```
Algorithm    ECDSA.RecoverPublicKey
Inputs: a message $m$, and a signature $\sigma = (r \in \mathbb{Z}_{q^*}, s \in \mathbb{Z}_{q^*}, v \in \mathbb{Z}_4)$
Outputs: $Q$, the public key.
$R_x \leftarrow r + q(v \mod 2)$
$R_y$ s.t. $R = (R_x, R_y) \in \mathbb{G}$.                (Use the curve equation)
Check $R_y \mod 2 \overset{?}{=} v \mod 2$ and ABORT if not
$d \leftarrow \mathsf{sha256}(m)$ and $m' \leftarrow (d \mod 2^{|q|})$, the $|q|$ leftmost bits of $d$
$Q = r^{-1}(s \cdot R - m' \cdot G)$
Check that $\mathsf{Verify}(Q, m, \sigma)$ is valid, ABORT if not
return $Q$
```

References