Ристо Малчески
Самоил Малчески
Скопје

БЕЛЕШКА ЗА РАСПРЕДЕЛБАТА НА ПРОСТИТЕ БРОЕВИ

Како што знаеме множеството прости броеви е бесконечно и, на пример, со помош на Евклидовиот алгоритам може да се провери дали еден природен број е прост или сложен. Понатаму, природно се наметнуваат прашањето како простите броеви се распоредени во множеството природни броеви? Во потрагата по одговор на распределбата на простите броеви, една од најчесто користените функции е функцијата $\pi(x)$, која се дефинира како што следува:

За секој реален број x со $\pi(x)$ го означуваме бројот на сите прости броеви кои се помали или еднакви на x. Јасно, функцијата $\pi(x)$ е неопаѓачка функција. На пример, $\pi(17)=7$, $\pi(\sqrt{34})=\pi(\sqrt{33})=\pi(5,5)=3$.

Функцијата $\pi(x)$ ја дава распределбата на простите броеви, за која може да се каже дека е прилично нерамномерна. Меѓутоа, додека на мали интервали распределбата на простите броеви изгледа крајно нерегуларна, за големи интервали случајот не е таков и постојат едноставни формули кои даваат приближни вредности на $\pi(x)$, кога x е многу голем број. Сепак, за распределбата на простите броеви не се знае многу и теоријата се заснива на хипотези. Исто така, докажани се малку теореми, дел од кои ќе презентираме во натамошните изагања. Притоа, да споменеме дека доказите на овие тврдења се крајно комплицирани, па затоа нема да ги презентираме. Во следниот пример ќе докажеме едно тврдење во врска со функцијата $\pi(x)$.

Пример 1. Нека p_n е $n-$тиот прост број ($p_1=2, p_2=3,\ldots$) и нека $\pi(n)$ е бројот на простите броеви кои се помаили или еднакви на n. Ако

$$A=\{n+p_n \mid n\in\mathbb{N}\} \text{ и } B=\{n+\pi(n)+1 \mid n\in\mathbb{N}\},$$

тогаш $A\cap B=\varnothing$ и $A\cup B=\mathbb{N}\setminus\{1\}$. Докажи!

Решение. Од дефиницијата на функцијата π следува:

i) $\pi(p_k)=k$, за секој $k\in\mathbb{N}$,

ii) $\pi(n)\le\pi(n+1)$, за секој $n\in\mathbb{N}$,

iii) $\pi(n)<\pi(n+1)$, ако $n+1$ е прост број.

Нека претпоставиме дека за некои *m* и *n* важи

iv) $m+p_m=n+\pi(n)+1$.

Можни се два случаи: $p_m \le n$ и $p_m > n$. Ако $p_m \le n$, тогаш ако се земе предвид дека $m = \pi(p_m) \le \pi(n)$ добиваме

$$m + p_m \le n + \pi(n) < n + \pi(n) + 1,$$

што противречи на *iv*). Ако $p_m > n$, тогаш од $m = \pi(p_m) > \pi(n)$ следува $m \ge \pi(n) + 1$ и $m + p_m > n + \pi(n) + 1$ што противречи на *i*). Според тоа $A \cap B = \varnothing$.

Ќе докажеме дека $A \cup B = \mathbb{N} \setminus \{1\}$. Јасно, $1 \notin A$ и $2 \in B$ е најмалиотелемент на B. Нека $n > 2$ е произволен природен број кој не припаѓа на множеството A. Ќе докажеме дека $n \in B$. Бидејќи за некој $m \in \mathbb{N}$ важи $m + p_m < n < m + 1 + p_{m+1}$, т.е. $p_m \le n - m - 1 < p_{m+1}$, добиваме дека $\pi(n - m - 1) = m$, па значи

$$n = \pi(n - m - 1) + (n - m - 1) + 1 \in B. \blacksquare$$

1. ТЕОРЕМА НА ЧЕБИШЕВ

Доказот на следната теорема излегува од рамките на нашите разгледувања, па затоа истиот нема да го презентираме.

Теорема 1 (Чебишев). Ако $n > 5$, тогаш меѓу броевите n и $2n$ постојат најмалку два прости броја. □

Пример 2. Ако $k > 3$, тогаш $p_{k+2} < 2p_k$, каде p_k е $k-$тиот прост број. Докажи!

Решение. Бидејќи $k > 3$ имаме $p_k > p_3 = 5$. Сега од теорема 1 следува дека постојат барем два прости броја q и r такви, да

$$p_k < q < r < 2p_k.$$

Но, $p_{k+1} \le q$ и $p_{k+2} \le r$, па затоа $p_{k+2} < 2p_k$. ■

Пример 3. Нека $n > 10$ е природен број. Докажи, дека во каноничното разложување на $n!$ учествуваат барем два прости броја со степен 1.

Решение. Во каноничното разложување на $11!$ простите броеви 7 и 11 учествуваат со степен 1. Затоа ќе претпоставиме дека $n > 11$. Сега, ако $n = 2k + r$, $r = 0$ или 1, тогаш $k > 5$ и согласно теоремата на Чебишев постојат барем два прости броја p и q такви што $k < p < q < 2k$. Имаме $k + 1 \le p < q < n$ и $n < 2p < 2q$, па затоа во каноничното разложување на бројот $n!$ секој од броевите p и q е со степен 1. ■

Пример 4. Докажи, дека за секој природен број $n > 4$ меѓу броевите n и $2n$ има најмалку еден број кој е производ на два различни прости броја.

Решение. Нека $n=2k$, каде $k>2$. Согласно теоремата на Чебишев постои прост број p, за кој важи $k<p<2k$. Но, $p>k>2$, па затоа p е непарен прост број. Тогаш

$$n=2k<2p<4k=2n,$$

па затоа бројот $2p$ го задоволува условот на задачата. Нека $n=2k+1, k\geq 2$. Повторно од теоремата на Чебишев следува дека постои прост број p, за кој важи $k<p<2k$. Но, $p>k\geq 2$, па затоа p е непарен прост број. Тогаш

$$n=2k+1<2k+2\leq 2p<4k<4k+2=2n,$$

па затоа бројот $2p$ го задоволува условот на задачата. ■

Пример 5. Ако $n>1$ и p_n е $n-$тиот прост број, тогаш $p_n<2^n$. Докажи!

Решение. Тврдењето ќе го докажеме со индукција по n. Од $p_2=3<2^2$ следува дека тврдењето важи за $n=2$.

Нека претпоставиме дека тврдењето важи за $n=k$, т.е. дека $p_k<2^k$.

За $n=k+1$ имаме $p_k<p_{k+1}$. Ако $p_{k+1}<2^k$, тогаш е јасно дека $p_{k+1}<2^{k+1}$. Нека $2^k<p_{k+1}$ и да ги разгледаме броевите $m=2^k$ и $2m=2^{k+1}$. Од теоремата на Чебишев следува дека меѓу броевите $m=2^k$ и $2m=2^{k+1}$ има најмалку два прости броја q и r. Но, $p_k<2^k$ и $2^k<p_{k+1}$, па затоа p_{k+1} и p_{k+2} се меѓу m и $2m$, т.е. $p_{k+1}<2m=2^{k+1}$.

Конечно, од принципот на математичка индукција следува дека $p_n<2^n$, за секој $n>1$. ■

Пример 6. Докажи, дека за секој природен број $n>15$ меѓу броевите n и $2n$ постои најмалку еден природен број, кој е производ на три различни прости броеви.

Решение. За $n=16,17,18,...,29$ имаме $n<30=2\cdot 3\cdot 5<2n$. Нека $n\geq 30$. Тогаш $n=6k+r$, каде $k\geq 5$ и $0\leq r\leq 5$. Од теоремата на Чебишев следува дека постои прост број $p>5$ таков да $k<p<2k$. Според тоа, $k+1\leq p<2k$, па затоа

$$n=6k+r<6(k+1)\leq 2\cdot 3p<12k\leq 2n$$

и бројот $2\cdot 3p$ го задоволува условот на задачата. ■

Пример 7. Докажи, дека за секои природни броеви n и s, $n>p_1p_2...p_s$, меѓу броевите n и $2n$ постои најмалку еден природен број кој е производ на s различни прости множители (p_k е $k-$тиот прост број).

Решение. Нека $n = kp_1p_2...p_{s-1} + r$, каде r е остатокот од делењето на n со $p_1p_2...p_{s-1}$. Од $n > p_1p_2...p_s$, следува

$$k \geq p_s \text{ и } 0 \leq r < p_1p_2...p_{s-1}.$$

Сега, од теоремата на Чебишев следува дека постои прост број p таков, да $k < p < 2k$. Точни се неравенствата

$$p > p_s,\ k+1 \leq p < 2k$$

и

$$\begin{aligned} n &= kp_1p_2...p_{s-1} + r \\ &< p_1p_2...p_{s-1}(k+1) \\ &\leq p_1p_2...p_{s-1}p \\ &< 2p_1p_2...p_{s-1}k \leq n \end{aligned}$$

па затоа бројот $p_1p_2...p_{s-1}p$ го задоволува условот на задачата.

2. ПОСТУЛАТ НА БЕРТРАН

Последица 1 (постулат на Бертран). Ако $n > 3$, тогаш меѓу броевите n и $2n-2$ постои најмалку еден прост број.

Доказ. Навистина, ако $n = 4$, тогаш 5 е меѓу 4 и 6, а ако $n = 5$, тогаш 7 е меѓу 5 и 8.

Ако $n > 5$, тогаш од теорема 1 следува дека меѓу n и $2n$ има најмалку два прости броја. Ако поголемиот од овие прости броеви е $2n-1$, тогаш бидејќи $2n-2 = 2(n-1)$ е сложен број, вториот прост број ќе биде помал или еднаков на $2n-3$, што значи дека меѓу n и $2n-2$ постои најмалку еден прост број. ■

Пример 7. Ако $n > 1$, тогаш во каноничното разложување на $n!$ има најмалку еден прост број со степен еден.

Решение. За $n \leq 7$ тврдењето на задачата е очигледно.

Ако $n = 2k$, $k \geq 4$, тогаш согласно постулатот на Бертран постои барем еден прост број p таков што $k < p < 2k-2 < n$. Но, тогаш $2p > 2k = n$, што значи дека $p < n < 2p$, од што следува дека простиот број p во каноничното разложување на $n!$ е со степен еден.

Ако $n = 2k+1, k \geq 4$, тогаш повторно од постулатот на Бертран следува дека постои прост број p таков што $k < p < 2k-2 < n$. И во овој случај $2k < 2p$, па значи и $2k+1 < 2p$, т.е. $p < n < 2p$, од што следува дека простиот број p во каноничното разложување на $n!$ е со степен еден. ■

3. ТЕОРЕМА НА ДИРИХЛЕ

Во врска со распределбата на простите броеви, ќе дадеме уште една теорема, чиј доказ излегува надвор од рамките на нашите разгледувања.

Теорема 2 (Дирихле). Секоја аритметичка прогресија $ak+b, k=0,1,2,\ldots$, каде a,b се заемно прости природни броеви, содржи бесконечно многу прости броеви. □

Последица 2. Секоја аритметичка прогресија $ak+b, k=0,1,2,\ldots$, каде a,b се заемно прости природни броеви, за секој природен број s содржи бесконечно многу членови кои се производ на s различни прости броеви.

Доказ. За $s=1$ тврдењето следува од теоремата на Дирихле.

Нека претпоставиме дека тврдењето важи за прирдниот број $s \geq 1$. Од $\text{NZD}(a,b)=1$ следува дека постои број k_0 таков што

$$ak_0+b=q_1q_2\ldots q_s$$

каде $q_1<q_2<\ldots<q_s$ се прости броеви. Согласно теоремата на Дирихле постојат бесконечно многу природни броеви k, такви што $ak+1=q$ е прост број поголем од q_s. За

$$t=q_1q_2\ldots q_sk+k_0$$

имаме

$$\begin{aligned} at+b &= q_1q_2\ldots q_s ak+ak_0+b \\ &= q_1q_2\ldots q_s\,(ak+1) \\ &= q_1q_2\ldots q_s\,q, \end{aligned}$$

т.е тврдењето важи за $s+1$.

Конечно, од принципот на математичка индукција следува дека тврдењето важи за секој $s\in\mathbb{N}$. ■

Пример 8. Докажи, дека за секој природен број m постои прост број чиј збир на цифрите е поголем од $9m$.

Решение. Нека m е природен број. Бидејќи $\text{NZD}(10^m,10^m-1)=1$, според теоремата на Дирихле, постои таков природен број k, што $p=10^mk+10^m-1$ е прост број. Бидејќи последните m цифри на p се еднакви на 9, добиваме дека збирот на цифрите на p е поголем од $9m$. ■

Пример 9. За простите броеви p и q, $p>q$ ќе велиме дека се прости броеви близнаци ако $p=q+2$. Докажи, дека постојат бесконечно многу прости броеви кои не припаѓаат на паровити прости броеви близнаци.

Решение. Согласно теоремата на Дирихле во аритметичката прогресија $15k+7,\ k=1,2,...$ се содржат бесконечно многу прости броеви. Ниту еден од овие броеви не припаѓа на ниту еден пар прости броеви близнаци, бидејќи

$$(15k+7)+2=3(5k+3) \text{ и } (15k+7)-2=5(3k+1)$$

се сложени броеви. ■

Пример 10. Докажи, дека за секој природен број m постои прост број, во чиј декаден запис има најмалку m нули.

Решение. Нека m е даден природен број. Бидејки $\text{NZD}(10^{m+1},1)=1$ од теоремата на Дирихле следува, дека постои природен број k таков што $p=10^{m+1}k+1$ е прост број. Последните $m+1$ цифра на бројот 10^{m+1} се нули, па затоа во декадниот запис на бројот бројот p има најмалку m нули. ■

Пример 11. Докажи дека за секој природен број n постои полином $f(x)$ со целобројни коефициенти таков што $f(1)<f(2)<\ldots<f(n)$ при што сите овие вредности се прости броеви.

Решение. Нека n е даден природен број. За $k\le n$ индуктивно ќе определиме природни броеви t_k на следниов начин.

Нека $t_0=1$. Да претпоставиме дека за даден $k\le n$ е определен бројот t_{k-1}. Според теоремата на Дирихле постои природен број t_k таков што бројот

$$q_k=(k-1)!(n-k)!t_k+1$$

е прост и кога $k>1$ тој е поголем од бројот

$$(k-2)!(n-k+1)!t_{k-1}+1.$$

Така, броевите $q_1,q_2,\ldots,q_n$ се прости и притоа важи $q_1<q_2<\ldots<q_n$. Нека

$$f(x)=1+\sum_{j=1}^{n}(-1)^{n-j}\frac{(x-1)(x-2)\ldots(x-n)}{x-j}\ .$$

Јасно, $f(x)$ е полином со степен помал или еднаков на $n-1$ со целобројни коефициенти и $f(k)=1+(k-1)!(n-k)!t_k=q_k$. ■

4. ДОПОЛНИТЕЛНИ ЗАДАЧИ

Пример 12. Докажи дека, за секој природен број n постои прост број p таков што секој од броевите $p-1$ и $p+1$ има повеќе од n различни природни делители.

Решение. Нека n е даден природен број. Согласно теоремата на Дирихле во аритметичката прогресија $6^n k+2\cdot 3^{2^{n-1}}-1$, каде $k\in\mathbb{N}$ постојат прости броеви.

Оттука бидејќи $2^{n-1} \geq n$, за $n \in \mathbb{N}$ добиваме дека $3^n \mid 6^n k + 2 \cdot 3^{2^{n-1}} = p+1$ и бројот $p+1$ има повеќе од n различни природни делители, на пример $1, 3, 3^2, ..., 3^n$. Согласно со теоремата на Ојлер имаме $3^{\varphi(2^n)} \equiv 1 \pmod{2^n}$, па е $2^n \mid 3^{2^{n-1}} - 1$, што значи $2^n \mid 6^n k + 2 \cdot 3^{2^{n-1}} - 2 = p-1$ и бројот $p-1$ има најмалку n различни природни делители, на пример броевите $1, 2, 2^2, \ldots 2^n$. ■

Пример 13. Докажи, за секој природен број n постојат прост број p и природен број m, такви што

1) $p \equiv 5 (\mathrm{mod}\, 6)$,
2) p не е делител на n,
3) $n \equiv m^3 (\mathrm{mod}\, p)$.

Решение. Од теоремата на Дирихле следува дека постојат бесконечно многу прости броеви од видот $6k+5$. Да избереме прост број $p = 6k+5$ кој е поголем од n. Јасно, бројот p ги задоволува условите 1) и 2). За $m = n^{4k+3}$ од теоремата на Ферма следува

$$m^3 \equiv n^{12k+9} \equiv n^{6k+4} n^{6k+4} n \equiv n^{p-1} n^{p-1} n \equiv n (\mathrm{mod}\, p) .$$ ■

Пример 14. Докажи, дека за секој природен број n постои прост број p таков, што секој од броевите $p-1, p+1, p+2$ има најмалку n различни прости делители.

Решение. Нека n е даден природен број, а p_i е $i-$тиот прост број. Од кинеската теорема за остатоци следува дека постои природен број b, таков што

$$b \equiv 1 (\mathrm{mod}\, p_1 p_2 \ldots p_n),$$
$$b \equiv -1 (\mathrm{mod}\, p_{n+1} p_{n+2} \ldots p_{2n}),$$
$$b \equiv -2 (\mathrm{mod}\, p_{2n+1} p_{2n+2} \ldots p_{3n}) .$$

Бидејќи $\mathrm{NZD}(b, p_1 p_2 \ldots p_{3n}) = 1$ од теоремата на Дирихле следува дека постои природен број k таков што

$$p = p_1 p_2 \ldots p_{3n} k + b$$

е прост број. Во овој случај $p_i \mid (b-1)$, за $i = 1, 2, ..., n$ и $p_i \mid (b+1)$, за $i = n+1, n+2, ..., 2n$, што значи $p_i \mid (p-1)$, за $i = 1, 2, ..., n$ и $p_i \mid (p+1)$, за $i = n+1, n+2, ..., 2n$. Аналогно $p_i \mid (b+2)$, за $i = 2n+1, 2n+2, ..., 3n$, па затоа $p_i \mid (p+2)$, за $i = 2n+1, 2n+2, ..., 3n$.

Конечно, секој од броевите $p-1, p+1, p+2$ има најмалку n различни прости делители. ■