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

$$f_1 + f_2 + ... + f_n = f_{n+2} - 1.$$

Solution: We prove it by induction.

Base: $n = 1$ gives $1 = 1$.

Step:

$$f_1 + f_2 + ... + f_n + f_{n+1} = (f_{n+2} - 1) + f_{n+1} = f_{n+3} - 1.$$

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

$$g_1 + g_2 + ... + g_n = g_{n+2} - b.$$

Solution: We prove it by induction.

Base: $n = 1$ gives $a = (a + b) - b$.

Step:

$$g_1 + g_2 + ... + g_n + g_{n+1} = (g_{n+2} - b) + g_{n+1} = g_{n+3} - b.$$

3. Find all sequences $\{a_n\}_{n\in\mathbb{N}}$ satisfying

$$a_{n+2} - 2a_{n+1} + a_n = 2.$$

Solution: There are many approaches. One can notice that

$$(a_{n+3} - 2a_{n+2} + a_{n+1}) - (a_{n+2} - 2a_{n+1} + a_n) = 2 - 2 = 0$$

and hence restrict to the sequences satisfying

$$a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n = 0.$$

It follows that such a_n can be expressed as

$$a_n = an^2 + bn + c.$$

Plugging back into original condition we get

$$2 = a(n+2)^2 - 2a(n+1)^2 + an^2 = 2a.$$

Hence general solution is given by

$$a_n = n^2 + bn + c.$$

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: $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 3\}$.

Solution: Let A_n denote the number of such subsets of $\{1, 2, 3, ..., n\}$. By induction we show that $A_n = f_{n+2}$.

Base: $n = 0$ gives one subset $\emptyset$ and $f_2 = 1$. $n = 1$ gives 2 subsets $\emptyset, \{1\}$ and $f_3 = 2$.

Step: we show that $A_{n+1} = A_n + A_{n-1}$. Indeed, if the set contains $n + 1$, then it must not contain adjacent element n, but then there are no restrictions on how we choose subset from $\{1, 2, ..., n - 1\}$ (hence it gives A_{n-1} choices). If the set does not contain element $n + 1$, then there are no restrictions on how we choose subset from $\{1, 2, 3, ..., n\}$ (hence it gives A_n choices). This argument shows that

$$A_{n+1} = A_n + A_{n-1}.$$

5. Find and prove closed form formulas for generating functions

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots.$$

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 $f_0 = 0, f_1 = f_2 = 1$).

Solution:

(a) Let $f(x) = \sum_{n=0}^{\infty} a^n x^n$. Then

$$axf(x) = \sum_{n=0}^{\infty} a^{n+1} x^{n+1} = f(x) - 1,$$

hence

$$f(x) = \frac{1}{1-ax}.$$

(b) Let $f(x) = \sum_{n=0}^{\infty} \binom{m}{n} x^n$. Note that this sum is, in fact, finite. One of the definitions of binomial coefficients implies that

$$f(x) = (1+x)^m.$$

Same formula can be proven by induction without assuming extra knowledge. Base case:

$$\binom{1}{0} + \binom{1}{1} x = (1+x)^1.$$

Step:

$$\sum_{n=0}^{\infty} \binom{m+1}{n} x^n = \sum_{n=0}^{\infty} (\binom{m}{n-1} x^n + \binom{m}{n} x^n) =$$

$$= x(1+x)^m + (1+x)^m = (1+x)^{m+1}.$$

(c) Let $f(x) = \sum_{n=0}^{\infty} f_n x^n$. We use the defining property of f_n to notice that

$$f(x) - xf(x) - x^2 f(x) = 0 + (1-0)x + \sum_{n=2}^{\infty} (f_n - f_{n-1} - f_{n-2}) x^n = x,$$

hence

$$f(x) = \frac{x}{1-x-x^2}.$$

6. Let $a, b \in \mathbb{N}^+$. Prove that

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

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

Solution:

(a) We will show that calculation of this gcd can be viewed as the Euclid algorithm for exponents a and b. Assume $a > b$, then

$$\gcd(2^a - 1, 2^b - 1) = \gcd(2^a - 2^b, 2^b - 1) =$$

$$= \gcd(2^b(2^{a-b} - 1), 2^b - 1) = \gcd(2^{a-b} - 1, 2^b - 1),$$

where the last step follows from the fact that

$$\gcd(2^b, 2^b - 1) = 1.$$

(b) The statement we are asked to prove involves the result of dividing $2^a - 1$ by $2^b - 1$. Let us actually carry out that division algebraically-long division of these expressions. The leading term in the quotient is 2^{a-b}(as long as $a \geq b$), with a remainder at that point of $2^{a-b} - 1$. If now $a - b \geq b$ then the next step in the long division produces the next summand in the quotient 2^{a-2b}, with a remainder at this stage of $2^{a-2b} - 1$. This process of long division continues until the remainder at some stage is less than the divisor,i.e.,$2^{a-kb} - 1 < 2^b - 1$. But then the remainder is $2^{a-kb} - 1$, and clearly $a - kb$ is exactly a mod b. This completes the proof.

7. Prove that all numbers in the sequence

$$1007, 10017, 100117, 1001117, ...$$

are divisible by 53.

Solution: We prove it by induction. Base: $1007 = 53 \cdot 19$. Step: difference between consecutive terms is given by 901000..., but $901 = 53 \times 17$.

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

Solution: $3^{77} - 1 \equiv_4 (-1)^{77} - 1 \equiv_4 -2$, hence it is not divisible by 4 and $(3^{77} - 1)/2$ must be odd. Since $3^{77} - 1$ is divisible by $3^7 - 1 > 2$, the number is composite.

9. Using the formula

$$\binom{n}{m} = \frac{n \cdot (n-1) \cdot (n-2) \cdot ... \cdot (n-m+1)}{m \cdot (m-1) \cdot ... \cdot 2 \cdot 1}$$

Prove that $\binom{p}{k}$ is divisible by p for $0 < k < p$. Deduce by induction on n that $n^p \equiv_p n$.

Solution: First claim follows from the fact that p appears in numerator but not in denomenator of a given fraction. Second claim follows from induction with base $1^p \equiv_p 1$, and step

$$(k+1)^p \equiv_p k^p + 1^p \equiv k+1.$$

10. Find

$$(3p)!/p^3 \mod p$$

for prime $p > 3$.

Solution: By Wilson Theorem $(p-1)! \equiv_p -1$. Hence

$$(3p)!/p^3 = 3{\cdot}2{\cdot}1{\cdot}(3p{-}1){\cdot}(3p{-}2){\cdot}\ldots{\cdot}(2p{+}1){\cdot}(2p{-}1){\cdot}(2p{-}2){\cdot}\ldots{\cdot}(p{+}1){\cdot}(p{-}1)! \equiv_p$$

$$\equiv_p 6 \cdot ((p-1)!)^3 \equiv_p 6 \cdot (-1)^3 \equiv_p -6.$$

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

$$\sum_{m=0}^{n} \binom{n}{m}^2 = \binom{2n}{n}.$$

Solution: Evaluating the coefficient of x^n on the left and right side of the identity we get

$$\sum_{m=0}^{n} \binom{n}{m}\binom{n}{n-m} = \binom{2n}{n}.$$

Noting that

$$\binom{n}{m} = \binom{n}{n-m}$$

we deduce the required identity.

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

Solution:
(a) 1 (Euclidean algorithm, see LN6)
(b) $2^3 3^5 5^5 7^3$

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 $(0, 2)$.

Solution: Let (x, y) denote the movement, then $x - y \equiv 0 (\text{mod} 3)$ for all movements. However, the initial point has $0 - 0 \equiv 0 \pmod 3$, but the final point has $3 \cdot 0 - 2 \equiv -2 \pmod 3$. By invariant methods, it can never reach (0,2).

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

$$a \equiv b \pmod{\frac{m}{gcd(c, m)}}$$

Solution: This is a similar question of cancellation in LN7. From $ac \equiv bc \pmod m$, we can obtain $ac \equiv bc \pmod{\frac{m}{gcd(c,m)}}$ because

$$m | ac - bc \Rightarrow \frac{m}{gcd(c, m)} | ac - bc$$

From $ac \equiv bc \pmod{\frac{m}{gcd(c,m)}}$, $gcd(\frac{m}{gcd(c,m)}, c) = 1$ and the claim in the lecture, we can do the cancellation as

$$a \equiv b \pmod{\frac{m}{gcd(c, m)}}$$

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, $b^n \bmod m$ 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.

Solution:

(a) The binary code for 222 is '11011110'

$$7^{2^1} \equiv 5 (\text{mod } 11)$$
$$7^{2^2} \equiv 3 (\text{mod } 11)$$
$$7^{2^3} \equiv 9 (\text{mod } 11)$$
$$7^{2^4} \equiv 4 (\text{mod } 11)$$
$$7^{2^5} \equiv 5 (\text{mod } 11)$$
$$7^{2^6} \equiv 3 (\text{mod } 11)$$
$$7^{2^7} \equiv 9 (\text{mod } 11)$$

Thus,

$$7^{222} \equiv 5 * 3 * 9 * 4 * 3 * 9 \equiv 14580 \equiv 5 (\text{mod } 11)$$

(b) By Fermat's little theorem we know that $7^{10} \equiv 1 (\text{mod } 11)$, so $(7^1 0)^k \equiv 1 (\text{mod } 11)$ for every positive integer k. To take advantage of this last congruence,

$$7^{222} = (7^{10})^{22} 7^2 \equiv (1)^{22} * 49 \equiv 5 \ (\text{mod } 11)$$

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

Solution: Note that the prime factorization of 42 is $2 \cdot 3 \cdot 7$. So it suffices to show that $2|n^7 - n$, $3|n^7 - n$, and $7|n^7 - n$. The first is trivial ($n^7 - n$ is either "odd minus odd" or "even minus even," both of which are even), and each of the other two follows immediately from Fermat's little theorem, because $n^7 - n \equiv (n^2)^3 \cdot n - n \equiv 1 \cdot n - n \equiv 0$ (mod3) and $n^7 - n \equiv n - n \equiv 0 \pmod 7$.

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

$$\begin{aligned} x &\equiv 5 \pmod 6 \\ x &\equiv 3 \pmod{10} \\ x &\equiv 8 \pmod{15} \end{aligned}$$

Solution: By Chinese reminder theorem, at the last part of LN7, we see these equations are equivalent to

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

Let $x = 3 \cdot 5 \cdot a + 2 \cdot 5 \cdot b + 2 \cdot 3 \cdot c$

$$\begin{array}{ccc} 15a \equiv 1 \pmod 2 & 10b \equiv 2 \pmod 3 & 6b \equiv 3 \pmod 5 \\ a \equiv 1 \pmod 2 & b \equiv 2 \pmod 3 & b \equiv 3 \pmod 5 \end{array}$$

Then $x = 15 * 1 + 10 * 2 + 6 * 3 \pmod{2 \cdot 3 \cdot 5} = 53 \pmod{30}$. Thus, the solution are $53 + 30y$, $\forall y \in \mathbb{Z}$.

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 $P_1 P_2 \cdots P_{n-1} + 1$.

Solution: When $n = 1$, the proposition is obviously true. Suppose that the proposition is true for $n \leq k$, then we can obtain the relation:

$$P_1 P_2 \cdots P_k < 2^{2^1 + 2^2 + \cdots + 2^k} = 2^{2^{k+1} - 2} P_1 P_2 \cdots P_k + 1 < 2^{2^1 + 2^2 + \cdots + 2^k} + 1 < 2^{2^k}$$

Since $P_1, P_2, \cdots, P_k$ cannot be the factor of the left term:

$$P_{k+1} \leq P_1 P_2 \cdots P_k + 1 < 2^{2^{k+1}}$$

From the strong induction, the proposition is true.

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.

Solution: We assume that there is no cycle of three players. Because there is at least one cycle in the round-robin tournament, the set of all positive integers n for which there is a cycle of length n is nonempty. By the well-ordering property, this set of positive integers has a least element k, which by assumption must be greater than three. Consequently, there exists a cycle of players $p_1, p_2, p_3, \cdots, p_k$ and no shorter cycle exists.

Because there is no cycle of three players, we know that $k > 3$. Consider the first three elements of this cycle, p_1, p_2, and p_3. There are two possible outcomes of the match between p_1 and p_3. If p_3 beats p_1, it follows that p_1, p_2, p_3 is a cycle of length three, contradicting our assumption that there is no cycle of three players. Consequently, it must be the case that p_1 beats p_3. This means that we can omit p_2 from the cycle $p_1, p_2, p_3, \cdots, p_k$ to obtain the cycle $p_1, p_3, p_4, \cdots, p_k$ of length $k-1$, contradicting the assumption that the smallest cycle has length k. We conclude that there must be a cycle of length three.

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*)

Solution: There are four base cases. If $n = 1$, then clearly the first player is doomed, so the second player wins. If there are two, three, or four matches ($n = 4 \cdot 0 + 2$, $n = 4 \cdot 0 + 3$, or $n = 4 \cdot 1$), then the first player can win by removing all but one match.
Now assume the strong inductive hypothesis, that in games with k or fewer matches, the first player can win if $k \equiv 0, 2 or, 3 \pmod 4$ and the second player can win if $k \equiv 1 \pmod 4$. Suppose we have a game with $k+1$ matches, with $k \geq 4$.

1. If $k+1 \equiv 0 \pmod 4$, then the first player can remove three matches, leaving $k-2$ matches for the other player. Since $k-2 \equiv 1 \pmod 4$, by the inductive hypothesis, this is a game that the second player at that point (who is the first player in our game) can win.

2. Similarly, if $k+1 \equiv 2(\text{mod } 4)$, then the first player can remove one match, leaving k matches for the other player. Since $k = 1(\text{mod } 4)$, by the inductive hypothesis, this is a game that the second player at that point (who is the first player in our game) can win.

3. And if $k+1 \equiv 3(\text{mod } 4)$, then the first player can remove two matches, leaving $k-1$ matches for the other player. Since $k-1 \equiv 1(\text{mod } 4)$, by the inductive hypothesis, this is again a game that the second player at that point (who is the first player in our game) can win.

4. Finally, if $k+1 \equiv 1(\text{mod } 4)$, then the first player must leave k, $k-1$, or $k-2$ matches for the other player.

Since $k \equiv 0(\text{mod } 4)$, $k-1 \equiv 3(\text{mod } 4)$, and $k-2 \equiv 2(\text{mod } 4)$, by the inductive hypothesis, this is a game that the first player at that point (who is the second player in our game) can win. Thus the first player in our game is doomed, and the proof is complete.