15-151 & 21-128 Additional Practice Final - Solution

Problem 1:

Prove that every integer greater than 55 can be written as the sum of three composite numbers.

Solution (Proof by Construction).

Note that $6 = 2 \times 3$ and $9 = 3 \times 3$ are composite by definition of composite.

It can be shown that any even integer $m > 2$ is composite. Suppose $m = 2k, k \in \mathbb{Z}^+, k > 1$. Then m is the product of two non-unit integers.

Let n be any integer, $n > 55$.

Case 1: n is even

- By definition of even, $n = 2k$ for some $k \in \mathbb{Z}$. Consider the numbers $6, 6, 2(k-6)$. We know that 6 is composite. Since $2k > 55, 2(k-6) > 43$. Then $2(k-6) > 2$, and by closure $k-6$ is an integer. This implies that $2(k-6)$ is composite since it is even.
- Because $6 + 6 + 2(k-6) = 2k = n$, these are three composite integers that sum to n.

Case 2: n is odd

- By definition of odd, $n = 2k+1$ for some $k \in \mathbb{Z}$. Consider the numbers $6, 9, 2(k-7)$. We know that both 6 and 9 are composite. Since $2k+1 > 55, 2(k-7) > 40$. Then $2(k-7) > 2$, and by closure $k-7$ is an integer. This implies that $2(k-7)$ is composite since it is even.
- Because $6 + 9 + 2(k-7) = 2k+1 = n$, these are three composite integers that sum to n.

In either case, n can be represented as a sum of three composite numbers. Since our choice of n was arbitrary, it holds for all integers $n > 55$.

Problem 2:

Prove that for any positive integer n,

$$\frac{n(n+1)(2n+1)}{6}$$

is an integer.

Solution (Proof by Induction).

Note that the statement is equivalent to proving that for all $n \in \mathbb{Z}^+$, $\frac{n(n+1)(2n+1)}{6} = k$ for some $k \in \mathbb{Z}$. Then $n(n+1)(2n+1) = 6k$, and it suffices to show that $6 \mid n(n+1)(2n+1)$.

For all $n \in \mathbb{Z}^+$, let P(n) be the statement

$$6 \mid n(n+1)(2n+1)$$

Base Case

- P(1) is true: $1(1+1)(2(1)+1) = 6, 6 \mid 6$.

Induction Step

- Suppose P(k) is true for some $k \in \mathbb{Z}^+$. We claim that P(k+1) is true:
- By expanding, $(k+1)(k+2)(2k+3) = 2k^3 + 9k^2 + 13k + 6$.
- By the induction hypothesis, we know that $6 \mid k(k+1)(2k+1)$. Then $k(k+1)(2k+1) = 2k^3 + 3k^2 + k = 6l$ for some $l \in \mathbb{Z}$.
- By subtracting $6l$, we have $2k^3+9k^2+13k+6-(2k^3+3k^2+k) = 6k^2+12k+6 = 6(k^2+2k+1) = 6m$, $m = (k^2+2k+1), m \in \mathbb{Z}$. Then $(k+1)(k+2)(2k+3) = 6(l+m)$ and is therefore also divisible by 6.

By induction, the statement is proven.

Problem 3:

Let

$$X = \sum_{k=1231}^{1985} F_k$$

where F_k is the k^{th} Fibonacci number.

It can be shown that X can be written in the form $F_i - F_j$ for some non-negative integers i and j. Find any such pair (i, j).

Solution (Proof by Induction).

By writing out the successive sums of Fibonacci numbers

Fibonacci Number	0	1	1	2	3	5	8	13	21	34
Running Sum	0	1	2	4	7	12	20	33	54	88

we hypothesize that for all $n \in \mathbb{N}$,

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

We proceed by induction. For all $n \in \mathbb{N}$, let P(n) be the above statement.

Base Case

- $n = 0$, $F_0 = 0 . F_2 - 1 = 1 - 1 = 0$. P(0) is true.

Induction Step

- Assume that for $k \in \mathbb{N}$, P(k) is true.
- We claim P(k+1) is true:
- $\sum_{i=0}^{k+1} F_i = \sum_{i=0}^{k} F_i + F_{k+1} = F_{k+1} + F_{k+2} - 1$ by induction hypothesis. Then this is equal to $F_{k+3} - 1$ by the Fibonacci identity and we are done.

We can write

$$\begin{aligned} X = &\sum_{k=1231}^{1985} F_k \\ = &\sum_{k=0}^{1985} F_k - \sum_{k=0}^{1230} F_k \\ = &(F_{1987} - 1) - (F_{1232} - 1) \\ = &F_{1987} - F_{1232}. \end{aligned}$$

So (1987, 1232) is one such pair.

Problem 4:

Show that

$$\forall a, b \in \mathbb{Z}^+, a \leq b \implies \exists k \in \mathbb{Z}^+ \text{ such that } a \bmod k = k \bmod b,$$

but that it is not true that

$$\forall a, b \in \mathbb{Z}^+, \exists k \in \mathbb{Z}^+ \text{ such that } a \bmod k = k \bmod b \implies a \leq b.$$

Solution (Direct Proof).

We first prove the first statement. Fix $a, b \in \mathbb{Z}^+$ such that $a \leq b$.

Case 1: $a \leq b$

- Let $k = a + b$.
- Then $a \bmod k = a \bmod (a + b) = a$, since $a < a + b$, and a, b are both positive.
- Also, $k \bmod b = (a + b) \bmod b = a$. So $a \bmod k = k \bmod b$.

Case 2: $a = b$

- Let $k = a$.
- Then $a \bmod k = a \bmod a = 0$.
- Also, $k \bmod b = a \bmod b = a \bmod a = 0$ since $a = b$. So likewise $a \bmod k = k \bmod b$.

We disprove the second statement with a counter-example.

Consider $a = 4, b = 2$. Then we find that with $k = 2$, $4 \bmod 2 = 2 \bmod 2$, but $4 > 2$.

Problem 5:

You have a deck of 20 numbered cards, with card 1 on top, card 2 being 2^{nd} from the top, and so on, up to card 20 being 20^{th} from the top (at the bottom).

You shuffle them, but in a predictable manner: the card currently k^{th} from the top in the deck becomes p_k^{th} from the top after one shuffle, where $p_1, p_2, \ldots, p_{20}$ is a permutation of the positive integers not exceeding 20.

It can be shown that, regardless of p, there always exists an $m \in \mathbb{Z}^+$ such that doing m shuffles gives back the original arrangement.

Across all 20! permutations $p_1, p_2, \ldots, p_{20}$, what is the maximum number of shuffles required for a deck of 20 cards to give back the original arrangement?

Solution.

Let $f(x)$ be the position that the card x^{th} from the top goes to after doing a single shuffle ($f(x) = p_x$). We know from the problem that there will exist a minimum m_x such that $f^{m_x}(x) = x$.

We can also easily verify that $x, f(x), f^2(2), \ldots, f^{m_x-1}(x)$ are all distinct, and that $f^k(x) = f^{k+m_x}(x)$ for all k.

Therefore, consider the set S of all distinct sets T_x, where we consider $T_x = \{x, f(x), f^2(x), \ldots, f^{m_x-1}(x)\}$. Note that $m_x = |T_x|$. Without loss of generality, we write $S = \{T_1, T_2, \ldots, T_k\}$ for some integer $k \geq 1$.

Since every element in [20] must appear in exactly one element T, we have $|T_1|+|T_2|+\cdots+|T_k| = 20$. Also, since for any particular T_x, every element in it will be back to the original every and only every $m_x = |T_x|$ iterations, we need the total number of iterations to be a multiple of $|T_1|, |T_2|, \ldots, |T_k|$. We are concerned with the first time every element in every set is back to the original, so we really want $\text{lcm}(|T_1|, |T_2|, \ldots, |T_k|)$, and we want this to be the maximum possible.

Hence, we reduce the problem to finding the maximum value of $\text{lcm}(n_1, n_2, \ldots, n_k)$ subject to $n_1 + n_2 + \cdots + n_k = 20$ with all $n_i \geq 1$.

Since we can always add arbitrary numbers of $n_i = 1$ without affecting the lcm, we can maximize $\text{lcm}(n_1, n_2, \ldots, n_k)$ subject to $n_1 + n_2 + \cdots + n_k \leq 20$ and all $n_i \geq 2$.

We can find the solution using brute force and some heuristics. We note that n_i should only be of the form p^k for some prime p and $k \geq 1$, since if we can write $n_i = rs$ with integers $r, s \geq 2$ and $gcd(r, s) = 1$, then separating n_i into r and s contributes the same lcm, but with smaller sum (since $r + s \geq rs = n_i$ when $r, s \geq 2$).

We also don't want to include both p^r and p^s with $r < s$ in a set, since $\text{lcm}(p^r, p^s) = p^s$, so p^r does not contribute to the lcm at all.

In essence, we need to choose at most one element from the set $\{2, 4, 8, 16\}$, at most one element from the set $\{3, 9\}$, and any subset of $\{5, 7, 11, 13, 17, 19\}$ such that the product of all elements chosen is maximized, and the sum of all elements chosen is at most 20.

We can list all valid (sum ≤ 20) of $\{5, 7, 11, 13, 17, 19\}$ and their corresponding sums and products:

Subset	**Sum**	**Product**
{}	0	1
{5}	5	5
{5,7}	12	35
{5,11}	16	55
{5,13}	18	65
{7}	7	7
{7,11}	18	77
{7,13}	20	91
{11}	11	11
{13}	13	13
{17}	17	17
{19}	19	19

We can eliminate all non-worthwhile subsets that can never be part of a maximum-product solution; for example, there is never a reason to choose $\{5, 13\}$ as we can always choose $\{7, 11\}$ whic has a larger product and same sum. We can also eliminate $\{13\}$ as we can always pick $\{5, 7\}$ which has a larger product and lower sum.

The only worthwhile subsets sorted by sum are:

Subset	**Sum**	**Product**
{}	0	1
{5}	5	5
{7}	7	7
{11}	11	11
{5,7}	12	35
{5,11}	16	55
{7,11}	18	77
{7,13}	20	91

We can also list all valid and worthwhile combinations of choosing at most one element from $\{2, 4, 8, 16\}$ and choosing at most one element from $\{3, 9\}$:

Subset	**Sum**	**Product**
{}	0	1
{2}	2	2
{3}	3	3
{4}	4	4
{2,3}	5	6
{3,4}	7	12
{3,8}	11	24
{4,9}	13	36
{8,9}	17	72

Now, we can pair every worthwhile subset from the first list with the worthwhile subset from the second list with the largest product that still keeps the total sum of the two sets to be at most 20.

Subset	**Pair**	**Total Sum**	**Total Product**
{}	{8,9}	17	72
{5}	{4,9}	18	180
{7}	{4,9}	20	252
{11}	{3,4}	18	132
{5,7}	**{3,4}**	**19**	**420**
{5,11}	{4}	20	220
{7,11}	{2}	20	154
{7,13}	{}	20	91

As we can observe, the largest possible product is 420, and therefore the maximum number of shuffles required for a deck of 20 cards to give back the original arrangement is 420.

In fact, we can give a permutation that requires 420 shuffles:

$$p = [2, 3, 1, 5, 6, 7, 4, 12, 8, 9, 10, 11, 19, 13, 14, 15, 16, 17, 18, 20]$$

Problem 6:

Call a binary relation R on a set S an *almost equivalence relation* if it satisfies *exactly two* of the properties:

1. Reflexive: $\forall x \in S, x \; R \; x$,
2. Symmetric: $\forall x, y \in S, x \; R \; y \implies y \; R \; x$,
3. Transitive: $\forall x, y, z \in S, (x \; R \; y) \wedge (y \; R \; z) \implies x \; R \; z$.

Define the *opposite* of a binary relation R on a set S as the binary relation R' on S such that

$$\forall x, y \in S, x \; R \; b \iff \neg(a \; R' \; b)$$

Show that, for all sets S, there is no binary relation R on S such that both R and R' are almost equivalence relations.

Solution.

We first prove a few lemmas.

Lemma 1 *For any non-empty set S and symmetric binary relation R on S, $\forall x, y \in S$, $\neg(x \; R \; y) \implies \neg(y \; R \; x)$.*

Proof. Fix any $x, y \in S$ such that $\neg(x \; R \; y)$. Now suppose for the sake of contradiction that $(y \; R \; x)$. Then since R is symmetric, $(x \; R \; y)$. But this is a contradiction.

Lemma 2 *For any non-empty set S and symmetric binary relation R on S, if R is reflexive, then R' is not reflexive.*

Proof. Since R is reflexive, for any $x \in S, x \; R \; x$. But by definition of R' this means that $\neg(x \; R' \; x)$.

Lemma 3 *For any non-empty set S and symmetric binary relation R on S, R is symmetric if and only if R' is symmetric.*

Proof. We consider both directions.

Suppose that R is symmetric. We want to prove that R' is also symmetric.

Fix any $x, y \in S$ such that $x \; R' \; y$. Then by definition of R', $\neg(x \; R \; y)$. Since R is symmetric, we can apply Lemma **??** to obtain $\neg(y \; R \; x)$. But this implies $y \; R' \; x$ by definition of R', and so R' is symmetric.

Suppose that R' is symmetric. We want to prove that R is also symmetric.

Fix any $x, y \in S$ such that $x \; R \; y$. Then by definition of R', $\neg(x \; R' \; y)$. Since R' is symmetric, we can apply Lemma **??** to obtain $\neg(y \; R' \; x)$. But this implies $y \; R \; x$ by definition of R', and so R is symmetric.

Lemma 4 *For any non-empty set S and symmetric binary relation R on S, R=(R')$'$.*

Proof.

Consider any $x, y \in S$.

Case 1: $x\ R\ y$

- By definition of R', $\neg(x\ R'\ y)$. By definition of $(R')'$, $\neg(\neg(x\ (R')'\ y))$. Simplifying the double negative, $x\ (R')'\ y$. Therefore $x\ R\ y \implies x(R')'\ y$.

Case 2: $\neg(x\ R\ y)$

- By definition of R', $x\ R'\ y$. By definition of $(R')'$, $\neg(x\ (R')'\ y)$. Therefore $\neg(x\ R\ y) \implies \neg(x\ (R')'\ y)$.

So for all $x, y \in S$, $x\ R\ y \iff x\ (R')'\ y$, and therefore $R = (R')'$.

We first prove the case where S is empty. Suppose S is empty. Then any binary relation R on S is reflexive, symmetric, and transitive. Then no such R can be an almost equivalence relation. Therefore such an R does not exist.

So S must be non-empty. We consider the following cases:

Case 1: R is reflexive and symmetric, but not transitive

- Since R is reflexive, by Lemma **??**, R' is not reflexive. Therefore R' must be symmetric and transitive (by definition of an almost equivalence relation).

  Case (a): $\forall x, y \in S, x\ R\ y$

  - Fix any $x, y, z \in S$ such that $x\ R\ y$ and $y\ R\ z$.
  - Then based on the assumption of the case, we also have $x\ R\ z$. Therefore R is transitive. This is a contradiction.

  Case (b): $\exists x, y \in S$ such that $\neg(x\ R\ y)$

  - Since R is reflexive, we have $x\ R\ x$.
  - By definition of R', $\neg(x\ R'\ x)$.
  - Since $\neg(x\ R\ y)$, by Lemma 1, we know $\neg(y\ R\ x)$.
  - From the above, based on definition of R', we obtain $x\ R'\ y$ and $y\ R'\ x$.
  - Since R' is transitive, this implies that $x\ R'\ x$. But this is a contradiction with the second line.

Case 2: R is reflexive and transitive, but not symmetric

- Since R is reflexive, by Lemma **??**, R' is not reflexive. By Lemma **??**, R' is also not symmetric. Therefore R' is not an almost equivalence relation. This is a contradiction.

Case 3: R is symmetric and transitive, but not reflexive

- Since R is symmetric, by Lemma **??**, R' is also symmetric.

- Suppose that R' is reflexive. Then by definition of an almost equivalence relation, R' is not transitive.
- Define $Q = R'$. Then $Q' = (R')' = R$ by Lemma **??**. Then Q is reflexive, symmetric, but not transitive. Q' is an almost equivalence relation on S by definition of R. But we showed that this is not possible in Case 1. Therefore, this is a contradiction.
- So R' is not reflexive, and instead R' is transitive.
- Since R is not reflexive, there exists $x \in S$ such that $\neg(x\ R\ x)$. Fix such an x.
- Suppose that there exists $y \in S$ such that $x \neq y$ and $x\ R\ y$. Since R is symmetric, $y\ R\ x$. Since R is transitive, $x\ R\ x$. But this contradicts the line above. Therefore $\forall y \in S, x \neq y \implies \neg(x\ R\ y)$.
- Since R' is not reflexive, there exists z such that $\neg(z\ R'\ z)$. Fix such a z. By definition of R', $z\ R\ z$.
- Suppose that $x = z$. Then $\neg(z\ R\ z)$ and $z\ R\ z$, so this is a contradiction. Therefore $x \neq z$.
- Since $x \neq z$ and $\forall y \in S, x \neq y \implies \neg(x\ R\ y)$, we know $\neg(x\ R\ z)$. By definition of R', $(x\ R'\ z)$. Then since R' is symmetric, $(z\ R'\ x)$. Since R' is transitive, $z\ R'\ z$. But this is a contradiction since $\neg(z\ R'\ z)$.

In all cases, there is a contradiction. Therefore, such a set S and binary relation R does not exist.

Problem 7:

Consider the set of all non-empty finite-length strings consisting of lowercase alphabet characters S, and define the binary relation R on S as

$$\forall a, b \in S, a \; R \; b \iff a \text{ is a subsequence of } b$$

A string s is called a *subsequence* of another string t if and only if we can remove zero or more letters from t to get s. For example, "`make`" is a subsequence of "`mackey`", since we can remove two letters in "`mackey`" to get "`make`", but "`cs`" is not a subsequence of "`cmu`".

(a) How many different $x \in S$ satisfy $x \; R$ "`alice`"?

Since all the characters are distinct, any non-empty subset of characters corresponds to exactly one subsequence.

Therefore, there are $2^5 - 1 = 31$ such strings.

(b) How many different $x \in S$ satisfy $x \; R$ "`aaron`"?

We can either choose zero, one, or two `a`'s, and then append it to any of the 2^3 subsequences of "`ron`". However, if we choose zero `a`'s, then we cannot have an empty subsequence of "`ron`".

Therefore, there are $(3 \cdot 2^3) - 1 = 23$ such strings.

(c) How many different $x \in S$ satisfy $x \; R$ "`terence`"?

Suppose we go through the string character-by-character, from left to right, counting all subsequences, and subtract 1 for the empty subsequence at the end.

- The number of subsequences of "`t`" is 2.
- The number of subsequences of "`te`" is $2 \cdot 2 = 4$.
- The number of subsequences of "`ter`" is $4 \cdot 2 = 8$.
- The number of subsequences of "`tere`" is $8 \cdot 2 - 2 = 14$. This is because all subsequences ending in the first occurence of `e` (`e` and `te`) are double counted.
- The number of subsequences of "`teren`" is $14 \cdot 2 = 28$.
- The number of subsequences of "`terenc`" is $28 \cdot 2 = 56$.
- The number of subsequences of "`terence`" is $56 \cdot 2 - 8 = 104$. This is because all subsequences ending in the second occurence of `e` (`e`, `te`, `ee`, `re`, `tee`, `tre`, `ere` and `tere`) are double counted.

So the answer is $104 - 1 = 103$.