CSC3001 Discrete Mathematics

Homework 2

Deadline: 23:59, Sunday, July 3, 2022

The details should be provided, and you can refer to any theorem in the lecture notes without proof. Otherwise, please provide a proof or cite the reference for that.

1. Let f_n be the n-th Fibonacci number, i.e. $f_1 = f_2 = 1$, $f_{n+2} = f_{n+1} + f_n$. Prove that
$$f_1 + f_2 + ... + f_n = f_{n+2} - 1.$$

2. Let g_n satisfy the same recurrence as Fibonacci sequence, but have different initial values: $g_1 = a, g_2 = b$, $g_{n+2} = g_{n+1} + g_n$. Prove that
$$g_1 + g_2 + ... + g_n = g_{n+2} - b.$$

3. Find all sequences $\{a_n\}_{n\in\mathbb{N}}$ satisfying
$$a_{n+2} - 2a_{n+1} + a_n = 2.$$

4. How many subsets of the set $\{1, 2, 3, ..., n\}$ contain no adjacent integers? E.g. for $n = 3$ there are 5 such subsets: $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 3\}$.

5. Find and prove closed form formulas for generating functions
$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots.$$
of the following sequences
   (a) $a_n = a^n$, where $a \in \mathbb{R}$;
   (b) $a_n = \binom{m}{n}$, where $m \in \mathbb{N}$;
   (c) $a_n = f_n$, where f_n is the n-th Fibonacci number (assume $f_0 = 0, f_1 = f_2 = 1$).

6. Let $a, b \in \mathbb{N}^+$. Prove that
   (a) $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1.$

(b) $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$.

7. Prove that all numbers in the sequence
$$1007, 10017, 100117, 1001117, \ldots$$
are divisible by 53.

8. Show that $(3^{77} - 1)/2$ is odd and composite.

9. Using the formula
$$\binom{n}{m} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-m+1)}{m \cdot (m-1) \cdot \ldots \cdot 2 \cdot 1}$$
Prove that $\binom{p}{k}$ is divisible by p for $0 < k < p$. Deduce by induction on n that $n^p \equiv_p n$.

10. Find
$$(3p)!/p^3 \quad \bmod p$$
for prime $p > 3$.

11. Using the identity
$$(1+x)^n(1+x)^n = (1+x)^{2n}$$
prove that
$$\sum_{m=0}^{n} \binom{n}{m}\binom{n}{n-m} = \binom{2n}{n}.$$
Deduce that
$$\sum_{m=0}^{n} \binom{n}{m}^2 = \binom{2n}{n}.$$

12. Show steps to find
(a) the greatest common divisor of 1234567 and 7654321.
(b) the greatest common divisor of $2^3 3^5 5^7 7^9 11$ and $2^9 3^7 5^5 7^3 13$.

13. A robot walks around a two-dimensional grid. He starts out at (0; 0) and is allowed to take four different types of steps as

    1. (+2, -1)
    2. (+1, -2)
    3. (+1, +1)
    4. (-3, 0)

    Prove that this robot can never reach $(0, 2)$.

14. Let $m \in \mathbb{N}$ with $m > 1$. Prove that if $ac \equiv bc \pmod{m}$, then

$$a \equiv b \quad (\text{mod } \frac{m}{gcd(c, m)})$$

15. Modular Exponentiation: in cryptography, it is very important to be able to calculate $b^n (\text{mod } m)$ efficiently, where $n \in \mathbb{N}, b \in \mathbb{N}$ and $m \in \mathbb{N}/\{0, 1\}$. In general, b^n will be very large, e.g., $b^n = 7^{222}$, so it is not practical to calculate b^n first and then compute the modulus. There is an efficient strategy to find a remainder by using binary expansion of n to compute b^n:

$$b^n = b^{a_{k-1}2^{k-1}+\cdots+a_1\cdot 2+a_0} = \prod_{j=0}^{k-1} b^{a_j 2^j}, \quad a_0, \cdots, a_{k=1} \in \{0, 1\}$$

    By noting $b^{2^{j+1}} = b^{2^j} \cdot b^{2^j}$ and modular multiplication, b^n mod m can be calculated.

    (a) Find $7^{222}(\text{mod } 11)$ by the binary expansion (show iteration).
    (b) Find $7^{222}(\text{mod } 11)$ by Fermat's little theorem.

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

17. Find all solutions, if any, solutions to the system

$$x \equiv 5 \pmod{6}$$
$$x \equiv 3 \pmod{10}$$
$$x \equiv 8 \pmod{15}$$

18. Label the first prime number 2 as P_1. Label the second prime number 3 as P_2. Similarly, label the n-th prime number as P_n. Prove that $P_n < 2^{2^n}$ for an arbitrary $n \in \mathbb{N}^+$. Hint: consider $P_1 P_2 \cdots P_{n-1} + 1$.

19. In a round-robin tournament, every team plays every other team exactly once and each match has a winner and a loser. We say that the team $p_1, p_2, \cdots, p_m$ form a cycle if p_1 beats p_2, p_2 beats p_3, $\cdots$, p_{m-1} beats p_m, and p_m beats p_1. Show that if there is a cycle of length m ($m \geq 3$) among the players in a round-robin tournament, there must be a cycle of three of these players. Hint: Use the well-ordering principle.

20. Nim is a famous game in which two players take turns removing items from a pile of n items. For every turn, the player can remove one, two, or three items at a time. The player removing the last match loses. Use strong induction to show that, **if each player plays the best strategy possible**, the first player wins if $n = 4j$, $4j + 2$, or $4j + 3$ for some non-negative integer j and the second player wins in the remaining case when $n = 4j + 1$ for some nonnegative integer j. (For your interest, refer the general NIM game to *this link*)