Прости бројеви

Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Прости бројеви

Вјероватно не постоји у историји математике појам који је привлачио више пажње како лаичке, тако и стручне математичке јавности од простих бројева. Прости бројеви се могу сматрати основним градивним компонентама цијелих бројева.

Дефиниција

Природан број p је прост ако је $p \geq 2$ и ако су једини позитивни дјелиоци броја p, бројеви 1 и p.

Лема

Нека је p најмањи дјелилац, већи од јединице, природног броја n. Онда је p прост број.

Теорема (Еуклид)

Скуп простих бројева је бесконачан.

Следеће леме су основ за доказивање **Основне теореме аритметике** коју ћемо представити касније.

Лема

Сваки природан број $n > 1$ може се приказати као производ простих бројева.

Лема

Нека је p прост број и претпоставимо да $p \mid ab$. Тада p дијели a или b. Општије, ако

$$p \mid a_1 a_2 \cdots a_n,$$

тада p дијели бар један од a_i, за $1 \leq i \leq n$.

Основна теорема аритметике

Теорема (Основна теорема аритметике)

Нека је $a \geq 2$ цио број. Тада се a може представити (факторисати) на следећи начин

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_r^{e_r}.$$

Ова факторизација је јединствена до на поредак простих бројева.

Значај претходне теореме је изузетне, што и само име потврђује. Прије свега, она нам говори да се сви цијели бројеви могу изградити помоћу простих бројева. Та чињеница има многе и значајне импликације у аритметици и математици уопште.

Примјер

Доказати да ако је n непаран број, онда је $n^2 - 1$ дјељив са 8, а ако је n прост број већи од 3, онда је $n^2 - 1$ дјељив са 24.

Пошто је $n^2 - 1 = (n-1)(n+1)$ производ два узастопна парна броја, онда је бар један од њих дјељив са 4, па је производ дјељив са 8. Уколико је n прост број већи од 3, онда n није дјељив са 3, али зато неки од његових сусједа, $n-1$ или $n+1$ мора бити. Стога је производ дјељив са 8 и 3, односно са 24.

Теорема

Ако је производ два релативно проста природна броја квадрат цијелог броја

$$ab = c^2, \ \textbf{нзд}(a, b) = 1,$$

онда су a и b такође квадрати неких цијелих бројева.

Примјер

Доказати да простих бројева облика $4k+3$ има бесконачно много.

Сви непарни прости бројеви су облика $4r+1$ или $4k+3$. Лако се уочава да се множењем два броја облика $4r+1$ добија број истог облика.

Претпоставимо да су $\{p_1, p_2, \ldots, p_n\}$ сви прости бројеви облика $4k+3$. Посматрајмо број

$$4p_1p_2\cdots p_n - 1.$$

Овај број није облика $4r+1$, што значи да има бар један прост фактор облика $4k+3$. Наиме, ако би сви његови чиниоци били облика $4k+1$, онда би и производ био тог облика. Дакле, један његов прост фактор облика $4k+3$ мора бити из скупа $\{p_1, p_2, \ldots, p_n\}$, а одатле слиједи да тај прост број дијели 1, што је немогуће. Закључујемо да је претпоставка да имамо коначно много простих бројева облика $4k+3$ је погрешна.

Примјер

Доказати да за сваки природан број n постоји n узастопних сложених бројева.

Посматрајмо бројеве

$$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+n,\ (n+1)!+n+1.$$

Сваки од датих бројева облика $(n+1)!+j$, гдје је $2 \leq j \leq n+1$ је сложен, јер се фактор j може извући као уаједнички за два сабирка.

Примјер

Доказати да не постоји полином $f(x)$ са цјелобројним коефицијентима степена $m \geq 1$, такав да је $f(n)$ прост за све $n \in \mathbb{N}$.

Нека је $f(1) = p$. Тада је p прост број. Како увијек $x - y$ дијели $x^m - y^m$, онда је $f(1 + kp) - f(1)$ дјељиво са $(1 + kp) - 1 = kp$. Одавдје слиједи да $p \mid f(1 + kp)$ за сваки $k \in \mathbb{N}$. Међутим, $f(1 + kp)$ је прост, па мора бити $f(1 + kp) = p$ за свако $k \in \mathbb{N}$. Значи, полином $f(x) - p$ има бесконачно много нула, одакле закључујемо да је $f(x) = p$, а што је у супротности са претпоставком да је степен полинома $f(x)$ већи од један.

Примјер

Нека је број $2^n + 1$ прост. Доказати да је тада $n = 0$ или $n = 2^k$ за неки $k \geq 0$.

Претпоставимо супротно, да је $n = 2^k m$, гдје је m непаран број већи од 1. Тада је

$$2^n + 1 = \left(2^{2^k}\right)^m + 1,$$

па $2^{2^k} + 1 \mid 2^n + 1$, јер $x + y \mid x^m + y^m$ за непарно m. Дакле, ако је $m > 1$, број $2^n + 1$ има нетривијални фактор, па није прост. Из тога слиједи тврђење.

Бројеви облика $2^{2^n} + 1$ називају се **Фермаови бројеви**. Иако је Ферма сматрао да су сви бројеви тог облика прости, постоје и сложени Фермаови бројеви. На примјер, број $2^{32} + 1$ је сложен.

Примјер

Нека је број $2^m - 1$ прост. Доказати да је тада m прост број.

Ако би било $n = n_1 n_2$, $1 < n_1, n_2 < n$, број $2^n - 1 = (2^{n_1})^{n_2} - 1$ би био дјељив са $2^{n_1} - 1$.

Бројеви облика $M_p = 2^p - 1$, за прост број p, називају се **Мерсенови бројеви**. Неки Мерсенови бројеви су прости као на примјер $M_7 = 127$, а неки сложени, као на примјер $M_{11} = 2047 = 23 \cdot 89$. Хипотеза је да има бесконачно много простих Мерсенових бројева.

Једно важно питање које се тиче простих бројева је процјена колико их има у неком интервалу, односно колико има простих бројева који су мањи од неког задатог природног броја n? Дефинишимо функцију $\pi(n)$ као број простих бројева који су мањи или једнаки n

$$\pi(n) = |\{p \in \mathbf{P} \mid p \leq n\}|.$$

У следећој табели су дате неколико првих вриједности функције $\pi(n)$. Примјетимо да је функција монотоно растућа

n	2	3	4	5	6	7	8	9	10	11	...
$\pi(n)$	1	2	2	3	3	4	4	4	4	5	...

Теорема

$$\lim_{n\to\infty} \frac{\pi(n)\ln(n)}{n} = 1$$

Дакле, претходна теорема даје прилично тачну апроксимацију о броју простих бројва мањих или једнаких n

$$\pi(n) \approx \frac{n}{\ln(n)},$$

што значи да је број простих бројева у интервалу (n_1, n_2) приближно $\pi(n_2) - \pi(n_1)$, односно

$$\frac{n_2}{\ln(n_2)} - \frac{n_1}{\ln(n_1)}.$$

Примјер

Ако су p и $8p^2+1$ прости бројеви, доказати да је и $8p^2+2p+1$ прост број.

Очигледно, тврђење вриједи за $p=3$. Сви остали прости бројеви, већи од 3, су облика $3k-1$, односно $3k+1$.
У случају да је p облика $3k-1$ или $3k+1$ видимо да је $8p^2+1$ дјељив са 3.
Тиме је показано да је за $p>3$, број $8p^2+1>3$ и дјељив са 3, што значи да није прост. Дакле, једина могућност је $p=3$.

Хвала на пажњи :)