בס"ד

מסקנה ממשפט פרמה הקטן: יהי p ראשוני, $a\in N$. אז $a^p \equiv a(p)$.

נוסף המשפט לבדוק אל הבמה...

הוכחה: אם $a|p$ נקבל ממשפט פרמה הקטן (הפעלת שני הצדדים כ-a)

אם $a|p$ אז $a^p \equiv 0 \equiv a\ (p)$

עוד מסקנה ממשפט פרמה: אם p ראשוני ! $a\in N$ קש"ל $a\nmid p$ אז a^{p-2} הוא ההפכי של a מודולו p.

הוכחה:

ממשפט פרמה $a^{p-1} \equiv 1\ (\mathrm{mod}\ p)$

$$a^{p-2}\cdot a \equiv 1\ (\mathrm{mod}\ p)$$

מסקנה אחרונה: יהי p ראשוני ויהי $a\in N$ קש"ל $a\nmid p$. אז למשוואה $ax\equiv b\ (p)$ יש פתרון יחיד מוד p, והוא $x\equiv a^{p-2}b\ (p)$

הוכחה: תזכורת: למשוואה $ax\equiv b\ (m)$ יש פתרון — מוד m כאשר $d|b$ כלומר אין פתרון

פתרון יחיד יש לפי האלגוריתם כי $1=(a,p)$.

(כלומר כי x אכן פתרון מוד p

$$ax = a\cdot(a^{p-2}b) = a^{p-1}b \underset{\text{משפט פרמה}}{\equiv} 1\cdot b \equiv b\ (p)$$

תרגיל לדוגמה: חשבו $3^{201}\ (11)$

פתרון: לפי משפט פרמה $3^{10}\equiv 1\ (11)$ ולכן

$$3^{201} = 3^{200}\cdot 3^1 = (3^{10})^{20}\cdot 3^1 \equiv 1^{20}\cdot 3 \equiv 3\ (11)$$

עוד תרגיל לדוגמה: הוכיחו כי לכל $a\in N$, $a^{21}\equiv a\ (\mathrm{mod}\ 15)$.

פתרון: הרעיון: הכנה לשימוש במשפט פרמה הבדוק ב-15 לא ראשוני

שלב א:

כלומר כי ① $a^{21}\equiv a\ (3)$
וכי ② $a^{21}\equiv a\ (5)$ } (*)

נבדוק לשניהם

① $a^3\equiv a\ (3) \Leftarrow$

לפי המסקנה ממפרמה הבדוק לשניהם בכבוד לאלגוריתם לפי אם $a\nmid p$

$$a^{21} = (a^3)^7 \equiv a^7 \equiv a^3\cdot a^3\cdot a \equiv a\cdot a\cdot a \equiv a\ (3)$$

② $a^5\equiv a\ (5) \Leftarrow$

$$a^{21} = (a^5)^4\cdot a \equiv a^4\cdot a \equiv a^5 \equiv a\ (15)$$

מסקנה פרמה

שלב ב: כלומר כי מ(*) נקבל $a^{21}\equiv a\ (15)$

אכן, לפי (*) $a^{21}\equiv a\ (3)$ וגם $a^{21}\equiv a\ (5)$

ולכן $\underset{15}{\mathrm{lcm}(3,5)} \mid a^{21}-a$

לפי תרגיל שקילות אלף 3

בס"ד

לפי תרגיל לדוגמה: יהי $a\in\mathbb{N}$ כך ש- $7\nmid a$. המשמעות: או $a^3\equiv 1\ (7)$ או $a^3\equiv -1\ (7)$.

בדיוק: לפי משפט פרמה $a^6\equiv 1\ (7)$

$$\Downarrow$$

$(a^3-1)(a^3+1)=a^6-1\ \vdots\ 7$ "לא ראשוני מתלך מספר חשב מתלך ב- אחד הגורמים"

לכן או ש $7\mid a^3-1$ ואז $a^3-1\equiv 0\ (7)$ כלומר $a^3\equiv 1\ (7)$

או ש $7\mid a^3+1$ ואז $a^3+1\equiv 0\ (7)$. כלומר $a^3\equiv -1\ (7)$.

בס"ד

מבחן ראשוניות לפי פרמה

תזכורת: **משפט פרמה קטן:** אם p ראשוני אז לכל $a\in\mathbb{N}$ $a^p\equiv a\ (p)$.

מבחן פרמה לראשוניות: אם קיים $a\in\mathbb{N}$ כך ש $a^n\not\equiv a\ (n)$, סימן ש-n לא ראשוני.

פלמאו: האם 341 ראשוני?

נבחר $a=7$. אם נקבל $7^{341}\not\equiv 7\ (341)$ סימן ש-341 לא ראשוני.

נחשב:

$$7^{341}=7^2\cdot 7^{339}=7^2\cdot(7^3)^{113}=7^2\cdot 343^{113}\equiv 7^2\cdot 2^{113}\equiv$$

קשה לשים לב כי $341=11\cdot 31$

אבל קל לשים לב כי $339=3\cdot 113$

$2^{10}=1024\equiv 1\ (341)$

כי $341\cdot 3=1023$

$$\equiv 7^2\cdot(2^{10})^{11}\cdot 2^3\equiv 7^2\cdot 1^{11}\cdot 2^3\equiv 49\cdot 8=392\equiv 51\pmod{341}$$

קיבלנו כי $7^{341}\equiv 51\not\equiv 7\ (341)$ ולכן 341 לא ראשוני.

הרעיון בהפוך של מבחן פרמה לראשוניות לא נכון! כלומר:

אם מצאנו $a\in\mathbb{N}$ כך ש- $a^n\equiv a\ (n)$ זה עדיין לא אומר ש-n ראשוני.

אבל אז n "מתפשט לראשוני" כאשר a "מעיד לו" להתפשט.

במקרה זה אומרים כי n פסאודו-ראשוני בבסיס a. (n מתנהג בדיוק לבסיס a כאילו הוא ראשוני.)

הגדרה: יהי $a\in\mathbb{N}$. מספר פריק $n\in\mathbb{N}$ המקיים $a^n\equiv a(n)$ נקרא פסאודו ראשוני בבסיס a.

דוגמה: (הגדרה ע"י Sarrus ב- 1919)

$341=11\cdot 31$ פריק, אבל הוא פסאודו ראשוני בבסיס 2. לדוגמה:

$$2^{341}\equiv 2\ (341)$$

שימו לב: 341 פסאודו ראשוני בבסיס 2 אבל לא בבסיס 7, כי ראינו

$$7^{341}\not\equiv 7\ (341)$$

הוכחת הדוגמה של Sarrus: עלינו להראות כי $2^{341}\equiv 2(341)$

מכיוון ש $341=11\cdot 31$

לפי התכונה 3' שקולה שני הפרטים:

תכונה (מתרגל שקולות חלק 3):
אם $a\equiv b\ (m_1)$ וגם $a\equiv b\ (m_2)$
אז $a\equiv b\ (\mathrm{lcm}(m_1,m_2))$.

א)

$2^{341}\equiv 2(31)$

אבל,

$2^5=32\equiv 1\ (31)$

$2^{340}=2^{5\cdot 68}=(2^5)^{68}\equiv$

$\equiv 1^{68}\equiv 1\pmod{31}$

לכן

$2^{341}=2\cdot 2^{340}\equiv 2\cdot 1\equiv 2(31)$

וגם ב)

$2^{341}\equiv 2\ (11)$

אבל,
ממשפט פרמה נובע

$2^{10}\equiv 1\pmod{11}$

ולכן

$2^{341}=2^1\cdot(2^{10})^{34}\equiv 2\cdot 1^{34}\equiv 2(11)$

שימו לב שאנחנו לומדים כאן כלים שונים בתדרוך בחשבון מודולרי!

כפולות לדעת (אבל לא נוכיח): לכל $b\in\mathbb{N}$ יש ∞ פסאודו ראשוניים בבסיס b, אבל הם נדירים יותר מאשר הראשוניים.

הערה: ראינו כי $n=341$ פסאודו ראשוני בבסיס 2 ולא בבסיס 7. לכן אם נשה לו מבחן ראשוניות לפי פרמה עם בסיס 7 נגלה שהוא לא ראשוני, אבל אם נשה לו מבחן זה בבסיס 2 לא נגלה כלום.

יש עוד n-ים שהם פסאודו-ראשוניים לפי כל בסיס, כלומר שעוברים בדיקת ראשוניות לפי פרמה לא תגלה לעולם! מספרים אלו נקראים מספרי קרמיכל, או "פסאודו ראשוניים אמיתיים".

למספרים הללו יש אפיון ברור, שלא נלמד הסמסטר. מספר קרמיכל הקטן ביותר הוא $561=3\cdot 11\cdot 17$

משפט אוילר (Euler)

מוטיבציה: למדנו את משפט פרמה $a^{p-1}\equiv 1 \ (p)$ (לכל a). המבחן שלום. p לפי הראשוני, משפט פרמה לא נותן כלום. משפט אוילר מאשר לכולל את משפט פרמה למודולו לא ראשוני.

הגדרה: (פונקציית אוילר)

לכל n טבעי

$$\varphi(n) = |\{k\in[n] \mid (k,n)=1\}| = \text{כמות המספרים שזרים/שונים ל-}n$$

לדוגמה:

$$\varphi(10) = \boxed{4} \qquad \varphi(1)=1$$

$$\{1,3,7,9\}$$

$$\varphi(7) = 6$$

$$\{1,2,3,4,5,6\}$$

(שמו לב לכך ש-7 הראשוני לכן לכל המספרים $1,\dots,6$ זרים לו)

אבחנה: $\varphi(n) = n-1$ אם ורק אם n ראשוני. (אם n ראשוני אז כל המספרים $1,\dots,n-1$ זרים לו ואם n פריק אז לפחות אחד מהם לא זר לו.)

משפט אוילר: לכל $n>1$ ולכל $a\in\mathbb{Z}$ כך ש $(a,n)=1$ מתקיים:

$$a^{\varphi(n)} \equiv 1 \pmod n$$

שימו לב - אם נציב $p=n$ ראשוני, קבל את משפט פרמה! (מקרה פרטי של משפט אוילר) ("משפט פרמה הכללי")

ההצהרה דומה מאוד להוכחת משפט פרמה! לסדר נקודתי בקבוצת הכפלת.

הגדרה: יהי $n>1$. מערכת שאריות מצומצמת מודולו n היא קבוצה של $\varphi(n)$ מספרים למספרים כך ש- ① כל אחד מהמספרים זר לו.

② כולם בעלי שקילות בדיוק מודולו n.

לדוגמה: מערכת שאריות מצומצמת מודולו 8: $\{1,3,5,7\}$ (הקטנה)

אך " " " " " $\{3,9,15,21\}$ → מכפלה ב-3 של הקטנה

$3 \quad 1 \quad 7 \quad 5$ (מודולו 8)

דיון: המכפלה ב-3 יצרה מערכת שאריות מצומצמת כן כי $(3,8)=1$. אולם היינו מכפלים ב-2 שאינו זר ל-8, היינו מקבלים $\{2,6,10,14\}$ ואז $10\equiv 2 \ (8)$.

למה יהי $a,n\in\mathbb{N}$ כך ש $(a,n)=1$. אם $r_1,\dots,r_{\varphi(n)}$ היא מערכת שאריות מצומצמת מודולו n, אז גם $a\cdot r_1,\dots,a\cdot r_{\varphi(n)}$ היא מערכת שאריות מצומצמת מודולו n.

הוכחת הלמה:

נראה כי: (א) לכל j משלים נ"ז ar_j זר ל-n

(ב) עבור $j \neq k$ $ar_j \not\equiv ar_k \ (n)$

אכן

(א) a זר ל-n ולכן אין לו גורם ראשוני משותף עם n.
r_j זר ל-n ולכן אין לו גורם ראשוני משותף עם n.
$\Leftarrow (ar_j, n) = 1$

(ב) נניח בשלילה $ar_j \equiv ar_k \ (n)$ עבור $j \neq k$ אז לפי כלל הצמצום (המקום: "מותר לצמצם בשני הצדדים זר למודולו") נקבל $r_j \equiv r_k \ (n)$ בסתירה לנתון. ☒

עכשיו סיימנו את ההכנה ונפנה להוכחת משפט אוילר. (שמו לב לדמיון להוכחת שלמה פרמה)

הוכחת משפט אוילר:

יהי a, n כנתוני המשפט. תהי $r_1, \dots, r_{\varphi(n)}$ מערכת שאריות מצומצמת מודולו n. לפי הלמה זה $ar_1, \dots, ar_{\varphi(n)}$ מערכת שאריות מצומצמת מודולו n.

$\Leftarrow$

$$(ar_1)\cdot(ar_2)\cdot\ldots\cdot(ar_{\varphi(n)}) \equiv r_1 \cdot \ldots \cdot r_{\varphi(n)} \ (n)$$

$$\Leftarrow a^{\varphi(n)} \cdot r_1 \cdot \ldots \cdot r_{\varphi(n)} \equiv r_1 \cdot \ldots \cdot r_{\varphi(n)} \ (n)$$

$$\Leftarrow a^{\varphi(n)} \equiv 1 \ (n),$$

לפי כלל הצמצום.
"אפשר לצמצם בשני הצדדים כל עוד המצומצם זר למודולו"
ולא r_j כי מעל אפס בשונה אל n

☒

נרשום כשהוא כי פונקציה אוילר φ כך תשובה, ולעתים אין לחשב אותה:

תשובה $\varphi(n)$

שלב א': תשובה $\varphi(p^k)$

טענה: עבור p ראשוני $k \in \mathbb{N}$ מתקיים $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$

הוכחה: המספרים בקטע $[1, p^k]$ שאינם זרים ל-p^k הם $p, 2p, 3p, 4p, \dots, p^{k-1}$. כלומר יש p^{k-1} מספרים בקטע שאינם זרים ל-p^k ולכן כמות הזרים ל-p^k בקטע זה, היא

$$p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$$

דוגמה:

$$\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$$

שלב ב: חישוב $\varphi(n)$ לכל n.

הסבר אינטואיטיבי:

$$\varphi(72) = \varphi(9\cdot 8) = \varphi(3^2\cdot 2^3) = \varphi(3^2)\cdot\varphi(2^3) = \underbrace{(3^2-3)}_{6}\underbrace{(2^3-2^2)}_{4} = 24$$

אנחנו מעוניינים לדעת הכפלתיות! כלומר $\varphi(mn)=\varphi(m)\varphi(n)$

הגדרה: פונקציה $f: \mathbb{N}\to\mathbb{N}$ נקראת כפלית אם לכל m,n עם $(m,n)=1$ מתקיים $f(mn)=f(m)\cdot f(n)$.

טענה: פונק' אוילר φ היא כפלית.

מסקנה - איך נחשב כל $\varphi(n)$: אם $n = p_1^{a_1}\cdot p_2^{a_2}\cdot\dots\cdot p_k^{a_k}$ (פירוק רגיל לראשוניים)

$$\varphi(n) = \varphi(p_1^{a_1})\cdot\dots\cdot\varphi(p_k^{a_k}) = p_1^{a_1}\left(1-\frac{1}{p_1}\right)\cdot\dots\cdot p_k^{a_k}\left(1-\frac{1}{p_k}\right) = n\left(1-\frac{1}{p_1}\right)\cdot\dots\cdot\left(1-\frac{1}{p_k}\right)$$

[הוכחת המסקנה - תרגיל (לפי כך ש-φ כפלית + אינדוקציה על k)]

הוכחת הטענה: יהיו m,n מקיימים $(m,n)=1$. נרצה להראות כי $\varphi(mn)=\varphi(m)\varphi(n)$.

נרשום בטבלה את כל המס' מ-1 עד mn (נרצה לספור כמה מהם זרים ל-mn).

דוגמה: $m=4$, $n=3$

1	2	3	4
5	6	7	8
9	10	11	12

1	2	3	...	r	...	m
m+1	m+2	m+3	...	m+r	...	2m
2m+1	2m+2	2m+3	...	2m+r	...	3m
			⋮			
m+1+m(n-1)	m+2+m(n-1)			m+r+m(n-1)		mn

נרצה לספור כמה l-ים בטבלה זרים ל-mn. **תזכורת 1:** $(l,mn)=1$ אמ"מ $(l,m)=1$ וגם $(l,n)=1$. (לא זר ל-mn אמ"מ l זר ל-m וl זר ל-n).

תזכורת 2: כל איבר בטור מס' r זר ל-m אמ"מ $(m,r)=1$. (להראות על הדוגמא)

לכן כל המספרים הזרים ל-m הם אברי $\varphi(m)$ השאריות המתחלקים בסך הכל ל-m.

נרשום נכונה שבמקום כל שאר כך יש בדיוק $\varphi(m)$ אברים זרים ל-m, וקיים נבדוק שמספר יש $\varphi(m)\cdot\varphi(n)$ אברים בטבלה הזרים ל-mn כלומר יש $\varphi(mn)=\varphi(m)\varphi(n)$.

נבחר שאר לשכן המתחלק ב-r ונראה כי כל אבר בלתי שלילי בצורה מקבלו n, כלומר נראה כי כל שאר מהווה מכפלת שארית שלמה מקבלו n ולכן בכל שאר יש בדיוק $\varphi(n)$ אברים הזרים ל-n.

אכן, אם נניח בשלילה כי בשאר המתחלק ב-r מתקיים

$$jm+r \equiv km+r \pmod n \qquad 0\le j<k\le n-1$$

$$jm \equiv km \pmod n$$

$$\Leftarrow \quad j\equiv k \pmod n \quad \text{סתירה.}$$

מותר לצמצם בגורם זר למודולו

לסיכום: יש $\varphi(m)$ שאריות שלמות אברים זרים ל-m ובכל שאר יש $\varphi(n)$ אברים שזרים ל-n, סה"כ $\varphi(m)\varphi(n)$ אברים $\underbrace{\text{שזרים ל-m וזרים ל-n}}_{\text{שזרים ל-mn (חוב 1)}}$. לכן $\varphi(mn)=\varphi(m)\varphi(n)$.

סכום חבורה:

חוב 1: $(l,mn)=1$ אם"ם $(l,m)=1$ וגם $(l,n)=1$.

($\Rightarrow$) אין ל-l גורם ראשוני משותף עם mn ואין לו גורם ראשוני משותף עם n ולכן אין ל-l גורם ראשוני משותף עם m.

($\Leftarrow$) אין ל-l גורם ראשוני משותף עם mn ולכן אין לו גורם ראשוני משותף עם m וגם אין לו גורם ראשוני משותף עם n.

חוב 2: אברי השאר המתחלק ב-r הם בדיוק מהצורה $qm+r$, $0\le q\le n-1$.

אם $(r,m)=(m,qm+r)$ (זה נמצא בעזרת האלגוריתם של אוקלידס)

ולכן כל אברי השאר זרים ל-m אם"מ r זר ל-m.

שימוש במשפט אוילר למציאת הפכי מודולו n: ניתן לענות בשאלות אלו גם לפי הקשר הפכי כשאר יש רוצים לחשב הפכים)

אם $(a,n)=1$ אז ההפכי של a מודולו n הוא $a^{\varphi(n)-1}$ כי

$$a\cdot a^{\varphi(n)-1}=a^{\varphi(n)}\equiv 1 \pmod n$$

לדוגמא: נחשב את ההפכי של 2 מודולו 25. **פתרון:** $2^{19}=2^{\varphi(25)-1}$

$$2^2=4\equiv 4 \pmod{25}$$
$$2^4\equiv 2^2\cdot 2^2\equiv 4\cdot 4\equiv 16 \pmod{25}$$
$$2^8=2^4\cdot 2^4\equiv 16\cdot 16\equiv 256\equiv 6 \pmod{25}$$
$$2^{16}=2^8\cdot 2^8\equiv 6\cdot 6\equiv 36\equiv 11 \pmod{25}$$
$$\Rightarrow 2^{19}=2^{16}\cdot 2^2\cdot 2^1\equiv 11\cdot 4\cdot 2=88 \pmod{25}$$

אז הדרך של המחלה ודרך בחירה לחשוב חיבור שלם

הפכי

$\varphi(m)=2$

מודולו m:

$\varphi(n)=2$

1 2 3 4
5 6 7 8
9 10 11 12

ברים ל m

כל שאר = מחלקת שארית שלמה מודולו 3.