Semi-prime factorization – Analysis of Fermat's Factorization method

By Essbee Vanhoutte
Version 20.0

Foreword

I am self-taught without formal math education as I dropped out of high-school. This represents 3 years of research and teaching myself mathematics.

Before this I was a self-taught software vulnerability researcher who briefly worked at companies such as Microsoft and Trend Micro and has well over 50+ CVEs in software such as Windows OS, OpenSsl and Adobe Reader attributed to their name (often under the handle SandboxEscaper or Polar Bear).

No AI was used for this research, I have only used it in the last couple of weeks to review my paper and get feedback and occasionally to produce code for well documented mathematical functions.

This paper mainly illustrates findings by example and companion code rather than rigorous mathematical notation and proofs. So perhaps rather than a formal academic paper, view this as a mathematical exploration by an enthusiast with prior experience in IT security.

To do: Add references and closing thoughts and clean everything up.
To do: Bunch of inconsistencies with signs on how I represent these quadratics on both sides

Chapter I – Fermat's Factorization method

In its most basic form the procedure for Fermat's Factorization method is as follows (where N is the semi-prime being factored).

1. Calculate $\lceil\sqrt{N}\rceil$
2. Starting from $x = \lceil\sqrt{N}\rceil$, calculate $f(x) = x^2 - N$ in a loop, incrementing x.
3. If $f(x)$ evaluates to a square, y^2, compute $GCD(x+y, N)$ and $GCD(x-y, N)$

It is plain to see why this works, because if $x^2 - N = y^2$ then it also follows that $N = x^2 - y^2 = (x-y)(x+y)$ hence anytime we have $x^2 \equiv y^2 \pmod{N}$ where $x \not\equiv \pm y \pmod{N}$ the factors can be computed via GCD

Taking $N = 4387$ as an example:

Step 1 (Calculate $\lceil\sqrt{N}\rceil$)

$\lceil\sqrt{4387}\rceil = 67$

Step 2 (Starting from $x = \lceil\sqrt{N}\rceil$, calculate $f(x) = x^2 - N$):

67^2–$4387 = 102$ (not a square)
68^2–$4387 = 237$(not a square)
69^2–$4387 = 374$ (not a square)
70^2–$4387 = 513$ (not a square)
71^2–$4387 = 654$ (not a square)
72^2–$4387 = 797$ (not a square)
73^2–$4387 = 942$ (not a square)
74^2–$4387 = 1089 = 33^2$ (square)

Step 3 (If the result is also a square, calculate the GCD on the difference.):

$74^2 \equiv 33^2 \pmod{4387}$

$GCD(74 + 33, 4387) = 107$
$GCD(74 – 33, 4387) = 41$

Both the Quadratic Sieve and Number Field Sieve algorithms (to do: insert references) are expansions on this method.

Chapter II – Analysis

a. Binomial expansion

As seen in chapter 1 the goal is to find the following numbers that we can use to take the GCD with:

$GCD(x + y, N) = q$
$GCD(x–y, N) = p$

x and y can thus be rewritten as the differences of the factors of N divided by 2, $(p + q)/2$ or $(p–q)/2$.
In addition, many such possible x and y solutions exist created by $(ap + bq)/2$ and $(ap–bq)/2$ where a and b are multipliers.
In practice we will not know the factors p and q, but treating them as unknowns we can calculate residues in Z/ℓ (for a prime ℓ) for them using the framework we're establishing here.

If $a = 13$, $b = 5$ and $N = 4387$ (and thus factors as $p = 41$ and $q = 107$)

We get:

$(13 \times 41 + 5 \times 107)/2 = 534$
$(13 \times 41–5 \times 107)/2 = –1$

And we can see this creates the following expression when we square 534 $\pmod{N}$:

$534^2 – 4387 \times 13 \times 5 = 1^2$

One way to represent x and y is through binomial expansion.
I will shorten binomial expansion as $BE(x–y)^e$.
For example $BE(x–74)^2 = x^2–148x + 5476$.

Substituting the binomial term x in $BE(x–74)^e$, with for example 33, we get:

$BE(33–74)^1 = 33–74 = –41$
$BE(33–74)^2 = 33^2–148 \times 33 + 5476 = –41^2$
$BE(33–74)^3 = 33^3–222 \times 33^2 + 16428 \times 33–405224 = –41^3$
$BE(33–74)^4 = 33^4–296 \times 33^3 + 32856 \times 33^2–1620896 \times 33 + 29986576 = –41^4$

Conversely we also see the following occurring if we substitute in the factor as root instead (or swapping a binomial term with the binomial value):

$BE(41–74)^1 = 41–74 = –33$
$BE(41–74)^2 = 41^2–148 \times 41 + 5476 = –33^2$
$BE(41–74)^3 = 41^3–222 \times 41^2 + 16428 \times 41–405224 = –33^3$
$BE(41–74)^4 = 41^4–296 \times 41^3 + 32856 \times 41^2–1620896 \times 41 + 29986576 = –33^4$

In addition, if we have even exponents we can substitute the constant by a multiple of N and generate a polynomial $g(x)$ to solve for 0.

$BE(41–74)^2 = 41^2–148 \times 41 + 5476 \rightarrow g(x) = 41^2–148 \times 41 + 4387 = 0$
$BE(41–74)^4 = 41^4–296 \times 41^3 + 32856 \times 41^2–1620896 \times 41 + 29986576 \rightarrow g(x) = 41^4–296 \times 41^3 + 32856 \times 41^2–1620896 \times 41 + 4387 \times 6565 = 0$

Note: If the binomial terms generated with $(ap + bq)/2$ and $(ap–bq)/2$ have multipliers a and b other than 1, then you may need to translate your polynomial into a non-monic to get p or q to solve for 0, otherwise if it is monic, it will be a multiple of p or q, decided by multipliers a and b.

Observe how at degree 2 we substitute by $1N$ and at degree 4 we substitute by $6565N$. $6565 = 74^2 + 33^2$. Which encodes the square of the two binomial terms that we are trying to find, since $74^2 \equiv 33^2 \pmod{N}$. This is useful to know and we will center our final algorithm around this by using p-adic lifting. To do: Rewrite chapter IV implementing an algorithm around this

Similarly, we can expand the other binomial term and generate a quadratic that solve for 0:

$BE(41 + 33)^2 = 41^2 + 66 \times 41 + 1089 \rightarrow g(x) = 41^2 + 66 \times 41 - 4387 = 0$

$BE(41+33)^4 = 41^4 + 132 \times 41^3 + 6534 \times 41^2 + 143748 \times 41 + 1185921 \rightarrow g(x) = 41^4 + 132 \times 41^3 + 6534 \times 41^2 + 143748 \times 41 - 4387 \times 6565 = 0$

From this we can constructed a two-sided quadratic which we will use a lot in this paper:

$x^2–148x + 4387 = x^2 + 66x - 4387$

This two sided setup has been the premise for my research.

b. The discriminant

Of-course we cannot blindly perform binomial expansion on random numbers hoping to find a difference of squares. We will need to construct a way to sieve this.

Take for example the following binomial expansion $BE(x–74)^2 = x^2–148x + 5476$ and on this quadratic polynomial , we substitute the constant with N (for example $N = 4387$):

$g(x) = x^2–148x + 4387$

If we now calculate the discriminant of $g(x)$, $DISC(g(x)) = 148^2–4 \times 4387 = 66^2$, we see that the result is also square.
And we now have the square relation $148^2 \equiv 66^2 \pmod{4387}$, where $GCD(148–66, 4387) = 41$.

An observation:

From this we can make the following generalization that we can derive the factorization of a semi-prime N, if we find a quadratic polynomial with a constant set to N, or a multiple there-of, and whose discriminant yields a square. And from this it is also true that the discriminant would yield a quadratic residue modulo any prime if the discriminant is square in Z. Hence we can use this property to calculate residues in Z/ℓ where valid solutions in Z/ℓ are a quadratic residue and discard residues for quadratics where this is not the case. Now it is also true, that if we find a polynomial whose discriminant is square in Z then it must have a multiple of the factor of N as root for polynomials g(x) at degree 2. That relation between polynomial and discriminant is still something I am researching. One way this is definitely useful is the fact that if the discriminant is square in Z, then the quadratic producing the discriminant must be reducible in Z. Furthermore, if a quadratic is reducible in Z/ℓ for prime ℓ, then this also tells us the discriminant is a quadratic residue in Z/ℓ. This lets us inspect wether or not a residue is square in Z/ℓ even when ℓ does not divide the discriminant.

c. An extended example

Let $N = 4387$
Let binomial $b = x–534$.

Hence $BE(x–534)^2 = x^2–1068x + 534^2$

We now need to substitute the constant in the resulting polynomial with a multiple of N.
For example let N multiplier $k = 1$:

$k = 1 \to g(x) = x^2–1068x + 4387$

$DISC(g(x))$ is not a square in Z hence we know $k = 1$ cannot be a valid solution.
However if $k = 65$:

$k = 65 \to g(x) = x^2–1068x + 4387 \times 65$ and $DISC(g(x)) = 2^2$

The discriminant is defined as $DISC(g(x)) = (2t)^2$, where t is the unknown binomial term, we can now substitute this into binomial b.
$b(1) = 1–534 = -533$ and $g(533) = 0$. Since g(x) evaluates to 0 at 533 we know we have a correct solution and we can take the gcd using our binomial terms:

$GCD(1 + 534, 4387) = 107$
$GCD(534–1, 4387) = 41$

In the next chapter we will see how to find these solutions in Z$/\ell$

Chapter III – Improvements

a. Calculating polynomial residues in Z$/\ell$

Let us restrict ourselves to binomial expansions to the second degree.
The way we calculate polynomial residues is that we must consider all possible coefficients whose discriminant evaluates to a quadratic residue or where ℓ divides the discriminant.
Here we calculate all possible residues for the quadratic polynomial $ax^2 + bx + Nk$ where $N = 4387$ (you can also calculate them for $ax^2 + bx–Nk$ instead, it just changes the side we are calculating in the expression $x^2 = y^2 \pmod N$). We will ignore the cases where the leading coefficient is 0, as this would downgrade the degree of our polynomial. And in addition we will also ignore the case where k = 0 for the sake of brevity.

Also note that we can figure out the coefficients for the other side, say we have $f(x) = g(x)$, where x is a shared root and $f(x) = ax^2 + b_0x + Nk$ and $g(x) = ax^2 + b_1x–Nk$ thus we get $ax^2 + b_0x + Nk = ax^2 + b_1x–Nk$, by taking the derivative of either $f(x)$ or $g(x)$, where $f(x)' = -b_1$ and $g(x)' = -b_0$ we can calculate the linear coefficient for the other side, which as we have seen has a direct relation to the binomial value.
You could use this to construct a residue map for both sides rather then one. You cannot simply choose a random b_0, b_1 pairing, they must be connected by derivative.

For example if we have $f(x) = 41^2 - 148 \times 41 + 4387$ then taking the derivative yields the linear coefficient for the other side $g(x)$, allowing us to construct the right side quadratic:

$f(x)' = 2 \times 41 - 148 = -66$ and thus $b_1 = -(-66)$ and $g(x) = 41^2 + 66 \times 41 - 4387$
note: Rather then negating the derivative, as in $f(x)' = -b_1$, my original research represented the roots as negative values, representing distance rather then residues for potential factors, which basically has the same result and creates the same quadratics. But worth a mention.

Below are the possible residues for $f(x)$ in $Z/3$ and $Z/5$:

Mod 3

$k = 1, a = 1$ and $b = -1 \rightarrow x = 2, k = 1, a = 1$ and $b = -2 \rightarrow x = 1, k = 1, a = 2$ and $b = 0 \rightarrow x = 1, 2$
$k = 2, a = 1$ and$b = 0 \rightarrow x = 2, 1, k = 2, a = 2$ and $b = -1 \rightarrow x = 1, k = 2, a = 2$ and $b = -2 \rightarrow x = 2$

Mod 5

$k = 1, a = 1$ and $b = -2 \rightarrow x = 4, 3, k = 1, a = 1$ and $b = -3 \rightarrow x = 2, 1, k = 1, a = 2$ and $b = 0 \rightarrow x = 3, 2,$
$k = 1, a = 2$ and $b = -1 \rightarrow x = 4, k = 1, a = 2$ and $b = -4 \rightarrow x = 1, k = 1, a = 3$ and $b = 0 \rightarrow x = 1, 4,$
$k = 1, a = 3$ and $b = -2 \rightarrow x = 2, k = 1, a = 3$ and $b = -3 \rightarrow x = 3, k = 1, a = 4$ and $b = -1 \rightarrow x = 3, 1,$
$k = 1, a = 4$ and $b = -4 \rightarrow x = 4, 2$
$k = 2, a = 1$ and $b = 0 \rightarrow x = 4, 1, k = 2, a = 1$ and $b = -1 \rightarrow x = 3, k = 2, a = 1$ and $b = -4 \rightarrow x = 2,$
$k = 2, a = 2$ and $b = -1 \rightarrow x = 2, 1, k = 2, a = 2$ and $b = -4 \rightarrow x = 3, 4, k = 2, a = 3$ and $b = -2 \rightarrow x = 3, 1,$
$k = 2, a = 3$ and $b = -3 \rightarrow x = 4, 2, k = 2, a = 4$ and $b = 0 \rightarrow x = 2, 3, k = 2, a = 4$ and $b = -2 \rightarrow x = 4,$
$k = 2, a = 4$ and $b = -3 \rightarrow x = 1$
$k = 3, a = 1$ and $b = 0 \rightarrow x = 3, 2, k = 3, a = 1$ and $b = -2 \rightarrow x = 1, k = 3, a = 1$ and $b = -3 \rightarrow x = 4,$
$k = 3, a = 2$ and $b = -2 \rightarrow x = 2, 4, k = 3, a = 2$ and $b = -3 \rightarrow x = 1, 3, k = 3, a = 3$ and $b = -1 \rightarrow x = 3, 4,$
$k = 3, a = 3$ and $b = -4 \rightarrow x = 2, 1, k = 3, a = 4$ and $b = 0 \rightarrow x = 4, 1, k = 3, a = 4$ and $b = -1 \rightarrow x = 2,$
$k = 3, a = 4$ and $b = -4 \rightarrow x = 3$
$k = 4, a = 1$ and $b = -1 \rightarrow x = 2, 4, k = 4, a = 1$ and $b = -4 \rightarrow x = 1, 3, k = 4, a = 2$ and $b = 0 \rightarrow x = 4, 1,$
$k = 4, a = 2$ and $b = -2 \rightarrow x = 3, k = 4, a = 2$ and $b = -3 \rightarrow x = 2, k = 4, a = 3$ and $b = 0 \rightarrow x = 2, 3,$
$k = 4, a = 3$ and $b = -1 \rightarrow x = 1, k = 4, a = 3$ and $b = -4 \rightarrow x = 4, k = 4, a = 4$ and $b = -2 \rightarrow x = 1, 2,$
$k = 4, a = 4$ and $b = -3 \rightarrow x = 3, 4$

The problem is, that we can Chinese remainder these together to modulo 15, but then the solution set of possible residues grows quickly (the product of the size of both sets of solutions). So we need to come up with a smart way to generate solutions with this setup.

b. Singular quadratic roots vs non-singular quadratic roots

In the above residue mapping, we will observe that sometimes a set of coefficients will have a single root solution, and sometimes it will have two root solutions.
For example, looking at Mod 5 we see the following two coefficient, root pairings:

$k = 1, a = 4$ and $b = -1 \to x = 3, 1$ Non-singular roots

$k = 1, a = 3$ and $b = -2 \to x = 2$ Singular root

Singular roots indicate that the corresponding binomial term has prime ℓ (5 here) as divisor and that the discriminant is also divided by prime ℓ.

We have calculated the above residues using polynomials of the shape $ax^2 + bx + Nk$.

If we calculate the derivative in Z/ℓ we get the residue for linear coefficient b in corresponding to a quadratic with the signs flipped $ax^2 + bx – Nk$ (the other side of the expression $x^2 = y^2 \pmod N$ that we are trying to solve for).

Calculating the derivative for coefficients with a singular root in Z/ℓ gives us a derivative that is 0 in Z/ℓ. Since a singular root means $DISC(g(x)) = 0 \pmod \ell$ and since $DISC(g(x)) = (2t)^2$,we have that $t \equiv 0 \pmod \ell$. (strictly speaking about degree 2 polynomials here).

For example:

Using $k = 1, a = 3$ and $b = -2 \to x = 2$ we construct the polynomial $g(x) = 3 \times 2^2 – 2 \times 2 + 2$ in $Z/5$.

And we see that the derivative $g(x)' \equiv 2 \times 3 \times 2 – 2 \equiv 0 \pmod 5$ (or in other words 0 in $Z/5$).

This implies that the binomial term y, in binomial b = t – y equals to 0 in Z/5.

Non-singular roots always yield non-zero residues for the binomial terms in Z/ℓ .

C. p-adic lifting of polynomials in $\mathbf{Z}/\ell$

Let us say we have the following coefficient and root pairing from our residue mapping:

$k = 4, a = 3$ and $b = -1 \to x = 1$ in $Z/5$ gives us polynomial $g(x) = 3 \times 1^2 – 1 \times 1 + 4387 \times 4 = 0 \pmod 5$

This gives us all of the following possible solutions in $Z/5^2$ where also the derivative yields 0 in $Z/5^2$, for the sake of brevity we will focus on these cases only:

$k = 4, a = 3$ and $b = -1 \to x = 21$, $k = 4, a = 8$ and $b = -6 \to x = 16$, $k = 4, a = 13$ and $b = -11 \to x = 11$

$k = 4, a = 18$ and $b = -16 \to x = 6$, $k = 4, a = 23$ and $b = -21 \to x = 1$

$k = 9, a = 3$ and $b = -11 \to x = 6$, $k = 9, a = 8$ and $b = -16 \to x = 1$, $k = 9, a = 13$ and $b = -21 \to x = 21$

$k = 9, a = 18$ and $b = -1 \to x = 16$, $k = 9, a = 23$ and $b = -6 \to x = 11$

$k = 14, a = 3$ and $b = -21 \to x = 16$, $k = 14, a = 8$ and $b = -1 \to x = 11$, $k = 14, a = 13$ and $b = -6 \to x = 6$

$k = 14, a = 18$ and $b = -11 \to x = 1$, $k = 14, a = 23$ and $b = -16 \to x = 21$

$k = 19, a = 3$ and $b = -6 \to x = 1$, $k = 19, a = 8$ and $b = -11 \to x = 21$, $k = 19, a = 13$ and $b = -16 \to x = 16$

$k = 19, a = 18$ and $b = -21 \to x = 11$, $k = 19, a = 23$ and $b = -1 \to x = 6$

$k = 24, a = 3$ and $b = -16 \to x = 11$, $k = 24, a = 8$ and $b = -21 \to x = 6$, $k = 24, a = 13 and b = -1 \to x = 1$

$k = 24, a = 18$ and $b = -6 \to x = 21$, $k = 24, a = 23$ and $b = -11 \to x = 16$

Each of these solutions map to the same solution in $Z/5$. We see a total of 25 (or 125 if we also count those with non-zero derivatives $Z/5^2$) possible solutions in $Z/5^2$ generated from a single solution in $Z/5$. I refer to p-adic lifting, but usually it is used in the context of lifting roots of polynomials, but in the context that I use this term, it is also used to lift coefficient residues in Z/ℓ p-adically. So please keep that in mind. I tend to create these abstractions in my head and the names I give these abstract concepts may not be strictly correct in formal mathematical terms. But to me it would seem, that whether we are lifting root residues or coefficient residues, the underlying mechanism are very similar and connected.

D. Converting singular roots to non-singular roots and visa versa

Because we are searching for two squares such that $x^2 = y^2 \pmod N$, and since both x and y can also be represented as binomials which can be expanded to the second degree, we can substitute the expression $x^2 = y^2 \pmod N$ with the more elaborate: $ax^2 – b_0x + Nk = ax^2 + b_1x – Nk$.

This also means that we can convert singular roots to non-singular roots temporarily, simply by transferring a root to the other side of the equation in Z/ℓ. As long as the side we transfer to has a discriminant that is not divisible by ℓ. (there is a few other edge cases that will complicate things, for example when k divides by ℓ).
For example $1x^2 + 66x – 4387 = 0 \pmod{37}$ has a singular root, while the other side, $1x^2 – 0x + 4387 = 0 \pmod{37}$ has two roots in Z/ℓ.

$b_1 = 66 \rightarrow 1 \times 4^2 + 66 \times 4 – 4387 = 0 \pmod{37}$

$b_0 = 0 \rightarrow 1 \times 4^2 – 0 \times 4 + 4387 = 0 \pmod{37}$
$b_0 = 0 \rightarrow 1 \times 33^2 – 0 \times 33 + 4387 = 0 \pmod{37}$

A polynomial that produces the other singular root can also be found, in this case all we have to do is flip the sign on linear coefficient b_1, then the singular root becomes the other non-singular root for b_0 (we must also swap a and k, but both are 1 here):
$b_1 = –66 \rightarrow 1 \times 33^2 – 66 \times 33 – 4387 = 0 \pmod{37}$

One way this ends up being useful is that with this construction we never have to p-adically lift singular roots (except for a couple of edge cases like $Z/2^e$ or when the leading coefficient or k is divisble by ℓ) , as we can just change them to non-singular, lift them and use them as lifted root for the singular side.

Chapter IV - PSieve, a novel algorithm

Finishing the code first.. then I'll write this chapter. The idea is the calculate the factors of a non-square B-smooth if we have a discriminant of the shape $ax^2 + 4Nk$ that is square but where $(ax)^2 + 4Nka$ is not square.. then it is still possible to calculate a root that contains a factor of N using quadratics mod p that are linked to this discriminant.

c. Benchmarks

to do

Closing thoughts and future work

to do