Exercise sheet 7, 13 January 2022

1. If the secret shared via Shamir secret sharing is an element in a finite field one can keep shares and Lagrange coefficients small(er) by computing the coefficients in the finite field. Note that this works for secrets in $\mathbb{Z}/n$ in general, but then care needs to be taken to avoid denominators that are not invertible.

   Use Shamir's secret sharing to share $a = 5$ modulo 103 in a 3-out-of-5 fashion. Verify for two sets of 3 users that you can recover the secret.

2. In Shamir's secret sharing there is a lot of trust on the party S that shares the keys. A malicious S could give invalid shares to some people, so that any group of t people involving at least one of them would compute the wrong secret. To prevent this, all parties insist on S publishing some extra information.

   Let S publish g^a and g^{f_i} for $1 \leq i < t$, where g is the generator of some large DH group. Show how participant j can verify that his share $(j, f(j)$ is correct given the information provided by S.

3. Let the DH secret a be shared in a t-out-of-N fashion. Show how to compute g^{ab} given g^b and the shares, without recomputing a, i.e. using the shares locally.

4. Let the RSA secret key d be shared in a t-out-of-N fashion. Show how to do RSA decryption using shares locally, i.e. without recovering the secret d.
   Note, this one is much harder than for DH.