Homework 2 Solutions

Due: Monday, July 7, 11:59:59pm

CS 70: Discrete Mathematics and Probability Theory, Summer 2014

1. **[22 points] Induction, from HW1**

   a. [5 points] Use simple induction to prove that for all positive integers n, all of the entries in the matrix
   $$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^n$$
   are $\leq 2n$. (Hint: Find a way to strengthen the inductive hypothesis!)

   b. [5 points] You are in a foreign country that has only 3-cent and 7-cent coins, and you have an unlimited supply of both types. Use strong induction to prove that for every integer $c \geq 12$, it is possible to form c cents exactly using these coins. How many base cases do you need?

   c. [6 points] Recall the definition of Fibonacci number: $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2} \forall n \geq 2$. Prove that $F_n = \frac{\phi^n - (1-\phi)^n}{\sqrt{5}}$ where $\phi = \frac{1+\sqrt{5}}{2}$ is the Golden Ratio. [Hint: you might wish to use the fact that $\phi^2 = \phi + 1$]

   d. [6 points] Let $f(n)$ be defined by the recurrence relation $f(n) = 7f(n-1) - 10f(n-2)$ (for all $n \geq 2$) and $f(0) = 1, f(1) = 2$. Try to find a direct expression of $f(n)$ for every $n \in \mathbf{N}$, and prove it using strong induction.

Solution

a. Before starting the proof, writing out the first few powers reveals a telling pattern:
$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$$
It appears (and we shall soon prove) that the upper left and lower right entries are always 1, the lower left entry is always 0, and the upper right entry is $2n$. We shall take this to by our inductive hypothesis.

Proof. : We shall use a proof by induction that the upper left and lower right entries of the matrix are always 1, the lower left entry is always 0, and the upper right entry is $2n$. This will prove that all entries in the matrix are less than or equal to $2n$ for all $n \geq 1$.

The base case of $n = 1$ is trivially true. Now suppose that our proposition is true for some $n \geq 1$, meaning

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$$

for some $n \geq 1$. Multiplying both sides of the equation by the original matrix yields

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{n+1} = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+0 & 2n+2 \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & 2(n+1) \\ 0 & 1 \end{pmatrix}$$

By the principle of induction, our proposition is therefore true for all $n \geq 1$, so all entries in the matrix will be less than or equal to $2n$. □

b. **Claim**: $\forall c \in \mathbf{N}\ \exists x \in \mathbf{N}\ \exists y \in \mathbf{N}\ \big(c \geq 12 \Rightarrow 3x + 7y = c\big)$
In other words, for every natural number c, if $c \geq 12$ then c is the sum of a multiple of 3 and a multiple of 7.

Proof. : We will prove this by strong induction. We will need 3 base cases, since $P(n) \Rightarrow P(n+3)$ where $P(n)$ is the predicate $\exists x \in \mathbf{N} \exists y \in \mathbf{N}\ \big(n \geq 12 \Rightarrow 3x + 7y = n\big)$. For our first base case, let $c = 12$, $x = 4$, and $y = 0$, which is trivially true because $3 \times 4 + 7 \times 0 = 12$. For our second base case, let $c = 13$, $x = 2$, and $y = 1$, which is trivially true because $3 \times 2 + 7 \times 1 = 13$. For our third base case, let $c = 14$, $x = 0$, and $y = 2$, which is trivially true because $3 \times 0 + 7 \times 2 = 14$. For our inductive hypothesis, assume that $P(c)$ are all true for some $12 \leq c \leq n$. Since $P(c)$ is true for some values x_1 and y_1, $P(c+3)$ must be true for values $x_1 + 1$ and y_1. In other words, adding a 3-cent coin to the set of coins that added up to n will give a set that adds up to $n + 3$. By the principle of strong induction, since $P(12)$, $P(13)$, and $P(14)$ are all true and $\big(P(n) \wedge P(n+1) \wedge P(n+2)\big) \Rightarrow P(n+3)$, $P(n)$ is true for all n. Hence, $\forall c \in \mathbf{N}\ \exists x \in \mathbf{N}\ \exists y \in \mathbf{N}\ \big(c \geq 12 \Rightarrow 3x + 7y = c\big)$. □

c. *Proof.* The proof is by induction over n. Let $P(n)$ be the proposition that $F_n = \frac{\phi^n - (1-\phi)^n}{\sqrt{5}}$.
Base Case: If $n = 0$, then $F_0 = 0 = \frac{1-1}{\sqrt{5}}$. If $n = 1$, then $F_1 = 1 = \frac{2\phi - 1}{\sqrt{5}}$. Thus the base cases $P(0)$ and $P(1)$ are correct.
Inductive hypothesis: Assume that for some $n \in \mathbf{N}$, for all $0 \leq k \leq n, P(k)$ is true, i.e., $F_k = \frac{\phi^k - (1-\phi)^k}{\sqrt{5}}$.
Inductive step: To prove the inductive step, first, we observe that for Golden Ration ϕ, both ϕ and $1 - \phi$ are roots of $x^2 - x - 1 = 0$. Therefore, we have

$$\begin{aligned} & \phi^2 - \phi - 1 = 0, \\ \Rightarrow\ & \phi^2 = \phi + 1, \\ \Rightarrow\ & \forall n \geq 1, \phi^{n+1} = \phi^n + \phi^{n-1}, \end{aligned}$$

and this is also true for $1 - \phi$, namely $\forall n \geq 1, (1-\phi)^{n+1} = (1-\phi)^n + (1-\phi)^{n-1}$.

We know that $F_{n+1} = F_n + F_{n-1}$ by problem statement. Since $n \leq n$ and $n - 1 \leq n$, by inductive hypothesis, we know that

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &= \frac{\phi^n - (1-\phi)^n + \phi^{n-1} - (1-\phi^{n-1})}{\sqrt{5}} \\ &= \frac{\phi^{n+1} - (1-\phi)^{n+1}}{\sqrt{5}} \end{aligned}$$

And we have completed the inductive step by showing that $\forall n \in \mathbf{N}.((P(0) \wedge P(1) \wedge \cdots \wedge P(n)) \Rightarrow P(n+1))$. Thus, we are done. □

d. By plugging several different n's, we can guess that $f(n) = 2^n$. It remains to prove our guess by induction.

Proof. The proof is by induction over n. Let $P(n)$ be the proposition that $f(n) = 2^n$.
Base Case: If $n = 0$, then $f(0) = 1 = 2^0$. If $n = 1$, then $f(1) = 2 = 2^1$. Thus the base cases $P(0)$ and $P(1)$ are correct.
Inductive hypothesis: Assume that for some $n \in \mathbf{N}$, for all $0 \leq k \leq n$, $P(k)$ is true, i.e., $f(k) = 2^k$.
Inductive step: We know that $f(n+1) = 7f(n) - 10f(n-1)$ by problem statement. Since $n \leq n$ and $n - 1 \leq n$, by inductive hypothesis, we know that

$$\begin{aligned} f(n+1) &= 7 \cdot (2^n) - 10 \cdot (2^{n-1}) \\ &= 7 \cdot (2^n) - 5 \cdot (2^n) \\ &= (7-5) \cdot (2^n) \\ &= 2^{n+1}. \end{aligned}$$

And we have completed the inductive step by showing that $\forall n \in \mathbf{N}.((P(0) \wedge P(1) \wedge \cdots \wedge P(n)) \Rightarrow P(n+1))$. Thus, we are done. □

What you should get out of this problem: This problem illustrates a simple proof by strong induction and you need to understand the solution fully (be sure to go to office hours if not). Notice that we needed two bases cases, which happens often in induction. Although you do not need to explicitly state what the proposition $P(n)$ is that you are trying to prove, you MUST know it very clearly.

2. **[9 points] Stable Marriage True or False**
For each of the following claims, state whether the claim is true or false, and give a short proof to justify your answer. (Note: By a stable marriage instance we mean an input for stable marriage, i.e., the sets of men and women and their preference lists.)

a. [3 points] In a stable marriage instance, if man M and woman W each put each other at the top of their respective preference lists, then M must be paired with W in every stable pairing.

b. [3 points] In a stable marriage instance with at least two men and two women, if man M and woman W each put each other at the bottom of their respective preference lists, then M cannot be paired with W in any stable pairing.

c. [3 points] For every $n \geq 2$, there exists a stable marriage instance with n men and n women that has an unstable pairing in which every unmatched man-woman pair is a rogue couple.

Solution

a. **True.** Assume for the sake of contradiction that there is a stable pairing in which M is paired with $W' \neq W$, and thus W is paired with $M' \neq M$. Since W is at the top of M's list, M would prefer to be paired with W rather than W'. Similarly, W would prefer to be paired with M rather than her mate M', and thus the pair M, W would be a rogue couple, contradicting the assumption that the given pairing is stable. Thus our assumption must have been false, and so in every stable pairing, M is paired with W.

b. **False.** Consider the instance with men $Brad$, and Bob, and women $Angelina$, and $Jane$. Say both men prefer $Angelina$ to $Jane$, and both women prefer $Brad$ to Bob. In this instance, the pairing consisting of $(Brad, Angelina)$ and $(Bob, Jane)$ is stable. (Note that if we now add $Jennifer$ to the mix, the problem becomes more difficult.)

c. **True.** First observe that it suffices to show that for every $n > 2$, there is an instance such that there exists a pairing in which each man, and each woman is paired with the person last on their list. (If such a pairing exists, then each man would prefer any of the other women to the woman he is paired with, and similarly for the women; thus every unmatched man-woman pair would be a rogue couple.) We construct such an instance as follows: let there be n men, $M_1, M_2, \ldots, M_n$ and n women $W_1, W_2, \ldots, W_n$, and let the list of man M_i have W_i at the end of the list (in the n^{th} spot), and the other $n-1$ women in any order in the first $n-1$ spots. Similarly, let the list of woman W_i have man M_i at the end of the list (in the n^{th} spot), and the other $n-1$ men in any order in the first $n-1$ spots. The pairing $(M_1, W_1), \ldots, (M_n, W_n)$ clearly has the desired property (everyone is paired with their worst-imaginable partner).

3. **[13 points] Stable Marriage and Hospital Residency**

Suppose we are given n medical students and m hospitals. Each hospital h has some number q_h of slots, and we assume that the total number of students is larger than the total number of slots (i.e., $\sum_{h=1}^{m} q_h < n$). Each student ranks the m hospitals in order of preference, and each hospital ranks the n students. The goal is to find an assignment of students to slots (one student per slot) that is stable in the sense that there is no rogue student-hospital pair. An unmatched student-hospital pair (s, h) is considered rogue (with respect to an assignment of students to slots) iff s would prefer h to her current situation (she is either unmatched or matched to a hospital she likes less than h) and h would prefer s over one of the students assigned to h. There are two main differences between this problem and the Stable Marriage Problem: (i) there are more students than slots, and (ii) each hospital generally has more than one slot.

a. [6 points] Modify the propose-and-reject algorithm from class so that it finds a stable

assignment of medical students to slots. (Hint: Let the students propose to hospitals, and let each hospital h maintain a waitlist of q_h provisionally accepted students.)

b. [7 points] Give a succinct proof that your algorithm does indeed find a stable assignment. Your proof should involve the following version of the Improvement Lemma (see Lecture Note 4): For each hospital, after its waitlist becomes full, its least favorite student on the waitlist can only improve over time.

Solution

a. The algorithm is stated in terms of days and proposals and maybes for convenience. Obviously, this can efficiently be implemented on a computer. The algorithm is as follows:

   i. Each student goes and "proposes" to the highest ranked hospital on their list that has not yet rejected them. If all of the hospitals on a student's list have rejected them, then they accept their fate of not being with a hospital (and maybe find a new hobby).

   ii. Each hospital h, from among the students who proposed to them, chooses the highest q_h ranked students with respect to their list (or less students if $< q_h$ proposed). They tell those students "maybe", and send off the rest of the students with a "better luck next time."

   iii. If no student has been rejected, then the algorithm is finished and a stable matching has been found. Else, repeat step (i.)

   It is good to note the similarities to the propose-and-reject algorithm. The main difference is that there is a "waiting list" of people that the hospitals say maybe to, and also there are students who will not get into a hospital at all.

b. First, we prove the new Improvement Lemma.

   Improvement Lemma: For each hospital h, after its waitlist becomes full, its least favourite student on the waitlist can only improve over time.

   Proof. Assume a general hospital h has its waitlist full, with its least favourite student being student s. According to the algorithm, if a student not on the waiting list,$\hat{s}$, proposes to hospital h, then if they're worse than s, they will be rejected because being worse than s makes you worse than at leastq_h students, so $\hat{s}$ can't be accepted. If $\hat{s}$ is better than s, then s will be rejected because, including $\hat{s}$, there are at least q_h people better than s, q_h of which will be accepted. So either h's worst student remains s or gets better than s. □

   Now to prove the algorithm yields a stable matching.

   Proof. Assume for the sake of contradiction that the algorithm yielded a rogue couple (h, s), where hospital h prefers student s over one of their students, and student s prefers hospital h over whatever hospital they got (or didn't get). As can be seen directly from the algorithm, s must have proposed to h at some point before the algorithm terminated because s is going down their list and wouldn't get to their hospital (or lack of one) unless they had gone through every hospital they liked better. When s proposed to h, if h wouldn't reject s until its waitlist was full because the algorithm doesn't have hospitals reject unless their waitlist is full. So we can assume s is still proposing to h

and that h's waitlist is full. But if that's the case, then by the Improvement Lemma, h's worst student can only improve over time. If s gets rejected by h, then every student h accepted had to have been more preferred than s. But this contradicts the assumption that h preferred s over one of their students. So, by contradiction, this algorithm can yield no rogue couples. □

4. **[11 points] Extended GCD and Recursion**

In class, given positive integers x, y, we saw how to use the Extended GCD algorithm to find integers d, a and b such that

$$d = \gcd(x, y) = ax + by. \tag{1}$$

However, the integers $a = a_0$ and $b = b_0$ found by the algorithm may not be the only a, b satisfying equation (**??**).

a. [4 points] Describe all the pairs of integers a, b that satisfy equation (**??**), in terms of the values a_0, b_0 found by the algorithm.

b. [4 points] Using part (a) and the extended GCD algorithm from class, describe the set of all pairs of integers (a, b) satisfying $30a + 18b = 6$. Show clearly the recursive calls made and values returned by the extended GCD algorithm.

c. [3 points] Give one pair of integers (a, b) satisfying $30a + 18b = 12$.

Solution

Since d divides both x and y, we can write $x = x'd$ and $y = y'd$ for some integers x' and y'. We also have $\gcd(x', y') = 1$, because $d = \gcd(x, y)$.

a. We wish to show a and b satisfy $d = ax + by$ iff $(a, b) = (a_0 + ky', b_0 - kx')$ for some integer k.

Proof. First we show that all such (a, b) are solutions, then we show that these are the *only* solutions. If $a = a_0 + ky'$ and $b = b_0 - kx'$ for some integer k, then $d = ax + by$.

$$\begin{aligned} ax + by &= (a_0 + ky')x + (b_0 - kx')y \\ &= a_0x + b_0y + k(y'x - x'y) \\ &= d + k \cdot 0 = d, \end{aligned}$$

because $d = a_0x + b_0y$ and $y'x = x'y$.

Now, we show these are the only solutions. If a and b satisfy $d = ax + by$, then $a = a_0 + ky'$ and $b = b_0 - kx'$ for some integer k.

Since $ax + by = d = a_0x + b_0y$, by collecting the x terms and the y terms, we have

$$(a - a_0)x = -(b - b_0)y.$$

Divide both sides by d, we get the integer equation

$$(a - a_0)x' = -(b - b_0)y'.$$

Since x' and y' are co-prime, we conclude that x' must divide $b - b_0$ and y' must divide $a - a_0$. If we let the integer $k = (a - a_0)/y' = -(b - b_0)/x'$, then we have $(a, b) = (a_0 + ky', b_0 - kx')$. □

b. The set of (a, b) satisfying $d = ax + by$ is given by $(-1+3k, 2-5k)$ where k is an integer.

For $x = 30$ and $y = 18$, we get $d = 6$, $a_0 = -1$ and $b_0 = 2$ with the following execution:

```
begin Call Extended-GCD(30, 18)
|  /* 30 mod 18 = 12                                                          */
|  begin Call Extended-GCD(18, 12)
|  |  /* 18 mod 12 = 6                                                       */
|  |  begin Call Extended-GCD(12, 6)
|  |  |  /* 12 mod 6 = 0                                                    */
|  |  |  begin Call Extended-GCD(6, 0)
|  |  |  |  return ⟨6, 1, 0⟩ ;                          /* 6 = 1·6 + 0·0 */
|  |  |  end
|  |  |  return ⟨6, 0, 1⟩ ;                  /* 12 div 6 = 2,  6 = 0·12 + 1·6 */
|  |  end
|  |  return ⟨6, 1, −1⟩ ;                  /* 18 div 12 = 1,  6 = 1·18 + (−1)·12 */
|  end
|  return ⟨6, −1, 2⟩ ;                    /* 30 div 18 = 1,  6 = −1·30 + 2·18 */
end
```

Since $x = 30$ and $y = 18$, we have $y' = 3$ and $x' = 5$. By part (a), the set of (a, b) satisfying $d = ax + by$ is precisely $(-1 + 3k, 2 - 5k)$ where k is an integer.

c. $(a, b) = (-2, 4)$

Since $6 = d = a_0x + b_0y$, we have $12 = 2 \cdot d = (2a_0)x + (2b_0)y$. So $(a, b) = (2a_0, 2b_0) = (-2, 4)$ would give $30a + 18b = 12$.

In general, all solutions to $30a + 18b = 12$ have the form $(a, b) = (-2 + 6k, 4 - 10k)$.

5. **[21 points] Modular Arithmetic** This problem will give you practice with modular arithmetic.

a. [3 points] Evaluate $(3002 + 6002 \times 9002) \bmod 3$. Show your work. Do it the easy way! Order of operations is as usual.

b. [3 points] Similarly to part 5a, evaluate $\left(1002^3 - 2468 \times 17 + 4\right) \bmod 5$.

c. [3 points] The numbers $\{0, 1, 2, \ldots, 19\}$ are "representatives" of the congruence classes mod 20. For each of these classes, determine whether it has an inverse mod 20, and if so, state the inverse. You may use brute force (no need for an algorithm).

d. [3 points] Evaluate $\frac{5-(19\times3)}{7\times9}$ in modulo 20 arithmetic. Show your work.

e. [3 points] Use the extended Euclidean algorithm to find the inverse of 36, mod 55. Show all the steps of the algorithm.

f. [3 points] Describe all the integer solutions to the equation $17x \equiv 4 \pmod{20}$. (This should be a single congruence class mod 20).

g. [3 points] Solve the following pair of simultaneous equations mod 19, showing your work:

$$5x + 3y \equiv 0 \pmod{19}$$

$$y \equiv 4 + 12x \pmod{19}$$

Solution

a. $(3002 + 6002 \cdot 9002) \mod 3 = (2 + 2 \cdot 2) \mod 3 = 0 \mod 3$.

b. 1002^3 is simply multiplication repeatedly, so the mod 5 can be applied to each 1002 being multiplied, giving $(1002 \mod 5)^3$. So $(1002^3 - 2468 \cdot 17 + 4) \mod 5 = (2^3 - 3 \cdot 2 + 4) \mod 5 = 1 \mod 5$.

c. The thing that will make this easier is recognizing that n can only have an inverse mod 20 iff it is relatively prime with 20 (i.e.: isn't a multiple of 2 or 5). This easily shows what numbers don't have inverses, like 15.

n	n^{-1}	n	n^{-1}
0	$\varnothing$	10	$\varnothing$
1	1	11	11
2	$\varnothing$	12	$\varnothing$
3	7	13	17
4	$\varnothing$	14	$\varnothing$
5	$\varnothing$	15	$\varnothing$
6	$\varnothing$	16	$\varnothing$
7	3	17	13
8	$\varnothing$	18	$\varnothing$
9	9	19	19

d. In modulo 20, $\frac{5-(19\cdot 3)}{7\cdot 9} = [5-(19\cdot 3)]\cdot(7\cdot 9)^{-1} = [5-17]\cdot(3)^{-1} = (-12)\cdot(7) = 8\cdot 7 = 16$

e. .

x	**y**	**d**	**a**	**b**
55	36	1	-17	26
36	19	1	9	-17
19	17	1	-8	9
17	2	1	1	-8
2	1	1	0	1
1	0	1	1	0

So $36^{-1} \mod 55 = 26$

f. $17x \equiv 4 \pmod{20}$. Multiply both sides by $17^{-1} \pmod{20} = 13$. $x \equiv (4 \cdot 13) \pmod{20}$, $x \equiv 12 \pmod{20}$.

g. Solving for y from the second equation into the first, we have:

$$\begin{gathered} 5x + 3 \cdot (4 + 12x) \equiv 0 \pmod{19} \\ 5x + 12 + 36x \equiv 0 \\ 3x \equiv -12 \\ 3x \equiv 7 \\ x \equiv 3^{-1} \cdot 7 \equiv 15 \end{gathered}$$

Where $13^{-1} \equiv 13$. Next, we plug back and solve the y equation.

$$y \equiv 4 + 12x$$
$$y \equiv 4 + 12 \cdot (15)$$
$$y \equiv 13$$

6. **[12 points] Fermat's Little Theorem**
Fermat's Little Theorem states that, if p is prime, then for every $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$. This theorem is a key ingredient in the proof of correctness of the RSA cryptosystem, and is useful for many other things (and it often shows up on CS70 exams).

   a. [7 points] Prove Fermat's Little Theorem. (Hint: Show that the set of $p-1$ numbers $\{a \cdot 1,\ a \cdot 2,\ \ldots,\ a \cdot (p-1)\}$ are all distinct and non-zero mod p. Then multiply them together.)

   b. [6 points] Prove the following generalization of Fermat's Little Theorem: For every positive integer n (not necessarily prime), let S_n be the set of integers $a \in \{1, 2, \ldots, n-1\}$ such that $GCD(a, n) = 1$. Then for every $a \in S_n$, we have $a^{|S_n|} \equiv 1 \pmod{n}$. (Here $|S_n|$ denotes the number of elements in S_n.)

Solution

a First we prove some lemmas we were guided to by the hints.
Lemma 1: For any $a \in \{1, \ldots, p-1\}$, $a \cdot k$, where $k \in \{1, \ldots, p-1\}$, is nonzero modulo p.

Proof. Assume for the sake of contradiction that $a \cdot k \equiv 0$, with $a, k \in \{1, \ldots, p-1\}$. Because a is relatively prime to p, $a^{-1} \pmod{p}$ exists, so we can multiply it to both sides. Then we get $k \equiv a^{-1} \cdot 0 \equiv 0$, which means that $k = 0$, but that contradicts our assumption$k \in \{1, \ldots, p-1\}$, and so we've proved lemma 1. □

Lemma 2: For any $a \in \{1, \ldots, p-1\}$, $a \cdot k$ is distinct for any $k \in \{1, \ldots, p-1\}$. I.e. $ak_1 \equiv ak_2 \pmod{p} \Rightarrow k_1 = k_2$.

Proof. Assume for the sake of contradiction that $ak_1 \equiv ak_2$ and that $k_1 \neq k_2$. Then $a(k_1 - k_2) \equiv 0$. Since $a \neq 0$, it has an inverse modulo p. So $k_1 - k_2 \equiv (a^{-1}) \cdot 0 \equiv 0$, and we finally have that $k_1 = k_2$, giving us a contradiction and proving lemma 2. □

Now for the actual proof, let's again follow the suggestive hints in the problem.

Proof. Consider the list $\{a \cdot 1,\ a \cdot 2,\ \ldots,\ a \cdot (p-1)\}$. Because everything is distinct and nonzero (by lemmas 1 and 2), then this list must be congruent to $\{1, 2, \ldots, p-1\}$ (mod p) (though not necessarily in the same order). Multiplying the elements of each list together and then equating them, we have that $a^{p-1} \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1)$. Multiplying both sides by $(1)^{-1}, \ldots, (p-1)^{-1}$, we have that $a^{p-1} \equiv 1 \pmod{p}$, proving Fermat's Little (but extremely important) Theorem. □

b. We will try doing the same thing we did in (a) except with the list S_n. We will work in modulo n. Note that we need an extra lemma to show that multiplying things in S_n still gives us things in S_n (we didn't need this for (a) because the list encompassed all of (mod p)).
Lemma 1: $\forall s_1, s_2 \in S_n,\ s_1 \cdot s_2 \in S_n$.

Proof. Both $s_1$and s_2 share no factors with n because they are relatively prime to it. So the product $s_1 \cdot s_2$ will obviously not share factors with n either, making it relatively prime with n as well. □

Lemma 2: Pick any a in S_n. Then $\forall s_1, s_2 \in S_n$, $a \cdot s_1 \equiv a \cdot s_2 \Rightarrow s_1 = s_2$, or in other words, $a \cdot s$ is distinct.

Proof. Suppose for the sake of contradiction that $a \cdot s_1 \equiv a \cdot s_2$ and $s_1 \neq s_n$. Then we have that $a \cdot (s_1 - s_2) \equiv 0$, and because a is relatively prime with n, $a^{-1} \pmod{n}$ exist and we get $s_1 - s_2 \equiv a^{-1} \cdot 0 \equiv 0$, and so $s_1 = s_2$, which is a contradiction, proving lemma 2. □

Lemma 3: Pick any a in S_n, then $\forall s \in S_n$, $a \cdot s$ is nonzero modulo n. Note that this lemma isn't completely necessary since it is implied by lemma 1.

Proof. Assume for the sake of contradiction that $a \cdot s \equiv 0$. a is relatively prime with n, so it has an inverse, and so $s \equiv a^{-1} \cdot 0 \equiv 0$, but s can't be 0 because $0 \notin S_n$, and so we've reached a contradiction and proved lemma 3. □

Now onto the main proof.

Proof. Let $S_n = \{s_1, s_2, \ldots, s_k\}$, which is just naming the elements of S_n. Observe that $k = |S_n|$. Pick any $a \in S_n$. Then $R = \{a \cdot s_1, a \cdot s_2, \ldots, a \cdot s_k\}$ are all nonzero, in S_n, and distinct. So the elements of R must be the same as those of S_n. So multiplying all the elements of R and S_n and equating them, we get $a^k s_1 \cdot s_2 \cdot \cdots \cdot s_k \equiv s_1 \cdot s_2 \cdot \cdots \cdot s_k$. Multiplying both sides by $(s_1)^{-1}, \ldots, (s_k)^{-1}$ (which must exist because they are all relatively prime to n), we get $a^k \equiv 1$, or plugging in for k, we have $a^{|S_n|} \equiv 1 \pmod{n}$, proving the generalization. □

7. **[12 points] Tower of Hanoi**

This puzzle was invented by the French mathematician, Edouard Lucas, in 1883. Accompanying the puzzle is a story:

In the great temple at Benares beneath the dome which marks the center of the world, rests a brass plate in which are fixed three diamond needles, each a cubit high and as thick as the body of a bee. On one of these needles, at the creation, God placed sixty-four disks of pure gold, the largest disk resting on the brass plate and the others getting smaller and smaller up to the top one. This is the Tower of Hanoi. Day and Night unceasingly, the priests transfer the disks from one diamond needle to another according to the fixed and immutable laws of Hanoi, which require that the priest on duty must not move more than one disk at a time and that he must place this disk on a needle so that there is no smaller disk below it. When all the sixty-four disks shall have been thus transferred from the needle on which at the creation God placed them to one of the other needles, tower, temple and Hanoians alike will crumble into dust, and with a thunderclap the world will vanish.

Find and prove what the minimum number of moves required to carry out this task in general is, if there are n disks on the original needle. Assuming that the priests can move a disk each

second, roughly how many centuries does the prophecy predict before the destruction of the World?

Solution

Proof. Let a_n denote the minimum number of moves needed to complete this task if there are n disks on the original needle. We claim that $a_n = 2^n - 1$. To prove this we will induct on n. In order to arrive at this result, we would have considered the simple cases when there is only 1 disk, 2 disks, etc.

Base case: When $n = 1$, we only need 1 move to complete the task. This agrees with our theorem, since $2^1 - 1 = 1$.

Inductive hypothesis: Assume $a_n = 2^n - 1$.

Inductive step: Suppose we have $n+1$ disks. Label the three needles A, B and C, and suppose the disks start on A. Consider the first time the largest disk is moved, say from needle A to C. Then the other n disks must be all in needle B. Then the minimum number of steps to get to that step is a_n. The minimum number of extra steps to finish moving all $n + 1$ disks is now simply to move the n disks from B to C without touching the largest disk again. Hence, the total minimum number of steps to move the $n + 1$ disks is $a_n + 1 + a_n$. Thus $a_{n+1} = 2a_n + 1$. By the inductive hypothesis $a_n = 2^n - 1$, so $a_{n+1} = 2(2^n - 1) + 1 = 2^{n+1} - 1$. □

The prophecy predicts

$$\frac{2^{64} - 1}{60 \times 60 \times 24 \times 365 \times 100} = 5,849,420,000$$

centuries before the destruction of the World. Since geologists predict that the Earth is 45,400,000 centuries old, and astronomers estimate the universe is 137,000,000 centuries old, we've still got some time left.