

15 תולדות

גודל מספרים ראשוניים

סממן של a ו- b $\left(\frac{a}{p}\right) = 1$ אם a חלקי p , $\left(\frac{a}{p}\right) = -1$ אם a אינו חלקי p

עבור מספרים ראשוניים a ו- b $\left(\frac{a}{b}\right) = 1$ אם a אינו חלקי b , $\left(\frac{a}{b}\right) = -1$ אם a חלקי b

$$\left(\frac{2}{15}\right) = \left(\frac{2}{5}\right) \cdot \left(\frac{2}{3}\right) = (-1) \cdot (-1) = 1$$

אם $x^2 \equiv a \pmod{p}$ אז $\left(\frac{a}{p}\right) = 1$, אם $x^2 \not\equiv a \pmod{p}$ אז $\left(\frac{a}{p}\right) = -1$

אם $a = p_1 \cdot p_2 \cdot \dots \cdot p_r$ אז $\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right) \cdot \dots \cdot \left(\frac{p_r}{p}\right)$

אם $x^2 \equiv a \pmod{p}$ אז $\left(\frac{a}{p}\right) = 1$, אם $x^2 \not\equiv a \pmod{p}$ אז $\left(\frac{a}{p}\right) = -1$

אם $x^2 \equiv a \pmod{p}$ אז $\left(\frac{a}{p}\right) = 1$, אם $x^2 \not\equiv a \pmod{p}$ אז $\left(\frac{a}{p}\right) = -1$

Prime Numbers Theorem

מספר ראשוניים קטנים מ- x $\pi(x)$

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1$$

$\pi(x) - \text{Li}(x)$ (הפרש) $\pi(x) - x/\log x$ (הפרש)

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t}$$

Riemann

אם $x > 2657$ אז $\pi(x) - \text{Li}(x) < \sqrt{x}$

$$\left| \pi(x) - \text{Li}(x) \right| < \frac{1}{8\pi} \sqrt{x} \log x$$

$$\pi(2x) - \pi(x) \geq 1$$

ישנן זוגות ראשוניים x ו- $x+2$

Goldbach

כל מספר זוגי $n \geq 4$ הוא סכום של שני מספרים ראשוניים

כל מספר זוגי $n \geq 7$ הוא סכום של שלושה מספרים ראשוניים

$$n-3 = p+q \quad n-3 \geq 4 \quad n-3 \text{ (מספר זוגי)}$$

השערת גולדבך

כל מספר זוגי $n \geq 4$ הוא סכום של שני מספרים ראשוניים

כל מספר זוגי $n \geq 4$ הוא סכום של שני מספרים ראשוניים

כל מספר זוגי $n \geq 4$ הוא סכום של שני מספרים ראשוניים

Yitang Zhang

הוכח שהם
↓
2014

יש ∞ ראשוניים p, q כך ש- $|p-q| < 70 \cdot 10^6$

ובכן הוכח שיש ∞ ראשוניים p, q ש- $|p-q| < 252$

ראשוניים מרסנה

$q = 2^n - 1$, $n \geq 2$, q ראשוני. אם n מתקיים: $(a-1) | (a^n - 1)$

דוגמה: $a=2$, $2^n - 1$

$a^n = (a^k)^m$ אם $1 < k, m \in \mathbb{N}$, $n = k \cdot m$

ובכן $(a^k - 1) | (a^n - 1)$ וכן $a^n - 1$ אינו ראשוני.

↓
דוגמה: אם $a=2$ ראשוני אזי $2^n - 1$ ראש n ראשוני.

$2^p - 1$ ראש p ראשוני - האם זהו ראש קהרן ראשוני?

אם $p=2, 3, 5, 7, 13, 17, 19, 31, 43, 47, 53, 59, 67, 71, 83, 107, 131, 149, 157, 179, 191, 239, 251, 281, 311, 347, 359, 383, 401, 431, 439, 463, 487, 509, 541, 571, 593, 607, 631, 647, 659, 683, 707, 727, 743, 767, 787, 811, 823, 853, 883, 911, 937, 953, 977, 991$

Marin Merenne: $2^p - 1$ ראש ראשוני עבור

$p < 257$ וזהו הרשימה הראשונית $p = 2, 3, 5, 7, 13, 17, 19, 31, 43, 47, 53, 59, 67, 71, 83, 107, 131, 149, 157, 179, 191, 239, 251, 281, 311, 347, 359, 383, 401, 431, 439, 463, 487, 509, 541, 571, 593, 607, 631, 647, 659, 683, 707, 727, 743, 767, 787, 811, 823, 853, 883, 911, 937, 953, 977, 991$

עבור $p = 2, 3, 5, 7, 13, 17, 19, 31, 43, 47, 53, 59, 67, 71, 83, 107, 131, 149, 157, 179, 191, 239, 251, 281, 311, 347, 359, 383, 401, 431, 439, 463, 487, 509, 541, 571, 593, 607, 631, 647, 659, 683, 707, 727, 743, 767, 787, 811, 823, 853, 883, 911, 937, 953, 977, 991$

כיום מצוינו את הראשוני (ה-48) מצוינה כן

ראשוניים מרסנה

שם $F_n = 2^{2^n} + 1$ כושר ראשוניים.

ובכן $F_0 = 3 \checkmark$, $F_1 = 5 \checkmark$, $F_2 = 17 \checkmark$, $F_3 = 257 \checkmark$, $F_4 = 65537 \checkmark$

אם $F_5 = 2^{2^5} + 1$ מתחלק ב-641

זה היום הראשון מצוינו עם אחר ראשוני.

על מנת להוכיח שיש ראשוניים מרסנה מסוימים נחוץ להוכיח

חומר תח"ס 15:

$$x^n + y^n = z^n \quad \text{משפט פטרה (פונקטיון)}$$

לא ניתן להשיג את החוקה חזית סוגר $n > 2$ כסכום של שני מס' החוקה חזית. (חזף מהפתרון (הסרוליאזי - (לסוח $= 0$).

הצפנה בלפתח פולבי

הצפנה: אלקריתים צחיסק למשתמש הסמך n_1, n_2, \dots, n_n -

k_1, k_2, \dots, k_n הסיס (קסו אולז נסנון סולנויאזי d_1, \dots, d_n \neq (קטני)

$$O(k_1^{d_1} \cdot \dots \cdot k_n^{d_n})$$

צטטא צאצאיתם עם יסמ מלממ b^n