Pairings

1. Which of the following properties does a pairing \( e: G_1 \times G_2 \rightarrow G_T \) have? (Mark as many options as you think are correct.)

- A) Bilinearity
- B) Collision-resistance
- C) Non-degeneracy

2. How many evaluations of a pairing \( e: G \times G \rightarrow G_T \) does each party have to perform in Joux's 3-party key exchange protocol to compute a shared key?

   1

3. (Requires knowledge about common cryptographic assumptions in cyclic groups.) Intuitively, a pairing allows one "multiplication in the exponent", at the cost of moving to another group \( G_T \). Why is a pairing with \( G_1=\mathbb{G}_2=\mathbb{G}_t \) (and \( e(g,g)=g \)) probably not very useful?

   Such a pairing would solve the CDH (computational Diffie-Hellman) problem. Not many applications of cyclic groups with easy CDH problem are known.

   Details:
   If \( e(g,g)=g \), we can solve the CDH problem by computing \( e(g^a, g^b) = e(g,g)^{ab} = g^{ab} \).

   In general however, \( e(g,g) \) can be any group generator, i.e. \( e(g,g) = g^x \) for some \( x \in \mathbb{Z}_p^* \). But then we can define another pairing \( e' \) by \( e'(h,h') = e(h,e(h',g^{(1/(x^2))})) \) and this paring has the property \( e'(g,g) = g \).

   The factor \( g^{(1/(x^2))} \) can be computed as follows: \( g^{(1/(x^2))} = g \cdot (x^{(p-3)}) \) where the latter can be computed with \( O(\log p) \) pairing evaluations in a square-and-multiply fashion.

   See also Lecture 11, Slide 4.

   \(^1\) For this equality we use Fermat's little theorem: \( x^p \equiv x \pmod{p} \iff x^{(p-3)} \equiv 1/(x^2) \pmod{p} \).