ראשונים, איך כמה ולמה?

12 בדצמבר 2021

כולנו מכירים עוד מהיסודי מה הם מספרים ראשוניים, אני אנסה היום להציג כמה משפטים בסיסיים על ההתנהגות שלהן.

משפט 0.1 אוקלידס: יש אינסוף מספרים ראשוניים.

למשפט ניתנו ברבות הזמן הוכחות שונות ומגוונות, המקורית היא להניח בשלילה ש $p_1, \ldots, p_k$ הם כל הראשוניים ואז להגיע לסתירה על ידי $N = p_1 \ldots p_k + 1$.

אבל באיזה הפרשים מגיעים הראשונים? באיזה תחומים הם נמצאים? אנחנו יודעים שלכל n קיימים שני ראשונים עוקבים p, q כך ש $|p - q| \geq n$ (הוכחה, התסכל על $(n+2)!+2, \ldots (n+2)!+n+2$). נסמן ב g_n את ההפרש בין הראשוני ה nי לראשוני $n+1$. מה אנחנו כן יכולים לומר?

משפט 0.2 השערת ברטאן: לכל m יש ראשוני $m < p < 2m-2$ בפרט $p_{n+1} < 2p_n$ ולכן $g_n < p_n$.

למשפט האחרון ניתנה הוכחה אלמנטרית על ידי ארדש. האם ניתן לשפר?

השערת לנזדר: לכל n יש ראשוני בין $n^2, (n+1)^2$. היא עדיין פתוחה! ממנה נובע ש $g_n = O\left(\sqrt{p_n}\right)$. הכללה שלה אומרת שתמיד יש ראשוני בין $n(n-1)$ ל n^2 ובין n^2 ל $n(n+1)$ וממנה נובע ישירות ש $g_n \leq \sqrt{p_n}$

משפט 0.3 תוצאה של אינגם: עבור n מספיק גדול תמיד יש ראשוני בין n^3 ל $(n+1)^3$

האם ניתן לומר משהו כמותי על כמות הראשונים?

משפט 0.4 משפט צבלי $\frac{\log 2}{2}\frac{x}{\log x} \leq \pi(x) \leq 6\log 2\frac{x}{\log x}$

הוכחה: נסתכל על $\binom{2n}{n}$ איזה ראשוניים מחלקים אותו? זה בדיוק ראשונים $n < p < 2n$ ולכן

$$n^{\pi(2n)-\pi(n)} \leq \prod_{n<p<2n} p \leq \binom{2n}{n} \leq 2^{2n}$$

ולכן

$$\pi(2n) - \pi(n) \leq 2\log 2\frac{n}{\log n}$$

מפה באינדוקציה

$$\pi\left(2^{k}\right)\leq3\frac{2^{k}}{k}$$

נשתמש בכך ש $f\left(x\right)=\frac{x}{\log x}$ עולה
ולכן אם $4\leq2^{k}<x\leq2^{k+1}$ אז

$$\pi\left(x\right)\leq\pi\left(2^{k+1}\right)\leq6\frac{2^{k}}{k+1}\leq6\log2\frac{2^{k}}{\log2^{k}}\leq6\log2\frac{x}{\log x}$$

אל תציג כיוון שני כי הוא מסובך יותר, תזכיר שהוא מתבצע על ידי ניתוח דומה של הראשונים שמחלקים את $\binom{2n}{n}$ ■

צבאלי גם הוכיח שאם הגבול $\lim\frac{\pi(x)}{\frac{x}{\log x}}$ קיים אז הוא בהכרח 1.

משפט 0.5 משפט המספרים הראשוניים: נסמן ב $\pi\left(x\right)$ את כמות הראשוניים עד x אזי $\pi\left(x\right)\sim\frac{x}{\log x}$

כתוצאה מכך מתקיים ש $p_{n}\sim n\log n$ כי

$$1=\lim\frac{\pi\left(p_{n}\right)}{\frac{p_{n}}{\log p_{n}}}=\lim\frac{n\log p_{n}}{p_{n}}$$

אז נותר להבין ש $\log p_{n}\sim n$ זה נובע כי

$$\lim\frac{\pi\left(x\right)\log x}{x}=1\Rightarrow\lim\left(\log\left(\pi\left(x\right)\right)+\log\left(\log x\right)-\log x\right)=0$$

$$\lim\log x\left(\frac{\log\left(\pi\left(x\right)\right)}{\log x}+\frac{\log\left(\log x\right)}{\log x}-1\right)=0$$

ולכן

$$\lim\frac{\log\left(\pi\left(x\right)\right)}{\log x}+\frac{\log\left(\log x\right)}{\log x}-1=0\Rightarrow\lim\frac{\log\left(\pi\left(x\right)\right)}{\log x}=1$$

ההוכחה הקלאסית משתמש בכלים אנליטיים של פונקציות מרוכבות(ואינה דורשת את התוצאה של צבאלי), אבל גם לזה ארדש הביא הוכחה אלמנטרית אבל היא מסובכת בהרבה.
תוצאה טיפה יותר מסובכת ממשפט המספרים הראשוניים היא ש $\lim\frac{g_{n}}{p_{n}}=0$
אם נחזור לדבר על g_{n} בנימה אנליטית מה כן אפשר לומר?

משפט 0.6 (קרמר) תחת השערת רימן מתקיים $g_n = O\left(\sqrt{p_n}\log p_n\right)$. הוא **שיער** ש $g_n = O\left(\log^2 p_n\right)$(ואולי אפילו $\limsup \frac{g_n}{\log^2 p_n} = 1$)

יש גם תוצאה שהוכיחו ללא השערת רימן ש $g_n = O\left(p_n^{0.525}\right)$ וגם ש $g_n < p_n^{\frac{5}{8}}$

אחת ההשערות המפורסמות במתמטיקה היא השערת הראשוניים התאומים שטוענת שיש אינסוף n כך ש $g_n = 2$, ב 2005 הוכח ש $\liminf \frac{g_n}{\log p_n} = 0$ ושיפור ניכר הגיע ב 2014 ש $\liminf g_n < 7 \cdot 10^7$ ולאחר מכן החסם גם שופר ל 246 ובהנחת כמה השערות הגיעו גם ל 6 ו 12.

מה עם הכמות של ראשוניים תאומים? אנחנו יודעים שהסיכוי למספר a בין 1 עד x להיות ראשוני הוא בערך $\frac{1}{\log x}$ אם הראשוניות של $a+2$ להיות ראשוני הייתה בלתי תלויה ב a אז היינו מצפים שכמות הראשוניים התאומים תיהיה $\frac{x}{\log^2 x}$ אבל זה ניתוח פשטני מדי.

השערת הארי ליטלווד: אם נסמן ב $P_2(x)$ את כמות הראשניים התאומים עד x אזי $P_2(x) \sim \frac{2C_2 x}{\log^2 x}$ עבור $C_2 = \prod_{p\geq 3}\left(1 - \frac{1}{(p-1)^2}\right) \sim 0.6601$.

נדבר טיפה על חסם מהצד השני ל g_n, ידוע ש $\limsup \frac{g_n}{\log p_n} = \infty$ ב1938 הוכח שעבור קבוע c מתקיים לאינסוף n

$$g_n \geq \frac{c \log n \log\log n \log\log\log\log n}{\left(\log\log\log n\right)^2}$$

ארדש הציע פרס של 10000\$ שהקבוע c יכול להיות גדול כרצוננו(הסבר היטב מה הכוונה), ב 2014 זה הוכח! והתוצאה גם שופרה שיש קבוע c כך שלאינסוף n מתקיים

$$g_n \geq \frac{c \log n \log\log n \log\log\log\log n}{\log\log\log n}$$

ובאותה רוח של ארדש טרנס טאו מציע פרס כספי של 10000 שהקבוע c יכול להיות גדול כרצוננו.

מקווה שנהנתם!(זמן לשאלות).