# Homework 7

*Due: Wednesday, April 12*

All homeworks are due at 11:59 PM on Gradescope.

**Please do not include any identifying information about yourself in the handin, including your Banner ID.**

Be sure to fully explain your reasoning and show all work for full credit.

## Problem 1

The CS22 plant nursery has grown 101 ferns, each of which has some nonnegative integer number of fronds. Prove that it is possible to find a set of 11 of these ferns whose total number of fronds is divisible by 11.

**HINT:** Associate to each fern its number of fronds mod 11, and consider two cases, one where there is a fern in each of the categories and one where there isn't.

# Problem 2

Prove the following equality.

Do not use any algebraic manipulation in your argument. Instead, give a ”counting argument”: why is the number of ways to choose $k$ objects from $n$ options the same as the sum shown on the right?

$$\binom{n}{k} = \binom{n-2}{k} + 2\binom{n-2}{k-1} + \binom{n-2}{k-2}$$

# Problem 3

This problem is a Lean question!

This homework question can be found by navigating to `BrownCs22/Homework/Hw7.lean` in the directory browser on the left of your screen in Gitpod. The comment at the top of that file provides more detailed instructions.

# Problem 4 (Mind Bender — *Extra Credit*)

Alice is the CEO of a popular plant-nursery chain, which uses RSA to communicate with its clients. Each of her stores has its own unique public key. However, business is booming, and Alice is tired of having to generate new prime numbers every time a new store opens. Instead, she generates just two prime numbers $p$ and $q$ and decides that from now on, all stores will use the same modulus $N = pq$. To maintain security, each store will use a different encryption exponent (and will therefore have a different private decryption exponent). Alice also decides that the encryption exponents of all stores will be relatively prime to each other (e.g., if store 1 has encryption exponent $e_1$ and store 2 has encryption exponent $e_2$, then $\gcd(e_1, e_2) = 1$).

Bob then sends a message containing his highly confidential plant-marketing technique to each of Alice's stores using this new scheme (i.e., he sends to each store the same message $m$ encrypted with the respective store's public key). Eve—the CEO of a rival company—intercepts all of Bob's ciphertexts. (Ordinarily, this would be fine—they're encrypted, after all.) But Eve then decrypts the message $m$ and steals Alice and Bob's trade secrets!

a. Describe a strategy Eve can use to do this, and prove that your strategy is correct. You should explicitly identify any nontrivial algorithms Eve needs to use in order to carry out her strategy.

   Note: your proposed strategy must be computationally feasible for large values of $N$. For example, your solution must not depend upon using brute force to factor $N$ or to compute $\phi(N)$.

   **HINT:** By the linear combination theorem, there exists a linear combination of any two stores' encryption exponents equal to 1.

b. Suppose that Alice publishes the modulus $N = 91$ and that Eve intercepts the ciphertexts encrypted using the exponents given in the table below.

| Encryption Exponent | Ciphertext |
|---|---|
| 5 | 2 |
| 28 | 74 |
| 81 | 57 |

   Using your strategy from part (a), decrypt Bob's message. Show your work.

   Note: your response *must* use your algorithm from part (a). You should show all steps of your algorithm, though you may use a calculator for exponentiation mod $N$. You may not need all the data provided.