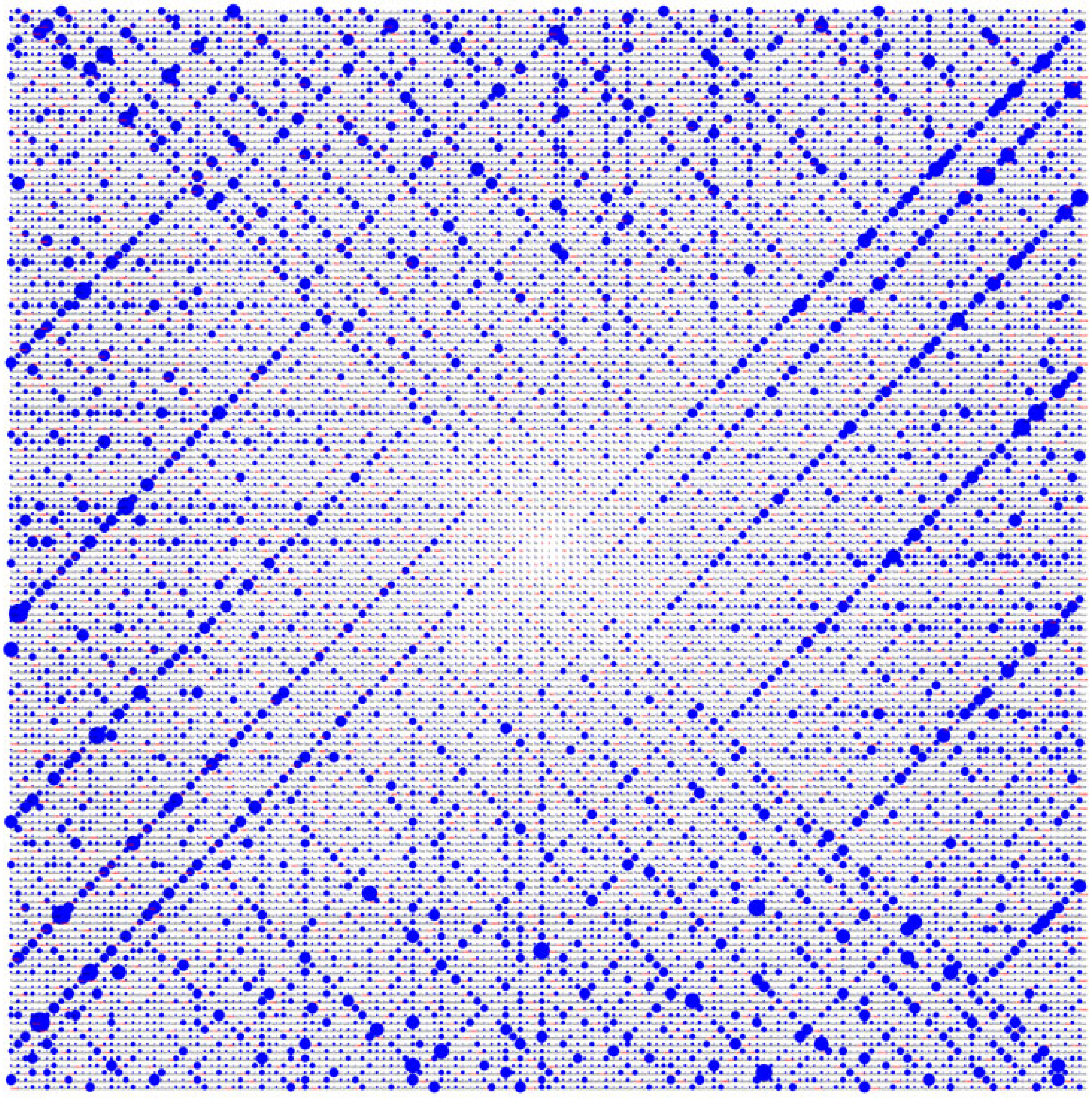

מבוא לתורת המספרים (104157)
אביב 2024
רשימות תרגולים

אלן סורני

הרשימות עודכנו לאחרונה בתאריך ה־29 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

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

וכי

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

פתרון. לפי תרגיל 6 מהתרגול הקודם,

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

נקבל כי

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

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

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

אז מתקיים גם

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

ולכן

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

כנדרש.

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

פתרון. ראשית, נראה כי $(n!)^2 \geq n^n$ 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 $0 < k \leq \frac{n}{2}$ מתקיים $n-k \geq \frac{n}{2}$ ואז

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

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

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

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

(א) מתקיים

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

ונשים לב כי

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

אז

$$(\nu*\mu)(n)=(1*1*\mu)(n)=1(n)=1\,,$$

כנדרש.

(ב) מתקיים

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

ונשים לב כי

$$\sigma(n)=\sum_{d|n}d=\left(\mathrm{Id}_{\mathbb{N}_+}*1\right)(n)\,.$$

אז

$$(\sigma*\mu)(n)=\left(\mathrm{Id}_{\mathbb{N}_+}*1*\mu\right)(n)=\mathrm{Id}_{\mathbb{N}_+}(n)=n\,,$$

כנדרש.

תרגיל 1.4 (פרק 2, תרגיל 16). הראו כי $\nu(n)$ אי־זוגי אם ורק אם n ריבוע.

פתרון. נכתוב $n=\prod_{i\in[k]}p_i^{r_i}$. ראינו כי אז

$$\nu(n)=\prod_{i\in[k]}(r_i+1)\,.$$

מספר זה אי־זוגי אם ורק אם כל ה־r_i זוגיים, מה שמתקיים אם ורק אם n ריבוע.

תרגיל 1.5 (פרק 2, תרגיל 16). הראו כי $\sigma\left(n\right)$ אי זוגי אם ורק אם n ריבוע או ריבוע כפול 2.

פתרון.

תרגיל 1.6 (פרק 2, תרגיל 18). הראו כי

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

פתרון. נזכיר כי עבור $x=p_{1}^{a_{1}}\cdot\ldots p_{\ell}^{a_{\ell}}$ מתקיים באופן כללי

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

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

$$\varphi\left(n\right)=n\left(\prod_{i\in[k]}\left(1-\frac{1}{p_{i}}\right)\right)\left(\prod_{i\in[\ell]}\left(1-\frac{1}{q_{i}}\right)\right)$$
$$\varphi\left(m\right)=m\left(\prod_{i\in[k]}\left(1-\frac{1}{p_{i}}\right)\right)\left(\prod_{i\in[\tilde{\ell}]}\left(1-\frac{1}{\tilde{q}_{i}}\right)\right)$$
$$\varphi\left(\gcd\left(n,m\right)\right)=\gcd\left(n,m\right)\prod_{i\in[k]}\left(1-\frac{1}{p_{i}}\right)$$
$$\varphi\left(\operatorname{lcm}\left(n,m\right)\right)=\operatorname{lcm}\left(n,m\right)\left(\prod_{i\in[k]}\left(1-\frac{1}{p_{i}}\right)\right)\left(\prod_{i\in[\ell]}\left(1-\frac{1}{q_{i}}\right)\right)\left(\prod_{i\in[\tilde{\ell}]}\left(1-\frac{1}{\tilde{q}_{i}}\right)\right)$$

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

$$\varphi\left(n\right)\varphi\left(m\right)=\varphi\left(\gcd\left(n,m\right)\right)\varphi\left(\operatorname{lcm}\left(n,m\right)\right),$$

כנדרש.

פרק 2

תרגול 4 - עוד פריקות יחידה, וחשבון מודולרי

תרגיל 2.1 (פרק 2, תרגיל 19). הראו כי

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

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

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

נקבל כי

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

לכן

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

כאשר בשוויון השני השתמשנו בתרגיל הקודם.

תרגיל 2.2 (פרק 2, תרגיל 20). הראו כי

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

היעזרו בעובדה הבאה: $\nu\left(n\right)$ 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

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

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 $\operatorname{ord}_{p_i}(n)=2\operatorname{ord}_{p_i}(m)$, לכן $\operatorname{ord}_{p_i}(m)=\frac{\operatorname{ord}_{p_i}n}{2}$. לכן די להוכיח כי

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

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

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

ולכן גם במקרה זה די להוכיח כי

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

נקבע $i\in[k]$. מתקיים

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

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 $\left|\bigcup_{r=0}^{r_i}A_r\right|=\nu(n)$, ולכן

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

לכל $r\in\{0,\ldots,r_i\}$. נקבל

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

כנדרש.

תרגיל 2.3 (פרק 3, תרגיל 1). הראו שיש אינסוף ראשוניים p עבורם $p\equiv 5\pmod 6$.

פתרון. נניח בדרך השלילה שיש מספר סופי של ראשוניים $p_1,\ldots,p_\ell$ עבורם $p_i\equiv 5\pmod 6$.
אם ℓ אי־זוגי, נגדיר $m=\prod_{i\in[\ell]}p_i+6$ ואז

$$m\equiv(-1)^\ell\equiv-1\pmod 6$$

וזה מספר שזר לכל p_i. אבל, $ab\equiv-1\pmod 6$ גורר שלפחות אחד מבין a,b שווה $-1\pmod 6$. מפריקות יחידה, נקבל כי m חייב להתחלק בראשוני ששווה $-1\pmod 6$, בסתירה לכך שהוא לא מתחלק באף p_i.
אם ℓ זוגי, נגדיר במקום זאת $m=5\prod_{i\in[\ell]}p_i+6$ ונחזור למקרה הקודם.

תרגיל 2.4 (פרק 3, תרגיל 6). יהי $n>0$. קבוצת מספרים $\left\{a_1,\ldots,a_{\varphi(n)}\right\}$ נקראת **מערכת שאריות מצומצמת מודולו** n אם $\gcd\left(a_i,n\right)=1$ לכל $i\in\left[\varphi\left(n\right)\right]$ וגם $a_i\not\equiv a_j\left(\mathrm{mod}\ n\right)$ כאשר $i\neq j$.
תהי $R:=\left\{a_1,\ldots,a_{\varphi(n)}\right\}$ מערכת שאריות מצומצמת מודולו n ויהי $a\in\mathbb{Z}$ עבורו $\gcd\left(a,n\right)=1$. הראו כי $aR:=\left\{aa_1,\ldots,aa_{\varphi(n)}\right\}$ מערכת שאריות מצומצמת מודולו n.

פתרון. ראשית, נשים לב כי לכל $i\in\left[\varphi\left(n\right)\right]$ מתקיים $\gcd\left(aa_i,n\right)=1$ כי a,a_i שניהם זרים ל־n.
נסמן ב־$G:=\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$ את קבוצת השאריות מודולו n שזרות ל־n, ונשים לב\ניזכר שקבוצה זאת היא חבורה ביחס לכפל.
אכן, עבור $x\in G$ כיוון שמתקיים $\gcd\left(x,n\right)=1$ קיימים $\alpha,\beta\in\mathbb{Z}$ עבורם $\alpha x+\beta n=1$, ואז $\alpha x\equiv1\left(\mathrm{mod}\ n\right)$, כלומר $\alpha\equiv x^{-1}\left(\mathrm{mod}\ n\right)$.
בפרט, קיים איבר הופכי ל־a מודולו n, ואז

$$\begin{aligned}\bar{a}^{-1}\overline{aa_1},\ldots,\bar{a}^{-1}\overline{aa_{\varphi(n)}} &= \bar{a}^{-1}\bar{a}\bar{a}_1,\ldots,\bar{a}^{-1}\bar{a}\bar{a}_{\varphi(n)}\\ &= \bar{a}_1,\ldots,\bar{a}_{\varphi(n)}\end{aligned}.$$

לכן ההעתקה

$$\begin{aligned}G&\to G\\ x&\mapsto\bar{a}x\end{aligned}$$

הינה הפיכה, ולכן פרמוטציה. לכן האיברים $\bar{a}\bar{a}_1,\ldots,\bar{a}\bar{a}_{\varphi(n)}$ כולם שונים, כנדרש.

פרק 3

תרגול 5 - עוד חשבון מודולרי

תרגיל 3.1 (פרק 3, תרגיל 7). היעזרו בתרגיל הקודם כדי להוכיח את משפט אוילר, $a^{\varphi(n)} \equiv 1 \pmod{n}$ כאשר $(a,n)=1$.

פתרון. יהיו $a \in \mathbb{Z}, n \in \mathbb{N}_+$ עבורם $\gcd(a,n)=1$. תהי $\bar{a}$ השארית של a מודולו n. ראינו כי $(\mathbb{Z}/n\mathbb{Z})^\times$ חבורה כפלית מסדר $\varphi(n)$, והחזקה של איבר בסדר של החבורה תמיד שווה ליחידה, לכן $a^{\varphi(n)} \equiv 1 \pmod{n}$, כנדרש.

תרגיל 3.2 (פרק 3, תרגיל 9). הראו כי $(p-1)! \equiv -1 \pmod{p}$ לכל $p \in \mathbb{N}_+$ ראשוני.

פתרון. אם $p=2$, הטענה ברורה. לכן נניח $p \neq 2$.
הביטוי $(p-1)!$ הוא מכפלת כל האיברים השונים מאפס מודולו p, כלומר איברי $\mathbb{Z}/p\mathbb{Z}$.
כל איבר במכפלה יצתמצם עם ההופכי שלו, אלא אם הוא ההופכי של עצמו. האיברים $a \in \mathbb{Z}/p\mathbb{Z}$ עבורם $a=a^{-1}$ הם אלו עבורם $a^2=1$. אלו שורשי הפולינום x^2-1, וכיוון ש־$\mathbb{Z}/p\mathbb{Z}$ שדה, יש לפולינום הזה בדיוק שני שורשים ± 1.
נקבל כי $(p-1)! = -1$.

תרגיל 3.3 (פרק 3, תרגיל 10). יהי $n \in \mathbb{N}_+$ שאינו ראשוני. הראו כי

$$(n-1)! \equiv 0 \pmod{n}$$

חוץ מכאשר $n=4$.

פתרון. נניח ראשית כי $n=4$. אז $(n-1)! = 3! = 6 \equiv 2 \pmod{4}$.
נניח כעת כי $n \neq 4$. ניתן לכתוב $n=ab$ עבור $a,b \in \{2,\ldots,n-1\}$. אם $a \neq b$ נקבל כי a,b שניהם מופיעים כגורמים במכפלה $(n-1)!$, ולכן $n = ab \mid (n-1)!$ ונקבל כי $(n-1)! \equiv 0 \pmod{n}$. אחרת, $n=p^2$ עבור p ראשוני שונה מ־2. נקבל כי $p(2p) \mid (n-1)!$ ולכן $n = p^2 \mid p(2p) \mid (n-1)!$ ולכן $(n-1)! \equiv 0 \pmod{n}$, כנדרש.

תרגיל 3.4 (פרק 3, תרגיל 11). תהי $a_1,\ldots,a_{\varphi(n)}$ מערכת שאריות מצומצמת מודלו n ויהי N מספר הפתרונות למשוואה $x^2 \equiv 1 \pmod{n}$. הראו כי

$$a_1 \cdot \ldots \cdot a_{\varphi(n)} \equiv (-1)^{N/2} \pmod{n}.$$

פתרון. ראשית, נשים לב כי N אכן זוגי כי אם $a^2 \equiv 1 \pmod{n}$ גם $(-a)^2 \equiv 1 \pmod{n}$, ואם $a \equiv -a \pmod{n}$ אז $2a \equiv 0 \pmod{n}$ כלומר a לא הפיך ב־$\mathbb{Z}/n\mathbb{Z}$, בסתירה.
כעת, במכפלה

$$\overline{a_1 \cdot \ldots \cdot a_{\varphi(n)}}$$

מופיעים איברים וההופכיים שלהם, כאשר ב־N מהאיברים המספר שווה להופכי של עצמו. נניח בלי הגבלת הכלליות שאיברים אלו הם $a_1,\ldots,a_N$ ונקבל כי

$$a_1 \cdot \ldots \cdot a_{\varphi(n)} \equiv a_1 \cdot \ldots \cdot a_N \pmod{n},$$

כאשר $a_i^2 = a_i$ לכל $i \in [N]$.
אם $x^2=1$, גם $(-x)^2=1$, ולכן בביטוי $a_1 \cdot \ldots \cdot a_N$ מופיעות $N/2$ כפולות של איבר והנגדי שלו. עבור x כזה מתקיים $x(-x) = -x^2 = -1$. לכן

$$a_1 \cdot \ldots \cdot a_N \equiv (-1)^{N/2} \pmod{n},$$

כנדרש.