ElGamal Signature

- KeyGen(1^λ) ; choose a large prime p and $g \xleftarrow{\$} \mathbb{Z}_p^*$.
  choose a secret key $s \xleftarrow{\$} \mathbb{Z}_p^*$.
  compute $y = g^s \mod p$.
  output $pk = (p, g, y)$ and $sk = (s)$.

- Sign(sk, m) ; choose a random $r \xleftarrow{\$} \mathbb{Z}_p^*$.
  compute $\sigma_1 = g^r \mod p$
  $\sigma_2 = r^{-1}(m - s \cdot \sigma_1) \mod p-1$. $m \equiv s\sigma_1 + r\sigma_2 \ (p-1)$
  output (m, σ) where $\sigma = (\sigma_1, \sigma_2)$.

- Verify(pk, m, σ) ; compute $g_1 = y^{\sigma_1} \cdot \sigma_1^{\sigma_2} \mod p$.
  $g_2 = g^m \mod p$
  if $g_1 \equiv g_2 \mod p$, output 1.
  if $g_1 \not\equiv g_2 \mod p$, output 0.
  $g_2 \equiv g^m \equiv g^{s\sigma_1 + r\sigma_2}$
  $\equiv y^{\sigma_1} \cdot \sigma_1^{\sigma_2} \mod p$.

- Suppose the same random r is used to generate signatures for $m_1 \neq m_2$.
  Then, σ_1 is the same in both signature.
  Since σ_2 is different, call them σ_2 and σ_2'.
  Then, $\sigma_2 r - m_1 \equiv -s\sigma_1 \equiv \sigma_2' r - m_2 \mod p-1$.
  $r(\sigma_2 - \sigma_2') \equiv m_1 - m_2 \mod p-1$. (*)
  Let $d = \gcd(\sigma_2 - \sigma_2', p-1)$.
  Then, there are d candidates for r. ($\because$ there are d solutions for (*)).
  r