Integer Factorization, Ceiling Squares, and the Ascent

An Informal Description of Recent Exploration

By J. Calvin Smith, B.A., Mathematics, Georgia College, Milledgeville, Georgia, United States of America (1979) - Retired Member, American Mathematical Society

Written from Autumn, 2022 to Spring, 2023 at Mountain River Chalet (the author's home), Talking Rock, Georgia, USA.

Preliminary Concepts

Consider an odd positive integer m. The author confines m to the odd positive integers for that set's elements' suitability in behaving according to the formulae that appear in the discussion which follows. Therefore, one may obtain a suitable value of m from any general positive integer by dividing by 2 as many times as necessary, recording, as appropriate, that two to that power is a prime-to-a-power factor of such an integer.

Because m is odd, any factors or divisors of m are also odd. The odd positive integers, like the non-negative even integers, are a closed set under the operation of multiplication, even though all even integers except simple powers of 2 have odd divisors.

Suppose we do not know whether m is prime or composite. That is to say, we know of no factors/divisors of m besides 1 and m itself. Even so, there are properties of m we can observe that may lead us to discover whether other factorizations are possible. Despite a well-known difficulty in general of finding the prime factors of very large values of m, there are ways of expressing m, moreover, that are not immediately apparent to the layman, which may help uncover more information about the integer. This article will discuss some of these concepts and possibilities for future study which have become apparent to the article's author.

The Integer m Expressed as the Difference of Perfect Squares

Whenever we know the factorization of odd positive integer m into two integer factors, say a and b, with a less than or equal to b, the following formula also gives us an expression for m as the difference of perfect squares. Choose $s = (a + b)/2$ and $t = (b - a)/2$. These positive integers, it can become clear by working out algebraically, satisfy $m = s^2 - t^2$.

The trivial factorization $m = 1 * m$ gives by the above formula $s = (m + 1)/2$ and $t = (m - 1)/2$ as the two consecutive integers the difference of whose perfect squares gives the value m. This works for all odd m, prime or composite, by virtue of this factorization being the trivial one.

If, however, we discover perfect squares of non-consecutive integers whose difference is m, we have found another, this time non-trivial, factorization of m. Pierre de Fermat discovered this method of expressing integers as differences of perfect squares, and the advantage it could give to the process of finding unknown factorizations. The puzzle recently has seemed to be how to discover the two perfect squares of non-consecutive integers that will give a solution.

Ceiling Squares and Ceiling Roots

The most recent focus of my study of integer factorization centers on how to use what we know about any particular composite m whose factors we do not know, in order to determine the factorization. I have come up, in my own study, with what I feel are new ways to look at what we know, although these ways have so far simply reframed the problem of factorization more than they have actually simplified it.

Chief among the concepts upon which I have stumbled, in terms of leading me down several paths of new (to me) insights, is the Ceiling Square, which I define as: the smallest perfect square greater than or equal to m. How does this number figure into the factorization of m? How does it relate to the actual differences of perfect squares which characterize any factorization of m into a and b? These are questions I continue to pursue.

In addition to the Ceiling Square, and its square root which I call the Ceiling Root, the smallest positive integer greater than or equal to the square root of m, there is a remainder for us to consider. If c denotes the ceiling square of m, then $m = c^2 - r$ for some nonnegative integer r. If r is 0, or a perfect square, our factorization search is probably

over. Most discrete semiprimes, however, do not seem to have ceiling squares with remainders r which are perfect squares. But since the s in the $s^2 - t^2$ expression is greater than or equal to the ceiling square (it is instructive to figure out why), I have found it tantalizing to wonder, and fruitful for my mathematical experience to investigate, just what relationships there may be between m's ceiling square c, its remainder r, and its factorization.

Squares Above, Squares Below, and Raising the Ceiling

This section deals with primarily personal notes, along the lines of "thinking out loud," on the intermediate stages of development of ideas, incomplete observations, and the like.

One observation I could not figure out where to fit in above is that, when considering the expression of odd integer m as the difference of the squares of s and t, one can take into consideration the value of m modulo 4 as follows. For all such expressions $m = s^2 - t^2$, corresponding to every possible factorization $m = ab$, when m is congruent to 1 modulo 4, s will be odd, and when m is congruent to 3 modulo 4, s will be even, with t being either even or odd correspondingly. This follows from the fact that all even perfect squares are congruent to 0 modulo 4 and all odd perfect squares are congruent to 1 modulo 4. In order for m to be congruent to 3 modulo 4, the only possible perfect square difference giving this result would be the subtraction of an odd t^2 from an even s^2, as $-1 \equiv 3 \pmod 4$.

Having said this, whether the Ceiling Square and Ceiling Root of an arbitrary m, though being of opposite odd/even parity as the remainder in the expression $m = c^2 - r$, has approximately an equal chance of being odd or even no matter what is the value of m modulo 4. Basically, the least perfect square greater than m does not much depend on whether m is congruent to 1 or 3 modulo 4. However, this was a thought that deserved further adjustment. (See the sections that follow.)

I began examining in the Summer and Fall of 2022 the possibility of a relationship between m (the Integer to Factor), c (m's Ceiling Root), r (the Difference between the Ceiling Square and m), and where m falls in the range of integers $c^2 - {a_0}^2 < m < c^2 - (a_0 + 1)^2$. Here the value a_0 is the Ceiling Root of r. If we increase c by 1 (I call this "raising the ceiling"), there will of course be a different remainder given by $m = (c + 1)^2 - r_1$, with r_1 having its own Ceiling Square and thus providing another range of values. The two ranges of values, between differences of perfect squares, has, I believe, some bearing on the integer n needed to add to c (a quantity I call the Ascent) to yield a value of r_n that is a perfect square, permitting Fermat factorization.

I also developed what I call a characteristic polynomial corresponding to the behavior of the Ceiling Square remainders obtained by "raising the ceiling" this way. If I take the remainders r and r_1 obtained by subtracting m from c^2 and $(c+1)^2$ and use them to create range lower bounds $c^2-a_0^2$ and $(c+1)^2-a_1^2$, and then create a third range lower bound linearly, $(c+2)^2-a_2^2$, where this time a_2 is $2a_1-a_0$, the difference between m and these three lower bound integers becomes a set of three values I consider to be the values for x=0, 1, and 2 of a quadratic polynomial in x that I call the characteristic polynomial, in this context, of m. I have only just begun looking into the behavior of this polynomial and whether it can simplify factorization calculations more than earlier calculations, revelations, and algorithms this study has brought to my attention and discovery.

There was, at this period in my integer factorization study, a great deal of work to be done, and a great amount of academic work that has been done of which I am aware, using modern methods that can often speed up calculations and enable factorization of huge numbers. The algebraic number theory finite field theory brought to bear on this problem has been substantial and theoretically complex, at least to my own understanding. Perhaps I suffer from severe naïveté in suspecting and pursuing simpler numerical relationships at work. However, I have received some small education, through my schooling and work training, in the more advanced methods of number theory, and I see possibilities based on where they and my own ideas have been headed. Additionally, as one of my mathematics instructors later in my life advised me, integer factorization is a process about which we know very little about the next breakthrough, and nothing at all about how simple it could be.

An Adjusted Approach

It occurred to me after a time that my approach outlined above would benefit from starting, not necessarily with the Ceiling Square c, but with c or c+1 corresponding to whether s^2-t^2 has even or odd s, and increasing by 2, to get x=0,2,4 points for the characteristic polynomial.

From my blog entry dated 15 September 2022 on jcsbimp.com:

> The Adjusted Ceiling Square of odd positive integer m is the least perfect square greater than m that is odd if m is congruent to 1 modulo 4, and is even if m is congruent to 3 (or -1) modulo 4. When constructing ranges in the algorithm most recently

discussed, then, one would set the greater square for the first range lower bound, c_0^2, to be the Adjusted Ceiling Square of m. Then, for the next two ranges, the greater squares will be $(c_0+2)^2$ and $(c_0+4)^2$, and the values of where m falls within the three ranges thus generated will be the values of f(x), the characteristic polynomial, at x=0, 2, and 4.

I simply thought it was much more sensible to base the characteristic polynomial on ranges of differences of perfect squares that matched the even/odd polarity of the actual difference-of-squares form of any solutions of m, based on its being congruent to 1 or -1 modulo 4. Why base a characteristic polynomial algorithm on range values that are immediately apparent not to be candidates for its "Fermat factorization"?

Zones and Bee Lines: New Revelations and a Current Algorithm

Now that I have verified the utility of adjusting the Ceiling Square, from this point on in this paper, and in my other writing, I will simply refer to the "Adjusted Ceiling Square" as the "Ceiling Square," and denote the value not adjusted by what it simply is: the square of the integer ceiling of the square root of m, or the least perfect square greater than m.

In late February or early March, 2023, I came upon a concept that led me to construct another factorization algorithm. While it was of debatable benefit in increasing computation speed, despite getting past some long-run-time conditions the older Perl scripts were hitting with randomly-entered odd integers, it is my current avenue of research and one that is showing a possibility of further insight into improvements.

Some months earlier, I had begun looking at where the successive remainders r_0, r_1, r_2, …, r_n obtained from $r_n=(c+n)^2-m$ fall between the consecutive perfect squares that bound them below and above. I had begun graphing them, so to speak, using typeset characters

using the letter X to position them in a row of periods between the bounding perfect squares, which I represented with asterisks. For example the row for a remainder of 7, between 4 and 9, would look like:

```
*..X.*
```

The series of remainders thus obtained, which are the values of $x^2+2cx+r$ for x=0,1,2,…, would form what I called a Beehive Chart, with a number of rows corresponding to how big an n to add to c to make $(c+n)^2-m$, the value of f(n), a perfect square For example, the following is the Beehive Chart for m=295, $f(x)=x^2+36x+29$:

```
                    25 *...X......* 36
                  64 *.X.............* 81
                100 *....X.............* 121
              144 *.X.....................* 169
             169 *.................X.....* 196
           225 *........X.....................* 256
          256 *.......................X.......* 289
        324 *.....X.............................* 361
       361 *.................X.................* 400
     400 *...............................X......* 441
   484 *....X.....................................* 529
  529 *...............X............................* 576
 576 *.............................X.................* 625
625 *.....................................X.........* 676
676 *.................................................X 729
```

I made several of these Beehive Charts, and began to notice a property I called the Bee Line: When the Beehive Charts had regions where their walls sloped straight with consecutive perfect squares defining their bounds, not only did the asterisks have those straight lines, but the X values fell in straight lines, too. This was beautiful to me, above and beyond the fact that consecutive perfect squares have an even number of integers between them, allowing the Beehive Chart to center nicely in typeset characters. Since in this chart and others, it seemed like the X's, or "bees," were seeming to discover a straight line to where they would hit the Beehive wall exactly (hopefully finding a doorway there!), I called this a Bee Line.

This takes the discussion to the revelation of the past month: I reexamined the Beehive Chart layout idea, and expanded it as follows: I began putting successive remainders on successive rows as before, but this time I included dots and asterisks for all of the intervening perfect squares, not just the consecutive squares that bounded the remainders. When I did this, I discovered the general case of what I just described above: If I arrange

rows corresponding to the integer number line, with asterisks marking perfect squares and periods the numbers between, and lined up x^2 in one row with $(x+1)^2$ in the row below it, followed by (x+2) in the row before that, and so on, it became apparent that sequences of consecutive perfect squares going from one number line to the next formed an infinite series of straight lines that crossed the number lines. Furthermore, marking the first remainder in the remainder series as an X on any such number line, the second on the row after that, and so on, I saw that the remainder series itself formed a straight line on this extended chart idea, corresponding to the Bee Line in the Beehive Charts when the slope of the chart's walls was constant with consecutive perfect squares.

This sent me into a flurry of programming activity, as I applied analytic geometry principles to the concept of placing these number line integers on a Cartesian Plane at the integer points of the grid, in a standard fashion, and converting Ceiling Squares and Remainder Series to lines on the graph. My newest algorithm has followed this method, jumping after a fashion from Zone to Zone, which term I use to denote areas on the graph between straight-line sequences of consecutive perfect squares, until the straight Remainder Line hits a Zone boundary at an integer point.

As said earlier, this approach has proven not to be much faster than earlier algorithms I've written taking advantage of the Ceiling Square concept. But the search for further advantage to be taken, and more rapid integer factorization, goes on.