High-efficiency divisibility-test prime factorization algorithm

Hernán Rodríguez

September 2, 2023

1. Introduction

Theorem 1 (Fundamental Theorem of Arithmetic)

Let $n \in \mathbb{Z}$, $n \geq 2$, then for $r \geq 1$ there are unique primes $p_1, ..., p_r$, such that $n = p_1 \cdots p_r$ and $p_1 \leq ... \leq p_r$.

Theorem 2

$n \in \mathbb{Z}$, $n \geq 2$ is non-prime if and only if there exists p prime such that $2 \leq p \leq \lfloor \sqrt{n} \rfloor$ and $p \mid n$.

Proof of Theorem 2

Assume $n \in \mathbb{Z}$, $n \geq 2$ be non-prime

$\Rightarrow n = p_1 \cdots p_r$, with $p_1 \leq ... \leq p_r$ (by Theorem 1) where $p_1, ..., p_r$ are primes and $r \geq 2$.

Assume $p_k > \lfloor \sqrt{n} \rfloor$, for each $k \in \{1, ..., r\}$

$\Rightarrow p_1 \cdots p_r > \underbrace{\lfloor \sqrt{n} \rfloor \cdots \lfloor \sqrt{n} \rfloor}_{\text{r times}}$.

Notice that $p_k > \lfloor \sqrt{n} \rfloor$ is equivalent to $p_k \geq \lfloor \sqrt{n} \rfloor + 1$, since p_k is an integer.

$\Rightarrow p_1 \cdots p_r \geq \underbrace{(\lfloor \sqrt{n} \rfloor + 1) \cdots (\lfloor \sqrt{n} \rfloor + 1)}_{\text{r times}} > \underbrace{\sqrt{n} \cdots \sqrt{n}}_{\text{r times}} \geq n$, which is false.

Hence, there must exist $k \in \{1, ..., r\}$ such that $p_k \leq \lfloor \sqrt{n} \rfloor$.

By definition, if n is prime, then it doesn't have any divisors. Hence the biconditional. $\blacksquare$

2. Primality test of i

Let i be an integer, then i is prime if and only if $p_0, ..., p_\beta \nmid i$ with $p_0 \leq ... \leq p_\beta \leq \lfloor \sqrt{i} \rfloor$ (Theorem 2).

3. Primes up to γ

For an ordered list $\mathbf{X} = (x_0, ..., x_\alpha)$ and some number $x_{\alpha+1}$, let $+\leftarrow$ denote the *append operator*, so then $\mathbf{X}+\leftarrow x_{\alpha+1}$ means $\mathbf{X} = (x_0, ..., x_\alpha, x_{\alpha+1})$. Let $\mathbf{P}(\gamma)$ be an ordered list with $\mathbf{P}_i(\gamma)$ being the i-th element of it. Initially $\mathbf{P}(\gamma) = (2)$. Let $i \geq 3$ be odd. Then

$S(i)$: If $\mathbf{P}_j(\gamma) \nmid i \ \forall \mathbf{P}_j(\gamma) \leq \lfloor\sqrt{i}\rfloor \Rightarrow i$ is prime and $\mathbf{P}(\gamma)+\leftarrow i$

for $0 \leq i \leq \alpha$, makes $\mathbf{P}(\gamma) = (2, ..., p_\alpha)$ contain all prime numbers up to γ.

4. Prime factorization of n

Let $m_i = n$ for $i = 0$, $\mathbf{F}(n)$ be an empty ordered list, $\gamma = \mathbf{P}(i)$ and r_i be the largest integer such that $(\mathbf{P}_i(\gamma))^{r_i} \mid m_i$. Then

$$T(i) : \begin{cases} \text{If } m_i > 1,\ r_i \neq 0 \text{ and } \mathbf{P}_i(\gamma) \leq \lfloor\sqrt{m_i}\rfloor \Rightarrow \mathbf{F}(n)+\leftarrow (\mathbf{P}_i(\gamma))^{r_i} \text{ and } m_{i+1} \leftarrow \frac{m_i}{(\mathbf{P}_i(\gamma))^{r_i}} \\ \text{If } m_i > 1,\ r_i = 0 \text{ and } \mathbf{P}_i(\gamma) > \lfloor\sqrt{m_i}\rfloor \Rightarrow m_i \text{ is prime, } \mathbf{F}(n)+\leftarrow (\mathbf{P}_i(\gamma))^{r_i} \text{ and process ends} \\ \text{If } m_i = 1 \Rightarrow \text{process ends} \end{cases} \tag{1}$$

for $0 \leq i \leq \alpha$, gives $\mathbf{F}(n) = (f_0, ..., f_\beta)$ as a list of prime factors of n (Theorem 1), where β is the positional index of the greatest factor of n.