(1)

<u>בעיה</u> נתון a,b,m. מצא x כך ש $x\cdot a\equiv b \pmod m$

לדוגמא: מצא x כך ש $9x\equiv 12 \pmod{15}$

<u>משפט:</u> נסמן $d=\gcd(a,m)$ $d=3$

אם $d\nmid b$ (לא מחלק) - אין פתרון

אם $d\mid b$ - יש d פתרונות שונים למודולו m.

<u>הוכחה ודרך הפתרון:</u> רוצים $m\mid(ax-b)$

<u>אז</u> $ax-b=my$

<u>אז</u> $ax-my=b$

אנחנו יודעים שיש פתרון אם ורק אם $\gcd(a,m)\mid b$

יהי (x_0,y_0) פתרון אחד. אז הפתרון הכללי הוא:

$x=x_0+\left(\frac{m}{d}\right)t$ ← מה שרצינו   (t שלמים)

$y=y_0+\left(\frac{a}{d}\right)t$ ← לא מעניין אותנו

טענה: ניקח שני פתרונות שבאים משני t שונים.

$x_2=x_0+\frac{m}{d}t_2$ $x_1=x_0+\frac{m}{d}t_1$

אז $x_1\equiv x_2 \pmod m$ <u>אם ורק אם</u> $t_1\equiv t_2 \pmod d$

[מכיוון שיש d מחלקות של t מודולו d $(t=0,1,\dots,d-1)$
אז יש d פתרונות שונים ל-x מודולו m]

שני הכוונים ביחד $x_1\equiv x_2 \pmod m$

$\Updownarrow$

$$x_0+\frac{m}{d}t_1\equiv x_0+\frac{m}{d}t_2 \pmod m$$

$\Downarrow$

$$\frac{m}{d}t_1\equiv\frac{m}{d}t_2 \pmod m$$

תזכורת: מתי מותר לצמצם: אם $ac\equiv bc \pmod z$

אז $a\equiv b \pmod{\frac{z}{F}}$

כאשר: $F=\gcd(c,z)$

(2)

דוגמא: מצא את כל הפתרונות מודולו 15 של

שקול ל-

$9x \equiv 12 \pmod{15}$

$9x - 12 = 15y$

$9x - 15y = 12$

פתרון: $a = 9$, $m = 15$, $b = 12$, $d = \gcd(a,m) = 3$

$\gcd(15,9)$ $15 = 1\cdot 9 + 6$

$\gcd(9,6)$ $9 = 1\cdot 6 + 3$

$\gcd(6,3) = 3$

נעשה gcd מורחב על 9,15

$3 = 1\cdot 9 - 1\cdot 6$

$6 = -1\cdot 9 + 1\cdot 15$

$3 = 1\cdot 9 - 1\cdot 15 + 1\cdot 9$

$3 = (-1)\cdot 15 + (2)\cdot 9$

$\times 4$

$12 = (-4)\cdot 15 + (8)\cdot 9$

פתרון ← $x_0 = 8$, $y_0 = 4$

פתרון כללי: $x = 8 + 5t$

$y = 4 + 3t$ ← לא מעניין

נבחר $t = 0,1,2$:

$x_1 = 8$, $x_2 = 13$, $x_3 = 18$

מסקנה: אם a,m זרים אז למשוואה $ax \equiv 1 \pmod{m}$ יש פתרון יחיד מודולו m

מסמנים את הפתרון הזה $a^{-1} \pmod{m}$

וקוראים לו "ההופכי של a מודולו m".

תרגיל: מצא את ההופכי של 22 מודולו 41.

פתרון: רוצים $22x \equiv 1 \pmod{41}$. מורחב $\gcd(41,22)$:

$\gcd(41,22) =$ $41 = 1\cdot 22 + 19$

$\gcd(22,19) =$ $22 = 1\cdot 19 + 3$

$\gcd(19,3) =$ $19 = 6\cdot 3 + 1$

$\gcd(3,1) = 1$ $1 = 19 - 6\cdot 3$

$3 = 22 - 19$

$1 = -6\cdot 22 + 7\cdot 19$

$19 = 1\cdot 41 - 1\cdot 22$

$1 = 7\cdot 41 - 13\cdot 22$

$1 - (-13)\cdot 22 = 7\cdot 41$

$41 \mid (1 - (-13)\cdot 22)$

תזכורת: $x \equiv y \pmod{z} \iff z \mid (x-y)$

במקרה שלנו: $1 \equiv (-13)\cdot 22 \pmod{41}$

לכן $x = -13$

בדיקה: $-13\cdot 22 = -286$

$41 \mid -287$

פתרון קטן:

$0 \le x < 41$

$x = -13 + 41 = 28$

$x = 28$

שאלת המשק: מצא y כך ש- $22y \equiv 30 \pmod{41}$

$y \equiv \underbrace{28 \cdot 22}_{\equiv 1} y = 28 \cdot 30 \pmod{41}$

$y = 28 \cdot 30 \pmod{41}$

פתרון: באופן כללי: מצא y כך ש- $ay = b \pmod m$ כאשר a, m זרים.

$a^{-1} a y \equiv a^{-1} b \pmod m$

a^{-1} מסמן מספר שלם כך ש- $a \cdot a^{-1} \equiv 1 \pmod m$

$5 \cdot x \equiv 1 \pmod{41}$

תזכורת: אם $x \equiv y \pmod m$

אז $xz \equiv yz \pmod m$

$28 \cdot 22 \equiv 1 \pmod{41}$

$\Downarrow$

$28 \cdot 22 y \equiv y \pmod{41}$

$y \equiv 28 \cdot 30 \equiv 8 \cdot 40 \equiv 20 \pmod{41}$ (שארית)

$840 = 20 \cdot 41 + 20$

~~תשובה לתרגיל~~

תשובה לתרגיל: $y = 20$

בדיקה:

תרגיל: חשב את $(129^6 \cdot 21 + 730) \bmod 5$

$\underbrace{129^6}_{\equiv 4} \cdot \underbrace{21}_{\equiv 1} + \underbrace{730}_{\equiv 0} \equiv 4^6 \cdot 1 + 0 \equiv 4096 \equiv 1 \pmod 5$

$129 \bmod 5 = 4$

$129 \equiv 4 \pmod 5$

אותה שארית.

פתרון: 1

למה זה מותר?

תזכורת: אם

$a \equiv b \pmod m$

$c \equiv d \pmod m$

אז

$a + c \equiv b + d \pmod m$

$a \cdot c \equiv b \cdot d \pmod m$

במקרה שלנו -

$a^6 \cdot b + c \quad a \equiv 4, b \equiv 1, c \equiv 0$

6 פעמים:

$a \equiv 4$

$a \equiv 4$

$a \equiv 4$

$a \equiv 4$

$a \equiv 4$

$a \equiv 4$

$a^6 \equiv 4^6 \pmod m$

$b \equiv 1 \pmod m$

$a^6 \cdot b \equiv 4^6 \cdot 1 \pmod m$

$c \equiv 0 \pmod m$

$a^6 \cdot b + c \equiv 4^6 \cdot 1 + 0 \pmod m$

שאלת המשק: מצא y כך ש- $22y \equiv 30 \pmod{41}$

ידוע - $22 \cdot 28 \equiv 1 \pmod{41}$

$$22 \cdot y \equiv 30 \pmod{41}$$
$$28 \equiv 28 \pmod{41}$$

$$\underbrace{22 \cdot 28}_{\equiv 1} y \equiv 28 \cdot 30 \pmod{41}$$

$$y \equiv 28 \cdot 30 \equiv 20 \pmod{41}$$

(20 ← שארית)

משפט: יהי p ראשוני.

אז a הופכי של עצמו מודולו p (A)

אם ורק אם $a \equiv \pm 1 \pmod{p}$ (B)

הוכחה: כיוון אחד קל. $(B \Rightarrow A)$

דוגמא: * 16 הופכי של עצמו מודולו 17.

* 1 הופכי של עצמו מודולו 17.

$$\underbrace{16}_{\equiv -1} \cdot \underbrace{16}_{\equiv -1} \overset{?}{\equiv} 1 \pmod{17}$$

$$16 \cdot 16 \equiv (-1) \cdot (-1) \equiv 1 \pmod{17}$$

נוכיח כיוון: $A \Rightarrow B$

נניח A $a \cdot a \equiv 1 \pmod{p}$ כלומר $p \mid (a^2 - 1)$

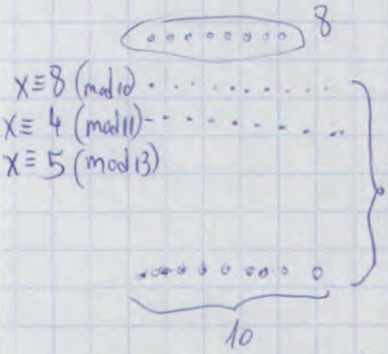
כלומר $p \mid (a+1)(a-1)$

$$p \mid (a-1) \text{ או } p \mid (a+1)$$

$$a \equiv 1 \pmod{p} \Leftrightarrow p \mid (a-1) \qquad a \equiv -1 \pmod{p} \Leftrightarrow p \mid (a+1)$$

$$Z \mid (x-y) \Leftrightarrow x \equiv y \pmod{Z}$$

מ.ש.ל



משפט השאריות הסיני

היה מפקד סיני שכדי לספור את החיילים שלו הוא כל הזמן אמר להם לעמוד בשורות של 10, בשורות של 11, בשורות של 13. הסתכל על החיילים שנשארו כל פעם בשורה לא שלמה. ולפי זה הוא חישב כמה חיילים יש לו.

משפט: נניח ש- $m_1,\dots,m_r$ זרים בזוגות (כל m_i זר לכל m_j)

נסמן $M = m_1 \cdot \ldots \cdot m_r$

נתון:

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_r \pmod{m_r}$

(מספרים נתונים)

אז יש פתרון יחיד ל-x מודולו M.

לפני ההוכחה - האם זה בכלל הגיוני?

\# אפשרויות ל-x מודולו 1430: 1430

\# אפשרויות לבחור a_1, a_2, a_3: 1430

(a_1: 10 אפשרויות, a_2: 11 אפשרויות, a_3: 13 אפשרויות)

הוכחה: נסמן

$$M_1 = \frac{M}{m_1}, \quad M_2 = \frac{M}{m_2}, \quad \ldots, \quad M_r = \frac{M}{m_r}$$

(שלמים)

תהי y_k ההופכי של M_k מודולו m_k. (זרים)

בדוגמה שלנו - $m_1 = 10$, $m_2 = 11$, $m_3 = 13$ (זרים)

$M_1 = m_2 \cdot m_3 = 143$ $\quad M_2 = m_1 \cdot m_3 = 130$ $\quad M_3 = m_1 \cdot m_2 = 110$

בדוגמה שלנו - y_1 ההופכי של 143 מודולו 10.

$130 y_2 \equiv 1 \pmod{11}$

$9 y_2 \equiv 1 \pmod{11}$

$\boxed{y_2 = 5}$

$143 \cdot y_1 \equiv 1 \pmod{10}$

$3 \cdot y_1 \equiv 1 \pmod{10}$

$\boxed{y_1 = 7}$

$110 \cdot y_3 \equiv 1 \pmod{13}$

$6 \cdot y_3 \equiv 1 \pmod{13}$

$\boxed{y_3 = 11}$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 8 \cdot 143 \cdot 7 + 4 \cdot 130 \cdot 5 + 5 \cdot 110 \cdot 11 = 8008 + 2600 + 6050 =$$
$$16{,}658 \equiv 928 \pmod{1430}$$

תרגיל: חשב את $137^{4309} \mod 177$. (יצא מס' בין 0-176, אבל השאלה איזה מספר?)

פתרון:

$$137^{4309} = 137^{2^{12}} \cdot 137^{2^7} \cdot 137^{2^6} \cdot 137^{2^4} \cdot 137^{2^2} \cdot 137$$

$$137^{2^i} = \left(137^{2^{i-1}}\right)^2$$

→ $137 \mod 177 = 137$ ה.3

$137^2 \mod 177 = 7$

~~$137^{2^2} \mod 177 = 7^2 = 49$~~ → $137^4 = 137^{2^2} \equiv 7^2 = 49 \pmod{177}$

~~$137^8 \mod 177 = 49^2 =$~~ $137^8 \equiv 49^2 \equiv 100 \pmod{177}$

~~$137 \mod 177$~~

→ $137^{16} \equiv 100^2 \equiv 88 \pmod{177}$

$137^{2^5} = 88^2 \equiv 133 \pmod{177}$

→ $137^{2^6} \equiv 133^2 \equiv 166 \pmod{177}$

→ $137^{2^7} \equiv 166^2 \equiv 121 \pmod{177}$

$137^{2^8} \equiv 121^2 \equiv 127 \pmod{177}$

$137^{2^9} \equiv 127^2 \equiv 22 \pmod{177}$

$137^{2^{10}} \equiv 22^2 \equiv 130 \pmod{177}$

$137^{2^{11}} \equiv 130^2 \equiv 85 \pmod{177}$

→ $137^{2^{12}} \equiv 85^2 \equiv 145$

הפתרון:

$145 \cdot 121 \cdot 166 \cdot 88 \cdot 49 \cdot 137$

משפט ווילסון - wilson

p הוא ראשוני אמ"ם $(p-1)! \equiv -1 \pmod p$.

דוגמה: $p=11$

$10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv 10 \equiv -1$

(2, 5, 2, 1, 5, 9, 5, 10)

תזכורת:

* לכל $a \neq 0$ מודולו p קיים הופכי מודולו p.
(קיים b כך ש $ab \equiv 1$)

* **הערה:** לשני מספרים שונים (מודולו p) יש הופכיים שונים מודולו p.

הוכחה: נניח ש- $a_1 \neq a_2$ מודולו p. אבל $a_1 b \equiv a_2 b$ סתירה. מש"ל.
(כי שניהם שקולים ל-1)

תזכורת:

1) אם $xz \equiv yz \pmod m$ אז $x \equiv y \pmod{\frac{m}{d}}$ כאשר $d = \gcd(m,z)$

2) המספרים היחידים שהם הופכיים של עצמם מודולו p הם ± 1.

* הערה: אם b הוא ההופכי של a אז a הוא ההופכי של b.

משפט וילסון

p הוא ראשוני אמ"מ $(p-1)! \equiv -1 \pmod p$
(A ⟸ B)

הוכחה: כיוון 1 (⇐):

$$(p-1)! = 1\cdot 2\cdot 3\cdots(p-2)\cdot(p-1) \equiv 1\cdot1\cdot1\cdot1\cdots1\cdot(-1) \equiv -1$$

(1 – הופכי של עצמו; $2\cdots(p-2)$ – מספר זוגי של איברים, הופכיים; $p-1 \equiv -1$ – הופכי של עצמו)

$1\cdot2\cdot3\cdots6\cdots9$ (הופכיים)

מ.ש.ל. B⇐A

כיוון 2 (⇒): A ⇐ B. נוכיח ¬B ⇐ ¬A

נניח n (בפרט) לא ראשוני. כלומר $n=a\cdot b$ כאשר $1<a,b$.

נניח בשלילה $(n-1)! \equiv -1 \pmod n$

כלומר $n \mid ((n-1)!+1)$

לכן $a \mid ((n-1)!+1)$

אבל $a \mid (n-1)!$ — $(n-1)! = 1\cdot2\cdot3\cdots a\cdots(n-1)$

ולכן $a \mid 1$ ⟸ סתירה! (כי $1<a$ בתנאים)

($a\mid x$, $a \mid y$ ⟸ $a \mid x-y$)

צריך לבדוק האם n ראשוני:

פשוט נחשב את $(n-1)! \pmod n$ ונבדוק האם יוצא -1.

לדוג' האם 91 ראשוני? $90! = 90\cdot89\cdot88\cdots \not\equiv -1 \pmod{91}$

אבל השיטה הזאת לא כל-כך יעילה אז יש משפט שלא תמיד עובד אבל יעיל יותר.

המשפט הקטן של פרמה Fermat's little theorem

אם p ראשוני ו- $a \not\equiv 0$ מודולו p אז $a^{p-1} \equiv 1 \pmod p$.

הוכחה: ניקח את המספרים $a, 2a, 3a, \dots, (p-1)a \pmod p$

* הם כולם שונים כי אם $ia \equiv ja$ ⟸ $i \equiv j$ ⟸ $i=j$
* הם כולם בין 1 לבין $p-1$.

$a, 2a, 3a, 4a, 5a, 6a \pmod 7$
$1, 2, 3, 4, 5, 6$

$a \equiv i_1$, $2a \equiv i_2$, …, $(p-1)a \equiv i_{p-1}$

$$a\cdot 2a\cdot 3a\cdot 4a\cdots(p-1)a \equiv 1\cdot2\cdot3\cdots(p-1) \pmod p$$

מש"ל $a^{(p-1)} \equiv 1 \pmod p$

לדוגמה: $p=7$

- $a=1$: $1^6 \equiv 1$
- $a=2$: $2^6 \equiv 1$
- $a=3$: $3^6 \equiv 3^3\cdot3^3 \equiv 1$
- $a=4$: $4^6 \equiv 4^3\cdot4^3 \equiv 1$
- $a=5$: $\equiv 1$
- $a=6$: $\equiv 1$

לכן ראשוני.

$p=9$

- $a=2$: $2^8 \equiv 4$

לכן 9 לא ראשוני.

שיעור 10

המשפט הקטן של פרמה

אם p הוא ראשוני ו-a לא מתחלק ב p
או $\gcd(a,p)=1$ אז $a^{p-1} \equiv 1 \bmod p$

הוכחה

טענה - המספרים $a, 2a, 3a, \dots, (p-1)a$
שקולים ל $1, 2, 3, \dots, p-1$ מודולו p, בסדר א
אם $i \neq j$ אז $ia \not\equiv ja \pmod p$
כי נניח ש $ia = ja$

$$\begin{aligned} a &\equiv 7 \\ 2a &\equiv 9 \\ 3a &\equiv 2 \\ &\vdots \\ (p-1)a &\equiv 13 \end{aligned} \pmod p \;\rightarrow\; 1 \dots p-1$$

בסדר מסוים.

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \bmod p$$

$$a^{p-1} \equiv 1 \pmod p$$

מסקנה

אם p ראשוני אז $a^p \equiv a \pmod p$

הוכחה שני מקרים

* אם a לא מתחלק ב p אז ממשפט פרמה
מכפל 2 אגפים ב-a

דוגמה $7, 8, 9$
$7 | m$
$8 | m$ $\quad 7 \cdot 8 \cdot 9 | m$
$9 | m$

למה שימושית אם $n_1 \dots n_k$ זרים בזוגות, m-ו
מתחלק בכל אחד מהם, אז $n_1 \cdots n_k | m$

מסקנה שימושית אם
$a \equiv b \pmod{n_1}$
$a \equiv b \pmod{n_2}$
$\vdots$
$a \equiv b \pmod{n_k}$
אז $a \equiv b \pmod{n_1 \cdots n_k}$

זרים בזוגות

הסדר של מסקנה שימושית

$a-b$ מתחלק ב n_1

$a-b$ מתחלק ב n_2

מסקנה: $a-b$ מתחלק ב $n_1 \cdots n_k$ א.מ.מ

$\Longleftarrow$ $a \equiv b$ (מודולו $n_1 \cdots n_k$)

<u>תרגיל</u>

חשב את $3^{201} \bmod 11$

<u>פתרון</u> 11 הוא ראשוני, לכן פרמה אומר:

$3^{10} \equiv 1 \pmod{11}$

[$a^{p-1} \equiv 1 \pmod p$ אם p ראשוני ו-a לא מתחלק ב-p.]

לכן:

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

<u>תרגיל</u>

<u>הוכח</u>: $a^{21} \equiv a \pmod{15}$ לכל a.

<u>הוכחה</u> נוכיח ש- $a^{21} \equiv a \pmod 3$

$a^{21} \equiv a \pmod 5$

ואז נפעיל את המסקנה השימושית, אז נקבל

$a^{21} \equiv a \pmod{15}$ וזהו

<u>יודעים</u> $a^5 \equiv a \pmod 5$

$\Downarrow$

$(a^5)^4 \equiv a^4 \pmod 5$

$\Downarrow$

$a^{20} \cdot a \equiv a^5 \pmod 5$ ← השקילות של ההתחלה

$a^{21} \equiv a \pmod 5$

<u>יודעים</u> $a^3 \equiv a \pmod 3$

$a^{21} \equiv a^7 \pmod 3$

$a^{21} \equiv a^3 \cdot a^3 \cdot a \pmod 3$

$a^{21} \equiv a \cdot a \cdot a \pmod 3$

$a^{21} \equiv a \pmod 3$

עפ"י המסקנה השימושית:

$a^{21} \equiv a \pmod{15}$

בדיקת ראשוניות של מספרים גדולים

$n = \underbrace{397 \ldots\ldots 27}_{\text{1000 ספרות}}$

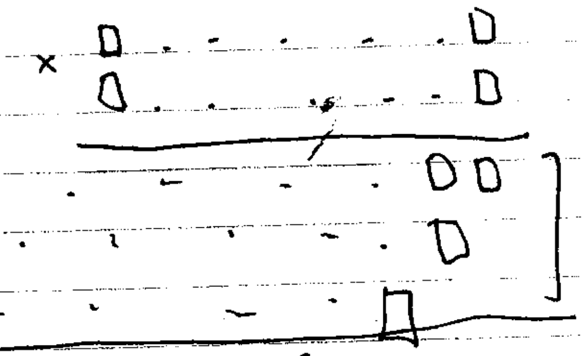
האם n ראשוני?

כפל מספרים -

$m = 235 \ldots\ldots 4$

$n = \underbrace{514 \ldots\ldots 7}_{\text{1000 ספרות}}$

רוצים - $m \cdot n$



1000×1000 פעולות.

תוצאה של 2000 ספרות

בדיקה האם n ראשוני?

$n/2$ לא
$n/3$ מתחלק
$n/4$
$\vdots$
$n/\sqrt{n}$

מספר פעולות $\sqrt{n}$

אם n לא מתחלק אף אחד אפשר לומר שהוא כן ראשוני.

$\sqrt{n} = $ 500 ספרות

בערך 10^{500} פעולות

המשפט הקטן של פרמה נותן פתרון חלקי לבדיקה

בדיקה (לא מדויקת): אם n לא ראשוני אז יש
סיכוי ½ כך ש: $a^{n-1} \not\equiv 1 \pmod n$

האם 63 ראשוני? נבחר $a=2$,
האם $2^{62} \pmod{63}$

$$2^{62} = 2^{32}\cdot 2^{16}\cdot 2^{8}\cdot 2^{4}\cdot 2^{2} = (4\cdot 16)(4\cdot 16)\cdot 4 \equiv 4$$

$4 \cdot 16 \cdot 256 \cdot 16 \cdot 4$; $256 \to 4$; $(4\cdot 16) \equiv 1$, $(4\cdot 16) \equiv 1$

$256 \equiv 4 \pmod{63}$

63 לא ראשוני.

$n = \underbrace{\qquad\qquad}_{1000}$ ספרות
בבסיס 10
כמה ספרות יש לn בבסיס 2

$n \approx 10^{1000}$
$10^{1000} = 2^{x}$
$1000\log_2 10 = x$
$x = 3320$

חישוב של $a^{n-1} = a^{\square}\cdot a^{\square}\cdot a^{\square}\cdot a^{\square}$
חזקות של 2
ריבוע מודולו n, ריבוע מודולו n
3320 פעולות
4 מס', כל 1000 ספרות.

הערה: לפעמים מספרים לא ראשוניים עוברים את הבדיקה.

דוגמה: $n=341$ $11 \cdot 31 = 341$

נחשב את $2^{340} \bmod 341$

טענה – $2^{340} \equiv 1 \pmod{341}$ ~~$2^{340} \bmod 341$~~

הוכחה –

נובע מ- $2^{10} \equiv 1 \pmod{11}$

$$\Downarrow$$

$$(2^{10})^{34} \equiv 1^{34} \pmod{11}$$

$$2^{340} \equiv 1 \bmod 11$$

$$2^{340} = (2^5)^{68} \equiv 1^{68} \equiv 1 \pmod{31}$$

$$2^5 = 32 \equiv 1 \pmod{31}$$

ננסה עם a אחר, $a=7$.

$$7^{340} \equiv 56 \pmod{341}$$

[...]

341 לא ראשוני.

מספרי Carmichael

מספרים מרוכבים שהם לא ראשוניים אבל עוברים את כל ~~הבדיקורת~~ הבדיקות של Fermat

<u>הגדרה</u>: מספר <u>לא ראשוני</u> n נקרא מס' carmichael אם לכל a שזר ל-n מתקיים:

$$a^{n-1} \equiv 1 \pmod{n}$$

<u>משפט</u>: $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$ הוא מספר carmichael <u>אם ורק אם</u> $p_1, \dots, p_k$ שונים וגם $p_i - 1 \mid n-1$ לכל $1 \le i \le k$

<u>דוגמה</u>:

$561 = 3 \cdot 11 \cdot 17$ הוא מספר קרמייקל

$3-1 \mid 561-1$

$11-1 \mid 561-1$

$17-1 \mid 561-1$

~~<u>הגדרה</u> מספר <u>לא ראשוני</u> n~~

<u>הוכחת הכיוון הקל</u>

נניח ש- $n = p_1 \cdot \dots \cdot p_n$

כך ש- $p_i - 1 \mid n-1$ לכל i

רוצה להוכיח: אם a זר ל-n אז $a^{n-1} \equiv 1 \pmod{n}$

<u>ידוע</u>: $a^{p_i - 1} \equiv 1 \pmod{p_i}$

$a^{n-1} \equiv 1 \pmod{p_i}$

$a^{n-1} \equiv 1 \pmod{p_i}$

$\vdots$

$a^{n-1} \equiv 1 \pmod{p_k}$

$a^{n-1} \equiv 1 \pmod{n}$

<u>מש"ל</u>

שיעור 11

פונקציית (טוטיינט) φ של אוילר
Eulers "totinet φ function

הגדרה: $\varphi(n)$ הוא מספר המספרים בין ~~1 ל-n הזרים ל-n~~

דוגמה: 1 2 3 4 5 6 7 8 9 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20. $\varphi(20)=8$.

לכן צריך למחוק מה שמתחלקים ב- 2 או 5. $20=2^2\cdot 5$

משפט אוילר: באם a זר ל-m [redacted]

(תזכורת: המשפט הקטן של פרמה- אם p ראשוני, ו-a זר ל-p אזי $a^{p-1}\equiv 1 \pmod p$)

למה: אם p [redacted] , $p=7$, 1,2,3,4,5,6 $\varphi(7)=6$

לכן משפט אוילר הוא הכללה של המשפט הקטן של פרמה.
(פרמה - מקרה פרטי של משפט אוילר)

תזכורת: הגדרה: אם n הוא מספר, מערכת שאריות שלמה מודולו n
היא קבוצה של n מספרים שהם כולם שונים מודולו n.

דוגמה: $n=4$. מערכת שאריות קנונית: $\{0,1,2,3\}$
אך אפשר גם לבחור: $\{12,-7,22,7\}$
מערכת שאריות אחרת.

reduced system of residus

קבוצה של $\varphi(n)$ מספרים, אחד מכל מחלקת שקילות שזרה ל-n.

דוגמה: $n=6$. מחלקות שקילות

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
⋮	⋮	⋮	⋮	⋮	⋮

$\varphi(6)=2$

rsor $=\{1,5\}$ קנוני

למה: יהי n מספר ויהי $\{a_1,a_2,\dots,a_{\varphi(n)}\}$ מערכת שאריות מצומצמת מודולו n.
יהי k מספר זר ל-n.
אז הקבוצה $\{ka_1,ka_2,\dots,ka_{\varphi(n)}\}$ היא גם מערכת שאריות מצומצמת מודולו n.

דוגמה:
$n=20$ $\varphi(n)=8$. מערכת שאריות מצומצמת: $\{1,3,7,9,11,13,17,19\}$
נבחר: $k=3$. $\{3,9,21,27,33,39,51,57\}$ היא גם מע' שא' מצומצמת (ע"פ הלמה).

הוכחה של הלמה:

נניח בשלילה ש ka_i, ka_j שייכים לאותה מחלקת שקילות:

$$ka_i \equiv ka_j \pmod n$$

ניתן לצמצם את k $a_i \equiv a_j \pmod n$ $cd(k,n)=1$

סתירה - כי הנחנו שלכל a_i, a_j הם ממחלקות שקילות אחרות

__עקרון שובך היונים pigeonhole principle__

יש n שובכים ... ; n יונים ...

כל יונה נכנסת לשובך

אין 2 יונים שנכנסו לאותו שובך

מסקנה: כל שובך קיבל יונה.

לכן: כל מחלקות השקילות מופיעות בקבוצה

החדשה: $\{ka_1, ka_2, \dots\}$

[redacted]

ניקח את מערכת שאריות מצומצמת מודולו n

$a_1, a_2, \dots, a_{\varphi(n)}$ ← אותם מספרים מודולו n רק בסדר אחר

נכפיל ב k $ka_1, ka_2, \dots, ka_{\varphi(n)}$

$$a_1 \cdot a_2 \cdots a_{\varphi(n)} \equiv ka_1 \cdot ka_2 \cdots ka_{\varphi(n)} \pmod n$$

נצמצם את כל ה a_i -ים כי הם זרים ל n

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

משל

חישוב של $\varphi(n)$:

① לגורמים: אם p ראשוני אז $\varphi(p)=p-1$

② אם $n=p^k$ כאשר p - ראשוני. ⇐ $\varphi(n)=p^k-p^{k-1} = p^{k-1}(p-1)$ למה:

__הוכחת הלמה:__ ניקח את המספרים $1,\dots,p$. ~~$p \le k \le p^k$ המספר לא זר ל p~~

המספר m לא זר ל p^k אם ורק אם $p|m$

כמה מספרים בין 1 ל p^k מתחלקים ב p ?

כמה מספרים בין 1 ל 2000 מתחלקים ב 10 ? $\frac{2000}{10}=200$

מורידים p^{k-1} מספרים. נשארים p^k-p^{k-1} משל

③ אם m,n זרים אז $\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$

דוגמה $m=8, n=9$

$\varphi(72)=\varphi(8)\cdot\varphi(9)$

$\varphi(8)=\varphi(2^3)=2^3-2^2=4$

$\varphi(9)=\varphi(3^2)=3^2-3^1=6$

$\varphi(72)=24$

מסקנה מ-3: נוסחה ל-$\varphi(n)$ עפ"י הפירוק לראשוניים של n.

$n=p_1^{a_1}\cdot\ldots\cdot p_k^{a_k}$

$\varphi(n)=\varphi(p_1^{a_1})\cdot\ldots\cdot\varphi(p_k^{a_k})$

$=p_1^{a_1}-p_1^{a_1-1}\ldots$

דוגמה:

$\varphi(2^3\cdot3^2\cdot5)=\varphi(360)$

$\varphi(2^3)\cdot\varphi(3^2)\cdot\varphi(5)=$

$4\cdot6\cdot4=96$

מסקנות: לכל $N>2$, $\varphi(n)$ זוגי.

הוכחה: 2 מקרים: ① בפירוק של n יש ראשוני אי זוגי

$n=\ldots\cdot p^k\cdot\ldots$

אי זוגי ← $\varphi(n)\cdot\ldots\cdot p^k(p-1)\cdot\ldots$ (זוגי)

② $n=2^k$ $\varphi(n)=2^{k-1}\cdot1$ $k\geq2$

② (תרגיל) אם בפירוק של n יש k ראשוניים שונים

אז $2^k|\varphi(n)$

[redacted] אם m,n זרים אז $\varphi(mn)=\varphi(m)\cdot\varphi(n)$

[redacted] נסדר את המספרים $1,\ldots,m\cdot n$

בטבלה $m\times n$

1	2	3	.....	m
m+1	m+2	m+3	.....	2m
2m+1	2m+2	2m+3	.....	3m
⋮				⋮
(n-1)m+1	(n-1)m+2		.....	nm

דוגמה: $m=5$, $n=3$

3	1	2	3	4	5
	6	7	8	9	10
	11	12	13	14	15

הערה: נתון ש m,n זרים אז:
a זר ל $n \cdot m$ אם ורק אם a זר ל m,n

צריך להוריד מהטבלה: * לא זרים לm * לא זרים לn.

נוריד את כל העמודות של מה שלא זר ל m כי כל מי שמופיע בעמודה הזו מתחלק בשקילות

בטבלה יש m עמודות, כל אחת בעלת n מספרים

מורידים את הלא זרים ל m ונשארו $\varphi(m)$ עמודות שלמות

<u>טענה:</u>
מורידים את הלא זרים ל n
בכל עמודה נשארים $\varphi(n)$ מספרים. (צ"ל)
$\Leftarrow$ נשארים $\varphi(n)\cdot\varphi(m)$ מספרים מש"ל

<u>הוכחת הטענה:</u>
העמודה מס' i מכילה את המספרים:
$i, m+i, 2m+i, \ldots\ldots (n-1)m+i$
טענה: זאת מערכת שאריות שלמה מודולו n.
צ"ל: * יש n מספרים
* כולם שונים מודולו n.
נניח בשלילה: $jm+i \equiv km+i \pmod{n}$
$jm \equiv km \pmod{n}$
$j \equiv k \pmod{n}$
מאחר כי m זר לn — סתירה. מש"ל. כי מלכתחילה הנחנו שהם שונים מודולו n

משפט: לכל n,

$$\sum_{d|n} \varphi(d) = n$$

דוגמה: $n=18$

$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)$
$+\varphi(9)+\varphi(18)$
$= 1+1+2+2+6+6=18$

הוכחה:
לכל d שמחלק את n, נגדיר את הקבוצה

$$C_d=\{i : 1\le i\le n,\ \gcd(n,i)=d\}$$

אז כל מספר בין 1 ל-n שייך בדיוק לקבוצה אחת כזאת.

דוגמה שלנו:

$C_1=\{1,5,7,11,13,17\}$
$C_2=\{2,4,8,10,14,16\}$
$C_3=\{3,15\}$
$C_6=\{6,12\}$
$C_9=\{9\}$
$C_{18}=\{18\}$

אבחנה אחת: $\sum |C_i| = n$ כי כל מספר מופיע בדיוק בקבוצה אחת

אבחנה שניה: $|C_1|=\varphi(n)$

תזכורת: $\gcd(a,b)=d$ אם ורק אם $\gcd(\frac{a}{d},\frac{b}{d})=1$

לכן: $i\in C_d$ אם ורק אם $\gcd(n,i)=d$
אם ורק אם $\gcd(\frac{n}{d},\frac{i}{d})=1$
אם ורק אם $\frac{n}{d}$ זר ל $\frac{i}{d}$

מספרים שזרים לו בין 1 ל 9 $= C_2=\{2\times\{1,2,4,5,7,8\}\}$

$$n=\sum_{d|n}|C_d| = \sum_{d|n}\varphi(\tfrac{n}{d}) \overset{??}{=} \sum_{d|n}\varphi(d)$$

(מתחת ל-$\sum|C_d|$: אבחנה אחת)

למה זה נכון? כי המחלקים של n באים בזוגות.

מחלקים של 18: $1,2,3,6,9,18$ $\quad (d,\frac{n}{d})$

מחלקים של 9: $1,3,9$

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) = \varphi(18)+\varphi(9)+\dots+\varphi(1)$$

$$\sum_{d|n} \varphi(d)=\varphi(1)+\dots+\varphi(9)+\varphi(18)$$

שיעור 12

הגדרה: יהי p ראשוני
יהי a מספר זר ל-p
a נקרא שארית ריבועית (quadratic residue)
אם קיים x כך ש: $x^2 \equiv a \pmod{p}$
אחרת, a נקרא אי שארית ריבועית (quadratic nonresidue).

דוגמה:
נמצא את השאריות ואי שאריות הריבועיות מודולו 11, $p=11$

אי שאריות ריבועיות:
$2, 7, 6, 8, 10$

שארית ריבועית:
$1^2 \equiv 1 \pmod{11}$
$6^2 = 36 \equiv 3 \pmod{11}$
$2^2 \equiv 4 \pmod{11}$
$4 \equiv 16 \equiv 5 \pmod{11}$
$3^2 \equiv 9 \pmod{11}$

שאלה: האם 68 היא שארית ריבועית מודולו 797?

למה: למשוואה $x^2 \equiv a \pmod{p}$ * כאשר הנעלם הוא x,
יש בדיוק 0 או 2 פתרונות מודולו p

* p ראשוני אי-זוגי, $gcd(a,p)=1$

שאריות ריבועיות (quadratic residues)

(1)

<u>הגדרה</u>: יהי p מספר ראשוני אי זוגי.

יהי a מספר זר ל-p.

a נקרא שארית ריבועית (quadratic residue) מודולו p אם קיים x כך ש- $x^2 \equiv a \pmod p$.

אחרת, a נקרא אי-שארית ריבועית (quadratic nonresidue).

<u>לדוגמה</u>: נמצא את השאריות והאי-שאריות הריבועיות מודולו 11. $p=11$

$1^2 = 1 \equiv 1$ $\quad$ $6^2 = 36 \equiv 3$

$2^2 = 4 \equiv 4 \pmod{11}$ $\quad$ $7^2 = 49 \equiv 5$

$3^2 = 9 \equiv 9$ $\quad$ $8^2 = 64 \equiv 9$

$4^2 = 16 \equiv 5$ $\quad$ $9^2 = 81 \equiv 4$

$5^2 = 25 \equiv 3$ $\quad$ $10^2 = 100 \equiv 1$

שארית ריבועית: 1,3,4,5,9

אי שארית ריבועית: 2,7,6,8,10

<u>שאלה</u>: האם 68 היא שארית ריבועית מודולו 97?

<u>למה</u>: למשוואה $x^2 \equiv a \pmod p$ (כאשר הנעלם הוא x) (p ראשוני אי זוגי, a זר ל-p) יש או 0 או 2 פתרונות מודולו p.

<u>הוכחה</u>: קודם נוכיח שאם יש פתרונות אז יש לפחות 2 פתרונות.

נניח שהמספר x_0 הוא פתרון (כלומר $x_0^2 \equiv a$).

אז $(-x_0)^2 = (-1)^2 x_0^2 = x_0 \equiv a$

לכן גם $-x_0$ (כלומר $p-x_0$) הוא גם פתרון.

(אולי $x_0 = p-x_0$? לא יתכן כי p הוא אי זוגי).

<u>רק חסר להוכיח</u>: אף פעם אין יותר משני פתרונות.

נניח ש x_1, x_0 הם שני פתרונות. $x_0^2 \equiv a \pmod p$, $x_1^2 \equiv a$.

$\Downarrow$ במילים אחרות

$x_0^2 \equiv x_1^2 \pmod p$

$p \mid (x_0^2 - x_1^2) \rightarrow p \mid (x_0+x_1)\cdot(x_0-x_1)$

מכיוון ש p ראשוני: $p \mid (x_0-x_1)$ או $p \mid (x_0+x_1)$

$x_0 \equiv x_1$ $\quad$ $x_1 = p - x_0$

הם אותו פתרון $\quad$ זה שראינו קודם. (אפס או 2 פתרונות) מ.ש.ל.

(2)

<u>מסקנה</u>: מודולו p. יש בדיוק $\frac{p-1}{2}$ שאריות ריבועיות.
ובדיוק $\frac{p-1}{2}$ אי-שאריות ריבועיות.

הוכחה:

$1^2 \equiv a_1$
$2^2 \equiv a_2$
$3^2 \equiv a_3$ } כולם שונים
⋮
$\left(\frac{p-1}{2}\right)^2 \equiv a_3$
$\left(\frac{p+1}{2}\right)^2 \equiv a_2$
⋮
$\left(\frac{p-1}{2}\right)^2 \equiv a_1$ } אותם מספרים שוב (בסדר הפוך)

השאריות יש $\frac{p-1}{2}$ כאלה.

מש"ל.

נניח שיש לנו דרך לפתור משוואות מהסוג $x^2 \equiv a \pmod p$.

איך זה עוזר לנו לפתור משוואות ריבועיות מודולו p? לדוג: $7x^2+12x+32 \equiv 0 \pmod{97}$

באופן כללי $ax^2+bx+c \equiv 0 \pmod p$. נכפיל שני האגפים ב- 4a

$$0 \equiv 4a\left(ax^2+bx+c\right)$$
$$= 4a^2x^2+4abx+4ac$$
$$= (2ax+b)^2+4ac-b^2 \pmod p$$
(נעביר אגף)
$$(2ax+b)^2 \equiv b^2-4ac \pmod p$$

נגדיר: $y=2ax+b$, $f=b^2-4ac$ ← מספר נתון.

אז המשוואה היא $y^2 \equiv f \pmod p$

נבודד את x: $y \equiv 2ax+b \pmod p$

$x \equiv (y-b)\cdot\left(\text{ההופכי של } 2a\right)$ {העברנו את b אגף והכפלנו בהופכי של 2a.

[הופכי של z: z' שמקיים $z'\cdot z \equiv 1 \pmod m$.]

הוכחנו: למשוואה מהסוג $ax^2+bx+c \equiv 0 \pmod p$ יש 0 או 2 פתרונות.

דוגמה: $10x^2+9x+8 \equiv 0 \pmod{11}$ $a=10, b=9, c=8$

<u>בדיקה</u>: $x_1=2$ $x_2=7$

$y=2ax+b=20x+9 \equiv 9x+9$

$10\cdot 2^2+9\cdot 2+8=44+8=66 \equiv 0 \pmod{11}$ V

$f=b^2-4ac=\underbrace{81}_{\equiv 4}-\underbrace{80}_{\equiv 3}\cdot 4 \equiv 4-3\cdot 4 \equiv -8 \equiv 3$

$10\cdot 7^2+9\cdot 7+8=490+63+8=561 \equiv 0 \pmod{11}$ V

$y^2 \equiv 3 \pmod{11}$ $y_1=5, y_2=6$

$x_1=(y_1-b)\cdot\left(\text{ההופכי של } 2a\right)$ $x_1=5(5-9)=-20 \equiv 2$

$x_2=(y_2-b)\cdot\left(\text{הופכי של } 2a\right)$ $x_2=5(6-9)=-15 \equiv 7$

(3)

משפט ~~לגראנז'~~ (לג'נדר): p ראשוני. ~~המשוואה~~

המשוואה: $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0 \pmod p$

יש לכל היותר n פתרונות שונים מודולו p.

הקריטריון של אוילר (Euler's Criterion)

a היא שארית ריבועית מודולו p אמ"מ $a^{\left(\frac{p-1}{2}\right)} \equiv 1 \pmod p$

דוגמה: $p=11$ $a=4$ כן ש"ר $a=10$ לא ש"ר

$4^5 = 4^2 \cdot 4^2 \cdot 4 \equiv 12 \equiv 1$ ($4^2 \equiv 5$, $4^2 \equiv 5$, $\equiv 3$) ⇐ כן ש.ר

$10^5 = 10^2 \cdot 10^2 \cdot 10 \equiv -1$ ($10^2 \equiv 1$, $10^2 \equiv 1$) ⇐ לא ש"ר

תזכורת: משפט קטן של פרמה: $a^{p-1} \equiv 1 \pmod p$. במילים אחרות $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1$ ($a^{\frac{p-1}{2}} = x$)

יודעים: למשוואה $x^2 \equiv 1 \pmod p$ יש בדיוק שני פתרונות $x = \pm 1$.

הוכחה של קריטריון של אוילר:

כיוון ראשון: נניח ש-a כן ש"ר.

ק"ם x כך ש $x^2 \equiv a \pmod p$. נפעיל משפט קטן של פרמה על x: $x^{p-1} \equiv 1$

$1 \equiv x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}}$ מש.ל. כיוון 1.

כיוון שני: נניח ש a אינה ש"ר.

יודעים: לכל $b = 1, \dots, p-1$ קיים y_b כך ש- $b \cdot y_b \equiv a \pmod p$

$\left[\, y_b = a \cdot (\text{הופכי של } b) \right]$

טענה: $y_b \neq y_{b'}$ עבור $b \neq b'$

טענה: $y_b \neq b$ (אחרת a היתה ש"ר)

לדוג': {1,7} {2,3} {4,3}

נגדיר את הקבוצה של זוגות $A = \{\{b, y_b\} : b = 1, \dots, p-1\}$

A מכילה $\frac{p-1}{2}$ זוגות. כל מספר בין 1 לבין p-1 מופיע בדיוק פעם אחת.

נכפיל את כולם ביחד: $1 \cdot 2 \cdot 3 \cdots (p-1) \equiv \underbrace{a \cdots a \cdot a \cdot a}_{(p-1)/2}$

$a^{(p-1)/2} \equiv (p-1)! \equiv -1 \pmod p$

ע"פ משפט Wilson

מ.ש.ל.

(4)

הגדרה: סימן של Legendre

$$\left(\frac{a}{p}\right)=\begin{cases}+1 & \text{a כן ש"ר,} \\ -1 & \text{a לא ש"ר,}\end{cases}$$

← לא שבר!!

לדוגמה:

$\left(\frac{1}{11}\right)=+1$ $\left(\frac{4}{11}\right)=+1$ $\left(\frac{7}{11}\right)=-1$ $\left(\frac{10}{11}\right)=-1$

$\left(\frac{2}{11}\right)=-1$ $\left(\frac{5}{11}\right)=+1$ $\left(\frac{8}{11}\right)=-1$

$\left(\frac{3}{11}\right)=+1$ $\left(\frac{6}{11}\right)=-1$ $\left(\frac{9}{11}\right)=+1$

קריטריון של אוילר: $\left(\frac{a}{p}\right)\equiv a^{(p-1)/2} \pmod{p}$

תכונות של סימן Legendre:

1. אם $a\equiv b \pmod{p}$ אז $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$

2. $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$

הוכחה עפ"י קריטריון אוילר: $\left(\frac{ab}{p}\right)\equiv (ab)^{(p-1)/2}=a^{(p-1)/2}\cdot b^{(p-1)/2}\equiv\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$

מ.ש.ל.

תזכורת: כל p אי-זוגי מקיים:

$p\equiv 1 \pmod 4$ או $p\equiv 3 \pmod 4$

משפט: -1 היא ש"ר מודולו p אמ"ם $p\equiv 1 \pmod 4$

$$\left(\frac{-1}{p}\right)=\begin{cases}+1, & p\equiv 1 \pmod 4\\ -1, & p\equiv 3 \pmod 4\end{cases}$$

האם -1 הוא ש"ר מודולו $p=127$?

תשובה: לא, כי $127\equiv 3 \pmod 4$.

הוכחה (עפ"י קריטריון אוילר):

$\left(\frac{-1}{p}\right)\equiv(-1)^{(p-1)/2}$ ← זוגי?

זוגי כאשר $p\equiv 1 \pmod 4$

אי זוגי כאשר $p\equiv 3 \pmod 4$

} די רק להוכיח ואז מש"ל.

(1)

תזכורת: סימן לז'נדר: $\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{a ש"ר} \\ -1 & \text{אחרת} \end{cases}$

מבחן אוילר: $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$

תזכורת: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

תזכורת: $\left(\frac{-1}{p}\right) = \begin{cases} +1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$

לדוגמא: $p=13$. יש משהו שהריבוע שלו שקול ל-(-1) מודולו 13. (5)

$p=23$. אין אף אחד שהריבוע שלו שקול ל-(-1) מודולו 23.

תזכורת: הוכחנו: יש אינסוף ראשוניים מהצורה $4n+3$.

נוכיח(*): יש אינסוף ראשוניים מהצורה $4n+1$. ← נובע ממשפט Dirichlet

משפט Dirichlet (לא הוכחנו):

אם a,b זרים יש אינסוף ראשוניים מהצורה $an+b$.

הוכחה של (*): נניח בשלילה ש- $p_1, p_2, p_3, \dots, p_k$ הם כל הראשוניים מהצורה $4n+1$.

נגדיר: $N = (2 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k)^2 + 1 = 4(\text{משהו}) + 1$

כלומר, N עצמו הוא מהצורה $4n+1$.

ל-N יש מחלק ראשוני אי-זוגי p. $\quad p \mid N$

$p \mid ((2 p_1 p_2 \cdots p_k)^2 + 1)$

במילים אחרות: $(2 p_1 p_2 \cdots p_k)^2 \equiv -1 \pmod p$

[תזכורת: $a \equiv b \pmod m \iff m \mid (a-b)$]

לכן -1 כן ש"ר מודולו p.

לכן $p \equiv 1 \pmod 4$ ובמילים אחרות: p מהצורה $4n+1$.

לכן p הוא אחד מ- $p_1, \dots, p_k$. נ"ל p_i $(1 \le i \le k)$

$(p=)\ p_i \mid N$

$p_i \mid N-1$

סתירה! מש"ל.

(2)

למה של גאוס: יהי $p>2$ ראשוני.

יהי $1 \le a \le p-1$.

נתבונן בשאריות: $a \bmod p,\ 2a \bmod p,\ 3a \bmod p, \ldots\ldots, \frac{p-1}{2}\cdot a \bmod p$

נסמן ב-s מספר השאריות האלה שגדולות מ-$\frac{p}{2}$.

אז $\left(\frac{a}{p}\right) = -1^{s}$ (כלומר, אפשר ככה לדעת אם יש ש"ר או אין ש"ר.)

דוגמה: נקח $p=11$. האם $a=6$ ש"ר מודולו p?

$a, 2a, 3a, 4a, 5a$

$6, 12, 18, 24, 30$

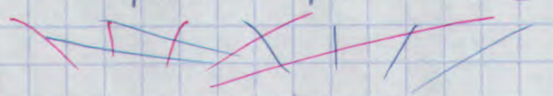
↓ שארית מודולו p $\circ > \frac{p}{2}$

$6, 1, 7, 2, 8$ $\circ < \frac{p}{2}$

$s=3$ אי זוגי לכן 6 לא ש"ר מודולו 11.

הוכחת הלמה של גאוס:

$a \bmod p,\ 2a \bmod p,\ 3a \bmod p, \ldots\ldots, \frac{p-1}{2}\cdot a \bmod p$



קטן מ-$\frac{p}{2}$ $v_1, v_2, \ldots, v_t$ | $u_1, u_2, \ldots, u_s$ גדול מ-$\frac{p}{2}$

$t+s = \frac{p-1}{2}$. ה-u-ים וה-v-ים הם כולם שונים.

נכפיל את כולם ביחד:

$v_1 \cdots v_t \cdot u_1 \cdots u_s \equiv a\cdot 2a\cdot 3a \cdots \frac{p-1}{2}\cdot a = \left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}}$

נקרא לו I. בשביל ההמשך.   עפ"י מבחן אוילר ↓

$\left(\frac{p-1}{2}\right)! \cdot \left(\frac{a}{p}\right)$ סימן לז'נדר

לכל u_i נגדיר $u_i' = p-u_i$ (נניח בדוגמה של $a=6$, $p=11$ אז ה-u' הם $u_i: 6\ 7\ 8$, $u_i' = 5, 4, 3$)

טענה: (*) $u_1', \ldots, u_s'$ הם שונים אחד מהשני. [קל].

(**) $u_1', \ldots, u_s'$ כולם שונים מ-$v_1, v_2, \ldots v_t$. [נוכיח] בפעם הבאה.

(3)

(**) הוכחה: נניח בשלילה ש- $u'_i = v_j$, כלומר $p - u_i \equiv v_j \pmod p$

$u_i \equiv r \cdot a \pmod p$

$v_j \equiv k \cdot a \pmod p$

$1 \le r, k \le \frac{p-1}{2} \qquad r \neq k$

$u'_i \equiv p - u_i$

$\equiv p - ra \pmod p$

$\equiv pa - ra \pmod p = (p-r)a \pmod p$ (בגלל ש $p \equiv a \pmod p$)

מכיוון ש- $u'_i \equiv v_j \pmod p$

$(p-r)a \equiv k \cdot a \pmod p$

$p - r \equiv k \pmod p$ סתירה!

~~עכשיו~~ בגלל עקרון שובך ~~השוב~~ היונים ($\frac{p-1}{2}$ יונים, $\frac{p-1}{2}$ שובכים)

$u'_1, \dots, u'_s, v_1, \dots, v_t$ הם בדיוק $1, 2, \dots, \frac{p-1}{2}$.

נכפיל אותם ביחד:

$\left(\frac{p-1}{2}\right)! = u'_1 \cdot u'_2 \cdots u'_s \cdot v_1 \cdots v_t \equiv (-u_1)(-u_2)\cdots(-u_s)\cdot v_1 \cdots v_t$ ($p - u'_1 \equiv -u_1$)

$= (-1)^s \cdot u_1 \cdots u_s \cdot v_1 \cdots v_t$ ← נקרא לו II

נציב את I בתוך II

$\left(\frac{p-1}{2}\right)! \equiv (-1)^s \cdot \left(\frac{p-1}{2}\right)! \left(\frac{a}{p}\right)_R$ (סימן לז'נדר) $/ \cdot (-1)^s$

$(-1)^s \equiv (-1)^s (-1)^s \left(\frac{a}{p}\right)$

$(-1)^s \equiv \frac{a}{p} \mod p$

משל.

(4)

שימוש של למת גאוס

מתי 2 הוא ש"ר מודולו p? כלומר מהו $\left(\frac{2}{p}\right)$?

$p>2$ ראשוני / ניקח $a=2$. נסתכל על: $2 \bmod p,\ 2\cdot 2 \bmod p,\ 3\cdot 2 \bmod p, \dots, \frac{p-1}{2}\cdot 2 \bmod p$ ($p-1$)

שאלה: כמה מהם גדולים מ- $\frac{a}{2}$?

$$1\cdot 2,\ 2\cdot 2,\ 3\cdot 2, \dots \ \big|\ \dots, \frac{p-1}{2}\cdot 2 \quad (p-1)$$

אם $p\equiv 1 \pmod 4$

$$1\cdot 2,\ 2\cdot 2,\ 3\cdot 2, \dots, \frac{p-1}{4}\cdot 2 \ \Big|_{\frac{p-1}{2}}\ \frac{p+3}{4}\cdot 2, \dots, \frac{p-1}{2}\cdot 2$$

$\frac{p-1}{4}$ אדומים

$p\equiv 1 \pmod 8$ ← זוגי

$p\equiv 5 \pmod 8$ ← אי זוגי

$$\# + \# = \frac{p-1}{2}$$

סה"כ		# (אדום)		# (כחול)	
$p\equiv 1 \pmod 8$	← זוגי סה"כ	זוגי	⇐	זוגי	זוגי כאשר $p\equiv 1 \pmod 4$
$p\equiv 5 \pmod 8$	← זוגי סה"כ	אי זוגי	⇐	אי-זוגי	
$p\equiv 3 \pmod 8$	אי זוגי סה"כ	זוגי	⇐	אי זוגי	אי-זוגי כאשר $p\equiv 3 \pmod 4$
$p\equiv 7 \pmod 8$	אי זוגי סה"כ	אי-זוגי	⇐	זוגי	

מסקנה:

$$\left(\frac{2}{p}\right)=\begin{cases} +1, & p\equiv 1, 7 \pmod 8 \\ -1, & p\equiv 3, 5 \pmod 8 \end{cases}$$

5

אחרון לקורס!!

משפט: יש אינסוף ראשוניים מהצורה $8k+7$.

הוכחה: נניח בשלילה שכל הראשוניים מהצורה $8k+7$ הם $p_n , \dots , p_1$.

נגדיר: $N = 8(p_1 \cdots p_n)^2 - 1$

קיים ראשוני $p|N$

$m|(a-b)$
$\Updownarrow$
$a \equiv b \pmod m$

~~$8(p_1 \cdots p_n)^2 \equiv -7 \pmod p$~~

נכפיל ב-2 $8(p_1 \cdots p_n)^2 \equiv 1 \pmod p$

$(4 \cdot p_1 \cdots p_n)^2 \equiv 2 \pmod p$

2 הוא לכן ש"ר מודולו p, לכן $p \equiv 1, 7 \pmod 8$

$N \equiv 7 \pmod 8$

פירוק של N לראשוניים $N = p \cdot p' \cdot p'' \cdot \dots$ ← אחד שקול ל-7, מודולו 8

אם כולם היו שקולים ל-1 מודולו 8 אז N היה שקול ל-1 מודולו 8. לא יכול להיות.

לכן, אחד מהם, נניח p, שקול ל-7 מודולו 8.

$p|N$

$p|N-1$

סתירה!

מש"ל!