How to create and use your own Lehmer Factor Stencils

KATHERINE E. STANGE

1. Introduction

This is a document to accompany my YouTube video about Lehmer's Factor Stencils. Please view the video for all the delicious history and surrounding information. The purpose of this document is to lay out the math clearly so you could produce and use your own stencils. You'll also find my Python scripts and SVG files of the stencils for you to use. If you are a Do-It-Yourselfer, this is for you.

Unfortunately, in the video there were a few small errors in the calculations shown. I'm going to correct them here. First is a subscript error in the recurrence formula for Q_n. Second, one needs to include $Q_{-1} = 1$ to get started. Third is that when recording my by-hand calculations, I copied my calculations from a table (to make the video smoother) and made an offset error, so every line for Q uses the wrong P_n values, but gets the correct answer (which is why I didn't notice!). I am very sorry – and embarrassed – about these errors. I wrote a computer program to verify the recurrences, but then made hand-copying errors in producing the video. Everything should be corrected now in this document, below.

2. Stencil Overview

The stencils themselves have positions corresponding to each prime number from three[1], up to some bound B. This will, in general, allow factoring numbers which have a prime in this range, so all numbers up to bound B^2, and many besides.

There's one stencil for each squarefree integer. Since you don't want to create infinitely many stencils, it makes sense to set a bound for your deck, which I'll call D. Then there should be a stencil for every squarefree number between $-D$ and D inclusive, except for 0 and 1. Numbers are squarefree with probability approximately $6/\pi^2$ (there are great YouTube videos about this too!), so this is around $12D/\pi^2 \sim D \cdot 1.215\ldots$ stencils.

On stencil with label X, you should punch out all the primes p for which X is a quadratic residue (including p dividing X).

3. Using the Stencils

To use the stencils to factor N, find quadratic residues $X_1, X_2, X_3, \ldots, X_k$ modulo N. More on how to do that below. Then, collect the stencils corresponding to those X_i, lay them over one another and check which primes are punched all the way through the stack. These are the possible prime factors of N below B. They are not guaranteed to be factors, but it is easy to check each one. If none of them are factors, then N has no prime factors below B. If $N < B^2$, this proves that N is prime.

Date: October 26, 2021, Draft #1.

[1] even numbers are fairly easy to factor, honestly

4. Finding Quadratic Residues With Continued Fractions (Recurrences)

To find quadratic residues, one way is to run the following set of recurrence relations:

$$\begin{aligned} P_0 &= S_0 = \lfloor \sqrt{N} \rfloor \\ Q_0 &= N - P_0^2, \quad Q_{-1} = 1 \\ S_n &= \left\lfloor \frac{S_0 + P_{n-1}}{Q_{n-1}} \right\rfloor \\ P_n &= S_n \cdot Q_{n-1} - P_{n-1} \\ Q_n &= S_n \cdot (P_{n-1} - P_n) + Q_{n-2}. \end{aligned}$$

The Q_i for i odd and $-Q_{i+1}$ for i even are all quadratic residues for N.

5. Improving Your Quadratic Residues

If you have quadratic residues $X_1, X_2, X_3, \ldots, X_k$, you may be able to derive smaller quadratic residues from them:

(1) You can divide out any square factors from any X_i. For example, if 18 is a quadratic residue, then 2 is a quadratic residue.
(2) You can multiply them together. You'd think this would make them bigger, but if you do this in such a way as to create squares to divide out, you can sometimes win. Sometimes you can get very clever at this, if you first factor your quadratic residues and look for factors to combine.

6. Finding Quadratic Residues by Squaring

You can also take k near $\sqrt{N}$ and try values $(k \pm \ell)^2 - N$ for small ℓ. These are all quadratic residues, and some will be smallish. It's possible to modify this strategy to try k near $\sqrt{2N}$, $\sqrt{3N}$ etc. This is the beginning of the so called *quadratic sieve*, which could be used to improve this method. (I'm thinking of making another video about that...)

7. Using my SVG Files

SVG is a fairly standard file format for paper cutting machines. You should be able to import it into your software, choose the parts to cut, and go for it.

8. Using my Python script

You can also modify my stencils to create a Sieve of Eratosthenes or other changes, using the Python code provided. It includes documentation within the code.

9. Worked Example

This is the example I did in the video. Let $N = 8416909$. The initial conditions for the recurrences are:

$$P_0 = S_0 = 2901, \quad Q_{-1} = 1, \quad Q_0 = 8416909 - 2901^2 = 1108.$$

The next step is

$$\begin{aligned} S_1 &= \lfloor (2901 + 2901)/1108 \rfloor = 5 \\ P_1 &= 5 \cdot 1108 - 2901 = 2639 \\ Q_1 &= 5 \cdot (2901 - 2639) + 1 = 1311 \end{aligned}$$

Then, continuing in this manner, I get:

i	S_i	P_i	Q_i	quad. res.
0	2901	2901	1108	-1108
1	5	2639	1311	1311
2	4	2605	$1244 = 4 \cdot 311$	-311
3	4	2371	2247	2247
4	2	2123	$1740 = 4 \cdot 435$	-435
5	2	1357	3779	3779
6	1	2422	$675 = 9 \cdot 25 \cdot 3$	-3
7	7	2303	$4612 = 4 \cdot 1153$	1153
8	1	2309	$669 = -3 \cdot -223$	223
9	7	2374	4157	4157
10	1	1783	$1260 = 4 \cdot 9 \cdot 35$	-35
11	3	1997	3515	3515
12	1	1518	1739	-1739

Notice that at row $i = 2$, I removed a factor of 4 to get a smaller residue. You'll see something similar in rows $i = 6$ and $i = 10$. Notice also that in row $i = 8$ I divided by -3, because I knew that to be a quadratic residue already.

I can get other quadratic residues by combination. For example, combining $-435, -3, -35$:

$$-435 \cdot -3 \cdot -35 = -3^2 \cdot 5^2 \cdot 7 \cdot 29 \text{ gives } -203.$$

Sometimes some of these are smaller than the inputs. So we can replace -435 with -203 if needed (if our deck doesn't go up as high as -435). Notice that this combination approach won't give totally independent stencils: the stencil for X and Y has a relationship to the stencil for XY. So the new stencils you come up with will tend to be kind of redundant. However, it does let you swap for smaller ones sometimes.

In this way, one can obtain quadratic residues

$$-3, -35, 105, -203, 223, -311, -435, 535.$$

Overlaying these stencils, one obtains the following possible primes:

$$3, 73, 631, 3463, 3517$$

In fact, since my number has square root around 2901, one of the first three of these must work if it isn't prime: 631 does. It turns out

$$8416909 = 631 \cdot 13339.$$

Department of Mathematics, University of Colorado, Campux Box 395, Boulder, Colorado 80309-0395

Email address: kstange@math.colorado.edu