Let a, b the elliptic curve parameters of the EC $S_{a,b} = \{(x,y) : y^2 = x^3 + ax + b\}$ over the finite field $\mathbb{F}_p$ with prime order p satisfying $p \% 4 = 3$.
Let G be the generator point of an associated ECDSA signature scheme, which generates a group of order n.

Assume that (r, s) is the output of ecdsa_sign given the private key e, message m and private nonce k. Show that $(r, n-s)$ is also a valid signature for this key-message pair (i.e., the verification function likewise returns "true".)

Since (r, s) is a valid signature for message m given private key e and private nonce k, it holds that

$$(r, R_y) = R = kG = \frac{z}{s}G + \frac{r}{s}G = \frac{z+re}{s}G,$$ where $z = hash(m)$.

Therefore, $$(sk)G = (z+re)G$$

and $$sG = \frac{(z+re)}{k}G. \quad (*)$$

Since n is the group order of the group generated by G, it holds that

$nG = O$, where O is the additive identity on $S_{a,b}$ (i.e., "point at infinity")

$$\Rightarrow (N-s)G = NG - sG = O - sG = -sG \overset{(*)}{=} -\left(\frac{z+re}{k}\right)G$$

$$(N-s) + \frac{z+re}{k} = 0$$

$$\Longrightarrow \quad N-s \,\%\, N = \left(-\frac{z+re}{k}\right) \%\, N$$

multiply with $k \in F_p$,

$$\Longrightarrow \quad k(N-s)^{-1}(N-s) \,\%\, N = k(N-s)^{-1} \, \frac{-z+re}{k} \,\%\, N$$

and with $(N-s)^{-1} \in F_p$

$$\Longleftrightarrow \quad k \,\%\, N = -\frac{z+re}{N-s} \,\%\, N$$

Therefore, it holds that $R = kG = -\frac{z+re}{N-s} G$

or equivalently $\frac{z+re}{N-s} G = -R$.

We have that ECDSAverify$(P, m, r, n-s)$ has a testval of $\frac{z}{N-s} G + \frac{r}{N-s} P = \frac{z+re}{N-s} G$, the x-coordinate of which coincides with the x-coordinate of $-R$.

Due to the definition of point addition on $S_{a,b}$, we have that $-R = (r, -R_y)$ if $R = (r, R_y)$, so $-R$ and R have the same x-coordinate

$\Rightarrow \frac{z+re}{N-s} G$ and R have same x-coordinate $\Rightarrow$ ECDSAverify$(P, m, r, n-s)$ returns "True".

$\square$

Schnorr signature private key leak after reuse of nonce k.

Solution sketch:

▷ Compute z_1, z_2 from P, R and m_1, m_2

▷ $s_1 = k + z_1 e$

$s_2 = k + z_2 \cdot e$

$s_1 - s_2 = k + z_1 e - (k + z_2 e) = (z_1 - z_2) e$

$\Rightarrow \quad e = \dfrac{s_1 - s_2}{z_1 - z_2}$

▷ Thus, compute $e = \dfrac{s_1 - s_2}{z_1 - z_2}$