

היום ראש השנה ה'תשסז, כלומר 5767, ולכן אני רוצה לדבר על מספרים ראשוניים.
האם 5767 ראשוני?

מספר ראשוני p זה מספר טבעי שיש לו בדיוק 2 מחלקים: 1 והוא עצמו.
0 הוא לא ראשוני, יש לו אינסוף מחלקים (בעצם כל מספר הוא מחלק שלו), והוא אפילו לא טבעי.
1 הוא לא מספר ראשוני, כי יש לא מחלק אחד בלבד.
2, 3, 5, 7 הם מספרים ראשוניים.
4, 6 הם לא מספרים ראשוניים, כי הם מתחלקים ב-2.
9 לא מתחלק ב-2, אבל הוא מתחלק ב-3.
1 הוא אמספר מיוחד במינו, מספרים אחרים מתחלקים לשני סוגים: מספרים ראשוניים ומספרים פריקים.
מספרים פריקים מתחלקים במספרים יותר קטנים, כלומר אפשר לפרק אותם למכפלה של מספרים יותר קטנים. המשפט היסודי של חשבון טוען, שכל מספר פריק אפשר לפרק בדרך יחידה, עד כדי סידור הגורמים, למכפלה של מספרים ראשוניים.

כדי לבדוק האם מספר הוא ראשוני צריך לבדוק האם הוא מתחלק באיזשהו מספר שקטן ממנו.
למשל בשביל לבדוק האם 5767 הוא מספר ראשוני מספיק לבדוק האם הוא מתחלק באיזשהו מספר בין 2 ל-5766.

אפשר לצמצם את הבדיקה. הרי אם $A \times B = 5767$ אז הגורם הקטן בריבוע אינו עולה על 5767.
לכן מספיק לבדוק האם 5767 מתחלק באיזשהו מספר בין 2 ל- $\sqrt{5767}$, כלומר במספיק לעשות פחות מ-80 בדיקות התחלקות.

אפשר לצמצם עוד את הבדיקה. הרי כל מספר לא ראשוני מתחלק במספר ראשוני. לכן מספיק לבדוק האם 5767 מתחלק במספרים ראשוניים 2, 3, 5, 7, ולא צריך כבר לבדוק האם הוא מתחלק ב-4, 6, 8, 9 (אם הוא לא מתחלק ב-2 אז ברור שהוא לא מתחלק ב-4).

לכן הבדיקה הייתה יותר פשוטה אם הייתה לנו רשימה מוכנה של כל המספרים הראשוניים מ-1 עד 80.

השיטה הקלאסית לבניית רשימת מספרים ראשוניים (שהומצאה לפני יותר מ-2000 שנה) נקראת **הנפה של ארטוסתנס** על שם המתמטיקאי שהמציא אותה.
נרשום רשימה של כל המספרים מ-1 עד 80:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80

נמחק את כל המספרים הזוגיים חוץ מ-2.

1	2	3		5		7		9		11		13		15		17		19	
21		23		25		27		29		31		33		35		37		39	
41		43		45		47		49		51		53		55		57		59	
61		63		65		67		69		71		73		75		77		79	

נמחק את כל המספרים שמתחלקים ב-3 החל מ-9.

1	2	3		5		7		9		11		13		15		17		19	
21		23		25		27		29		31		33		35		37		39	
41		43		45		47		49		51		53		55		57		59	
61		63		65		67		69		71		73		75		77		79	

נמחק את המספרים שמתחלקים ב-5 החל מ-25.

1	2	3		5		7		9		11		13		15		17		19	
21		23				27		29		31		33				37		39	
41		43		45		47		49		51		53				57		59	
61		63				67		69		71		73		75		77		79	

(המספרים הפריקים נופלים, ונשארים מספרים ראשוניים).

נשאר למחוק מספרים שמתחלקים ב-7 החל מ-49:

1	2	3		5		7		11		13		17		19	
		23				29		31				37			
41		43			47			53				59			
61					67			71		73				79	

מספרים שמחלקים ב-11 כבר לא צריך למחוק, כי המספר הפריק הכי קטן שמתחלק ב-11 ולא מתחלק במספרים קטנים יותר זה.

ובכן יש לנו רשימה של מספרים ראשוניים עד 80:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79

סה"כ 22 מספרים וזה מצמצם עוד פי 4 את כמות הבדיקות.

כמובן בזמנינו אפשר למצוא טבלת מספרים ראשוניים ב-google ולבדוק האם מספר הוא ראשוני תוך שנייה במחשב, אבל אנחנו לא נקשיב לאותם בכינים שלא רוצים לעשות שום דבר בעצמם. נניח שכל מה שיש לנו זה מחשבון (במקרה הטוב) ו-5 דקות של זמן.

אבל זאת לא השיטה הפשוטה ביותר לראות שהמספר 5767 הוא לא ראשוני (ולפרק אותו לגורמים). פרמה (לפני כמעט 400 שנים) המציא שיטה שעבור מספרים מסוימים, למשל עבור 5767, היא הרבה יותר מהירה. הרעיון הוא ללכת מהסוף ולא מהתחלה.

נניח שאפשר לפרק את 5767 לגורמים. ברור ששניהם אי-זוגיים. אז אפשר לרשום שגורם ראשון הוא $N + K$ וגורם שני הוא $N - K$. אז

$$5767 = (N + K)(N - K) = N^2 - K^2$$

כלומר

$$5767 + K^2 = N^2$$

ולכן צריך למצוא מספר K שאם נוסיף את הריבוע שלו ל- 5767 נקבל ריבוע.

הריבוע הראשון שגדול מ-5767 הוא $76^2 = 5776$.

וזה הרי $5767 + 9$. כלומר

$$5767 = 76^2 - 3^2 = (76 - 3)(76 + 3) = 73 \cdot 79$$

שני הגורמים ראשוניים ודי גדולים, לכן אם היינו בודקים את המספרים לפי הסדר היה לוקח יותר זמן.

שנה טובה!