Discrete Structures	Final exam sample questions
CS2800	Questions selected for fall 2017

1. Determine the prime factorizations, greatest common divisor, and least common multiple of the following pairs of numbers (m, n). In each case, give Bézout coefficients s and t such that $sm + tn = gcd(m, n)$.

   (a) $(6, 8)$ prime factorizations = ☐ ☐

   gcd = ☐ lcm = ☐ s = ☐ t = ☐

   (b) $(5, 7)$ prime factorizations = ☐ ☐

   gcd = ☐ lcm = ☐ s = ☐ t = ☐

   (c) $(21, 12)$ prime factorizations = ☐ ☐

   gcd = ☐ lcm = ☐ s = ☐ t = ☐

2. Prove that $7^m - 1$ is divisible by 6 for all positive integers m.

3. 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.

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

   (b) What are their inverses?

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

5. 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 $3 \cdot 5$).

6. Compute $10101b + 101b$ (recall that b indicates the strings of digits should be interpreted as integers using the binary representation). Express your answer in both binary and decimal.

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

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

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

8. Suppose you are given a function $f : \mathbb{N} \to \mathbb{N}$, and are told that $f(1) = 1$ and for all n, $f(n) \leq 2f(\lfloor n/2 \rfloor) + 1$.

   Use strong induction on n to prove that for all $n \geq 2$, $f(n) \leq 2n \log_2 n$.

   You may write log to indicate $\log_2$. Here is a reminder of some facts about $\lfloor x \rfloor$ and $\log x$:

   - $\lfloor x \rfloor \leq x$
   - $\log 1 = 0$, $\log 2 = 1$
   - $\log(x/2) = \log x - 1$
   - $\log(2^x) = x$
   - $\log(x^2) = 2 \log x$
   - if $x \leq y$ then $\log x \leq \log y$

9. (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).

10. 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?

11. (a) Explain carefully what the flaw is with the following "proof" that every postage of three cents or more can be formed using just three-cent and four-cent stamps.

    We use regular induction to prove that $P(n)$ holds for all $n \geq 3$, where $P(n)$ says that postage of n cents cents can be formed using just three-cent and four-cent stamps.

    Base Case: We can form postage of three cents with a single three-cent stamp and we can form postage of four cents using a single four-cent stamp.

    Inductive Step: Assume that we can form postage of j cents for all nonnegative integers j with $j \leq k$ using just three-cent and four-cent stamps. We can then form postage of $k + 1$ cents by replacing one three-cent stamp with a four-cent stamp or by replacing two four- cent stamps by three three-cent stamps.

    (b) Show that every postage of six cents or more can be formed using just three-cent and four-cent stamps.

12. Complete the following proof.

    Claim: For all $k > 0$ and all $a, b \geq 0$, $gcd(ka, kb) = k \cdot gcd(a, b)$.
    Proof: By (strong) induction on b. Let $P(b)$ be the statement "for all $k > 0$ and all a, $gcd(ka, kb) = k \cdot gcd(a, b)$."
    $P(0)$ is clearly true: $gcd(ka, kb) = gcd(ka, 0) = ka = k \cdot gcd(a, 0)$.
    For the inductive step, assume $P(0)$, $P(1)$, ... $P(b-1)$. We wish to show $P(b)$. Use Euclidean division to write $a = qb + r$ with $0 \leq r < b$. By Euclid's algorithm, we know $g(a, b) =$ **[FILL IN]**. Similarly $g(ka, kb) =$**[FILL IN]** where **[FILL IN]**.

    [FILL IN]

    Therefore $gcd(ka, kb) = k \cdot gcd(a, b)$.

13. Prove by induction that $3^{2n-1} + 1 \equiv 0 \pmod 4$ for all $n \geq 1$.

14. (a) Build a proof tree showing that $\vdash \neg(P \vee Q) \to \neg P$. You may refer to the list of rules given at the end of the exam.

    (b) Show, using truth tables, that $\models \neg(P \vee Q) \to \neg P$.

15. Because we reordered the topics this semester, past semesters have not had many questions on logic. A good exercises is to use truth tables to find valid statements and then build proof trees for them. For example, you might prove $P \to (Q \to R) \vdash P \wedge Q \to R$, or $P \to Q \vdash Q \vee \neg P$ or $\vdash \neg(P \wedge Q) \to (\neg P \vee \neg Q)$.

16. Explain carefully what the bug is in the following argument:

    We prove by strong induction that all orders of fish for at least 6 pounds of fish can be filled using only 3-pound fish. Let $P(n)$ be the statement that an order of fish for n pounds of fish can be filled using only 3-pound fish. We prove $P(n)$ for $n \geq 6$. Clearly $P(6)$ is true: an order

for 6 pounds of fish can be filled using two 3-pound fish. Suppose that $P(6), \ldots, P(n)$ are all true. We prove $P(n+1)$. We want to show that we can fill an order for $n+1$ pounds of fish using 3-pound fish, if $n \geq 6$. By the induction hypothesis, we can fill an order for $n-2$ pounds of fish using 3-pound fish. Add one more 3-pound fish, and we've filled the order for $n+1$ pounds. This completes the induction argument.

17. [4 points] 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.

18. (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 $m|n$.

19. For $n \geq 0$, let $F_n = 2^{2^n} + 1$. (Those numbers F_n which are prime are called *Fermat primes.*)

    (a) [5 points] Prove by induction that $\prod_{r=0}^{n-1} F_r = F_n - 2$.

    (b) [5 points] Prove that $\gcd(F_m, F_n) = 1$ for all m, n with $m < n$. (Hint: use part (a)—which you can use even if you haven't proved it—and some standard facts about divisibility.)