Prime Factorization and b Division Attack

Henry Samuelson
hes227@cornell.edu

July 2019

1 Introduction

Let: $q, p \in$ prime. Let: $N = qp$. Fermat's Factorization states:

$$N = (a+b)(a-b) \tag{1}$$

Unless $\sqrt{N} \in \mathbb{Z}$, then $q > \left\lceil \sqrt{N} \right\rceil$, and $p < \left\lceil \sqrt{N} \right\rceil$. Hence we define:

$$\begin{aligned} a &= \left\lceil \sqrt{N} \right\rceil \\ N &= (\left\lceil \sqrt{N} \right\rceil + b)(\left\lceil \sqrt{N} \right\rceil - b) \end{aligned} \tag{2}$$

This works if the difference of the perfect square above N, $\left\lceil \sqrt{N} \right\rceil^2$, and N is also square.

$$\sqrt{\left\lceil \sqrt{N} \right\rceil^2 - N} \in \mathbb{Z} \tag{3}$$

To account for situations where the difference isn't square we can add an k to make this always true.

$$\sqrt{(\left\lceil \sqrt{N} \right\rceil + k)^2 - N} \in \mathbb{Z} \tag{4}$$

The k insures that the square root will be in $\mathbb{Z}$. Hence we can adapt the earlier equation too:

$$N = (\left\lceil \sqrt{N} \right\rceil + k + b)(\left\lceil \sqrt{N} \right\rceil + k - b) \tag{5}$$

For all cases where the difference between $\sqrt{\left\lceil \sqrt{N} \right\rceil^2 - N} \in \mathbb{Z}$ we assume $k = 0$. For non-zero k's, the complexity is NP hard, whereas when $k = 0$ the equation can be solved with basic algebra.

2 Determining b

We first define some rules for k and b. It is clear that $b > 0$ as $b = 0$ would mean $q = p$. We make the assumption that $k < b$. Then we can determine a relation between q, p, b.

$$\frac{q-p}{2} = b \tag{6}$$

This equation can be shown to be objectively true if the purpose of b is thought of correctly. If b is the distance from some middle point $(\left\lceil \sqrt{N} \right\rceil + k)^2$ between q and p then b must be half of $q - p$, allowing b to be added and subtracted in either direction, to find q and p.

This next definition of b is less obvious but crucial to defining a range for b.

$$b = \sqrt{(\left\lceil \sqrt{N} \right\rceil + k)^2 - N} \tag{7}$$

It turns out that equation (4), the one we want to solve for an integer to determine the correct k is actually b. Now that we have to equations for b we can eliminate b, and derive a direct relationship between k, q, p.

$$q - p = 2 * \sqrt{(\left\lceil \sqrt{N} \right\rceil + k)^2 - N} \tag{8}$$

This equation tells allot about the relation between q, p and k, as we now have a solid equation for determining spacing which is very helpful in deriving the bounds of b, k, q and p.

3 Determining Variable Bounds

These variable bounds are only true if we assume $k \neq 0$, as we can assume if $k = 0$, then $q - p$ must $= 2$, and it would be very algebraically simple. We can first work to determine bounds for k. As stated earlier $k < b$, this can function as our top bound, k_{max}. The top bound of $b_{max} = \left\lceil \sqrt{N} \right\rceil$ There is a very import relationship between the growth rate of b and k. b grows at a faster rate than k, which is given by eq (7). If we assume b_{max}, we can determine k_{min}.We know from the definition of p, that $p = (\left\lceil \sqrt{N} \right\rceil + k - b)$. Plugging in b_{max} yields $k = 3$.

$$\begin{aligned} &p = (\left\lceil \sqrt{N} \right\rceil + k_{min} - b_{max}) \geq 3 \\ &p = (\left\lceil \sqrt{N} \right\rceil + k_{min} - \left\lceil \sqrt{N} \right\rceil) \geq 3 \\ &k_{min} \geq 3 \end{aligned} \tag{9}$$

If $b_{max} = \left\lceil \sqrt{N} \right\rceil$ and $k < b$, we can use the relationship between k and b to calculate k_{max}. The larger the b the larger the k. According to eq (7) we can solve using b_{max} to yield k_{max}.

$$\begin{aligned}
b_{max} &= \left\lceil \sqrt{(\left\lceil \sqrt{N} \right\rceil + k_{max})^2 - N} \right\rceil = \left\lceil \sqrt{N} \right\rceil \\
k_{max} &= \left\lceil \sqrt{b_{max}^2 + N} \right\rceil - \left\lceil \sqrt{N} \right\rceil \\
k_{max} &= \left\lceil \sqrt{\left\lceil \sqrt{N} \right\rceil^2 + N} \right\rceil - \left\lceil \sqrt{N} \right\rceil
\end{aligned} \tag{10}$$

Now we have k_{max} directly in terms of N. This is what we need to determine a final bound. We can use $k_{min} \geq 3$ to help us solve the bottom bound for b, b_{min}.

$$\begin{aligned}
b_{min} &= \left\lceil \sqrt{(\left\lceil \sqrt{N} \right\rceil + k_{min})^2 - N} \right\rceil \\
b_{min} &= \left\lceil \sqrt{(\left\lceil \sqrt{N} \right\rceil + 3)^2 - N} \right\rceil
\end{aligned} \tag{11}$$

Now we have the top and bottom bounds for both b and k we can can rewrite b and k as,

$$\begin{gathered}
3 \leq k \leq \left\lceil \sqrt{\left\lceil \sqrt{N} \right\rceil^2 + N} \right\rceil - \left\lceil \sqrt{N} \right\rceil \\
\left\lceil \sqrt{(\left\lceil \sqrt{N} \right\rceil + 3)^2 - N} \right\rceil \leq b \leq \left\lceil \sqrt{N} \right\rceil
\end{gathered} \tag{12}$$

Solid b and k bounds allow us to now determine bounds for q and p. We will acknowledge the obvious but important relationships,

$$\frac{N}{q_{min}} = p_{max}, \;\; \frac{N}{p_{min}} = q_{max} \tag{13}$$

This is helpful, because calculating q_{max} and q_{min} is easy, whereas one cannot calculate p_{min} and p_{max} using the standard definitions of q and p, due to the definitions of p including a $-$ sign.

$$\begin{aligned}
&q = (\left\lceil \sqrt{N} \right\rceil + k + b) \\
&q_{max} = (\left\lceil \sqrt{N} \right\rceil + k_{min} + b_{max}) = (2\left\lceil \sqrt{N} \right\rceil + 3) \\
&q_{min} = (\left\lceil \sqrt{N} \right\rceil + k_{min} + b_{min}) = (\left\lceil \sqrt{N} \right\rceil + 3 + \left\lceil \sqrt{(\left\lceil \sqrt{N} \right\rceil + 3)^2 - N} \right\rceil)
\end{aligned} \tag{14}$$

The bounds for q are complete along with the bounds of p using eq (13),

$$\begin{aligned} \left\lceil\sqrt{N}\right\rceil + 3 + \left\lceil\sqrt{(\left\lceil\sqrt{N}\right\rceil + 3)^2 - N}\right\rceil \leq q \leq 2\left\lceil\sqrt{N}\right\rceil + 3 \\ \frac{N}{2\left\lceil\sqrt{N}\right\rceil + 3} \leq p \leq \frac{N}{\left\lceil\sqrt{N}\right\rceil + 3 + \left\lceil\sqrt{(\left\lceil\sqrt{N}\right\rceil + 3)^2 - N}\right\rceil} \end{aligned} \tag{15}$$

For example the for $N = 2231 = qp = (97)(23)$, $k = 12, b = 37$, the estimated bounds are as follows:

$$\begin{aligned} 3 \leq k \leq 20 \\ 20 \leq b \leq 48 \\ 71 \leq q \leq 99 \\ 23 \leq p \leq 32 \end{aligned} \tag{16}$$

These bounds are quite good.

4 Solving For k

We can rewrite the b relation equation– eq(8)– to be in terms of k to determine how many k's we have to brute force directly in order to deterine the factors of N, p and q.

$$k_{actual} = \frac{1}{2}(q + p - 2\left\lceil\sqrt{N}\right\rceil) \tag{17}$$

This means that the number of k's we have to guess is directly dependent upon the distance between p and q, and the actual value of N. Since we can calculate the bottom bound of k we can subtract it from the number of steps it takes to solve to calculate a new complexity.

$$k_{guesses} = \frac{1}{2}(q + p - 2\left\lceil\sqrt{N}\right\rceil) - 3 \tag{18}$$

Given the equation it would appear to make N as resistant as possible to brute forcing k's, the best thing to do would be to maximize the first half of the equation by maximizing both q and p. And then to minimize the second half of the equation by making N or $q * p$ smaller. This means that there is an optimal ratio that exists that maximizes $q + p$ while minimizing $q * p$. This may seem counter intuitive at first, as it is commonly thought that a larger N is better, but it is really only better when $q - p$ and $q + p$ are larger.

5 b division attack

If $b \mod k = 0$ or $k = \frac{b}{D}$ where, $D \in \mathbb{Z}$ and is unknown; then the factorization of $N = qp$ is insecure, and can be exploited. Equation (5) can be written to have k in terms of b.

$$
\begin{aligned}
N &= (\left\lceil\sqrt{N}\right\rceil + k + b)(\left\lceil\sqrt{N}\right\rceil + k - b) \\
N &= (\left\lceil\sqrt{N}\right\rceil + \frac{b}{D}) + b)(\left\lceil\sqrt{N}\right\rceil + \frac{b}{D} - b)
\end{aligned}
\tag{19}
$$

The equation can be solved for b where $b \in \mathbb{Z}$. The equation for b in terms of D is:

$$
b = \frac{\sqrt{D^4\left\lceil\sqrt{N}\right\rceil^2 - D^4N + D^2N} + D\left\lceil\sqrt{N}\right\rceil}{D^2 - 1} \tag{20}
$$

This equation makes a lot of sense as $b > k$ which means $D > 1$. This holds true as seen in the denominator of (9). Solving for a $b \in \mathbb{Z}$, yields the correct solution for both b and D. We can simplify the operations to guess the correct D. We can break up the definition of b into three distinct integer parts, the numerator in the square root, the numerator, and the denominator. Assuming they are all integers we can determine a simplification for determining b.

$$
\begin{aligned}
&A, B, C \in \mathbb{Z} \\
&\frac{\sqrt{A} + B}{C} \\
&\sqrt{A} \notin \mathbb{Z}, \text{then,} \\
&\sqrt{A} + B \notin \mathbb{Z} \\
&\frac{(\sqrt{A} \notin \mathbb{Z}) + B}{C} \notin \mathbb{Z}
\end{aligned}
\tag{21}
$$

(10) shows that $b \in \mathbb{Z}$ is entirely dependent upon, the contents of the square root being square. So we can now instead solve for an integer solution for:

$$
\sqrt{D^4\left\lceil\sqrt{N}\right\rceil^2 - D^4N + D^2N} \in \mathbb{Z} \tag{22}
$$

After finding an integer solution for (11), we can plug the values of b and D back into (8).

6 Example

$$
\begin{aligned}
&N = qp = 101 * 23 = 2323 \\
&\text{Assume, } D = 2 \\
&\sqrt{D^4 \left\lceil \sqrt{N} \right\rceil^2 - D^4 N + D^2 N} = \\
&\sqrt{2^4 \left\lceil \sqrt{2323} \right\rceil^2 - 2^4 * 2323 + 2^2 * 2323} = \sqrt{10540} \\
&\sqrt{10540} \notin \mathbb{Z} \text{ So, } D = D + 1 \\
&\sqrt{3^4 \left\lceil \sqrt{2323} \right\rceil^2 - 3^4 * 2323 + 3^2 * 2323} = \sqrt{27225} \\
&\sqrt{27225} = 165 \in \mathbb{Z}
\end{aligned}
\tag{23}
$$

Though we know the contents of the square root are square, there is still a chance that given our estimate for D that $b \notin \mathbb{Z}$. So we must now calculate all of b and confirm it is an integer using (9).

$$
\begin{aligned}
b &= \frac{\sqrt{27225} + D \left\lceil \sqrt{N} \right\rceil}{D^2 - 1} \\
b &= \frac{\sqrt{27225} + 3 * 49}{3^2 - 1} \\
b &= 39 \in \mathbb{Z}
\end{aligned}
$$

We now plug b and D into (8).

$$
\begin{aligned}
N &= (\left\lceil \sqrt{2323} \right\rceil + \frac{39}{3}) + 39)(\left\lceil \sqrt{2323} \right\rceil + \frac{39}{3} - 39) \\
N &= (101)(23)
\end{aligned}
\tag{24}
$$

7 Conclusion

Though there are good rules put in place to insure that $\sqrt{(\left\lceil \sqrt{N} \right\rceil + k)^2 - N} \in \mathbb{Z}$, there isn't proper rules in place to insure that that $b \mod k \neq 0$, which allows for the b division attack.