Discrete Structures	Prelim 2 sample questions
CS2800	Questions selected for Spring 2019

1. Prove that $7^m - 1$ is divisible by 6 for all positive integers m (try this both inductively and using equivalence classes).

2. [6 points] *Pascal's triangle* is a sequence of rows, where each entry is formed by adding the two adjacent entries from the previous row:

$$\begin{array}{c} 1 \\ 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \\ 1 \quad 4 \quad 6 \quad 4 \quad 1 \\ \cdots \end{array}$$

   If we let $P_{n,k}$ stand for the kth entry in the nth row of Pascal's triangle, then $P_{n,k}$ is given by the formulas $P_{1,1} ::= 1$, $P_{n,0} ::= 0$ for all n, and $P_{n+1,k} ::= P_{n,k-1} + P_{n,k}$ if $n \geq 1$.

   Prove by induction on n that for all $n \geq 1$, for all k with $1 \leq k \leq n$, $P_{n,k} = \binom{n}{k} = \frac{n!}{k!(n-k)!}$.

   Note: The definition of $n!$ is $0! ::= 1$ and $n! ::= n \cdot (n-1)!$ for all $n \geq 1$.

3. Prove the following claim using induction: for any $n \geq 0$, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

4. The Fibonacci numbers $F_0, F_1, F_2, \ldots$ are defined inductively as follows:

$$\begin{aligned} F_0 &= 1 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \quad \text{for } n \geq 2 \end{aligned}$$

   That is, each Fibonacci number is the sum of the previous two numbers in the sequence. Prove by induction that for all natural numbers n (including 0):

$$\sum_{i=0}^{n} F_i \;=\; F_{n+2} - 1$$

5. Prove by induction that for any integer $n \geq 3$, $n^2 - 7n + 12$ is non-negative.

6. Chapter 5 of MCS has a bunch of good induction exercises (and you can find even more by searching)

7. Suppose that Alice sends the message a to Bob, encrypted using RSA. Suppose that Bob's implementation of RSA is buggy, and computes $k^{-1} \mod 4\phi(m)$ instead of $k^{-1} \mod \phi(m)$. What decrypted message does Bob see? Justify your answer.

8. (a) What are the units of $\mathbb{Z}$ mod 12?

   (b) What are their inverses?

   (c) What is $\phi(12)$?

9. Use Euler's theorem and repeated squaring to efficiently compute $8^n \mod 15$ for $n = 5$, $n = 81$ and $n = 16023$. Hint: you can solve this problem with 4 multiplications of single digit numbers. Please fully evaluate all expressions for this question (e.g. write 15 instead of $3 \cdot 5$).

10. In this problem, we are working mod 7, i.e. $\equiv$ denotes congruence mod 7 and $[a]$ is the equivalence class of a mod 7.

(a) What are the units of $\mathbb{Z}_7$? What are their inverses?

(b) Compute $[2]^{393}$.

11. (a) Recall Bézout's identity from the homework: for any integers n and m, there exist integers s and t such that $gcd(n, m) = sn + tm$. Use this to show that if $gcd(k, m) = 1$ then $[k]$ is a unit of $\mathbb{Z}_m$.

    (b) Use part (a) to show that if p is prime, then $\phi(p) = p - 1$.

    (c) Use Euler's theorem to compute $3^{38} \mod 37$ (note: 37 is prime).

12. Bob the Bomber wishes to receive encrypted messages from Alice the Accomplice. He generates a public key pair $m = 21$ and $k = 5$. Luckily, you have access to an NSA supercomputer that was able to factor 21 into $7 \cdot 3$.

    (a) Use this information to find the decryption key k^{-1}.

    (b) Without changing m, what other possible keys k could Bob have chosen? Find the decryption keys for those keys as well.

    (c) Alice encrypts a secret message msg using Bob's public key ($k = 5$), and sends the ciphertext $c = 4$. What was the original message?

13. Which of the following does RSA depend on? Explain your answer briefly.

    (a) Factoring is easy and testing primality is hard.

    (b) Factoring is hard and testing primality is easy.

    (c) Both factoring and testing primality are hard.

    (d) Both factoring and testing primality are easy.

14. (a) Let m and n be integers greater than 1. Show that the function $f : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m$ given by $f : ([a]_m, [b]_n) \to [a + b]_m$ is not necessarily well defined. [Hint: you just need an example here.]

    (b) Show that f is well defined if $m|n$.

15. We define a set S of functions from $\mathbb{Z}$ to $\mathbb{Z}$ inductively as follows:

    Rule 1. For any $n \in \mathbb{Z}$, the translation (or offset) function $t_n : x \mapsto x + n$ is in S.

    Rule 2. For any $k \neq 0 \in \mathbb{Z}$, the scaling function $r_k : x \mapsto kx$ is in S.

    Rule 3. If f and g are elements of S, then the composition $f \circ g \in S$.

    Rule 4. If $f \in S$ and f has a right inverse g, then g is also in S.

    In other words, S consists of functions that translate and scale integers, and compositions and right inverses thereof.

    > **Note:** This semester, we made a bigger distinction between the elements of an inductively defined set and the meaning of an inductively defined set. We probably would have phrased this question as follows: Let S be given by
    >
    > $$s \in S ::= t_n \mid r_k \mid s_1 \circ s_2 \mid rinv\ s$$
    >
    > and inductively, let the function defined by s (written $F_s : \mathbb{Z} \to \mathbb{Z}$) be given by the rules $F_{t_n}(x) ::= x + n$, $F_{r_k}(x) ::= ks$, $F_{s_1 \circ s_2}(x) ::= F_{s_1} \circ F_{s_2}$ and let $F_{rinv\ s} ::= g$ where g is a right inverse of F_s.

    (a) [1 point] Show that the function $f : x \mapsto 3x + 17$ is in S.

    (b) Use structural induction to prove that for all $f \in S$, f is injective. You may use without proof the fact that the composition of injective functions is injective.

(c) Give a surjection ϕ from S to $\mathbb{Z}$ (proof of surjectivity not necessary). Remember that this surjection must map a *function* to an *integer*, and for every integer there must be a function that maps to it.

16. Draw a finite automaton (DFA, NFA or ϵ-NFA) with alphabet $\{a, b\}$ to recognize strings of the form $x_1 x_2 x_3 \cdots$ where each x_i is either "ab" or "ba".

17. Build a deterministic finite automaton that recognizes the set of strings of 0's and 1's, that only contain a single 0 (and any number of 1's). Describe the set of strings that lead to each state.

18. (a) In lecture, we proved that if $[a]_m$ is a unit, then $[a]_m^{\varphi(m)} = [1]$.

    Use this to show that $a^{[b]_{\varphi(m)}} := [a^b]_m$ is well defined.

    (b) Use Euler's theorem to prove that if p is prime, then $[a]_p^p = [a]_p$ (whether $[a]_p$ is a unit or not).

19. Give a DFA that accepts strings in $\{0, 1\}^*$ if and only if they contain at most one 0 **and** an even number of 1's. For each state, describe the strings that reach that state.

20. In this question we formalize the usual algorithm for adding numbers represented in base b. Let $\Sigma = \{0, 1, \ldots, b - 1\}$.

    (a) Give an *inductive* definition of the base b interpretation function $n : \Sigma^* \to \mathbb{N}$. Check that if $b = 2$ then $n(110) = 6$.

    (b) Consider the following inductive definition of a function

    $$add : \Sigma^* \times \Sigma^* \times \{0, 1\} \to \Sigma^*$$

    given by

    $$\begin{aligned}
    add(\varepsilon, \varepsilon, c) &:= \varepsilon c \\
    add(xd, \varepsilon, c) &:= add(x, \varepsilon, q)r \qquad \text{where } q = quot(d + c, b) \text{ and } r = rem(d + c, b) \\
    add(\varepsilon, xd, c) &:= add(x, \varepsilon, q)r \qquad \text{where } q = quot(d + c, b) \text{ and } r = rem(d + c, b) \\
    add(xd, ye, c) &:= add(x, y, q)r \qquad \text{where } q = quot(d + e + c, b) \text{ and } r = rem(d + e + c, b)
    \end{aligned}$$

    Note: you know this algorithm well; c stands for "carry".

    Prove that $n(add(x, y, c)) = n(x) + n(y) + c$. If multiple cases are substantially similar, you may say so instead of repeating the proof.