1. All elements that would be a part of Z\*10 are elements from 1 to 9 that are relatively prime to 10.

So, Z\*10 = {1, 3, 7, 9}

If an element is its own inverse, then we have:

a \* a = 1 (mod 10)

Hence, result = {1, 9}.

1. Suppose the CDH assumption holds; we want to prove that the DL assumption holds. In other words, let ADL be any PPT DL solver; we want to prove that Pr[ADL wins] is negligible. We use ADL to construct a PPT CDH solver, which we call ACDH.

CDH Solver ACDH:

* ACDH is given input gx and gy , where x 🡪 Zq and y 🡪 Zq; its task is to compute gxy.
* Sample x ← Zq and compute h: = gx.
* Run x′ ← ADL(h).
* A wins if x′ = x.
* Now, we have gy from game challenger and computed x. So, we can compute g(y)x = gxy.

If ADL wins, this means that ADL outputs gxy, so ACDH —which copies ADL’s output — also outputs gxy, which is exactly what it is supposed to output.

Thus, Pr[ACDH wins] ≥ Pr[ADL wins],

But since the CDH assumption holds, we know that Pr[ACDH wins] is negligible — which implies that Pr[ADL wins] is also negligible.

This completes the proof.

1. The proof is incorrect since the given reduction must simulate the experiment, which is not ASDH here. Moreover, ACDH is given input (gx, gx) which are not independent of each other. it doesn’t make use of a random value r such that r 🡪 Zq. The SDH solver simply passes the two inputs to the CDH solver and outputs its result.
2. Suppose the SDH assumption holds; we want to prove that the CDH assumption holds. In other words, let ACDH be any PPT CDH solver; we want to prove that Pr[ACDH wins] is negligible. We use ACDH to construct a PPT SDH solver, which we call ASDH :

SDH solver ASDH :

* ASDH is given input gx; its task is to compute gx^2.
* Choose a random value r from {1, 2, ..., q-1}, where q is the order of the group G.
* Compute gr, gxr.
* Run gx\*x\*r 🡨 ACDH (gr, gxr).
* A wins if gx\*x\*r = g(x^2) \*r.
* Compute gxy = (g(x^2) \*r)1/r = gx^2.

If ACDH wins, then it outputs gx^2. In this case, ASDH, which copies ACDH's output, also outputs gx^2, which is exactly what it is supposed to output. Thus, we have:

Pr[ASDH wins] ≥ Pr[ACDH wins]

But since the SDH assumption holds, we know that Pr[ASDH wins] is negligible, which implies that Pr[ACDH wins] is also negligible.

This completes the proof.

1. The proof states that CDH wins assuming that SDH wins three consecutive times. Later it states that the probability that SDH wins three consecutive times is (Pr[ASDH wins])3. The assumption that the probability of winning three times in a row is (Pr[ASDH wins])3 is not correct, as each run of ASDH is dependent on the previous runs. This means that the probability of winning three times in a row is not simply the cube of the probability of winning a single time. Therefore, the conclusion that Pr[ASDH wins] ≤ 3√Pr[ACDH wins] is also not valid.