Three Triangles Integer Factorization Algorithm

> "Discovery consists of seeing what everybody has seen and thinking what nobody has thought."
>
> — Albert Szent-Györgyi

Abstract:

Factor the composite number $C=(a+1)(a+b)$ by finding the solution to $C=T(a)+T(a+b)-T(b-1)$ where $T(n)$ is the nth triangular number.

Definitions:

- T(n) := n(n+1)/2
- S(a, b) := T(a)+T(a+b)-T(b-1)

Theorem:

For every composite number $C=(a+1)(a+b)$ there exist three triangular numbers such that $C=T(a)+T(a+b)-T(b-1)$.

Proof:

1. $(a+1)(a+b)=T(a)+T(a+b)-T(b-1)$
2. $a^2+ab+a+b=a(a+1)/2+(a+b)(a+b+1)/2-(b-1)b/2$
3. $2a^2+2ab+2a+2b=a(a+1)+(a+b)(a+b+1)-(b-1)b$
4. $2a^2+2ab+2a+2b=a^2+a+a(a+b+1)+b(a+b+1)-b^2+b$
5. $2a^2+2ab+2a+2b=a^2+a+a^2+ab+a+ba+b^2+b-b^2+b$
6. $2a^2+2ab+2a+2b=2a^2+2ab+2a+2b$
7. $0=0$

Theorem:

For natural numbers a, b it holds that $S(a, b) > S(a-1, b+1)$.

Proof:

1. $S(a, b) > S(a-1, b+1)$
2. $(a+1)(a+b) > (a+1-1)(a-1+b+1)$
3. $a(a+b)+a+b > a(a+b)$
4. $a+b > 0$

Theorem:

For natural number a, b it holds that $S(a, b) < S(a, b+max(1, ceil((C-S(a, b))/(a+1))))$.

Proof:

1. $S(a, b) < S(a, b+max(1, ceil((C-S(a, b))/(a+1))))$
2. $(a+1)(a+b) < (a+1)(a+b+max(1, ceil((C-S(a, b))/(a+1))))$
3. $a+b < a+b+max(1, ceil((C-S(a, b))/(a+1)))$
4. $0 < max(1, ceil((C - S(a, b))/(a+1)))$
5. $0 < 1$

Algorithm:

input: natural number C
output: found factors, or 1 and C if C is a prime number

1. let a = floor(sqrt(C)) - 1
2. let b = 1
3. if $S(a, b) > C$ then $a=a-1$, $b=b+1$
4. else if $S(a, b) < C$ then $b=b+max(1, ceil((C-S(a, b))/(a+1)))$
5. else if $S(a, b) = C$ then exit: found factors $(a+1)$ and $(a+b)$
6. if $a = 0$ then exit: C is a prime number
7. go to step 3

Examples

51

1. S(6, 1) = 49 => b = b + max(1, ceil(2/7))
2. S(6, 2) = 56 => a = a - 1, b = b + 1
3. S(5, 3) = 48 => b = b + max(1, ceil(3/6))
4. S(5, 4) = 54 => a = a - 1, b = b + 1
5. S(4, 5) = 45 => b = b + max(1, ceil(6/5))
6. S(4, 7) = 55 => a = a - 1, b = b + 1
7. S(3, 8) = 44 => b = b + max(1, ceil(7/4))
8. S(3, 10) = 52 => a = a - 1, b = b + 1
9. S(2, 11) = 39 => b = b + max(1, ceil(12/3))
10. S(2, 15) = 51 => 51 = 3 * 17

23

1. S(3, 1) = 16 => b = b + max(1, ceil(7/4))
2. S(3, 3) = 24 => a = a - 1, b = b + 1
3. S(2, 4) = 18 => b = b + max(1, ceil(5/3))
4. S(2, 6) = 24 => a = a - 1, b = b + 1
5. S(1, 7) = 16 => b = b + max(1, ceil(7/2))
6. S(1, 11) = 24 => a = a - 1, b = b + 1
7. a = 0 => 23 = 1 * 23

221

1. S(13, 1) = 196 => b = b + max(1, ceil(25/14))
2. S(13, 3) = 224 => a = a - 1, b = b + 1
3. S(12, 4) = 208 => b = b + max(1, ceil(13/13))
4. S(12, 5) = 221 => 221 = 13 * 17

36

1. S(5, 1) = 36 => 36 = 6 * 6

Conclusion

To my knowledge this is not based on any existing solutions. I do not claim it to be efficient or useful, I'm only concerned with its correctness and completeness. Some optimizations are omitted for simplicity. Hope it inspires some ideas.