Factorization via Difference of Squares (Alternate Method)

$kN = a^2 - b^2 = (a + b)(a - b)$,

- There is a reasonable chance that the factors of *N are separated by the* right-hand side of the equation, i.e., that *N has a nontrivial factor in common* with each of $a + b$ *and* $a - b$.

- *It is then a simple matter to recover the factors* by computing gcd $(N, a + b)$ *and* $\gcd(N, a - b)$.

Factorization via Difference of Squares (Alternate Method)

Example. Factor $N = 203299$. If we make a list of $N + b^2$ for values of *$b = 1, 2, 3, \ldots,$ say up to $b = 100$, we do not find any square values.*

So next try listing the values of $3N + b^2$ *and we find*

$3 \cdot 203299 + 1^2 = 609898$ *not a square,*

$3 \cdot 203299 + 22 = 609901$ *not a square,*

$3 \cdot 203299 + 3^2 = 609906$ *not a square,*

$3 \cdot 203299 + 4^2 = 609913$ *not a square,*

$3 \cdot 203299 + 52 = 609922$ *not a square,*

$3 \cdot 203299 + 6^2 = 609933$ *not a square,*

$3 \cdot 203299 + 7^2 = 609946$ *not a square,*

$3 \cdot 203299 + 8^2 = 609961 = 7812$ *Eureka! ** square **.*

Factorization via Difference of Squares (Alternate Method)

Thus
$3 \cdot 203299 = 7812 - 82 = (781 + 8)(781 - 8) = 789 \cdot 773$,
So compute gcd(203299, 789)=263 *and* gcd(203299, 773) = 773,

Find nontrivial factors of N. *The numbers 263 and 773 are prime*,

so the full factorization of N *is* $203299 = 263 \cdot 773$.