The Factoring by Base Algorithm version 9.

Given that we want to factorize N, we assume that N is made up of two factors, p and q. If we let p and q be two linear polynomials, the resultant of their product, N would be a quadratic polynomial.

However, to solve it as integer solutions we present the following method.

Notice we present x and y as separate equations however they are the result when . We do this so that we can solve x and y separately so that we can find rational solutions.

Let D be the discriminant of , it follows that:

Due to the discriminant, x and y are now linked together. Now to link with z we know that:

where r is a constant.

Also on expanding our pool space for the discriminant we let:

and

The discriminants must be real and preferably integers since irrational solutions are difficult to work with. For the first case we used the derivative function, hence for the next case we will use the integral function instead to improve our algorithm.

After some research, we discover that if p and q are some roots to a quadratic function, G(x), then

and if the sum of roots is then

Applying this for our previous functions we have:

which simplifies to

In the case of we let

Here we use the sum of roots instead since we cannot predict the roots.

where then we have

which simplifies to:

Similarly if we do the same for F(x) and F(y) we get:

We notice that

To establish a link between x,y and z with e we let the following:

We know that: which expands to:

Which gives us: and

Suppose we integrate with the new derived function, we obtain:

After this, we solve the solution by initializing two variables. After some analysis, these two combinations worked well better than others.

First is inserting value for x and B. After finding the parametric solution, you use the one with C to find the possible solutions of C and parametric value.

Second is inserting the value of z and d. After finding the parametric solution, you use the one with u to find the possible solutions of u and parametric value.

Examples given below were solved using sympy (symbolic python) library in python programming language.

N=667 (First Case using x and B)

>>> solve([A\*x\*\*2+B\*x+C-N, A\*y\*\*2+B\*y+C-N, A\*z\*\*2+B\*z+C, B\*\*2-4\*A\*C-d\*\*2, B\*\*3-6\*A\*B\*C-6\*e\*A\*\*2, B\*\*2-4\*A\*(C-N)-D\*\*2, B\*\*3-6\*A\*B\*(C-N)-6\*E\*A\*\*2, 2\*A\*x+B-D, 2\*A\*y+B+D, 2\*A\*z+B-d,2\*A\*x\*\*3+3\*B\*x\*\*2+6\*(C-N)\*x+2\*A\*y\*\*3+3\*B\*y\*\*2+6\*(C-N)\*y-6\*E,D\*\*2-d\*\*2-N\*r, E-e-N\*u, **x-10, B-24**])

[{A: -24/(y + 10), B: 24, C: (427\*y + 6670)/(y + 10), D: 24\*(y - 10)/(y + 10), E: 4\*y\*\*2 - 160\*y + 400, d: -4\*sqrt(36\*y\*\*2 + 3282\*y + 43620)/(y + 10), e: 4\*y\*\*2 + 507\*y + 7070, r: -96/(y + 10), u: -y - 10, x: 10, z: y/2 + sqrt(36\*y\*\*2 + 3282\*y + 43620)/12 + 5}, {A: -24/(y + 10), B: 24, C: (427\*y + 6670)/(y + 10), D: 24\*(y - 10)/(y + 10), E: 4\*y\*\*2 - 160\*y + 400, d: 4\*sqrt(36\*y\*\*2 + 3282\*y + 43620)/(y + 10), e: 4\*y\*\*2 + 507\*y + 7070, r: -96/(y + 10), u: -y - 10, x: 10, z: y/2 - sqrt(36\*y\*\*2 + 3282\*y + 43620)/12 + 5}]

>>> diophantine(C\*(y+10)-(427\*y+6670))

{(-773, -12), (547, 10), (397, -90), (439, 190), (435, 290), (459, 65), (307, -30), (1627, -8), (452, 86), (457, 70), (467, 50), (395, -85), (727, -2), (1027, -6), (347, -40), (433, 390), (379, -60), (907, -5), (417, -250), (327, -34), (425, -1210), (412, -170), (426, -2410), (627, 2), (432, 470), (2827, -9), (411, -160), (451, 90), (827, -4), (277, -26), (377, -58), (187, -20), (502, 22), (587, 5), (-373, -13), (477, 38), (367, -50), (431, 590), (407, -130), (421, -410), (423, -610), (430, 790), (527, 14), (1227, -7), (424, -810), (352, -42), (577, 6), (403, -110), (27, -16), (443, 140), (447, 110), (422, -490), (487, 30), (523, 15), (267, -25), (437, 230), (429, 1190), (667, 0), (-53, -15), (387, -70), (507, 20), (402, -106), (-1973, -11), (442, 150), (331, -35), (227, -22), (475, 40), (419, -310), (415, -210), (127, -18), (-173, -14), (428, 2390)}

N=667 (Second Case using z and d)

>>> solve([A\*x\*\*2+B\*x+C-N, A\*y\*\*2+B\*y+C-N, A\*z\*\*2+B\*z+C, B\*\*2-4\*A\*C-d\*\*2, B\*\*3-6\*A\*B\*C-6\*e\*A\*\*2, B\*\*2-4\*A\*(C-N)-D\*\*2, B\*\*3-6\*A\*B\*(C-N)-6\*E\*A\*\*2, 2\*A\*x+B-D, 2\*A\*y+B+D, 2\*A\*z+B-d,2\*A\*x\*\*3+3\*B\*x\*\*2+6\*(C-N)\*x+2\*A\*y\*\*3+3\*B\*y\*\*2+6\*(C-N)\*y-6\*E,D\*\*2-d\*\*2-N\*r, E-e-N\*u, **2\*z+3, d-12**])

[{A: 4\*C/9 - 8, B: 4\*C/3 - 12, D: -4\*sqrt(667\*C - 11925)/3, E: (-C\*\*3 + 2028\*C\*\*2 - 54027\*C + 322704)/(C\*\*2 - 36\*C + 324), d: 12, e: (-C\*\*3 + 27\*C\*\*2 - 1458)/(C\*\*2 - 36\*C + 324), r: 16\*C/9 - 32, u: 3\*(C - 9)/(C - 18), x: 3\*(-C - sqrt(667\*C - 11925) + 9)/(2\*(C - 18)), y: 3\*(-C + sqrt(667\*C - 11925) + 9)/(2\*(C - 18)), z: -3/2}, {A: 4\*C/9 - 8, B: 4\*C/3 - 12, D: 4\*sqrt(667\*C - 11925)/3, E: (-C\*\*3 + 2028\*C\*\*2 - 54027\*C + 322704)/(C\*\*2 - 36\*C + 324), d: 12, e: (-C\*\*3 + 27\*C\*\*2 - 1458)/(C\*\*2 - 36\*C + 324), r: 16\*C/9 - 32, u: 3\*(C - 9)/(C - 18), x: 3\*(-C + sqrt(667\*C - 11925) + 9)/(2\*(C - 18)), y: 3\*(-C - sqrt(667\*C - 11925) + 9)/(2\*(C - 18)), z: -3/2}]

>>> diophantine(u\*(C-18)-3\*(C-9))

{(19, 30), (9, 0), (45, 4), (-9, 2), (15, -6), (21, 12), (27, 6), (17, -24)}

Notes: The first case is faster but the second case is more accurate.

Not all of the output will work, therefore we test them if they satisfy our given equations to get our preferred answers.

In the first Case the solution will be finding y such that it exists in all Diophantine solutions of A, C and D. Take a look at this:

>>> diophantine(D\*(y+10)-24\*(y-10))

{(32, -70), (25, -490), (21, 150), (27, -170), (16, 50), (120, -15), (-72, -5), (-16, 2), (22, 230), (23, 470), (-96, -6), (29, -106), (34, -58), (504, -11), (-6, 6), (4, 14), (-56, -4), (84, -18), (72, -20), (12, 30), (56, -25), (-216, -8), (19, 86), (184, -13), (0, 10), (9, 22), (8, 20), (20, 110), (30, -90), (264, -12), (-24, 0), (18, 70), (28, -130), (40, -40), (39, -42), (48, -30), (36, -50), (-36, -2), (26, -250), (54, -26), (104, -16), (64, -22), (-456, -9), (-8, 5), (-136, -7), (14, 38), (44, -34), (144, -14)}

>>> diophantine(A\*(y+10)-24)

{(-6, -14), (-1, -34), (-3, -18), (3, -2), (-8, -13), (2, 2), (24, -9), (-2, -22), (1, 14), (-4, -16), (4, -4), (6, -6), (8, -7), (12, -8), (-12, -12), (-24, -11)}

>>> diophantine(C\*(y+10)-(427\*y+6670))

{(-773, -12), (547, 10), (397, -90), (439, 190), (435, 290), (459, 65), (307, -30), (1627, -8), (452, 86), (457, 70), (467, 50), (395, -85), (727, -2), (1027, -6), (347, -40), (433, 390), (379, -60), (907, -5), (417, -250), (327, -34), (425, -1210), (412, -170), (426, -2410), (627, 2), (432, 470), (2827, -9), (411, -160), (451, 90), (827, -4), (277, -26), (377, -58), (187, -20), (502, 22), (587, 5), (-373, -13), (477, 38), (367, -50), (431, 590), (407, -130), (421, -410), (423, -610), (430, 790), (527, 14), (1227, -7), (424, -810), (352, -42), (577, 6), (403, -110), (27, -16), (443, 140), (447, 110), (422, -490), (487, 30), (523, 15), (267, -25), (437, 230), (429, 1190), (667, 0), (-53, -15), (387, -70), (507, 20), (402, -106), (-1973, -11), (442, 150), (331, -35), (227, -22), (475, 40), (419, -310), (415, -210), (127, -18), (-173, -14), (428, 2390)}

The values of y which existed in all the sets were 14, -16, -14, -34, -18, … the ones found in set A.

In as much as it is the fastest way, we cannot recommend it, because there is no guarantee that it will result in the z and d which will give us deterministic prime solutions.

Because of this, we use the other solution in which we know z and d, then we find p by using the identity of since we know, if true, will give us a prime solution.

When using the Second solution, we notice that it takes longer to process when we just insert the z and d initial values. But after some analysis, we noticed that the relationship of u and C is actually deterministic and it falls into this equation, regardless of the size of N.

where are the initial values.

Meaning if we find the Diophantine solutions, we then insert u and C into the general solution, which will make our processing faster. However, when testing for 3293 using z=1, d=9, there were no integer solutions for D, x and y, meaning that it’s not enough.

Another important identity is that of: which resulted in deterministic solutions for B, E, e and u which were 0, and r=4\*A being found also. Meaning the only important relationship is finding A and d, or A and x