Theorems for long division and root extraction

Viktor Krapivensky

January 15, 2021

1 Notations

$\mathbb{N} = \{0, 1, 2, \ldots\}$.

2 Three-by-two theorem

This theorem is extremely useful for basecase division.

Theorem 1 (three-by-two)**.** *Fix $B \in \mathbb{N}$, $B > 1$, the base of our positional number system. Fix also numbers $x \in \mathbb{R}$, $y \in \mathbb{R}$ such that:*

- $0 \leq x < B^3$;
- $B \leq y < B^2$;
- $x/y < B$.

Define:

- $q = \lfloor \frac{x}{y} \rfloor$, *the true quotient;*
- $q_e = \lfloor \frac{\lfloor x \rfloor}{\lfloor y \rfloor} \rfloor$, *our estimate of the quotient.*

Then either $(q = q_e)$ or $(q = q_e - 1)$.

Proof.

Lemma 1. $q \leq q_e$.

Proof. Define $\delta = x - \lfloor x \rfloor$; note that $0 \leq \delta < 1$.

We have $\frac{x}{y} \leq \frac{x}{\lfloor y \rfloor} = \frac{\lfloor x \rfloor + \delta}{\lfloor y \rfloor}$. Then $q = \lfloor \frac{x}{y} \rfloor \leq \lfloor \frac{\lfloor x \rfloor + \delta}{\lfloor y \rfloor} \rfloor$.

We now want to prove $\lfloor \frac{\lfloor x \rfloor + \delta}{\lfloor y \rfloor} \rfloor = \lfloor \frac{\lfloor x \rfloor}{\lfloor y \rfloor} \rfloor$. Since $\delta < 1$, for any integers M, N, K, the following holds: $(M < KN) \implies ((M + \delta) < KN)$.

Substitute $M = \lfloor x \rfloor$, $N = \lfloor y \rfloor$, $K = \lfloor \frac{M}{N} \rfloor + 1$. □

Lemma 2. $\lfloor x \rfloor < B(\lfloor y \rfloor + 1)$.

Proof. $\lfloor x \rfloor \le x < By < B(\lfloor y \rfloor + 1)$. □

Define now the following values:

- $u = \lfloor x \rfloor$;
- $v = \lfloor y \rfloor$;
- $q_{\max} = \frac{u+1}{v}$;
- $q_{\min} = \frac{u}{v+1}$.

Lemma 3. *The following bounds hold:*

1. $q_{\max} - \frac{u}{v} \le \frac{1}{B}$;
2. $\frac{u}{v} - q_{\min} < 1$.

Proof. 1. $\frac{u+1}{v} - \frac{u}{v} = \frac{1}{v} \le \frac{1}{B}$;

2. $\frac{u}{v} - \frac{u}{v+1} = \frac{u}{v(v+1)}$. By lemma 2, $u < B(v+1)$, so

$$\frac{u}{v} - q_{\min} < \frac{B(v+1)}{v(v+1)} = B/v \le 1.$$

□

Lemma 4. $q \ge q_e - 1$.

Proof. We have:

- $q_{\min} < \frac{x}{y} < q_{\max}$;
- $q_{\min} < \frac{u}{v} < q_{\max}$.

Taking floor of both sides of these inequalities, we get:

- $\lfloor q_{\min} \rfloor \le q \le \lfloor q_{\max} \rfloor$;
- $\lfloor q_{\min} \rfloor \le q_e \le \lfloor q_{\max} \rfloor$.

By lemma 3, $q_{\max} - q_{\min} < 1 + \frac{1}{B} < 2$. This means that $\lfloor q_{\max} \rfloor - \lfloor q_{\min} \rfloor$ is either 0, 1, or 2. We are only interested in the case of it being 2, as in other cases ($q \ge q_e - 1$) holds automatically.

Suppose $\lfloor q_{\max} \rfloor - \lfloor q_{\min} \rfloor = 2$ and $q_e - q = 2$. Then,

- $\lfloor q_{\max} \rfloor = q_e = \lfloor \frac{u}{v} \rfloor$, which implies $\frac{u}{v} \ge q_e = q + 2$;
- $\lfloor q_{\min} \rfloor = q$, which implies $q_{\min} < q + 1$.

Together, these statements imply $\frac{u}{v} - q_{\min} > 1$, contradicting lemma 3. □

□

3 Approximation of inverse theorem

This theorem is useful for calculating the inverse of a number with Netwon's method; namely, it tells us how to find the initial approximation of the inverse.

Theorem 2 (approximation of inverse). *Fix $B \in \mathbb{N}$, $B > 1$, the base of our positional number system. Fix then $n \in \mathbb{N}$, $n > 0$, the number of words in our initial approximation. Fix a number $x \in \mathbb{R}$ such that $B^n \leq x < B^{n+1}$. Define:*

- $r = \frac{B^{2n}}{x}$, *the true inverse (scaled up by $2n$ places);*
- $r_e = \lfloor \frac{B^{2n}}{\lfloor x \rfloor + 1} \rfloor$, *our estimate of the scaled-up inverse.*

Then:

- $r - 2 < r_e < r$;
- $B^{n-1} \leq r_e < B^n$.

Proof. $r_e < r$ is trivial: we increased the denominator ($\lfloor x \rfloor + 1 > x$) and then took floor of the fraction.

Define now the following values:

- $u = \lfloor x \rfloor$;
- $r' = \frac{B^{2n}}{u+1}$.

Note that $r_e = \lfloor r' \rfloor$. Then $r - r' = \frac{B^{2n}}{u(u+1)} \leq \frac{B^{2n}}{B^{2n}+B^n} < 1$. Now we have

$$r - r_e = (r - r') + (r' - \lfloor r' \rfloor) < 1 + 1 = 2.$$

We can prove $B^{n-1} \leq r_e < B^n$ by substituting the maximum and minimum possible values of $\lfloor x \rfloor + 1$ into $r_e = \lfloor \frac{B^{2n}}{\lfloor x \rfloor + 1} \rfloor$. The maximum possible value, B^{n+1}, gives us $r_e \geq B^{n-1}$; and the minumum possible value, $B^n + 1$, gives us $r_e \leq B^n - 1$. □

4 Root extraction

We are given $d \in \mathbb{N}$ and root order $n \in \mathbb{N}, n \geq 2$. We need to calculate $\lfloor \sqrt[n]{d} \rfloor$.

Define the "true" root $\xi = \sqrt[n]{d}$. Using unmodified Newton's method, we are going to iterate $y \mapsto \Phi(y)$, where

$$\Phi(y) = \tfrac{1}{n}\big(\tfrac{d}{y^{n-1}} + (n-1) \cdot y\big).$$

If $y = \xi \cdot \delta$, then $\Phi(y) = \xi \cdot \varphi(\delta)$, where

$$\varphi(x) = \frac{1 + (n-1)x^n}{nx^{n-1}}.$$

Theorem 3 (icky)**.** *$1 < \varphi(x) < x$ for $x > 1$.*

Proof. We have

$$\varphi(x) < x \Leftrightarrow 1 + (n-1)x^n < nx^n \Leftrightarrow 1 - x^n < 0.$$

Now we will prove $\varphi(x) > 1$.

$\frac{1+(n-1)x^n}{nx^{n-1}} > 1 \Leftrightarrow (1+\varepsilon)^{n-1}(\varepsilon(n-1) - 1) > -1$, where $\varepsilon = x - 1 > 0$.

Substituting $\lambda = \varepsilon(n-1) > 0$ and $m = n - 1$, we get

$$(1 + \tfrac{\lambda}{m})^m(\lambda - 1) > -1.$$

The sequence $E_m = (1 + \frac{\lambda}{m})^m$ increases monotonically for $\lambda > 0$, and $\lim_{m\to\infty} E_m = e^\lambda$. This means $0 < (1 + \frac{\lambda}{m})^m < e$; we are now going to prove

$$e^\lambda(\lambda - 1) > -1$$

for $\lambda > 0$.

The derivative $\frac{\mathrm{d}}{\mathrm{d}\lambda} e^\lambda(\lambda - 1) = e^\lambda \cdot \lambda$ is positive for $\lambda > 0$; and $e^\lambda(\lambda - 1) = -1$ for $\lambda = 0$.

□

Theorem 4 (root extraction)**.** *Consider now the following process: we start with an arbitrary integer $y_0 \geq \xi$, and then, while $y_i > \xi$, put $y_{i+1} = \lfloor \Phi(y_i) \rfloor$.*

This process will terminate at some finite step $k \geq 0$ with $y_k = \lfloor \xi \rfloor$.

Proof. Note that $\Phi(y) = \xi\varphi(y/\xi)$.

Lemma 5. *$\lfloor \Phi(y_i) \rfloor < y_i$ for any integer $y_i > \xi$.*

Proof. $\lfloor \Phi(y_i) \rfloor \leq \Phi(y_i) < y_i$. □

Lemma 6. *If, for some integer y_i, we have $y_i > \xi$ and $y_{i+1} = \lfloor \Phi(y_i) \rfloor \leq \xi$, then $y_{i+1} = \lfloor \xi \rfloor$.*

Proof. We have $y_{i+1} = \lfloor \Phi(y_i) \rfloor \leq \xi < \Phi(y_i)$. □

□

Note that $(y > \xi) \Leftrightarrow (y^n > d)$, and

$$\lfloor \Phi(y) \rfloor = \lfloor (\lfloor d/y^{n-1} \rfloor + (n-1) \cdot y)/n \rfloor.$$