Assume we know the RSA public key \((n, e)\), and suppose we discover \(d\). In practice, we can use this information to factor \(n\) by the following procedure:

1. Compute \((de - 1)/n\) and round off to the nearest integer. Call this \(k\).

2. Compute 
   \[
   \phi(n) = \frac{de - 1}{k}.
   \]

3. Solve the quadratic equation 
   \[
   X^2 - (n + 1 - \phi(n))X + n = 0.
   \]

   The solutions are \(p\) and \(q\).

**Example.** Let \(n = 670726081\) and \(e = 257\). We discover that \(d = 524523509\). Compute 

\[
\frac{de - 1}{n} = 200.98 \ldots .
\]

Therefore, \(k = 201\). Then 

\[
\phi(n) = \frac{de - 1}{201} = 670659412.
\]

The roots of the equation

\[
X^2 - (n + 1 - \phi(n))X + n = X^2 - 66670X + 670726081 = 0
\]

are \(12347.00 \ldots \) and \(54323.00 \ldots \), and we can check that \(n = 12347 \times 54323\).

Why does this work? We know that \(de \equiv 1 \mod (p-1)(q-1)\), so we write 
\(de = 1 + (p-1)(q-1)k\). Since \(d < (p-1)(q-1)\), we know that 

\[
(p-1)(q-1)k < de < (p-1)(q-1)e,
\]

so \(k < e\). We have 

\[
k = \frac{de - 1}{(p-1)(q-1)} > \frac{de - 1}{n} = \frac{(p-1)(q-1)k}{n} = \frac{(pq - p - q + 1)k}{n}
\]

\[
= k - \frac{(p + q - 1)k}{n}.
\]

Usually, both \(p\) and \(q\) are approximately \(\sqrt{n}\). In practice, \(e\) and therefore \(k\) are much smaller than \(n\). Therefore, \((p + q - 1)k/n\) rounds off to 0.

Once we have \(k\), we use \(de - 1 = \phi(n)k\) to solve for \(\phi(n)\). As we have already seen, once we know \(n\) and \(\phi(n)\), we can find \(p\) and \(q\) by solving the quadratic equation.

(thanks to Ben Anderson for pointing out this method)