从ECDSA生成的签名中恢复公钥

现在假设我们已知所生成的签名 (r, s) 以及被签名的消息 m。额外的，我们还需要知道所使用的椭圆曲线以及hash函数。具体的步骤如下：

1. 根据所生成的签名 (r, s) ，在曲线上找到以 r 为横坐标的两个点 P_1, P_2 .
2. 然后我们计算 $t = r^{-1} \mod n$
3. 接下来计算消息的哈希值 $e = H(m)$

所以我们就可以得到两个可能的公钥 $Q_1 = t(sP_1 - eG)$ 和 $Q_2 = t(sP_2 - zG)$。并且两个公钥都可以通过验证即

$$(s^{-1}eG + s^{-1}rQ_i)_x = (s^{-1}eG + s^{-1}rr^{-1}(sP_i - eG))_x = (s^{-1}eG + P_i - s_{-1}eG)_x = r \mod n$$