EXAMPLE

Stinson, Problem 5.32: Suppose that $n = 317940011$ and $b = 77537081$ in the *RSA Cryptosystem*. Using Wiener's Algorithm, attempt to factor n. If you succeed, determine the secret exponent a and $\phi(n)$.

Solution: Running Wiener's algorithm we get:

j	r_j	q_j	c_j	d_j	n'
0	77537081	0	1	0	-
1	317940011	0	0	1	-
2	77537081	4	1	4	310148323
3	7791687	9	9	37	318763555.111
4	7411898	1	10	41	317902032
5	379789	19	199	816	317940995.452
6	195907	1	209	857	
⋮	⋮	⋮	⋮	⋮	⋮

$j = 2$ no solution, since n' is odd ($\phi(n)$ is divisible by 4).

$j = 3$ no solution, since n' is not integer.

$j = 4$ looks promising. Substitute $n = 317940011$ and $n' = 317902032$ to equation $x^2 - (n - n' + 1)x + n = 0$ and get

$$x^2 - 37980x + 317940011 = 0,$$

from where we get solutions for p and q, which are $x = 18990 \pm 6533$. Then $a = d_4 = 41$, and $\phi(n) = n' = 317902032$.