Digital Signature (ECDSA)

Purpose: To sign a given message $m$.

System parameters: $E/\mathbb{F}_p$, $P \in E(\mathbb{F}_p)$, $q = \text{ord}(P)$.  
Note: $p$ and $q$ are primes of similar size: $q \approx p$.

Key Generation: $A$ chooses $x_A$ with $1 < x_A < q$.  
$A$’s Public Key is $Q_A := x_A P$. ($x_A$ is secret.)

Protocol for $A$ to sign the message $m$:

1) Select a random integer $k$ with $1 < k < q$.
2) Compute $kP = (x_1, y_1)$ and $r = \text{rem}(x, q)$.  
   (If $r = 0$, return to step 1 and choose a new $k$.)
3) Compute $s = \text{rem}((H(m) + x_A r)/k, q)$, where $H(m)$ is the hash value of $m$. ($s = 0 \rightarrow$ step 1.)
4) The signature is the pair $(r, s)$.

Verification of the signature (by $B$):

1) Obtain an authenticated copy of $Q_A$.
2) Check that $1 < r, s < q$.
3) Compute $w = \text{rem}(1/s, q)$ and $H(m)$.
4) Compute $u_1 = \text{rem}(H(m)w, q)$, $u_2 = \text{rem}(rw, q)$.
5) Compute $u_1 P + u_2 Q_A = (x_0, y_0)$, $v = \text{rem}(x_0, q)$.
6) Accept the signature if and only if $v = r$.  