Homework 7 solutions

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.

Solution:

-Assign each fern a number equal to the equivalence class of the number of fronds it has $\pmod{11}$. You now have 101 ferns numbered between 0 and 10 inclusive. Separate the ferns into groups based on their assigned number, which gives 11 groups.

Case 1: There is an empty group. In this case, we are separating 101 ferns into only 10 groups. Since $\frac{101}{10}$ gives a number that is bigger than 10, at least one of the groups must contain at least 11 ferns. Therefore, you can then choose 11 ferns from one group. Adding their fronds $\pmod{11}$ gives a result that is congruent to $0 \pmod{11}$ since every number of fronds in our group can be written as $11 * a_i + r$ where r is the group number. Thus their sum is $\sum_{i=1}^{11}(11 * a_i + r) = 11(k + r)$ where $k = a_1 + ... + a_{11}$. We know that $11(k + r) \equiv 0 \pmod{11}$ for any $k \in \mathbb{Z}$.

Case 2: There is no empty group. In this case, there is at least one fern in each group. Choose one fern from each group. Those ferns' total number of fronds is congruent to $0 \pmod{11}$ since $0 + 1 + 2 + ...10 = 55 = 5 * 11$. We know that $11 * k + 55 \equiv 0 \pmod{11}$ for any $k \in \mathbb{Z}$.

Since in both cases, which are mutually exclusive and which cover all possible cases, you are able to choose 11 ferns where the sum of the number of fronds on the 11 ferns is congruent to $0 \pmod{11}$, then it is possible to pick 11 ferns from 101 ferns

whose total number of fronds is divisible by 11.

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?

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

Solution:

We will prove this using a counting argument; that is, we will show that the LHS and RHS of the equation both count the same number.

Consider some set A with n elements. The LHS counts the number of subsets of A that have k elements.

Choose two arbitrary elements from set A (call them a_1 and a_2). The first term on the RHS, which is $\binom{n-2}{k}$, counts the number of subsets of A with k elements that include neither a_1 nor a_2 (we're essentially choosing k elements from the remaining $n-2$ elements in set A, since neither of our fixed elements are in the subsets we are counting).
The second term on the RHS, which is $2 * \binom{n-2}{k-1}$, counts the number of subsets of A with k elements that include exactly one of a_1 and a_2 (the coefficient of 2 accounts for both elements - we are choosing $k-1$ elements from the remaining $n-2$ elements in A for the case where a_1 is in the subsets and then the case where a_2 is in the subsets).
The third term on the RHS, which is $\binom{n-2}{k-2}$, counts the number of subsets of A with k elements that include both a_1 and a_2 (we are choosing $k-2$ elements from the remaining $n-2$ elements in A, since a_1 and a_2 are both in the subsets we are counting).

Since we've counted the subsets of A with k elements that have both a_1 and a_2, exactly one of a_1 and a_2, and neither a_1 nor a_2, we've covered all cases and have shown equality of the LHS and RHS.

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.

> Question 3 Autograded on Lean/Gradescope.

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.

Solution:

a. Suppose - Eve intercepts a ciphertext c for a store with encryption exponent e. Let e' be the encryption exponent for some other store and c' be the ciphertext for that other store.

Since $\gcd(e, e') = 1$, Eve can use the extended Euclidean algorithm to compute $a, b \in \mathbb{Z}$ such that $ae + be' = 1$.

Notice that it would now suffice for Eve to compute $c^a \cdot c'^b \equiv m^{ea} \cdot m^{e'b} \equiv m^{ea+e'b} \equiv m^1 \equiv m \pmod{N}$.

However, there is a complication: we know that one of a, b is negative (since $e, e' > 1$). Without loss of generality, suppose $a < 0$. Then $c^a \equiv (c^{-1})^{|a|} \pmod{N}$. So Eve must first compute $c^{-1} \pmod{N}$. If c is relatively prime to N, the she can do this using the extended Euclidean algorithm; with c^{-1} in hand, she can then compute $c^a \cdot c'^b \equiv (c^{-1})^{|a|} c^b \equiv m \pmod{N}$, since exponentiation modulo N can be done efficiently.

If c is *not* relatively prime to N, then Eve can compute $\gcd(c, N)$ using the Euclidean algorithm. If $\gcd(c, N) \neq N$, then we must have $\gcd(c, N) = p$ or $\gcd(c, N) = q$; without loss of generality, say $\gcd(c, N) = p$. Then Eve can compute $N/p = q$ as well, and thus can multiply to obtain $\phi(N) = (p-1)(q-1)$. She then computes $d \equiv e^{-1} \pmod{(p-1)(q-1)}$ using the extended Euclidean algorithm, using which she can compute $c^d \equiv (m^e)^d \equiv m \pmod{N}$.

If $\gcd(c, N) = N$, then c is a multiple of N, i.e., is congruent to 0 modulo N. But since we know that RSA is lossless and $m \in \{0, 1, \ldots, N-1\}$, Eve immediately knows that $m = 0$, since $0^e = 0$.

Thus, in all cases, Eve recovers Bob's message.

b. We only need two exponent-ciphertext pairs to carry out our attack; we'll take the first two for simplicity.

We first need to find a linear combination of $e = 5$ and $e' = 28$ equal to 1. We first perform the Euclidean algorithm:

$$\begin{array}{lll} \gcd(28, 5) & 28 = 5 \cdot 5 + 3 & 3 = 28 - 5 \cdot 5 \\ = \gcd(5, 3) & 5 = 1 \cdot 3 + 2 & 2 = 5 - 1 \cdot 3 \\ = \gcd(3, 2) & 3 = 1 \cdot 2 + 1 & 1 = 3 - 1 \cdot 2 \\ = \gcd(2, 1) & 2 = 2 \cdot 1 + 0 & \\ = \gcd(1, 0) = 1 & & \end{array}$$

Then work backwards:

$$1 = 3 - 1 \cdot 2 = 3 - 1(5 - 1 \cdot 3)$$

$$= 2 \cdot 3 - 1 \cdot 5 = 2 \cdot (28 - 5 \cdot 5) - 1 \cdot 5$$
$$= -11 \cdot 5 + 2 \cdot 28$$

So $a = -11$ and $b = 2$. We want to compute

$$c^a c'^b = 2^{-11} \cdot 74^2$$

modulo 91, so we first must find 2^{-1} modulo 91. We again use the extended Euclidean algorithm:

$$\begin{aligned} &\gcd(91, 2) && 91 = 45 \cdot 2 + 1 \\ &= \gcd(2, 1) && 2 = 2 \cdot 1 + 0 \\ &= \gcd(1, 0) = 1 \end{aligned}$$

The first equation immediately gives us that $1 = 91 - 45 \cdot 2$, so that $2^{-1} \equiv -45 \pmod{91}$.

Substituting, we find that

$$\begin{aligned} c^a c'^b &\equiv 2^{-11} \cdot 74^2 \\ &\equiv (-45)^{11} \cdot 74^2 \\ &\equiv 2 \cdot 16 \\ &\equiv 32 \pmod{91} \end{aligned}$$

So Bob's secret message was 32.