The questions below are intended for practice only. It is your responsibility to study all material covered in this course, whether represented here or not.

1. Be able to state and use any named propositions and definitions.

Solution: STUDY!

2. Consider the propositional statement $((P \to Q) \leftrightarrow R) \wedge (R \vee (Q \oplus (\neg P)))$.

   (a) Build a truth table for the statement.

Solution:

P	Q	R	$((P \to Q)$	$\leftrightarrow$	$R)$	$\wedge$	$(R$	$\vee$	$(Q$	$\oplus$	$(\neg P)))$
T	T	T	T	T		$\boxed{T}$		T		T	F
T	T	F	T	F		$\boxed{F}$		T		T	F
T	F	T	F	F		$\boxed{F}$		T		F	F
T	F	F	F	T		$\boxed{F}$		F		F	F
F	T	T	T	T		$\boxed{T}$		T		F	T
F	T	F	T	F		$\boxed{F}$		F		F	T
F	F	T	T	T		$\boxed{T}$		T		T	T
F	F	F	T	F		$\boxed{F}$		T		T	T

   (b) Write the statement in Disjunctive Normal Form.

Solution: Letting $\mathbb{A}$ denote the statement above we have

$$\text{dnf}(\mathbb{A}) = [P \wedge Q \wedge R] \vee [(\neg P) \wedge Q \wedge R] \vee [(\neg P) \wedge (\neg Q) \wedge R].$$

   (c) Write the statement in Conjunctive Normal Form.

Solution: Letting $\mathbb{A}$ denote the statement above we have

$$\text{cnf}(\mathbb{A}) = [(\neg P) \vee (\neg Q) \vee R] \wedge [(\neg P) \vee Q \vee (\neg R)] \wedge [(\neg P) \vee Q \vee R] \wedge [P \vee (\neg Q) \vee R] \wedge [P \vee Q \vee R]$$

3. Let $a, b, c, d \in \mathbb{Z}$ and let $m \in \mathbb{Z}_{>0}$.

   (a) Prove that if $a \mid c$ and $b \mid d$, then $ab \mid cd$.

Solution: Let $a, b, c, d \in \mathbb{Z}$ be arbitrary and suppose $a \mid c$ and $b \mid d$. By definition of divisibility we have $c = ak$ and $d = bn$ for some $k, n \in \mathbb{Z}$; thus $cd = (ak)(bn) = ab(kn)$, and $kn \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$. Hence $ab \mid cd$ by definiiton of divisibility.

   (b) Prove that if $a \mid b$ and $a \mid c$, then $a \mid bs + ct$ for all $s, t \in \mathbb{Z}$.

Solution: Let $a, b, c \in \mathbb{Z}$ be arbitrary and assume $a \mid b$ and $a \mid c$, and let $s, t \in \mathbb{Z}$ be arbitrary. Now $b = au$ and $c = av$ for some $u, v \in \mathbb{Z}$ by definition of divisibility. Thus we compute $bs + ct = (au)s + (av)t = a(us) + a(vt) = a(us + vt)$. Let $k := us + vt$ and note $k \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$. Hence $bs + ct = ak$ and $a \mid (bs + ct)$ by definition.

4. This question concerns equivalence relations.

   (a) Let $f\colon S \to T$ be an arbitrary function. Is $R = \{(a, b) \in S \times S : f(a) = f(b)\}$ an equivalence relation on S? Prove or disprove.

Solution: This is an equivalence relation (in fact, this was on a quiz).
Let $f : S \to T$ be an arbitrary function. We must verify reflexivity, symmetry, and transitivity.
Reflexive: Let $x \in S$ be arbitrary. As f is a function, we have $f(x) = f(x)$. Hence $x \ R \ x$.
Symmetric: Let $x, y \in S$ be arbitrary and suppose $x \ R \ y$. Thus $f(x) = f(y)$, yielding $f(y) = f(x)$ by symmetry of equality. Hence $y \ R \ x$.
Transitive: Let $x, y, z \in S$ be arbitrary and suppose $x \ R \ y$ and $y \ R \ z$. By definition of R we see $f(x) = f(y)$ and $f(y) = f(z)$; thus $f(x) = f(z)$ by transitivity of equality and $x \ R \ z$.
Hence R is an equivalence relation, as claimed.

   (b) Is $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x^2 + y^2 = 0\}$ an equivalence relation? Prove or disprove.

Solution: This is not an equivalence relation; it is not reflexive ($(1, 1) \notin R$), but it is both symmetric and transitive.

   (c) Is $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x^2 = y\}$ an equivalence relation? Prove or disprove.

Solution: This is not an equivalence relation; it is not reflexive ($(2, 3) \notin R$), not symmetric ($(2, 4) \in R$ but $(4, 2) \notin R$), and not transitive ($(2, 4) \in R$ and $(4, 16) \in R$, but $(2, 16) \notin R$).

   (d) Is $R = \{(x, y) : xy \geq 0\}$ an equivalence relation on $\mathbb{Z} \setminus \{0\}$? Prove or disprove.

Solution: This is an equivalence relation.
Reflexive: For all $x \in \mathbb{Z} \setminus \{0\}$ we have $x \cdot x = x^2 \geq 0$ by elementary properties of arithmetic. Hence $x \ R \ x$ as desired.
Symmetric: Let $x, y \in \mathbb{Z} \setminus \{0\}$ have $x \ R \ y$. Thus $xy \geq 0$ by definition of R; moreover $yx = xy \geq 0$ yields $y \ R \ x$ as desired.
Transitive: Let $x, y, z \in \mathbb{Z} \setminus \{0\}$ satisfy $x \ R \ y$ and $y \ R \ z$. Thus $xy \geq 0$ and $yz \geq 0$; by elementary properties of arithmetic $0 \leq (xy)(yz) = xy^2z$. As $y \neq 0$ we have $0 < y^2$, and we may divide through by y^2 to obtain $0 = \frac{0}{y^2} \leq \frac{xy^2z}{y^2} = xz$; hence $x \ R \ z$ as desired.

5. Let $f\colon A \to B$ and $g\colon B \to C$ be functions.

   (a) Prove that if $g \circ f$ is injective, then f is injective.

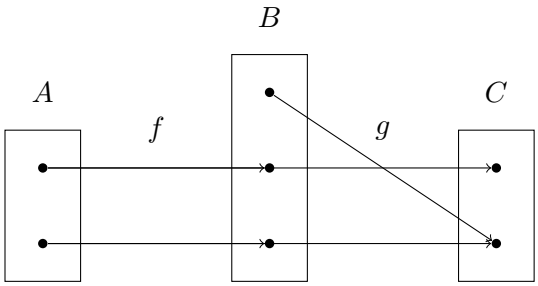
Solution: Let $f\colon A \to B$ and $g\colon B \to C$ be functions with $g \circ f$ injective. Let $x, y \in A$ be arbitrary and suppose $f(x) = f(y)$. Thus $(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y)$ by definition of the composite function. Hence $x = y$ and f is injective.

(b) Prove that if $g \circ f$ is surjective, then g is surjective.

Solution: Let $f\colon A \to B$ and $g\colon B \to C$ be functions with $g \circ f$ surjective. Let $y \in C$ be arbitrary. By surjectivity of $g \circ f$, there is an $a \in A$ with $y = (g \circ f)(a) = g(f(a))$. Letting $x = f(a)$, we note $x \in B = \mathrm{dom}(g)$ has $g(x) = y$; hence g is surjective.

(c) Give an example of functions f and g as above with $g \circ f$ a bijection, but neither f nor g is a bijection (a clear picture is an acceptable answer).

Solution: There are many. One of them is depicted below.



6. This question concerns induction.

(a) Prove $\displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$ for all $n \geq 1$.

Solution: We proceed by induction on n.
Base Case: If $n = 1$ we have $1^3 = 1 = 1^2 = (\frac{2}{2})^2 = (\frac{1(1+1)}{2})^2$, as desired.
Inductive Step: Assume $\displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$ for some $n \geq 1$. We compute

$$\begin{aligned}\sum_{k=1}^{n+1} k^3 &= \sum_{k=1}^{n} k^3 + (n+1)^3 \\ &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 \\ &= (n+1)^2 \cdot \frac{n^2 + 4(n+1)}{4} \\ &= \frac{(n+1)^2(n+2)^2}{4} \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2.\end{aligned}$$

Hence the original statement holds by weak mathematical induction.

(b) Prove $\displaystyle\sum_{k=0}^{n} 2F_{3k+3} = F_{3n+5} - 1$ for all $n \geq 0$ where F_k is the k^{th} Fibonacci number.

Solution: We proceed by induction on n.

Base Case: If $n = 0$ we have $2F_3 = 2 \cdot 2 = 4 = 5 - 1 = F_5 - 1$, as desired.

Inductive Step: Assume $\sum_{k=0}^{n} 2F_{3k+3} = F_{3n+5} - 1$ for some $n \geq 0$. We compute

$$\begin{aligned}\sum_{k=0}^{n+1} 2F_{3k+3} &= \sum_{k=0}^{n} 2F_{3k+3} + 2F_{3n+6} \\ &= (F_{3n+5} - 1) + 2F_{3n+6} \\ &= (F_{3n+6} + (F_{3n+5} + F_{3n+6})) - 1 \\ &= (F_{3n+6} + F_{3n+7}) - 1 \\ &= F_{3n+8} - 1 \\ &= F_{3(n+1)+5} - 1.\end{aligned}$$

Hence the original statement holds by weak mathematical induction.

(c) Prove $\sum_{k=1}^{n} F_k^2 = F_n F_{n+1}$ for all $n \geq 1$ where F_k is the k^{th} Fibonacci number.

Solution: We proceed by induction on n.

Base Case: If $n = 1$ we have $F_1^2 = 1^2 = 1 \cdot 1 = F_1 F_2$, as desired.

Inductive Step: Assume $\sum_{k=1}^{n} F_k^2 = F_n F_{n+1}$ for some $n \geq 1$. We compute

$$\begin{aligned}\sum_{k=1}^{n+1} F_k^2 &= \sum_{k=1}^{n} F_k^2 + F_{n+1}^2 \\ &= F_n F_{n+1} + F_{n+1}^2 \\ &= F_{n+1}(F_n + F_{n+1}) \\ &= F_{n+1} F_{n+2}.\end{aligned}$$

Hence the original statement holds by weak mathematical induction.

7. Let $A_0, A_1, \cdots, A_n$ be sets and $f_i \colon A_{i-1} \to A_i$ a bijection for all $1 \leq i \leq n$. Prove that $f_n \circ f_{n-1} \circ \cdots \circ f_1$ is also bijective.

Solution: Let $A_0, A_1, \cdots, A_n$ be sets and $f_i \colon A_{i-1} \to A_i$ a bijection for all $1 \leq i \leq n$. We proceed by induction on n.

Base Case: If $n = 1$, then the statement holds as $f_n \circ \cdots \circ f_1 = f_1$ is a bijection by assumption.

Inductive Step: Suppose that the result holds for some $n \geq 1$. Now we must show that the result holds for $n+1$ as well. Let $g = f_n \circ \cdots \circ f_1 \colon A_0 \to A_n$. Thus we may write $f_{n+1} \circ f_n \circ \cdots \circ f_2 \circ f_1 = f_{n+1} \circ g$. Note g is a bijection by the inductive hypothesis. We must show $f_{n+1} \circ g$ is a bijection.

To see that $f_{n+1} \circ g$ is injective, let $x, y \in A_0$ be arbitrary with $f_{n+1}(g(x)) = (f_{n+1} \circ g)(x) = (f_{n+1} \circ g)(y) = f_{n+1}(g(y))$. Thus $g(x) = g(y)$ as f_{n+1} is injective; thus $x = y$ as g is injective. Hence $f_{n+1} \circ g$ is injective.

To see that $f_{n+1} \circ g$ is surjective, let $y \in A_{n+1}$ be arbitrary. By surjectivity of f_{n+1}, there is a $z \in A_n$ with $f_{n+1}(z) = y$; by surjectivity of g there is an $x \in A_0$ with $g(x) = z$. Hence $(f_{n+1} \circ g)(x) = f_{n+1}(g(x)) = f_{n+1}(z) = y$ and $f_{n+1} \circ g$ is surjective, as desired.

We conclude that the original statement holds by weak mathematical induction.

8. Solve $250x \equiv 93 \pmod{927}$ for an integer x with $0 \leq x \leq 927$.

Solution: First we compute $\gcd(250, 927)$ via Euclid's Algorithm:

$$\begin{aligned} 927 &= 250 \cdot 3 + 177 \\ 250 &= 177 \cdot 1 + 73 \\ 177 &= 73 \cdot 2 + 31 \\ 73 &= 31 \cdot 2 + 11 \\ 31 &= 11 \cdot 2 + 9 \\ 11 &= 9 \cdot 1 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Next we back substitute to write $1 = \gcd(250, 927)$ as a linear combination of 250 and 927:

$$\begin{aligned} 1 &= 9 + 2(-4) \\ &= 9 + (11 + 9(-1))(-4) \\ &= 11(-4) + 9(5) \\ &= 11(-4) + (31 + 11(-2))(5) \\ &= 31(5) + 11(-14) \\ &= 31(5) + (73 + 31(-2))(-14) \\ &= 73(-14) + 31(33) \\ &= 73(-14) + (177 + 73(-2))(33) \\ &= 177(33) + 73(-80) \\ &= 177(33) + (250 + 177(-1))(-80) \\ &= 250(-80) + 177(113) \\ &= 250(-80) + (927 + 250(-3))(113) \\ &= 250(-419) + 927(113) \end{aligned}$$

Hence the inverse of 250 is $-419 \equiv= 508 \pmod{927}$. Finally, $250x \equiv 20 \pmod{927}$ when

$$x \equiv 508(250x) \equiv 508 \cdot 20 = 10160 \equiv 10160 - 927(10) = 10160 - 9270 = 890 \pmod{927}.$$

9. This question concerns the RSA Cryptosystem. Let $p = 13$, $q = 17$, and $e = 19$.
   (a) Encrypt the message $m = 15$.

Solution: Note $n = 13 * 17 = 221$ and that we have the following congruences (we will use these below; I found that I needed these by doing the computation out...):

$$\begin{aligned} 15^2 = 225 &\equiv 4 \pmod{221} \\ 4^4 = 256 &\equiv 35 \pmod{221} \\ 300 &\equiv 79 \pmod{221} \\ 245 &\equiv 24 \pmod{221} \\ 79 \cdot 24 = 221 \cdot 8 + 128 &\equiv 128 \pmod{221} \end{aligned}$$

Encrypting we obtain

$$\begin{aligned} m^e = 15^{19} = (15^2)^9 \cdot 15 & \\ &\equiv 4^9 \cdot 15 = (4^4)^2 \cdot 4 \cdot 15 \\ &\equiv 35^2 \cdot 4 \cdot 15 = 2^2 \cdot 3 \cdot 5^3 \cdot 7^2 \\ &= 300 \cdot 245 \equiv 79 \cdot 24 \\ &\equiv 128 \pmod{221} \end{aligned}$$

(b) Decrypt the message $\widehat{m} = 7$.

Solution: First we must compute the private key d. We apply Euclid's (Extended) Algorithm to compute $\gcd(e, (p-1)(q-1)) = \gcd(19, 12 \cdot 16) = \gcd(19, 192)$:

$$\begin{aligned} 192 &= 19 \cdot 10 + 2 \\ 19 &= 2 \cdot 9 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Back substituting we obtain $1 = 19 + 2(-9) = 19 + (192 + 19(-10))(-9) = 19(91) + 192(-9)$, and thus the private key is $d = 91$. We notice the following congruences modulo 221:

$$\begin{aligned} 7^5 = 343 \cdot 49 \equiv 122 \cdot 49 = 854 \cdot 7 \equiv 191 \cdot 7 = 1377 = 221 \cdot 6 + 11 &\equiv 11 \pmod{221} \\ 11^3 = 1331 = 221 \cdot 6 + 5 &\equiv 5 \pmod{221} \\ 5^5 = 625 \cdot 5 \equiv 183 \cdot 5 = 915 = 221 \cdot 4 + 31 &\equiv 31 \pmod{221} \end{aligned}$$

Finally we decrypt $\widehat{m} = 7$ as follows:

$$\begin{aligned} \widehat{m}^d = 7^{91} = (7^5)^{18} \cdot 7 &\equiv 11^{18} \cdot 7 = (11^3)^6 \cdot 7 \\ &\equiv 5^6 \cdot 7 = 5^5 \cdot 5 \cdot 7 \\ &\equiv 31 \cdot 5 \cdot 7 = 155 \cdot 7 = 1085 = 221 * 4 + 201 \\ &\equiv 201 \pmod{221} \end{aligned}$$