Essays on the arithmetic of quadratic fields

Bill Casselman
University of British Columbia
`cass@math.ubc.ca`

Integer square roots

In this note I'll explain how to calculate $\lfloor\sqrt{N}\rfloor$ for N a positive integer. The final algorithm can be found easily in many places, but justification is more difficult to locate..

Contents

1. Newton's method [intsqrt.tex]

I start by recalling Newton's method for finding square roots of real numbers. Define

$$f\colon\ x \longmapsto x - \frac{x^2 - N}{2x} = \frac{x + N/x}{2}\,.$$

Start with any initial value $x_0 > 0$, then calculate successively

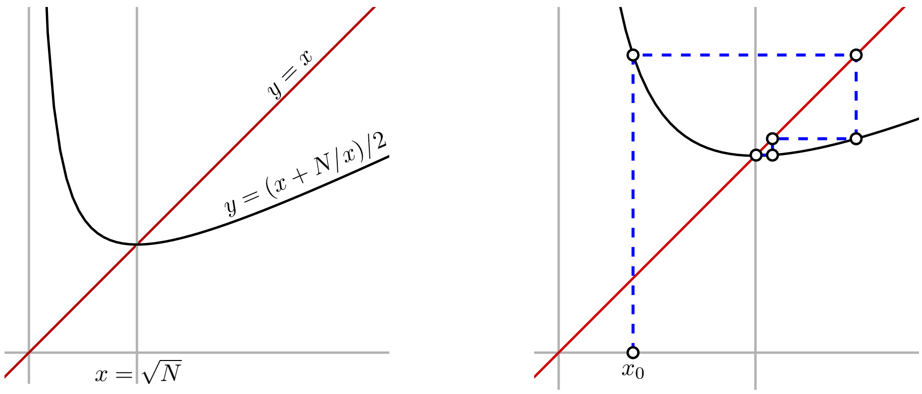
$$x_{n+1} = x_n - \frac{x_n^2 - N}{2x_n} = \frac{x_n + N/x_n}{2} = f(x_n)\,.$$

[newton] **1.1. Proposition.** *Suppose* $n > 0$, $y = f(x)$. *Then*

(a) *if* $x > \sqrt{N}$ *then* $\sqrt{N} < y < x$;
(b) *if* $x^2 = N$ *then* $y = x$;
(c) *if* $x < \sqrt{N}$ *then* $y > \sqrt{N} > x$.

Proof. The derivative of f is $(x + N/x)/2$, which is $(1/2)(1 - N/x^2)$. This is negative if $x < \sqrt{N}$ and positive if $x > \sqrt{N}$, so that $x = \sqrt{N}$ is a minimum.

It is instructive to look at some graphs. On the left you can see the basic data. On the right you see a trajectory of the iteration $x_{n+1} = \varphi(x_n)$, starting with $x_0 < \sqrt{N}$.



Replace x by $y = f(x)$ successively. If we start any value of x other then $\sqrt{N}$, the next will be larger than $\sqrt{N}$, and that will remain true from then on. Now

$$\begin{aligned} y^2 - N &= \frac{(x^2-N)^2}{4x^2} \\ \frac{y^2-N}{x^2-N} &= \left(\frac{1}{4}\right)\left(1-\frac{N}{x^2}\right) \\ &\le \frac{1}{4}\,. \end{aligned}$$

So that at each stage the error $x^2 - N$ is cut down by a factor of at least $1/4$. But also

$$y^2 - N \le \frac{(x^2-N)^2}{4x^2} \le \frac{(x^2-N)^2}{4N}\,,$$

so that from some point on the convergence of x^2 to N is quadratic.

Furthermore

$$x - \sqrt{N} = \frac{x^2-N}{x+\sqrt{N}} \le \frac{x^2-N}{2\sqrt{N}}$$

so that the same is true of the convergence of x.

2. The integer version [intsqrt.tex]

Let

$$F\colon\, n \mapsto \left\lfloor \frac{n + \lfloor N/n \rfloor}{2} \right\rfloor$$

[fn-sqrt] **2.1. Proposition.** *Suppose* $n > \sqrt{N}$. *Then*

(a) $F(n) < n$;
(b) $F(n) \le F(n+1)$;
(c) *if* $n = \lfloor \sqrt{N} \rfloor + 1$ *then* $F(n) = \lfloor \sqrt{N} \rfloor$.

Hence if we start with $n = N$, we get a decreasing sequence until $n^2 < N$. Suppose $n_\circ$ to have been the previous value of n, which was larger than $\sqrt{N}$. Therefore $n_\circ \ge \lfloor \sqrt{N} \rfloor + 1$, and hence $F(n_\circ) \ge F(\lfloor N \rfloor + 1)$. Thus n is now $\lfloor \sqrt{N} \rfloor$. If $N + 1$ is a perfect square $(n+1)^2$, then from that point on F will cycle between n and $n+1$. Otherwise $F(n) = n$.

Proof. I recall first some simple properties of the function $\lfloor x \rfloor$.

(i) If $x \le y$ then $\lfloor x \rfloor \le \lfloor y \rfloor$;
(ii) $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$.
Together, these imply that
(iii) if $y \le x \le y + 1$ then $\lfloor x \rfloor - 1 \le y \le \lfloor x \rfloor$.

Proof of **(a).** Since $\lfloor N/n \rfloor \le N/n$,

$$n + \lfloor N/n \rfloor \le n + N/n, \quad \left\lfloor \frac{n + \lfloor N/n \rfloor}{2} \right\rfloor \le \left\lfloor \frac{n + N/n}{2} \right\rfloor\,.$$

But since $N/n < n$,

$$\frac{n + N/n}{2} < n, \quad \left\lfloor \frac{n + N/n}{2} \right\rfloor < n\,.$$

Combining:

$$\left\lfloor \frac{n + \lfloor N/n \rfloor}{2} \right\rfloor \le \left\lfloor \frac{n + N/n}{2} \right\rfloor < n \, .$$

Proof of **(b).** Start with

$$\frac{N}{n} - \frac{N}{n+1} = \frac{N}{n(n+1)} < \frac{N}{n^2} < 1 \, ,$$

or

$$\frac{N}{n+1} < \frac{N}{n} < \frac{N}{n+1} + 1 \, .$$

This implies by (iii) that

$$(n+1) + \lfloor N/(n+1) \rfloor \ge n + \lfloor N/n \rfloor$$

and finally

$$\left\lfloor \frac{n + 1 + \lfloor N/(n+1) \rfloor}{2} \right\rfloor \le \left\lfloor \frac{n + \lfloor N/n \rfloor}{2} \right\rfloor \, .$$

Proof of **(c).** If $n = \lfloor \sqrt{N} \rfloor$, then

$$n^2 \le N < (n+1)^2, \quad \frac{n^2}{n+1} \le \frac{N}{n+1} < n + 1 \, .$$

But

$$n - 1 < \frac{n^2}{n+1}$$

so

$$n - 1 \le \frac{N}{n+1} < n + 1 \, .$$

But then

$$n \le F(n+1) = n + 1 + \left\lfloor \frac{N}{n+1} \right\rfloor < n + 1$$

which implies that $F(n+1) = n$.

Here is the final algorithm (where // signifies integer division):

```
def intsqrt(N):
    n = N
    m = (1 + N)/2
    while n > m:
        p = m + N//m
        n = m
        m = p//2
    # now n <= m
    return n
```