

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:

- $a, b :=$ natural numbers
- $T(n) := n(n+1)/2$
- $S(a, b) := T(a)+T(a+b)-T(b-1)$
- $\text{make_even}(n) :=$ if n is odd return $n-1$ else return n

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 every natural number $a \geq 2$ and $b > 1$ it holds that $S(a, b) > S(a-2, b+2)$.

Proof:

1. $S(a, b) > S(a-2, b+2)$
2. $(a+1)(a+b) > (a+1-2)(a-2+b+2)$
3. $a^2+a+b > (a-1)(a+b)$
4. $a^2+a+b > a^2-(a+b)$
5. $a+b > -(a+b)$
6. $1 > -1(a+b) > 0$ since $a \geq 2$ and $b > 1$

Theorem:

For every natural number $a, b > 0$ it holds that $S(a, b) < S(a, b+\max(1, \text{ceil}((C-S(a, b))/(a+1))))$.

Proof:

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

Algorithm:

input: $C \Rightarrow$ odd integer greater than 4

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

1. let $a = \text{make_even}(\text{floor}(\text{sqrt}(C)) - 1)$
2. let $b = 1$
3. if $S(a, b) > C$ then $a=a-2, b=b+2$

4. if $S(a, b) < C$ then $b = b + \max(1, \text{ceil}((C - S(a, b)) / (a + 1)))$
5. 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. goto step 3.

Examples

Factor 51

1. $S(6, 1) = 49 \Rightarrow b = b + \max(1, \text{ceil}(2 / 7))$
2. $S(6, 2) = 56 \Rightarrow a = a - 2, b = b + 2$
3. $S(4, 4) = 40 \Rightarrow b = b + \max(1, \text{ceil}(11 / 5))$
4. $S(4, 7) = 55 \Rightarrow a = a - 2, b = b + 2$
5. $S(2, 9) = 33 \Rightarrow b = b + \max(1, \text{ceil}(18 / 3))$
6. $S(2, 15) = 51 \Rightarrow 51 = 3 * 17$

Factor 23

1. $S(2, 1) = 9 \Rightarrow b = b + \max(1, \text{ceil}(14 / 3))$
2. $S(2, 6) = 24 \Rightarrow a = a - 2, b = b + 2$
3. $a = 0 \Rightarrow 23 = 1 * 23$

factor 221

1. $S(12, 1) = 169 \Rightarrow b = b + \max(1, \text{ceil}(52 / 13))$
2. $S(12, 5) = 221 \Rightarrow 221 = 13 * 17$

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. One potential benefit I see is the reduced magnitude of dividends used in divisions. Hope it inspires some ideas.