

1 Interpol Warning

Consider the set of four points $\{(-1, 1), (0, 2), (1, 5), (2, 40)\}$.

Find the unique polynomial over \mathbb{R} of degree ≤ 3 that passes through these points by either solving a system of linear equations or by Lagrange Interpolation.

2 Secrets in the United Nations

The United Nations (for the purposes of this question) consists of n countries, each having k representatives. A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. The vault should only be opened in one of two situations. First, it can be opened if all n countries in the UN help. Second, it can be opened if at least m countries get together with the Secretary General of the UN.

(a) Propose a scheme that gives private information to the Secretary General and n countries so that s can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: in order for a country to help, all of the country's k representatives must agree. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary General and to each representative of each country.

3 Erasure Warm-Up

Working over $\text{GF}(q)$, you want to send your friend a message of $n = 4$ packets and guard against 2 lost packets. What is the minimum q you can use? What is the maximum degree of the unique polynomial that describes your message?