# CS201: Discrete Math for Computer Science
# 2022 Spring Semester

Total number of questions: $10 + 1$ (optional)
Total points: $100 + 10$ (bonus)

**Q. 1.** (10 points) Determine whether the following statements are correct or incorrect. Explain your answer. Assume that $p, q$ and $r$ are logical propositions, $x$ and $y$ are real numbers, and $m$ and $n$ are integers.

(1) $(\neg p \wedge (p \to q)) \to \neg q$ is a tautology.

(2) $(p \vee q) \to r$ and $(p \to r) \wedge (q \to r)$ are equivalent.

(3) Under the domain of all real numbers, the truth value of $\exists x \forall y (y \neq 0 \to xy = 1)$ is T.

(4) Under the domain of all integers, the truth value of $\exists n \exists m (n^2 + m^2 = 5)$ is T.

**Solution:**

(1) Incorrect. This can be proven using truth table.

| $p$ | $q$ | $\neg p$ | $p \to q$ | $\neg p \wedge (p \to q)$ | $\neg q$ | $(\neg p \wedge (p \to q)) \to \neg q$ |
|---|---|---|---|---|---|---|
| T | T | F | T | F | F | T |
| T | F | F | F | F | T | T |
| F | T | T | T | T | F | F |
| F | F | T | T | T | T | T |

Since the truth value of $(\neg p \wedge (p \to q)) \to \neg q$ is not always $T$, it is not a tautology. (Any proof is acceptable, as long as it explains that under some $p$ and $q$, the truth value of $(\neg p \wedge (p \to q)) \to \neg q$ is false.)

(2) Correct. This can be proven as follows:

$$\begin{aligned}
(p \vee q) \to r &\equiv \neg(p \vee q) \vee r && \text{(Useful Law)} \\
&\equiv (\neg p \wedge \neg q) \vee r && \text{(De Moegan's Law)} \\
&\equiv (\neg p \vee r) \wedge (\neg q \vee r) && \text{(Distributive Law)} \\
&\equiv (p \to r) \wedge (q \to r) && \text{(Useful Law)}
\end{aligned}$$

Any proof that shows the equivalence is acceptable.

(3) Incorrect. This proposition means that there is a real number $x$ for which $y \neq 0 \rightarrow xy = 1$ for every real number $y$. Consider an arbitrary $x$. Suppose $y_1 \neq 0$ and $xy_1 = 1$. Let $y_2 = 2y_1$. Then, $xy_2 = 2$, i.e., $y \neq 0 \rightarrow xy = 1$ does not hold for every $y$.

(4) Correct. When $n = 1$ and $m = 2$, $n^2 + m^2 = 5$.

**Q. 2.** (8 points) For each of the following argument, determine whether it is valid or invalid. Explain using the validity of its argument form.

(1) Premise 1: If you did not finish your homework, then you cannot answer this question.

Premise 2: You finished your homework.

Conclusion: You can answer this question.

(2) Premise 1: If all students in this class has submitted their homework, then all students can get 100 in the final exam.

Premise 2: There is a student who did not submit his or her homework.

Conclusion: It is not the case that all student can get 100 in the final exam.

**Solution:**

(1) Invalid. Let $p$ denote "you finished your homework". Let $q$ denote "you can answer this question". Thus, premises 1 and 2 can be represented as $\neg p \rightarrow \neg q$ and $p$, respectively. Conclusion can be represented as $q$. This argument form is not valid, since $((\neg p \rightarrow \neg q) \wedge p) \rightarrow q$ is not a tautology. This is because when $p$ is T and $q$ is F, the truth value of $((\neg p \rightarrow \neg q) \wedge p) \rightarrow q$ is F.

(2) Invalid. Consider the domain of this class. Let $P(x)$ denote "student $x$ has submitted his or her homework". Let $Q(x)$ denote "student $x$ can get 100 in the final exam". Premises 1 and 2 can be represented as $\forall x P(x) \rightarrow \forall x Q(x)$ and $\exists x(\neg P(x))$, respectively. The conclusion can be represented as $\neg \forall x Q(x)$. This argument form is not valid, since $((\forall x P(x) \rightarrow \forall x Q(x)) \wedge \exists x(\neg P(x)) \rightarrow \neg \forall x Q(x)$ is not a tautology. Consider the case where both $\exists x(\neg P(x))$ and $\forall x Q(x)$ are T. Thus, $\forall x P(x)$ is F, since $\neg \forall x P(x) \equiv \exists x(\neg P(x))$ is T. Hence, $((\forall x P(x) \rightarrow \forall x Q(x)) \wedge \exists x(\neg P(x))$ is T. However, since $\neg \forall x Q(x)$ is F, the entire proposition is F.

**Q. 3.** (8 points) Suppose that $p$, $q$, $r$, $s$ are all logical propositions. You are given the following statement

$$(\neg r \vee (p \wedge \neg q)) \rightarrow (r \wedge p \wedge \neg q)$$

Prove that this implies $r \vee s$ using logical equivalences and rules of inference.

**Solution:**

| | | |
|---|---|---|
| | $(\neg r \vee (p \wedge \neg q)) \rightarrow (r \wedge p \wedge \neg q)$ | |
| $\equiv$ | $\neg(\neg r \vee (p \wedge \neg q)) \vee (r \wedge p \wedge \neg q)$ | Useful |
| $\equiv$ | $(r \wedge \neg(p \wedge \neg q)) \vee (r \wedge p \wedge \neg q)$ | De Morgan's |
| $\equiv$ | $(r \wedge (\neg p \vee q)) \vee (r \wedge p \wedge \neg q)$ | De Morgan's |
| $\equiv$ | $(r \wedge (\neg p \vee q)) \vee (r \wedge (p \wedge \neg q))$ | Associative |
| $\equiv$ | $r \wedge ((\neg p \vee q) \vee (p \wedge \neg q))$ | Distributive |
| $\equiv$ | $r \wedge ((\neg p \vee q) \vee \neg(\neg(p \wedge \neg q)))$ | Double negation |
| $\equiv$ | $r \wedge ((\neg p \vee q) \vee \neg(\neg p \vee q)))$ | De Morgan's |
| $\equiv$ | $r \wedge T$ | Negation |
| $\equiv$ | $r$ | Identity |
| $\rightarrow$ | $r \vee s$ | Addition |

**Q. 4.** (16 points) Consider sets $A$ and $B$. Prove or disprove the following.

(1) $\mathcal{P}(A \times B) = \mathcal{P}(B \times A)$.

(2) $(A \oplus B) \oplus B = A$, where $A \oplus B$ denotes the set containing those elements in either $A$ or $B$, but not both.

(3) For any function $f : A \rightarrow B$, $f(S \cap T) = f(S) \cap f(T)$, for any two sets $S, T \subseteq A$.

(4) For function $f : A \rightarrow B$, suppose its inverse function $f^{-1}$ exists. $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$, for any $S, T \subseteq B$.

**Solution:**

(1) This statement is false. Consider a counterexample $A = \{1\}$ and $B = \{2\}$. Thus, $A \times B = \{(1, 2)\}$ and $B \times A = \{(2, 1)\}$. Hence, $\mathcal{P}(A \times B) = \{\emptyset, (1, 2)\}$ and $\mathcal{P}(B \times A) = \{\emptyset, (2, 1)\}$. Since $(1, 2) \in \mathcal{P}(A \times B)$ and $(1, 2) \notin \mathcal{P}(B \times A)$, $\mathcal{P}(A \times B) = \mathcal{P}(B \times A)$ does not hold.

(2) This statement is true. This can be proven using membership table.

| $A$ | $B$ | $A \oplus B$ | $(A \oplus B) \oplus B$ |
|---|---|---|---|
| 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 |

(3) The statement is false. A counterexample is: $f(n) = n^2$ for $A = \mathbf{R}$ and $B = \mathbf{R}^+$. Consider $S = \{1\}$ and $T = \{-1\}$. Then, $f(S) = \{1\}$ and $f(T) = \{1\}$. Thus, $f(S) \cap f(T) = \{1\}$. However, $S \cap T = \emptyset$ and hence $f(S \cap T) = \emptyset$.

(4) This statement is true. Since the inverse function $f^{-1}$ exists, $f$ must be a bijection, i.e., it is both one-to-one and onto. Thus, $f^{-1}$ is also a bijection. We complete the proof by showing that $f^{-1}(S \cap T)$ and $f^{-1}(S) \cap f^{-1}(T)$ are subsets of each other:

- $f^{-1}(S \cap T) \subseteq f^{-1}(S) \cap f^{-1}(T)$: For any $x \in f^{-1}(S \cap T)$, there exists a $y$ such that $y \in S \cap T$ and $f^{-1}(y) = x$. Thus, we have $y \in S$ and $y \in T$. This implies that $x \in f^{-1}(S)$ and $x \in f^{-1}(T)$. Hence, $x \in f^{-1}(S) \cap f^{-1}(T)$.
- To prove $f^{-1}(S) \cap f^{-1}(T) \subseteq f^{-1}(S \cap T)$: If $x \in f^{-1}(S) \cap f^{-1}(T)$, then $x \in f^{-1}(S)$ and $x \in f^{-1}(T)$. Then, there exists $y_1 \in S$ and $y_2 \in T$ such that $f^{-1}(y_1) = x$ and $f^{-1}(y_2) = x$. Since $f^{-1}$ is a bijection, it is one-to-one. Thus, $y_1 = y_2 \in S \cap T$. This implies that $x \in f^{-1}(S \cup T)$.

**Q. 5.** (10 points) Prove or disprove that there exists an infinite set $A$ such that $|A| < |\mathbf{Z}^+|$.

**Solution:** This statement is false. Suppose there exists an infinite set $A$ such that $|A| < |\mathbf{Z}^+|$. This means that $|A| \leq |\mathbf{Z}^+|$ and $|A| \neq |\mathbf{Z}^+|$.

- Since $|A| \neq |\mathbf{Z}^+|$, there does not exist any one-to-one correspondence that maps from $A$ to $\mathbf{Z}^+$. Thus, $A$ cannot be countable infinite.
- Since $|A| \leq |\mathbf{Z}^+|$, there exists a one-to-one function maps from $A$ to $\mathbf{Z}^+$. There is a subset $S \subset \mathbf{Z}^+$ such that there exists a one-to-one correspondence that maps from $A$ to $S$. Since the subset of a countable set is also countable, $S$ is countable. Thus, $S$ is either finite or there exists a one-to-one correspondence from $S$ to $\mathbf{Z}^+$. This leads to the fact that $A$ is either finite or countable infinite.

Thus, contradiction occurs. This complete the disprove.

**Q. 6.** (10 points) Order the following functions by asymptotic growth rates, that is, list them as $f_1(n), f_2(n), \ldots, f_6(n)$, such that $f_i(n) = O(f_{i+1}(n))$ for all $i$. Then, explain your answer related to the first pair, i.e., $f_1(n)$ and $O(f_2(n))$. (Note: providing the explanation of the first pair is sufficient. There is no need to explain all pairs.)

$$2^n, n^{20}, n^2(\log n)^{20}, (n!)^5, (\log n)^{\log\log n}, \log(n^n),$$

where the base of the logarithm is 2.

**Solution:**

$$(\log n)^{\log\log n}, \log(n^n), n^2(\log n)^{20}, n^{20}, 2^n, (n!)^5$$

To prove $(\log n)^{\log\log n} = O(\log(n^n))$, let $n = 2^{2^k}$, then we need to show:

$$(\log 2^{2^k})^{\log\log 2^{2^k}} = O(2^{2^k}\log(2^{2^k})).$$

As a result, we need to show $(2^k)^k = O(2^{2^k}2^k)$, i.e., $2^{k^2} = O(2^{2^k+k})$. Equation $2^{k^2} = O(2^{2^k+k})$ is true, since $2^{k^2} \leq 2^{2^k+k}$ for all $k \geq 0$.

**Q. 7.** (12 points) There are a group of people. If we count them by 2's, we have 1 left over; by 3's, we have nothing left; by 4, we have 1 left over; by 5, we have 4 left over; by 6, we have 3 left over; by 7, we have nothing left; by 8, we have 1 left over; by 9, nothing is left. How many people are there? Give the details of your calculation.

**Solution:** This is equivalent to solve the following system of congruences:

$$\begin{aligned}
x &\equiv 1 \pmod 2\\
x &\equiv 0 \pmod 3\\
x &\equiv 1 \pmod 4\\
x &\equiv 4 \pmod 5\\
x &\equiv 3 \pmod 6\\
x &\equiv 0 \pmod 7\\
x &\equiv 1 \pmod 8\\
x &\equiv 0 \pmod 9.
\end{aligned}$$

Since $x \equiv 3 \pmod 6$, we have $x = 6k + 3$ and further have $x \equiv 1 \pmod 2$ and $x \equiv 0 \pmod 3$. Thus, $x \equiv 3 \pmod 6$ is redundant in the system and can be ignored. Note that $x \equiv 1 \pmod 8$ implies both $x \equiv 1 \pmod 2$ and $x \equiv 1 \pmod 4$, and $x \equiv 0 \pmod 9$ implies $x \equiv 0 \pmod 3$. We thus have an equivalent but refreshed system of congruences as:

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 0 \pmod 7 \\ x &\equiv 1 \pmod 8 \\ x &\equiv 0 \pmod 9. \end{aligned}$$

All the $m_i$'s are pairwise relatively prime, and we are able to use Chinese Remainder Theorem or back substitution to solve this system of congruences. Note that $m = 5 \cdot 7 \cdot 8 \cdot 9 = 2520$, $M_1 = 7 \cdot 8 \cdot 9 = 504$, $M_2 = 5 \cdot 8 \cdot 9 = 360$, $M_3 = 5 \cdot 7 \cdot 9 = 315$, and $M_4 = 5 \cdot 7 \cdot 8 = 280$. By extended Euclidean algorithm, we have $y_1 = 4$, $y_2 = 5$, $y_3 = 3$ and $y_4 = 1$. Then by Chinese Remainder Theorem, we have the solution is

$$x \equiv 4 \cdot 504 \cdot 4 + 0 + 1 \cdot 315 \cdot 3 + 0 \pmod{2520} \equiv 1449 \pmod{2520}.$$

**Q. 8.** (12 points) Compute the following without calculator and explain your answer.

(1) $(33^{15} \mod 32)^3 \mod 15$

(2) $\gcd(210, 1638)$

(3) $34x \equiv 77 \pmod{89}$

(4) The last decimal digit of $3^{1000}$ (Hint: Fermat's little theorem)

**Solution:**

(1) This is mainly computed based on Corollary 2 on page 242, i.e., $ab \mod m = ((a \mod m)(b \mod m)) \mod m$. It is perfectly fine if the student does not mention this corollary.

$$\begin{aligned} & (33^{15} \mod 32)^3 \mod 15 \\ = \ & ((33 \mod 32)^{15} \mod 32)^3 \mod 15 \\ = \ & (1 \mod 32)^3 \mod 15 \\ = \ & 1 \mod 15 \\ = \ & 1 \end{aligned}$$

(2) Using Euclidean Algorithm

$$\begin{aligned} 1638 &= 210 \cdot 7 + 168 \\ 210 &= 168 \cdot 1 + 42 \\ 168 &= 42 \cdot 4 \end{aligned}$$

Thus, $\gcd(210, 1638) = 42$.

(3) Consider the inverse $\bar{a}$ such that $\bar{a} \cdot 34 \equiv 1 \pmod{89}$. We use the extended Euclidean to solve $\bar{a}$. In particular,

$$\begin{aligned} 89 &= 34 \cdot 2 + 21 \\ 34 &= 21 \cdot 1 + 13 \\ 21 &= 13 \cdot 1 + 8 \\ 13 &= 8 \cdot 1 + 5 \\ 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 1 \end{aligned}$$

Thus,

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (5 - 3 \cdot 1) \cdot 1 && = -5 \cdot 1 + 3 \cdot 2 \\ &= -5 \cdot 1 + (8 - 5 \cdot 1) \cdot 2 && = 8 \cdot 2 - 5 \cdot 3 \\ &= 8 \cdot 2 - (13 - 8 \cdot 1) \cdot 3 && = -13 \cdot 3 + 8 \cdot 5 \\ &= -13 \cdot 3 + (21 - 13 \cdot 1) \cdot 5 && = 21 \cdot 5 - 13 \cdot 8 \\ &= 21 \cdot 5 - (34 - 21 \cdot 1) \cdot 8 && = -34 \cdot 8 + 21 \cdot 13 \\ &= -34 \cdot 8 + (89 - 34 \cdot 2) \cdot 13 && = 89 \cdot 13 - 34 \cdot 34 \end{aligned}$$

Thus, we have $-34 \cdot 34 \bmod 89 = 1$, which implies that $55 \cdot 34 \bmod 89 = 1$. Thus, $\bar{a} = 55$. As a result, we have $x \equiv 55 \cdot 77 \pmod{89} \equiv 52 \pmod{89}$.

(4) The last decimal digit of $3^{1000}$ is equivalent to computing $3^{1000} \bmod 10$. By Fermat's little theorem, we have $3^4 \equiv 1 \pmod 5$. Thus, $3^{1000} \equiv 3^{4 \times 250} \equiv 1 \pmod 5$. In addition, $3^{1000} \equiv 1 \pmod 2$, because $3^{1000}$ has only 3 as its factor and hence is an odd number. Then, since system $3^{1000} \equiv 1 \pmod 5$ and $3^{1000} \equiv 1 \pmod 2$ is equivalent to $3^{1000} \equiv 1 \pmod{10}$, we have $3^{1000} \bmod 10 = 1 \bmod 10 = 1$.

**Q. 9.** (8 points) Prove that if $2^m + 1$ is an odd prime, then $m$ does not has any odd factor that is greater than one. (Note: $x^m + 1 = (x^k + 1)(x^{k(t-1)} - x^{k(t-2)} + ... - x^k + 1)$, where $m = kt$ and $t$ is odd.)

**Solution:** Since $2^m + 1$ is an odd prime, then $m \geq 1$. When $m = 1$, $m$ does not have any odd factor that is greater than one. Suppose $m > 1$ and $m$ has at least an odd factor that is greater than one. Let $t > 1$ denote such an odd factor. Let $k = m/t$. Thus,

$$2^m + 1 = 2^{kt} + 1 = (x^k + 1)(x^{k(t-1)} - x^{k(t-2)} + ... - x^k + 1).$$

Since $t > 1$, $x^k + 1 < 2^m + 1$. This implies that

$$(x^{k(t-1)} - x^{k(t-2)} + ... - x^k + 1) > 1.$$

Thus, $2^m + 1$ is a product of two integers that are larger than one, which means that $2^m + 1$ cannot be a prime.

**Q. 10.** (6 points) Recall the RSA public key cryptosystem. Consider prime numbers $p = 89$ and $q = 61$. Answer whether the following pairs of public key $(n, e)$ and private key $d$ are valid (whether the pair satisfies the required properties) or not, and explain your answer.

(1) $n = 5429$, $e = 61$; $d = 4501$

(2) $n = 5429$, $e = 89$; $d = 2829$

(3) $n = 5429$, $e = 30$; $d = 1568$

**Solution:** Since $p = 89$ and $q = 61$, we have $n = pq = 5429$. Recall that the conditions for a pair to be correct is

- $n = pq$
- $\gcd(e, (p-1)(q-1)) = 1$
- $ed \equiv 1 \pmod{(p-1)(q-1)}$

According to these conditions:

(1) This is valid.

(2) This is not valid, because $ed \equiv 1 \pmod{(p-1)(q-1)}$ does not hold.

(3) This is not valid, because $\gcd(e, (p-1)(q-1)) = 1$ does not hold.

**Q. 11.** (Optional, bonus 10 points) The following ciphertext is encrypted with one of the encryption methods we taught in lecture. Try to recover the plaintext and describe the method (and parameters) used for encryption. Please explain the process how you get the answer. For example, if you write a program, please provide the code (uploading the source file as well). If you make a guess and use number theory, please provide the details.

"Qy qaq iloiyu uiwx lwhc oiu lwgc i nat ah srasalizcu. Yae vcjcp gvao oriz yae'pc mavvi mcz."

**Solution:** "My mom always said life was like a box of chocolates. You never know what you're gonna get" (1 point). It is encrypted with affine cipher with $a = 5$ and $b = 8$ (1 point). Explanation (8 points):

- The student wrote a program: Run the program. If it works well (i.e., inputting the ciphertext can lead to an output of the plaintext), then he or she can get the point. Note: If the program can output the correct sentence, but he or she did not write the sentence in the homework. It is ok to give he or she the above 1 point. So as $a$ and $b$.

- The student used number theory techniques (on page 296 in our textbook): He or she needs to show $p \equiv \bar{a}(c - b) \pmod{26}$, where $c$ is a letter in ciphertext and $p$ is a letter in plaintext.

- The student used approaches other than programming and number theory: If the explanation makes sense, he or she can get the points. For example, the student may guess "yae'pc" as "you're" based on English language using, and solve $a$ and $b$ using linear equation systems. Note that the explanation must be complete and make sense.