Прости бројеви

Број $p \in \mathbb{N} \setminus \{0,1\}$ је прост ако су му једини делиоци 1 и p.

Ако $p \in \mathbb{N} \setminus \{0,1\}$ није прост, кажемо да је сложен број.

Теорема: Постоји бесконачно много простих бројева.

доказ:

пп: Нека има коначно много простих бројева и нека су то бројеви

$$p_1, p_2, \dots, p_k$$

Посматрајмо број $p = p_1 p_2 \cdots p_k + 1$.

Приметимо да је $p \neq p_i$ за све $i \in \{1, \dots, k\}$, па је p сложен број

$\Rightarrow$ постоји прост број q који дели број p

тада је $q = p_j$, за неко $j \in \{1, \dots, k\}$, па $p_j \mid p$ ↯

□

Тврђење: Ако је p прост број и $p \mid ab$, онда $p \mid a$ или $p \mid b$.

доказ:

Нека $p \mid ab$ и претпоставимо да $p \nmid a$, докажимо да $p \mid b$.

Ако је $НЗД(a,p) > 1$, онда $НЗД(a,p) = p$ јер је p прост.
Како $p \nmid a$, а из $НЗД(a,p) = p$ следи да $p \mid a$, закључујемо да је $НЗД(a,p) = 1$.

Дакле, $\left.\begin{matrix} p \mid ab \\ НЗД(p,a)=1 \end{matrix}\right\} \Rightarrow p \mid b$

Важи и општије тврђење:

ако $p \mid a_1 a_2 \cdots a_k \Rightarrow p \mid a_1$ или $p \mid a_2$ или ... или $p \mid a_k$

Теорема: Сваки природан број $n>1$ је прост или се може представити као производ простих бројева.

доказ:

потпуном индукцијом по n: $\Phi(n) = n$ је производ простих

(ИХ) претпостављено да је за сваки природан број мањи од n задовољено својство Φ

тј. за свако $k<n$, k је производ простих

Доказимо да је n производ простих:

- ако је n прост: крај
- ако је n сложен: $n = k \cdot m$, за неке $1 < m, k < n$

по (ИХ) m и k су производи простих па је $n = m \cdot k$ такође производ простих.

Основна теорема аритметике:

Сваки природан број $n>1$ се (до на редослед чинилаца) на јединствен начин записује као производ простих бројева

доказ:

На основу претходне теореме, сваки природан број је производ простих бројева. Покажимо да је запис још

производа једнозначан (до на редослед чинилаца).

Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$.

$\alpha_i, \beta_1 \geq 1$

$p_1 < p_2 < \cdots < p_k$

$q_1 < q_2 < \cdots < q_\ell$

За свако $i \in \{1, \dots, k\}$ следи да $p_i \mid n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$

$\Rightarrow$ постоји је $\{1, \dots, \ell\}$ тј. $p_i \mid q_j$, па $q_j = p_i$.

Дакле, $\{p_1, \dots, p_k\} \subseteq \{q_1, \dots, q_\ell\}$.

Аналогно се доказује да је $\{q_1, \dots, q_\ell\} \subseteq \{p_1, p_2, \dots, p_k\}$

Према томе, $\{p_1, \dots, p_k\} = \{q_1, \dots, q_\ell\}$, па је $k = \ell$ и како је $p_1 < p_2 < \cdots < p_k$ и $q_1 < q_2 < \cdots < q_\ell$ закључујемо да је $p_1 = q_1$, $p_2 = q_2$, $\dots$ $p_k = q_k$.

За сада имамо:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \quad / : p_1^{\alpha_1}$$

Нпр. ако је $\alpha_1 < \beta_1$:

$$\underbrace{p_2^{\alpha_2} \cdots p_k^{\alpha_k}}_{p_1 \nmid} = \underbrace{p_1^{(\beta_1 - \alpha_1)} p_2^{\beta_2} \cdots p_k^{\beta_k}}_{p_1 \mid} \quad (\beta_1 - \alpha_1 \geq 1)$$

$\Rightarrow \alpha_1 = \beta_1$, па важи

$$p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_2^{\beta_2} \cdots p_k^{\beta_k}$$

Настављањем поступка добијамо $\alpha_2 = \beta_2, \dots \alpha_k = \beta_k$.

$\square$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, где $p_1 < p_2 < \dots < p_k$ је канонска факторизација броја n.

Приметимо да, по дефиницији, број 1 није ни прост ни сложен. Један од разлога је управо претходна теорема: уколико би 1 био прост, тада не бисмо имали јединствену факторизацију:

нпр. $56 = 2^3 \cdot 7 = 1 \cdot 2^3 \cdot 7 = 1^2 \cdot 2^3 \cdot 7 \dots$

Дакле, да бисмо знали више о броју, потребно је одредити његове просте делиоце.
У овој лекцији, за дати број n, бавимо се ефикасним решавањем следећих проблема:

1° Одредити да ли је n прост број.
2° Пронаћи све делиоце броја n.
3° Пронаћи канонску факторизацију броја n, тј. пронаћи низове (p_i) и (α_i).

Испитивање да ли је број прост може се урадити врло једноставно: испитивањем да ли је n дељив неким од бројева $2, 3, \dots, n-1$.
Међутим, у ситуацијама када радимо са великим бројевима (нпр. реда величине 10^9 или 10^{15}) поменути приступ резултира врло спорим алгоритмом.

За проверу да ли је број прост довољно је испитати да ли бројеви $2, 3, \dots, [\sqrt{n}]$ деле број n. Следећа теорема говори о томе:

Теорема: ("$\sqrt{n}$ теорема") Сваки сложен природан број n има делилац d за који важи $1 < d < \sqrt{n}$.

Доказ:

Ако је d делилац броја n, тада је и $\frac{n}{d}$ такође делилац. Јасно, уколико је $1<d<n$, тада је и $1 < \frac{n}{d} < n$. Покажимо да је бар један од бројева d и $\frac{d}{n}$ мањи од $\sqrt{n}$.

Заиста, уколико је $d>\sqrt{n}$ и $\frac{n}{d} > \sqrt{n}$, тада је $n = d \cdot \frac{n}{d} > n$ ↯

⊠

Тврђење: Сваки прост број већи од 3 је облика $6k+1$ или $6k-1$, за неко $k \in \mathbb{N}$.

Доказ:

Могући остаци при дељењу природног броја са 6 су:

$0, 1, 2, 3, 4, 5$ ($5 = -1$)

Ако је број већи од 3 и даје остатак 0, 2 или 4, онда је он паран, па није прост.
Ако број већи од 3 даје остатак 3, онда је он дељив са 3, па опет није прост.
Дакле, једини могући остаци су 1 и $5=-1$.

⊠

Приметимо да обрат тврђења не важи: нису сви бројеви облика $6k \pm 1$ прости. (Нпр $25 = 6 \cdot 4 + 1$ или $35 = 6 \cdot 6 - 1$).

Како претходна теорема може "убрзати" алгоритам за проверу да ли је број прост?

Ако неко $d \mid n$, $d \in [2, \sqrt{n}]$, тада сваки прост делилац броја d дели n.

Дакле, довољно је испитати да ли прости бројеви из интервала $[2, \sqrt{n}]$ деле n. Шта више, на основу претходног извођења, довољно је испитати да ли потенцијалне кандидате за просте бројеве – бројеви облика $6k \pm 1, 2, 3$ деле n.

На тај начин, међу 6 узастопних природних бројева, довољно је испитивати само 2, што даје 3 пута бржи алгоритам.

Одређивање свих делилаца броја n:

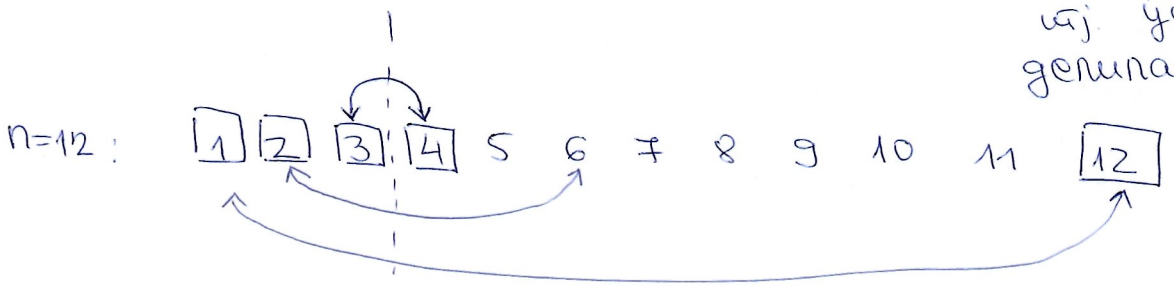
Сви делиоци броја n долазе у пару $(d, \frac{n}{d})$.

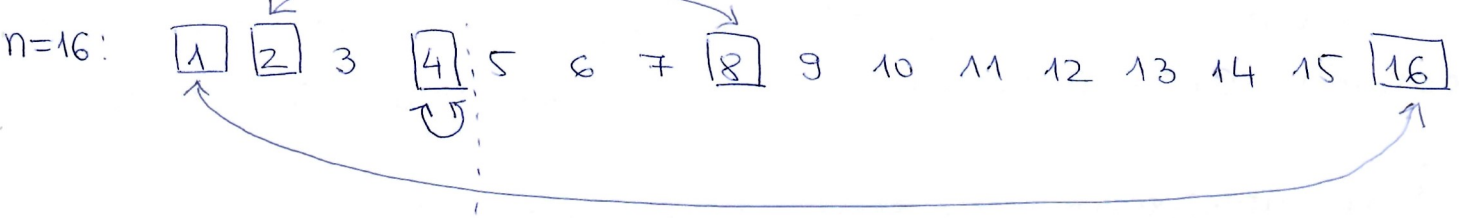
Претпоставимо, уколико су $1 = d_1 < d_2 < \dots < d_m = n$ сви делиоци броја n, тада за свако $i \in \{1, 2, \dots, m\}$ важи $d_i = \frac{n}{d_{m+1-i}}$.

Сваки $d = \frac{n}{d}$ је еквивалентан са $n = d^2$, тј. уколико је n потпун квадрат (и само тада) један делилац (његов корен) нема свој пара.

За $n = 12$ парови су: $(1, 12)$, $(2, 6)$ и $(3, 4)$
За $n = 16$ парови су: $(1, 16)$, $(2, 8)$ и $(4, 4)$

тј. "усамљени" делилац 4





Како је у сваком пару мањи делилац $\leq \sqrt{n}$, довољно је испитати бројеве из сегмента $[1, \sqrt{n}]$ и за сваки пронађени делилац d исписати и $\frac{n}{d}$. Посебно треба водити рачуна

да ли је n потпун квадрат да се његов корен не би исписао два пута.

Одређивање канонске факторизације:

Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

Испитивати редом бројеве $2, 3, \dots, [\sqrt{n}]$ и први (најмањи) који дели n је његов најмањи прост чинилац p_1. Затим, докле је год потуно, делимо број n бројем p_1 и тако одређујемо α_1.

Остаје број $n' = p_2^{\alpha_2} \dots p_k^{\alpha_k}$ над којим се наставља претходни поступак, при чему се са тражењем броја p_2 полази од p_1+1 (и тражи се до $[\sqrt{n_1}]$).