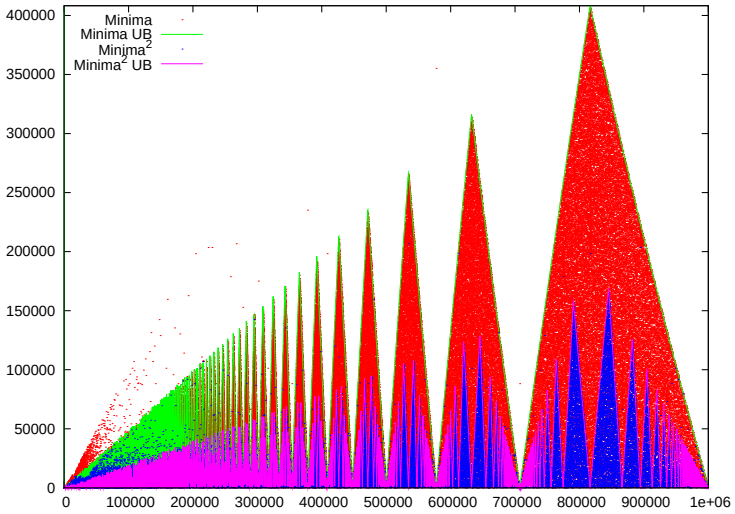
1 Introduction

During one of several attempts to find a factorization algorithm, Elfi came up with the following idea: if $k|n$ then $n \bmod k = 0$ and so $n \bmod k$ is a local minimum in the sequence $n \bmod i, i = 1, \ldots, \lfloor\sqrt{n}\rfloor$. Moreover, it is a local minimum in the local minima sequence, and so on. The following graph presents the first two iterates in this series.



Along with the sequences themselves, there is a projected upper bound, which we shall calculate below. Note however two exceptions to this upper bound. The first is near the beginning, where the upper bound (and our theory) fail miserably. Secondly, between the 'triangles' there are some hard to see outliers.

2 Minima Upper Bound

In this section we will develop formulas for the upper bounds. The first step is to write $n \bmod i$ as $i\lfloor n/i \rfloor$. Now consider three consecutive elements of the minima sequence. We will make the simplifying assumption $i-1 \approx i \approx i+1$, which is justified (in our context) given $\lfloor n/i \rfloor$ is not too small. Given this assumption, $n \bmod i$ is a local minimum when $\lfloor n/i \rfloor$ is.

We are thus led to study the sequence $\lfloor n/i \rfloor$. This quantity changes roughly by $\{n/i^2\}$ in each direction, where $\{x\}$ is the fractional part function. In fact, for our purposes it is more natural to take the signed fractional part function, which can be defined as $x - \text{round}(x)$. This is a value in the range $[-\frac{1}{2}, \frac{1}{2}]$ which is the same as the usual fractional part modulo 1. This function is more suited to our cause since it satisfies the rule $\{-x\} = -\{x\}$, which

means that the amount by which $\lfloor n/i \rfloor$ changes differs by sign only from left to right.

Let us consider what is happening. Define $\alpha(x) = |\{x\}|$. The value $\alpha(n/i^2)$ is the unsigned amount by which $\lfloor n/i \rfloor$ changes. Looking at the 'neighborhood' of a certain i, the value $n \bmod i$ changes (either going up or down) by $\alpha(n/i^2)$ until it reaches the boundaries of the interval $[0, 1]$, and then it suddenly 'loops'. If going down, the last value before looping will be a local minimum, while if going up, the first value after looping will be a local minimum. We can thus derive the upper bound as $i\alpha(n/i^2)$.

2.1 Scaling

At this point we mention a trivial observation: up to scaling, the upper bound graph looks the same for any n (thus, we do not expect it to help factoring n...), and so it is natural to scale it by $\sqrt{n}$ in each axis. The new upper bound is $x\beta(x)$, where $\beta(x) := x\alpha(1/x^2)$.

2.2 Nature of Upper Bound

The upper bound at the graph looks rather like a collection of triangles. In this subsection we will find its exact shape.

First, the critical points — points of discontinuity of the derivative — are $1/k^2$. In the range $\left[1/\sqrt{k+\frac{1}{2}}, 1/\sqrt{k}\right]$, the expression $1/x^2$ takes the value range $[k, k+\frac{1}{2}]$ and so $x\beta(x) = x\alpha(1/x^2) = x(1/x^2 - k) = 1/x - kx$. Similarly, in the range $\left[1/\sqrt{k+1}, 1/\sqrt{k+\frac{1}{2}}\right]$ we have $x\beta(x) = kx - 1/x$. The function $1/x$ is nearly constant in each of these regions, and for this reason the range looks linear in each such region.

3 Iterated Upper Bounds

In this section we shall compute the upper bounds corresponding to minima of minima, minima of minima of minima and so on. The next section will concern itself with maxima.

We start with minima of minima. We have already seen that the 'critical' value of minima (of the sequence $\{n/i]\}$) is given by $\beta(x)$. That is the amount by which the original sequence changes. How does the value of the minimum itself change? Approximately $\text{round}(1/\beta(x))$ points separate one minima from another. The value itself changes by $\alpha(\beta(x)\text{round}(1/\beta(x)))$. This ex-

pression simplifies (prove!) to $\beta(x)\alpha(1/\beta(x))$. Defining $\gamma(x) = x\alpha(1/x)$, we get the the upper bound for minima of minima is $x\gamma(\beta(x))$.

We continue with minima of minima of minima. This time the value of minima of minima changes by $\gamma(\beta(x))$. This time the number of values seperating adjacent minimas of minimas is round$(\beta(x)/\gamma(\beta(x)))$, since the relevant 'window' of minimas is of height $\beta(x)$. Redefining $\gamma(x, y) := y\alpha(x/y)$, we recover our old definition $\gamma(x) = \gamma(1, x)$, and get the following upper bound for minimas of minimas of minimas: $x\gamma(\beta(x), \gamma(\beta(x)))$.

Generally, the following function ν gives the correct iteration formula for the γ's:

$$\begin{aligned}
\nu_0(x) &= 1, \\
\nu_1(x) &= \beta(x), \\
\nu_d(x) &= \gamma(\nu_{d-2}(x), \nu_{d-1}(x)).
\end{aligned}$$

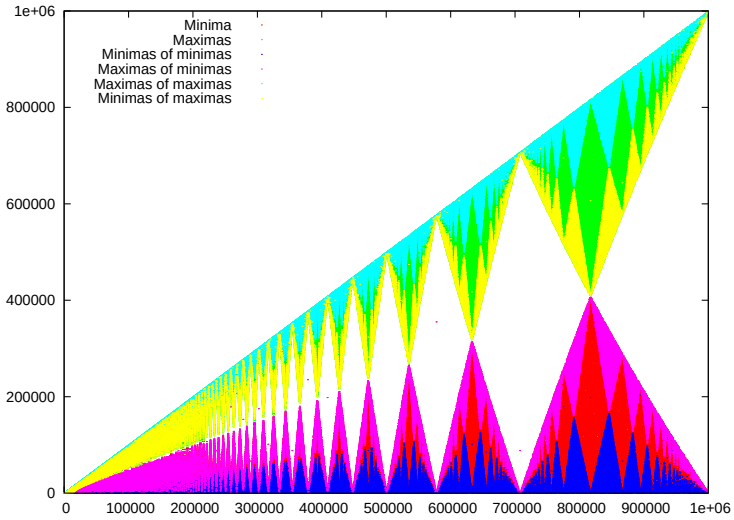
The upper bound for d'th minimas is given by $x\nu_d(x)$. We can incorporate the multiplication by x to get a new function sequence μ:

$$\begin{aligned}
\mu_0(x) &= x, \\
\mu_1(x) &= x\beta(x), \\
\mu_d(x) &= x\gamma(\nu_{d-2}(x), \nu_{d-1}(x)).
\end{aligned}$$

The upper bound for the d'th minimas is simply $\mu_d(x)$.

4 Maxima Bounds

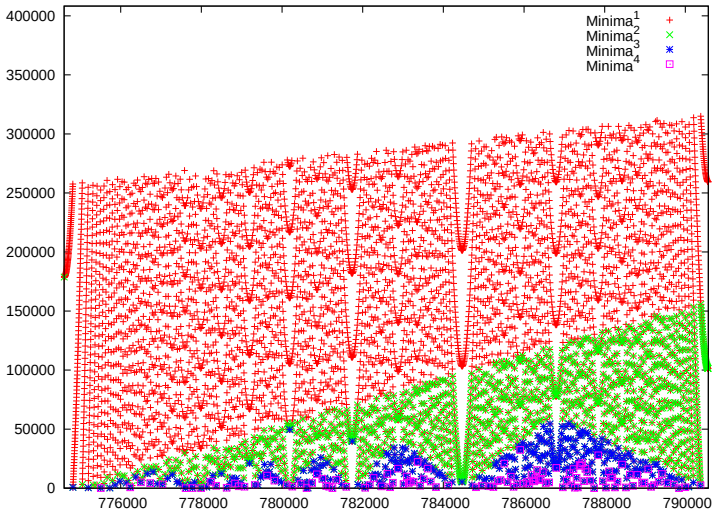
We can generalize the ongoing discussion to bounds on maximas. We start by extending the plot to include also maximas:



We see the the maximas are a mirror reflection of the minimas. We can thus get a lower bound for the maximas by subtracting from x the upper bound of the minimas. The similar changes needed to obtain bounds for the other types, as well as arguments explaining the formulas, are all left for the reader to contemplate.

5 Closeup

The following is a closeup of the plot in the range $[\sqrt(3/5), \sqrt(5/8)]$.



The close shows some interesting phenomena. There are yet things for the reader to explore!