Discrete Mathematics Homework 2

Section 2-4

8 . Find at least three different sequences beginning with the terms 3, 5, 7 whose terms are generated by a simple formula or rule.

1. $\{a_n\} : a_n = 2n + 1, n \in \mathbb{N}$
2. $\{a_n\} : a_n = 2^n + 3, n \in \mathbb{N}$
3. $\{a_n\} : a_n = a_{n-1} + a_{n-2} - 1, a_1 = 3, a_2 = 5, n = 3, 4, 5...$

14 . For each of these sequences find a recurrence relation satisfied by this sequence. (The answers are not unique because there are infinitely many different recurrence relations satisfied by any sequence.)

- (b) $a_n = 2n$
  - $a_n = a_{n-1} + 2$
- (h) $a_n = n!$
  - $a_n = na_{n-1}$

16 . Find the solution to each of these recurrence relations with the given initial conditions. Use an iterative approach such as that used in Example 10.

- (d) $a_n = 2a_{n-1} - 3, a_0 = -1$
  - $a_n = 2a_{n-1} - 3$
    $= 2(2a_{n-2} - 3) - 3 = 2^2a_{n-2} - 3 \times (1 + 2)$
    $= 4(2a_{n-3} - 3) - 9 = 2^3a_{n-3} - 3 \times (1 + 2 + 3)$
    $= 2^ia_{n-i} - 3 \times \frac{1(2^i-1)}{2-1}$
    $= 2^na_0 - 3 \times (2^n - 1)$
    $= -2^n - 3 \times 2^n + 3$
    $= 3 - 2^{n+2}$

34 . Compute each of these double sums.

- (d) $\sum\limits_{i=0}^{2}\sum\limits_{j=0}^{3} i^2j^3$
  $= \sum\limits_{i=0}^{2}(i^2(\frac{3^2\times4^2}{4})) = \sum\limits_{i=0}^{2} 36i^2 = 36 \times \frac{2\times3\times5}{6} = 180$

Section 4-1

14 . Suppose that a and b are integers, $a \equiv 11(mod\,19)$ and $b \equiv 3(mod\,19)$. Find the integer c with $0 \le c \le 18$ such that

- (d) $c \equiv 7a + 3b\ (mod\,19)$.
  - $c \equiv 7a + 3b \equiv 7 \times 11 + 3 \times 3 \equiv 86 \equiv 10$.

34 . Show that if $a \equiv b\ (mod\,m)$ and $c \equiv d\ (mod\,m)$, where a, b, c, d and m are integers with $m \ge 2$, then $a - c \equiv b - d\ (mod\,m)$.

- *There are integers s, t with $a = b + ms, c = d + mt$, then*
  $a - c = (b + ms) - (d + mt) = (b - d) + m(s - t)$
  So $a - c \equiv b - d \ (mod\, m)$.

38 . Show that if n is an integer then $n^2 \equiv 0$ or $1 (mod\, 4)$.

1. n *is even:* $n = 2k, k \in \mathbb{N}^0 \Rightarrow n^2 = 4k^2 \equiv 0 \ (mod\, 4)$.
2. n *is odd:* $n = 2k + 1, k \in \mathbb{N}^0 \Rightarrow n^2 = (2k + 1)^2 = 4(k^2 + k) + 1 \equiv 1 \ (mod\, 4)$.

Section 4-2

2 . Convert the decimal expansion of each of these integers to a binary expansion.

- (c) $100632 = (11000100100011000)_2$

4 . Convert the binary expansion of each of these integers to a decimal expansion.

- (c) $(1110111110)_2 = 958$

8 . Convert $(BADFACED)_{16}$ from its hexadecimal expansion to its binary expansion.

- $(10111010110111111010110011101101)_2$

22 . Find the sum and product of each of these pairs of numbers. Express your answers as a base 3 expansion.

- (b) $(2112)_3, (12021)_3$
  - *Sum :* $(21210)_3$
  - *Product :* $(111020122)_3$

28 . Use Algorithm 5 to find $123^{1001} mod\, 101$.

- 87

Section 4-3

10 . Show that if $2^m + 1$ is an odd prime , then $m = 2^n$ for some nonnegative interger n. [Hint : First show that the ploynomial identity $x^m + 1 = (x^k + 1)(x^{k(t-1)} - x^{k(t-2)} + ... - x^k + 1)$ holds, where $m = kt$ and t is odd.]

- *We want to show that if $m \neq 2^n$, then $2^m + 1$ is not an odd prime. Let t be an odd prime so that $m = kt$, where $k = \frac{m}{t}$ is a positive integer, then $2^m + 1 = (2^k + 1)(2^{k(t-1)} - ...)$. To have $2^m + 1$ an odd prime, we must have $m = k$ and $t = 1$, which is cotradict to "t is an odd prime", so $2^m + 1$ can't be an odd prime if m can not only be divided by 2.*

12 . Prove that for every positive integer n, there are n consecutive composite integers. [Hint : Consider the n consecutive integers strating with $(n + 1)! + 2$.]

- $2|(n + 1)! + 2,\ 3|(n + 1)! + 3,\ ......, n|(n + 1)! + n,\ n + 1|(n + 1)! + (n + 1)$
  So there are n consecutive composite integers since $k|(n + 1)! + k,\ \forall 2 \leq k \leq n + 1$

16 . Determine whether the integers in each of these sets are pairwise relatively prime.

- (c) $25, 41, 49, 64$

- *These numbers are whether perfect squares or primes, so they are pairwise relatively prime.*

28 . Find $gcd(1000, 625)$ and $lcm(1000, 625)$ and verify that $gcd(1000, 625) \cdot lcm(1000, 625) = 1000 \cdot 625$

- $gcd(1000, 625) = 125$
- $lcm(1000, 625) = 5000$
- $gcd(1000, 625) \cdot lcm(1000, 625) = 125 \cdot 5000 = 1000 \cdot 625$

32 . Use the Euclidean algorithm to find

- (c) $gcd(123, 277) = 1$

52 . Prove or disprove that $p_1p_2...p_n + 1$ is prime for every positive integer n, where $p_1, p_2, ..., p_n$ are the n smallest prime numbers.

- *It doesn't hold at* $n = 6(2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509)$.

Section 4-4

6 . Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2.

- (a) $a = 2, m = 17$
  - $17 = 8 \times 2 + 1$
    $\Rightarrow -8 \times 2 + 17 = 1$
    $\Rightarrow -8 \times 2 \equiv 1\ (mod\ 17)$
    $\bar{a} = -8$
- (c) $a = 144, m = 233$
Euclidean		Bezout
$233 = 144 + 89$	|	$1 = 3 - 2 = 3 - (5 - 3) = -5 + (2 \times 3)$
$144 = 89 + 55$	|	$= -5 + 2 \times (8 - 5) = 2 \times 8 - 3 \times 5$
$89 = 55 + 34$	|	$= 2 \times 8 - 3 \times (13 - 8) = -3 \times 13 + 5 \times 8$
$55 = 34 + 21$	|	$= -3 \times 13 + 5 \times (21 - 13) = 5 \times 21 - 8 \times 13$
$34 = 21 + 13$	|	$= 5 \times 21 - 8 \times (34 - 21) = -8 \times 34 + 13 \times 21$
$21 = 13 + 8$	|	$= -8 \times 34 + 13 \times (55 - 34) = 13 \times 55 - 21 \times 34$
$13 = 8 + 5$	|	$= 13 \times 55 - 21 \times (89 - 55) = -21 \times 89 + 34 \times 55$
$8 = 5 + 3$	|	$= -21 \times 89 + 34 \times (144 - 89) = 34 \times 144 - 55 \times 89$
$5 = 3 + 2$	|	$= 34 \times 144 - 55 \times (233 - 144) = -55 \times 233 + 89 \times 144$
$3 = 2 + 1$	|	

    So $\bar{a} = 89$.

12 . Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 6.

- (b) $144x \equiv 4\ (mod\ 233)$
  - $4 \times 89 = 356 \equiv 123\ (mod\ 233)$
    $x = 233$

20 . Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruence $x \equiv 2\ (mod\ 3)$, $x \equiv 1\ (mod\ 4)$, and $x \equiv 3\ (mod\ 5)$

- $m_1 = 3, m_2 = 4, m_3 = 5, m = 3 \times 4 \times 5 = 60$
  $M_1 = 20, M_2 = 15, M_3 = 12, y_1 = 2, y_2 = 3, y_3 = 3$
  $x = 2 \times 20 \times 2 + 1 \times 15 \times 3 + 3 \times 12 \times 3 = 233 \equiv 53\ (mod\ 60)$
  $\forall x \in \{x | 53 + 60n, \forall n \in \mathbb{Z}^+\}$

38 . Use Fermat's little theorem to compute $3^{302} mod\ 5$, $3^{302} mod\ 7$, and $3^{302} mod\ 11$. Then use your results above and the Chinese remainder theorem to find $3^{302} mod\ 385\ (385 = 5 \times 7 \times 11)$.

- $3^{302}\ mod\ 5:$
  - $3^4 \equiv 1\ (mod\ 5)$
    $3^{300} \equiv 1\ (mod\ 5)$
    $3^{300} \times 3^2 \equiv 3^2\ (mod\ 5)$
    $3^2 \equiv 4\ (mod\ 5)$
    $3^{302} \equiv 4\ (mod\ 5)$
- $3^{302}\ mod\ 7:$
  - $3^6 \equiv 1\ (mod\ 7)$
    $3^{302} \equiv 3^2 \equiv 2\ (mod\ 7)$
- $3^{302}\ mod\ 11:$
  - $3^{10} \equiv 1\ (mod\ 11)$
    $3^{302} \equiv 3^2 \equiv 9\ (mod\ 11)$

40 . Show with the help of Fermat's little theorem that if n is a positive integer, then 42 divides $n^7 - n$.

- $42 = 2 \times 3 \times 7$
- $2 | n^7 - n : n^7 - n$ ***will be even either*** n ***is odd or even.***
- $3 | n^7 - n : n^7 - n \equiv (n^2)^3 \times n - n \equiv 1 \times n - n \equiv 0\ (mod\ 3)$.
- $7 | n^7 - n : n^7 - n \equiv n^6 \times n - n \equiv 1 \times n - n \equiv 0\ (mod\ 7)$.

Section 4-6

24 . Encrypt the message ATTACK using the RSA system with $n = 43 \times 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in Example 8.

- $e = 13, n = 43 \times 59 = 2537$
  $AT = 0019, TA = 1900, CK = 0210$
  $19^{13} \equiv 2299\ (mod\ 2537)$
  $1900^{13} \equiv 1317\ (mod\ 2537)$
  $210^{13} \equiv 2117\ (mod\ 2537)$
  So ATTACK means : $2299\ 1317\ 2117$

26 . What is the original message encrypted using the RSA system with $n = 53 \times 61$ and $e = 17$ if the encrypted message is 3185203824602550? (To decrypt, first find the decryption exponent d, which is the inverse of $e = 17$ modulo 52×60.)

- $d = e^{-1} = 2753\ (mod\ 52 * 60)$
  $n = 53 * 61 = 3233$
  $3185^{2753} \equiv 1816\ (mod\ 3233) \rightarrow SQ$
  $2038^{2753} \equiv 2008\ (mod\ 3233) \rightarrow UI$

$2460^{2753} \equiv 1717\ (mod\ 3233) \rightarrow RR$
$2550^{2753} \equiv 0411\ (mod\ 3233) \rightarrow EL$
So $3185\ 2038\ 2460\ 2550$ ***means : SQUIRREL***

Section 5-1

8 . Prove that $2 - 2 \times 7 + 2 \times 7^2 - ... + 2(-7)^n = \frac{(1-(-7)^{n+1})}{4}$ whenever n is a nonnegative integer.

- $Basis\ Step$: $n = 0, \frac{1-(-7)}{4} = 2$
- $Inductive\ Step$: ***assume that when*** $n = k, \sum\limits_{i=0}^{k} 2(-7)^i = \frac{(1-(-7)^{k+1})}{4}$

  Then when $n = k+1, \sum\limits_{i=0}^{k+1} 2(-7)^i = \frac{(1-(-7)^{k+1})}{4} + 2(-7)^{k+1} = \frac{1-(-7)^{k+1}+8(-7)^{k+1}}{4} = \frac{1-(-7)^{k+2}}{4}$

  So $\forall n \in \mathbb{Z}^+ (\sum\limits_{i=0}^{n} 2(-7)^i = \frac{(1-(-7)^{n+1})}{4})$

32 . Prove that 3 divides $n^3 + 2n$ whenever n is a positive integer.

- $Basis\ Step$: $n = 0, n^3 + 2n = 3$
- $Inductive\ Step$: ***assume that when*** $n = k, 3 | k^3 + 2k$

  Then when
  $n = k+1, (k+1)^3 + 2(k+1) = k^3 + 3k^2 + 3k + 1 + 2k + 2 = (k^3 + 2k) + 3(k^2 + k + 1) \equiv 0\ ($

38 . Prove that if $A_1, A_2, ..., A_n$ and $B_1, B_2, ..., B_n$ are sets such that $A_j \subseteq B_j$ for $j = 1, 2, ..., n$, then $\bigcup\limits_{j=1}^{n} A_j \subseteq \bigcup\limits_{j=1}^{n} B_j$

- $Basis\ Step$: $\bigcup\limits_{j=1}^{1} A_j = A_1 \subseteq \bigcup\limits_{j=1}^{1} B_j = B_1$
- $Inductive\ Step$: ***assume that when*** $n = k, \forall j \in \{1, 2, ..., k\}((A_j \subseteq B_j) \rightarrow (\bigcup\limits_{j=1}^{k} A_j \subseteq \bigcup\limits_{j=1}^{k} B_j))$

  Then when $n = k+1$:

  Let $x \in \bigcup\limits_{j=1}^{k+1} A_j = (\bigcup\limits_{j=1}^{k} A_j) \cup A_{k+1}$. ***From the hypothesis we know that*** $x \in \bigcup\limits_{j=1}^{k} A_j \rightarrow x \in \bigcup\limits_{j=1}^{k} B_j$***, and form the given fact we know that*** $A_{k+1} \subseteq B_{k+1}$***, that is,*** $x \in A_{k+1} \rightarrow x \in B_{k+1}$. ***Therefore, in either case*** $x \in (\bigcup\limits_{j=1}^{k} B_j) \cup B_{k+1}$

56 . Suppose that $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, where a and b are real numbers. Show that $A^n = \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix}$ for every positive interger n.

- $Basis\ Step$: $A = A$
- $Inductive\ Step$: ***assume that when*** $n = k, A^k = \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix}$

  Then when $n = k+1 : A^{k+1} = AA^k = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix} = \begin{bmatrix} a^{k+1} & 0 \\ 0 & b^{k+1} \end{bmatrix}$

  Thus $\forall n \in \mathbb{N}(A^n = \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix})$

Section 5-2

6 . ...

- (a) Determine which amounts of postage can be formed using just 3-cent and 10-cent stamps.
denomination	combination	denomination	combination
3	3	15	3+3+3+3+3
6	3+3	16	10+3+3
9	3+3+3	18	3+3+3+3+3+3
10	10	19	10+3+3+3
12	3+3+3+3	20	10+10
13	10+3	...	

      Claim: We can form any amount of postages greater than or equal to 18 cents using just 3-cent stamps and 10-cent stamps.
- (b) Prove your answer to (a) using the principle of mathematical induction. Be sure to state explicitly your inductive hypothesis in the inductive step.
    - $Basis\ Step$: $P(n)$: ***We can form*** n ***cents of postages using just 3-cent stamps and 10-cent stamps. Form the tabel above,*** $P(18)$ ***is true.***
    - $Inductive\ Step$: ***Assume that we can form*** k ***cents of postage, Then if it included two 10-cent stamps, replace them by seven 3-cent stamps. Otherwise, it is formed either from just 3-cent stamps or from one 10-cemt stamp and*** $k-10$ ***cents in 3-cent stamps. Replace three 3-cent stamps by one 10-cent stamp ,and then we can get*** $k+1$ ***cents in postage.***
- (c) Prove your answer to (a) using strong induction. How does the inductive hypothesis in this proof differ from that in the inductive hypothesis for a proof using mathematical induction?
    - ***Assume that*** $\forall j \in [18, k] P(j)$, ***where*** k ***is an integer greater than or equal to*** 20. ***To show that*** $P(k+1)$ ***is true, we already knew that*** $P(k-2)$ ***is true because*** $k \geq 18$, ***then we just simply add another 3-cent stamp to it, thus*** $k+1$ ***cents postage will be formed.***

12 . Use strong induction to show that every positive integer n can be written as a sum of distinct powers of two, that is, as a sum of a subset of the integers $2^0 = 1, 2^1 = 2, 2^2 = 4$, and so on. [Hint: For the inductive step, separately consider the case where $k+1$ is even and where it is odd. When it is even, note that $(k+1)/2$ is an integer.]

- ***Assume that*** $P(k)$ ***holds, that is, every integer up to*** k ***can be written as a sum of distinct powers of two, we want to know if*** $P(k+1)$ ***holds.***
  If $k+1$ ***is odd, then we can just add*** $2^0 = 1$ ***to it.***
  If $k+1$ ***is even, then*** $\frac{(k+1)}{2}$ ***is an positive integer. By the inductive hypothesis, we know that*** $P(\frac{(k+1)}{2})$ ***holds.***
  $\frac{(k+1)}{2} = 2^a + 2^b + 2^c + ..., (\forall a, b, c, ... \in \mathbb{N})$
  $(k+1) = 2 \times (2^a + 2^b + 2^c + ...) = 2^{a+1} + 2^{b+1} + 2^{c+1} + ..., (\forall a, b, c, ... \in \mathbb{N})$
  As shown, $P(k+1)$ ***holds if*** $P(k)$ ***holds.***

26 . Suppose that $P(n)$ is a propositional function. Determine for which nonnegative integers n the statement $P(n)$ must be true if

- (b) $P(0)$ is true; for all nonnegetive integers n, if $P(n)$is true then $P(n+3)$ is true.
    - $n : \{x | x = 3n, \forall n \in \mathbb{N}\}$

- (d) $P(0)$ is true; for all nonnegative integers n, if $P(n)$ is true, then $P(n+2)$ and $P(n+3)$ are true.
  - $n : \{x | x \in \mathbb{N} \wedge x \neq 1\}$

32 . Find the flaw with the following "proof" that every postage of three cents or more can be formed using just 3-cent and 4-cent stamps.
$Basis\ Step$ **: We can form postage of three cents with a single 3-cent stamp and we can form postage of four cents using a single 4-cent stamp.**
$Inductive\ Step$ **: Assume that we can form postage of j cents for all nonnegative integers j with $j \leq k$ using just 3-cent and 4-cent stamps. We can then form postage of $k+1$ cents by replacing one 3-cent stamp with a 4-cent stamp or by replacing two 4-cent stamps by three 3-cent stamps.**

1. ***j shuold be greater than or equal to 3.***
2. ***It doesn't hold at $j = 5$.***

Section 5-3

8 . Give a recursive definition of the sequence $\{a_n\}, n = 1, 2, 3, \ldots$ if

- (a) $a_n = 4n - 2$.
  - $a_n = a_{n-1} + 4, a_1 = 2, \forall n \in \mathbb{N} \geq 2$
- (c) $a_n = n(n+1)$.
  - $a_n = a_{n-1} + 2n, a_1 = 2, \forall n \in \mathbb{N} \geq 2$

12 . Prove that $f_1^2 + f_2^2 + \ldots + f_n^2 = f_n f_{n+1}$ when n is a positive integer. (f_n is the n th Fibonacci number.)

- $Basis\ Step : n = 1, f_1^2 = f_1 f_2 = 1^2$.
- $Inductive\ Step$: ***Assume that when*** $n = k, \sum_{i=1}^{k} f_i^2 = f_k f_{k+1}$

  Then when $n = k+1, \sum_{i=1}^{k+1} f_i^2 = \sum_{i=1}^{k} f_i^2 + f_{k+1}^2 = f_k f_{k+1} + f_{k+1}^2 = f_{k+1}(f_k + f_{k+1}) = f_{k+1} f_{k+2}$.

  So $\sum_{i=1}^{n} f_n^2 = f_n f_{n+1}$***. By mathematical induction.***

26 . Let S be the subset of the set of ordered pairs of integers defined recursively by Basis step: $(0,0) \in S$. Recursive step: If $(a,b) \in S$, then $(a+2, b+3) \in S$ and $(a+3, b+2) \in S$.

- (a) List the elements of S produced by the first five applications of the recursive definition.
  - $S : \{(0,0), (2,3), (3,2), (4,6), (5,5), (6,4), (6,9), (7,8), (8,7), (9,6), (8,12), (9,11)$ $(10,10), (11,9), (12,8), (10,15), (11,14), (12,13), (13,12), (14,11), (15,10)\}$
- (b) Use strong induction on the number of applications of the recursive ste of the definition to show that $5 | a+b$ when $(a,b) \in S$.
  - ***Let*** $P(n) : 5 | a+b$, ***whenever*** $(a,b) \in S$ ***is obtained by n applications of the recursive step.***
  - $Basis\ Step : n = 0, P(0)$ ***is true because*** $5 | 0+0$
    $Inductive\ Step$: ***Assume the strong inductive hypothesis that for every fixed*** $k, P(j),\ \forall j (0 \leq j \leq k)$
    Then when $n = k+1,\ 5 | a+2+b+3$ ***Since*** $5 | a+b$ ***and*** $5 | 2+3$.
- (c) Use structural induction to show that $5 | a+b$ when $(a,b) \in S$.
  - ***Same as (b), it holds for P(0).***