CS3000 Algorithms

Solutions to Recitations 01

Akshar Varma *Date: 11 July 2023*

Problem 1 (Induction)

a. Prove the following formulas for the sums of the arithmetic and geometric series/progression.

(a) Arithmetic Progression: $\sum_{i=1}^{n} a + (i-1)d = \frac{1}{2}n(a + (a + (n-1)d))$

The summation is half of n times the first term + last term.

(b) Geometric Progression: $\sum_{i=0}^{n-1} ar^i = \frac{a-ar^n}{(1-r)}$, where $r \neq 1$.

The sum is first term - next term divided by 1 - common ratio.

b. (a) **(∗)** Prove that the following statements hold using induction; clearly provide the base case as well as the proof of the inductive step.

$$\sum_{r=1}^{n} r(r+1)(r+2)\cdots(r+p-1) = \frac{1}{p+1}n(n+1)(n+2)(n+3)\cdots(n+p)$$

(b) **(∗)** As a further exercise, try to find formulas for $\sum_{i=1}^{n} i$ (sum of first n natural numbers), $\sum_{i=1}^{n} i^2$ (sum of squares of first n natural numbers), $\sum_{i=1}^{n} i^3$ (sum of cubes of first n natural numbers) using the above formulas.

Solution:

a. (a) Arithmetic Progression: $\sum_{i=1}^{n} a + (i-1)d = \frac{1}{2}n(a + (a + (n-1)d))$

We prove this by induction:

Base case, $n = 1$: $\sum_{i=1}^{n} a + (i-1)d = a = \frac{1}{2}n(a + (a + (n-1)d))$

Assume: $\sum_{i=1}^{n-1} a + (i-1)d = \frac{1}{2}(n-1)(a + (a + (n-2)d))$

Then,

$$\begin{aligned}\sum_{i=1}^{n} a + (i-1)d &= \left(\sum_{i=1}^{n-1} a + (i-1)d\right) + a + (n-1)d \\ &= \frac{1}{2}(n-1)(a + (a + (n-2)d)) + a + (n-1)d \\ &= \frac{1}{2}n(a + (a + (n-1)d))\end{aligned}$$

Alternate Proof. Write $a_i = a + (i-1)d$ so $S_n = \sum_{i=1}^{n} a + (i-1)d = \sum_{i=1}^{n} a_n$. Thus we can write S_n in the following two ways:

$$\begin{aligned}S_n &= a_1 + (a_1 + d) + (a_1 + 2d) + \cdots + (a_1 + (n-2)d) + (a_1 + (n-1)d) \\ S_n &= (a_n - (n-1)d) + (a_n - (n-2)d) + \cdots + (a_n - 2d) + (a_n - d) + a_n\end{aligned}$$

Adding the above equations gives us: $2S_n = n(a_1 + a_n)$ which gives the required result.

(b) Geometric Progression: $\sum_{i=0}^{n-1} ar^i = \frac{a-ar^n}{(1-r)}$, where $r \neq 1$.

We prove this by induction:

Base case, $n = 1$: $\sum_{i=0}^{n-1} ar^i = a = \frac{a(1-r^n)}{(1-r)}$

Assume: $\sum_{i=0}^{n-1} ar^i = \frac{a-ar^n}{(1-r)}$

Then,

$$\begin{aligned}\sum_{i=0}^{n} ar^i &= \left(\sum_{i=0}^{n-1} ar^i\right) + ar^n \\ &= \frac{a - ar^n}{(1-r)} + ar^n \\ &= \frac{a - ar^{n+1}}{(1-r)}\end{aligned}$$

Alternate Proof. Let $S_n = \sum_{i=0}^{n-1} ar^i$.

$$\begin{aligned}(1-r)S_n &= (1-r)(ar^0 + ar^1 + ar^2 + ar^3 + \cdots + ar^{n-1}) \\ &= ar^0 + ar^1 + ar^2 + ar^3 + \cdots + ar^{n-1} - ar^1 - ar^2 - ar^3 - \cdots - ar^{n-1} - ar^n \\ &= a - ar^n\end{aligned}$$

If $r \neq 1$, then we can divide both sides by $(1-r)$ to get the required formula.

b. (a) **(∗)** $\sum_{r=1}^{n} r(r+1)(r+2)\cdots(r+p-1) = \frac{1}{p+1} n(n+1)(n+2)(n+3)\cdots(n+p)$

Here, we will assume an arbitrary value of p and solve for the induction in a similar way as the previous examples.

Base case: $n = 1 \implies \sum_{r=1}^{r=1} r(r+1)\cdots(r+p-1) = p! = \frac{1}{p+1} 1 \cdot 2 \cdots p \cdot (p+1) = p!$ as required.

Inductive step: Let this be true for all $n \leq k$ and consider $n = k+1$

$$\begin{aligned}\sum_{r=1}^{k+1} r(r+1)\cdots(r+p-1) &= \sum_{r=1}^{k} r(r+1)\cdots(r+p-1) + (k+1)(k+2)\cdots(k+p) \\ &= \frac{1}{p+1} k(k+1)\cdots(k+p) + (k+1)(k+2)\cdots(k+p) \\ &= \frac{k(k+1)(k+2)\cdots(k+p) + (p+1)(k+1)(k+2)\cdots(k+p)}{p+1} \\ &= \frac{(k+1)(k+2)(k+3)\cdots(k+p+1)}{p+1}\end{aligned}$$

which proves the statement. The second equality uses the inductive assumption.

Note: We could have assumed the statement to be true just for $n = k$, instead of for all $n \leq k$ and we would still have been able to prove this statement. Both ways would be proofs by induction and we can use whichever is easier.

(b) For the further exercises, note that $\sum_{r=1}^{n} r^2 = \sum_{r=1}^{n} r(r+1) - \sum_{r=1}^{n} r$. For sum of cubes, note that $\sum_{r=1}^{n} r(r+1)(r+2) = \sum_{r=1}^{n} r^3 + 3r^2 + 2r$. Since we already know the sum for linear and quadratic terms, we can rearrange the above equation to get the value for sum of cubes. A similar relationship can be derived for higher powers of r as well.

■

Problem 2 (Basic Prerequisite Recap)

These are some basic mathematical prerequisites that you should know. They will be covered during the recitation only if time permits.

a. We are going to prove the classic result that $\sqrt{2}$ is irrational. To do this, we use proof by contradiction. Let's call the statement we are trying to prove P. If we want to prove that P is true (in this case, we want to prove that $\sqrt{2}$ is irrational), we make the assumption that $\neg P$ is true. Using this assumption, we try to derive find some other statement C, so that $\neg P \implies C \wedge \neg C$, which is logically impossible (a contradiction). And this means that P has to be true.

First we need this result.

(a) Explain why if n^2 is even, then n is even.

(b) Now prove that $\sqrt{2}$ is irrational.

Note: This can also be proven through the Fundamental Theorem of Arithmetic, where every rational number has a unique decomposition based on prime numbers...

b. (a) How many ways can you rearrange the letters in the word: ALGORITHM?

(b) What about the word: ALGARATHM?

(c) What if no two vowels can appear together (in ALGORITHM)?

(d) What if you cannot have more than two consonants together at a time (in ALGORITHM)?

c. You are picking 3 different numbers from 1 to 15.

(a) How many ways can you do it such that the product is divisible by either 2 or 3?

(b) How many ways can you do it such that the product is divisible by 4?

d. Assume that friendship is a symmetric property (if Alice is friends with Bob, then Bob is friends with Alice). Show that in a group of n people, there will always be at least two people with the same number of friends.

e. (a) Prove that $\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$ by counting a set in two different ways.

(b) Prove that $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ by counting a set in two different ways.

f. Determine whether or not the expression converges to a value. If it converges, determine its value.

(a) $\sum_{i=1}^{\infty} \frac{1}{2^i}$ (b) $\sum_{i=1}^{\infty} \frac{1}{i}$ (c) $\sum_{k=0}^{n} \binom{n}{k}$

Solution:

a. (a) If n is odd then n^2 is odd.

(b) Suppose $\sqrt{2}$ is irrational. Let p/q be simplified fraction for it (meaning $gcd(p,q) = 1$). Then $2 = p^2/q^2$, or $2q^2 = p^2$. So this means p^2 has to be even, which by above means p is even. But then then if p is even, then p^2 is divisible by 4, meaning q^2 is divisible by 2, which means q is divisible by 2. So therefore, p and q share a common factor, which is a contradiction.

b. (a) 9!

(b) 9!/3!

(c) We set the 6 consonants. There are 7 spots for the vowels to go in so that they are not next to each other. After choosing the 3 spots, we can permute the vowels. So we get $\binom{7}{3}6!3!$

(d) We set the three vowels and then we have a stars and bars situation. We can think of having an equation $x_1 + x_2 + x_3 + x_4 = 6$, where each x_i represents the number of consonants at the i spot. We have the condition that $x_i < 3$. We have 6 because there are 6 total consonants. Counting this carefully gives you correct solution (if this isn't clear don't worry about this, this problem is harder than we meant).

c. (a) Can count directly, but need to be careful about double counting. Can also take the complement and count products not divisble by either 2 or 3. There are five numbers to choose from (1,5,7,11,13), so we get $\binom{15}{3} - \binom{5}{3}$

(b) Can count directly, but need to break down numbers into groups divisible by 4, then divisible by 2 but not 4 etc. Easier to count complement, which would be odd products or products with only one even factor (that's not divisible by 4). There are 8 odd factors, and 4 factors divisible by 2 but not 4. So either all 3 factors are odd, or 2 are odd and 1 is divisible by 2 but not by 4. So we get $\binom{15}{3} - (\binom{8}{3} + \binom{8}{2}\binom{4}{1})$

d. So a person can have at most $n-1$ friends. First case: suppose everyone in the group has at least one friend. Then there are n people, and the range of friends is between 1 and $n-1$, so there must be at least 2 people with same number of friends. Second case: suppose there is one person with no friends. Then the other $n-1$ people all have at least one friend, and they can all have at most $n-2$ friends. So $n-1$, and range of $n-2$ values, so at least 2 people have the same number of friends.

e. (a) Left side: Pick k committee members, then out of those k pick j to be the leaders.
Right side: Pick j leaders, and from the remaining members pick out $k-j$ to be the rest of the committee members.

(b) Fix some element i. Either element i is included in the k elements chosen on the left or its not. If it is, then $\binom{n-1}{k-1}$ counts ways to pick $k-1$ other elements to include with i. If it is not, then $\binom{n-1}{k}$ counts ways to pick k elements (since i not included).

f. (a) Let S denote the sum. Then $2S - S = 1$, so we get $S = 1$

(b) Doesn't converge. To see this, note that

$$1/3 + 1/4 > 1/2$$
$$1/5 + 1/6 + 1/7 + 1/8 > 1/2$$
and so on...

Always is a sequence that adds to more than 1/2, so this never converges.

(c) This counts all possible subsets of a set of size n, so this is 2^n

■

Problem 3 (Basics of Asymptotics)

Make sure you are familiar with the definitions of the various Big-Oh notations:
$f(n) = o(g(n)); f(n) = O(g(n)); f(n) = \Theta(g(n)); f(n) = \Omega(g(n)); f(n) = \omega(g(n))$

(a) Show that for $a, b \in \mathbb{R}^+$, the following hold:

a. $n^a = O(n^b)$, whenever $a \leq b$.

b. $n^a = o(n^b)$, whenever $a < b$.

c. $n^a + n^b = O(n^b)$, whenever $a \leq b$.

d. $n^a + n^b = o(n^b)$, whenever $a < b$.[1]

You could think about similar statements that use ω and Ω instead.

(b) Let $f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0$ and $g(n) = n^b$. Using the facts you proved in subpart (a), come up with a value of b in relation to k such that the following hold:

a. $f(n) = o(g(n))$

b. $f(n) = O(g(n))$

c. $f(n) = \omega(g(n))$

d. $f(n) = \Omega(g(n))$

e. $f(n) = \Theta(g(n))$

(c) Show that for $a, b, c, d, k \in \mathbb{R}^+$ and $k > 1$, the following holds: $a \ll \log_b^c n \ll n^d \ll k^n \ll n^n$, where we define and use $x \ll y$ as a shorthand notation which denotes that $x = o(y)$.

Note that here only n is growing to infinity, everything else is a constant. Thus, in words, this is asking you to prove that: Constants grow slower than logarithms, which grow slower than polynomials, which grow slower than constants raised to an exponent, which grow slower than n^n where both the base and the exponent are dependent on n.

Solution:

(a) We use the limit of the ratio of the two functions to prove each of these.

a. $n^a = O(n^b)$, whenever $a \leq b$.

$$\lim_{n\to\infty} \frac{n^a}{n^b} = \lim_{n\to\infty} n^{a-b} < \infty$$

Since $a \leq b$ the largest value the limit can take is 1 when $a = b$.

An alternate proof would be to find a c such that for all $n \geq n_0$, we have that $n^a \leq c \cdot n^b$. Note that this is easily done, for example $c = 1$ and any $n_0 \geq 1$ suffice.

b. $n^a = o(n^b)$, whenever $a < b$.

$$\lim_{n\to\infty} \frac{n^a}{n^b} = \lim_{n\to\infty} n^{a-b} = 0$$

[1] This is incorrect, but is being kept as is to illustrate how to prove its incorrectness.

The final inequality holds since $a < b$, hence we are taking the limit of the inverse of a polynomial. Since the polynomial would tend to ∞, its inverse would tend to 0.

An alternate proof would be to show that for all $\epsilon > 0$ there exists an n_0 such that $n^a < \epsilon \cdot n^b$. Note that this can be done by solving for n in the inequality to get $n_0 > \epsilon^{1/a-b}$.

c. $n^a + n^b = O(n^b)$, whenever $a \leq b$.

$$\lim_{n\to\infty} \frac{n^a + n^b}{n^b} = \lim_{n\to\infty} n^{a-b} + 1 = 1$$

The final inequality holds for similar reasons as the first subpart.

Alternatively, we can set $c = 2$ and $n_0 = 1$ to show that $n^a + n^b \leq c \cdot n^b$ for all $n \geq n_0$.

d. $n^a + n^b = o(n^b)$, whenever $a < b$. The previous subpart shows why this subpart cannot be true. For this to be true, the limit must be 0, but we already saw that the limit was 1.

This was a typo and the correct version of this subpart might have been to show that $n^a + n^b = \Omega(n^b)$, which the limit proof in the previous part does show since the limit is strictly greater than 0.

For the proof using c and n_0, simply setting $c = 1, n_0 = 1$ should suffice.

(b) First, note that using the previous subpart repeatedly to compare $a_i n^i$ vs $a_j n^j$ we can show that $f(n) = \Theta(n^k)$. This implies that we only need to compare n^k and n^b which we already know how to do from the previous subpart.

Secondly, this illustrates that the intuitive idea of the asymptotic notations as growth rates being compared using the inequalities of $\leq, <, =, >, \geq$ will carry over pretty much exactly when comparing the degrees of the polynomials.

a. $f(n) = o(g(n))$ whenever $k < b$

b. $f(n) = O(g(n))$ whenever $k \leq b$

c. $f(n) = \omega(g(n))$ whenever $k > b$

d. $f(n) = \Omega(g(n))$ whenever $k \geq b$

e. $f(n) = \Theta(g(n))$ whenever $k = b$

(c) We prove each of these one by one.

i. $a \ll \log_b^c n$, that is, $a = o(\log_b^c n)$

Formal definition approach: It is easy to see that since the RHS depends on n while the LHS does not, for any $\epsilon > 0$, there exists an n_0 such that $\log_b^c n$ will grow larger than the constant value of a/ϵ.

Alternatively, we can use the L'Hospital rule for differentiation to prove this using the limit definition.

$$\lim_{n\to\infty} \frac{a}{\log_b^c n} = \lim_{n\to\infty} \frac{0}{c \log_b^{c-1} n \cdot (n \ln n)^{-1}} = 0$$

ii. $\log_b^c n \ll n^d$, that is, $\log_b^c n = o(n^d)$

First, note that $\log_b n = \ln n / \ln b \implies \log_b n = \Theta(\ln n)$. Thus, without loss of generality, we can replace $\log_b$ with $\ln n$. Let us also assume, without loss of generality, that c is an integer.[2]

[2] If c is not an integer, we can take the ceiling of c to get an integer. It is easy to see that $\log_b^c n = O(\log_b^{\lceil c \rceil} n)$.

Formal definition approach: If $d > c$, then this follows from the fact that $\ln x \leq x$ for $x > 0$ and hence constant $c = 1$ works. If $d < c$, then $\ln n \leq n \implies (\ln n)^c \leq n^c \implies \frac{(\ln n)^c}{n^{c-d}} \leq n^d$. Choosing a constant such that n^{b-a} is positive completes the proof for all n.

Using L'Hospital's rule:

$$\lim_{n\to\infty} \frac{\ln^c n}{n^d} = \lim_{n\to\infty} \left(\frac{\ln n}{n^{d/c}}\right)^c = \left(\lim_{n\to\infty} \frac{\ln n}{n^{d/c}}\right)^c = \left(\lim_{n\to\infty} \frac{c}{dn \cdot n^{d/c-1}}\right)^c = 0$$

iii. $n^d \ll k^n$

Without loss of generality, we can assume that d is an integer.

Formal definition approach:

- First, we'll show that $2^n \geq n$ for all non-negative integers n using induction. The base case is trivial and $2^{n+1} = 2 \cdot 2^n \geq 2n \geq n + 1$ for all $n \geq 1$ completes the induction.
- Next, note that $2^n = \left(2^{n/c}\right)^c \geq (n/c)^c$ for any positive c.
- For any value of d, we choose $n_0 = (d+1)^{d+1}$ and for all $n \geq n_0$, $2^n \geq (n/(d+1))^{d+1} = n^d \cdot (n/n_0) \geq n^d$.
- For $k > 1$, $k^n = \left(2^{\lg k}\right)^n = 2^{n \lg k} \geq (n \cdot \lg k)^d = (\lg k)^d \cdot n^d$.
- Thus, for any $k > 1, d > 0$ we have a $c > 0$ with $n_0 = (d + 1)^{d+1}$ such that $k^n \geq c \cdot n^d$ which completes the formal proof.

To use the limit definition, we will repeatedly use the L'Hospital rule for differentiation. Note that $\frac{d}{dn} k^n = k^n \ln k$.

$$\lim_{n\to\infty} \frac{n^d}{k^n} = \lim_{n\to\infty} \frac{dn^{d-1}}{k^n \ln k} = \cdots d \text{ times} \cdots = \lim_{n\to\infty} \frac{d!}{k^n (\ln k)^d} = 0$$

iv. $k^n \ll n^n$

Formal definition approach: In this case, it is straightforward to find a constant c such that $k^n \leq c \cdot n^n$ for all $n \geq n_0$ for some $n_0 \in \mathbb{N}$. To do this, note that as soon as $n > k$, $k^n \leq n^n$ which allows us to can set $c = 1$ for $n_0 = (k + 1)$.

■

Problem 4 (Number theory practice)

Solve the following number theoretic problems:

1. Find the values of the following without explicit calculation:
   - $6^{987382934023} \mod 37$
   - $7^{99288399289} \mod 5$
   - $13^{12301293120} \mod 17$
   - $GCD(21, 28, 49)$
   - $7^{920} \pmod 5$
   - $6^{273} \pmod 1)1$
2. What is the remainder of $1! + 2! + 3! + \ldots$ when divided by 9?

3. Prove that $2^n + 6 \cdot 9^n$ is always divisible by 7 for any positive integer n.
4. Let $n \in \mathbb{N}^+$ be an integer not divisible by 17. Prove that 17 divides either $n^8 + 1$ or $n^8 - 1$.
5. Let p be a prime. Prove that $(p-1)! \equiv -1 \pmod{p}$.
6. Find all positive integers n such that $3^n - n^2$ is divisible by 5.

Solution:

1. Calculations:
   - $6^{987382934023} \mod 37$

     Note that $6^2 \equiv -1 \pmod{37}$ and that this implies that $6^4 \equiv 1 \pmod{37}$. Thus, $6^{4k} \equiv 1 \pmod{37}$ for any positive integer k. Further, note that $987382934023 = 4k + 3$ for some k. Thus, under $\mod 37$ we have $6^{987382934023} = 6^3 = 6^2 \cdot 6 = -1 \cdot 6 = -6 = 31 \pmod{37}$.
   - $7^{99288399289} \mod 5$

     Note that $7^2 = 49 = -1 \pmod{5} \implies 7^4 = 1 \pmod{5}$. As above, $7^{99288399289} \mod 5 = 7^{4k+1} = 7 = 2 \pmod{5}$.
   - $13^{12301293120} \mod 17$

     Note that $13^2 = 169 = -1 \pmod{17} \implies 13^4 = 1 \pmod{17}$. As in both cases above, $13^{12301293120} \mod 17 = 13^{4k} = 1 \pmod{17}$.
   - $GCD(21, 28, 49)$

     We can break this down as follows: $GCD(21, 28, 49) = GCD(GCD(21, 28), 49)$. Solving individually, we get: $GCD(21, 28) = GCD(3 \cdot 7, 2^2 \cdot 7) = 7$ and $GCD(7, 49) = GCD(7, 7 \cdot 7) = 7$. Thus $GCD(21, 28, 49) = 7$.
   - $7^{920} \pmod{5}$

     We'll use the fast binary exponentiation approach. First, we write out the binary expansion of $920 = 512 + 256 + 128 + 16 + 8 = 2^9 + 2^8 + 2^7 + 2^4 + 2^3$. We now need to perform repeated squaring: $7^1 \mod 5 = 2, 7^2 \mod 5 = 4, 7^4 \mod 5 = 1, 7^8 \mod 5 = 1, \ldots$. So $7^{2^{4+k}} \mod 5 = 1$ for all non-negative k.

     $$7^{920} = 7^{2^9+2^8+2^7+2^4+2^3} = 7^{2^9} \cdot 7^{2^8} \cdot 7^{2^7} \cdot 7^{2^4} \cdot 7^{2^3} = 2 \cdot 4 \cdot 1 \cdot 1 \cdots 1 = 6 = 1 \pmod{5}$$

   - $6^{273} \pmod{11}$

     Writing out the binary expansion of 273 gives us: $273 = 256 + 16 + 1 = 2^8 + 2^4 + 2^0$. Repeatedly squaring gives us: $6^1 = 6 \pmod{11}; 6^2 = 3 \pmod{11}; 6^4 = 9 \pmod{11}; 6^8 = 4 \pmod{11}; 6^{16} = 5 \pmod{11}; 6^{32} = 3 \pmod{11}; 6^{64} = 9 \pmod{11}; 6^{128} = 4 \pmod{11}; 6^{256} = 5 \pmod{11}$.

     $$6^{273} = 6^{2^8+2^4+2^0} = 6^{2^8} \cdot 6^{2^4} \cdot 6^{2^0} = 5 \cdot 5 \cdot 6 = 3 \cdot 6 = 18 = 7 \pmod{11}$$

2. What is the remainder of $1! + 2! + 3! + \ldots$ when divided by 9?

Note that $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 2 \cdot 4 \cdot 5 \cdot 3 * (3 * 2)$ is divisible by 9 and so will all larger factorials. Further, $1! + 2! + 3! = 1 + 2 + 6 = 9$ is also divisible by 9. Thus, the remainder of the sum of all factorials when divided by 9 is the same as the remainder of $4! + 5!$ when divided by 9.

$4! + 5! = 4!(1 + 5) = 8 \cdot 3 \cdot 6$ which is also divisible by 9. Thus the whole expression is divisible by 9 so the remainder is 0.

3. Prove that $2^n + 6 \cdot 9^n$ is always divisible by 7 for any positive integer n.

   $2^n + 6 \cdot 9^n \mod 7 = 2^n + 6 \cdot 2^n = 2^n(1 + 6) = 7 \cdot 2^n = 0 \pmod 7$.

4. Let $n \in \mathbb{N}^+$ be an integer not divisible by 17. Prove that 17 divides either $n^8 + 1$ or $n^8 - 1$.

   We'll look at each number from $1, 2, \ldots, 15, 16$, consider them raised to 8 and show that that must equal ± 1.

   (a) $1^8 = 1 \pmod{17}$.

   (b) $2^8 = 256 = 1 \pmod{17}$ since $255 = 15 \cdot 17$.

   (c) $3^8 = (3^4)^2 = (81)^2 = (-4)^2 = 16 = -1 \pmod{17}$.

   (d) $4^8 = (4^2)^4 = (-1)^4 = 1 \pmod{17}$.

   (e) $5^8 = (5^3)^2 \cdot 5^2 = 6^2 \cdot 8 = 2 \cdot 8 = -1 \pmod{17}$ since 34 and 119 are multiples of 17.

   (f) $6^8 = (6^2)^4 = 2^4 = 4^2 = -1 \pmod{17}$.

   (g) $7^8 = (7^2)^4 = 2^4 = 4^2 = -1 \pmod{17}$.

   (h) $8^8 = (2 \cdot 4)^8 = 1 \cdot (1) = 1 \pmod{17}$

   (i) $9^8 = (3^2)^8 = (-1)^8 = 1 \pmod{17}$.
   Alternatively, $9^8 = (-8)^8 = 8^8 = 1 \pmod{17}$

   (j) $10^8 = (2 \cdot 5)^8 = 1 \cdot (-1) = -1 \pmod{17}$.
   Alternatively, $10^8 = (-7)^8 = 7^8 = -1 \pmod{17}$

   (k) $11^8 = (11^2)^4 = 2^4 = -1 \pmod{17}$ since 119 is a multiple of 17.
   Alternatively, $11^8 = (-6)^8 = 6^8 = -1 \pmod{17}$

   (l) $12^8 = (4 \cdot 3)^8 = 1 * (-1) = -1 \pmod{17}$.
   Alternatively, $12^8 = (-5)^8 = 5^8 = -1 \pmod{17}$

   (m) $13^8 = (13^2)^4 = (-1)^4 = 1 \pmod{17}$ since 170 is a multiple of 17.
   Alternatively, $13^8 = (-4)^8 = 4^8 = 1 \pmod{17}$

   (n) $14^8 = (2 * 7)^8 = 1 \cdot (-1) = -1 \pmod{17}$.
   Alternatively, $14^8 = (-3)^8 = 3^8 = -1 \pmod{17}$

   (o) $15^8 = (3 \cdot 5)^8 = (-1) \cdot (-1) = 1 \pmod{17}$.
   Alternatively, $15^8 = (-2)^8 = 2^8 = 1 \pmod{17}$

   (p) $16^8 = (-1)^8 = 1 \pmod{17}$.

5. Let p be a prime. Prove that $(p - 1)! \equiv -1 \pmod p$.

Proof 1. **Cyclic group:** The numbers $\{1, 2, \ldots, p - 1\}$ are a cyclic group when multiplication is performed $\mod p$. Thus, there is a generator g such that considering everything $\mod p$ the set $\{g^0, g^1, g^2, \ldots, g^{p-1}\}$ is the same as $\{1, 2, \ldots, p - 1\}$. This also implies that $g^{p-1} = 1 \mod p$ as there are p terms in the first set and $p - 1$ in the second so some element is repeated. If $g^k = 1$ for $0 < k < p - 1$ then the first set will not produce $p - 1$ distinct elements and similarly if $g^{k_1} = g^{k_2}$ then once again $p - 1$ distinct elements won't be produced. Note that the squares of g^0 and $g^{(p-1)/2}$ are both 1. Further note that for any i, $g^i \cdot g^{p-1-i} = g^{p-1} = 1 \pmod p$. So every number other than g^0 and $g^{(p-1)/2}$ can be paired up so that their product is 1. g^0 is 1 and since $(p - 1)^2 = (-1)^2 = 1 \pmod p$, $g^{(p-1)/2}$ must be $p - 1$. If all of other elements are paired up, then their product $\mod p$ will be 1 and the only remaining term will be $p - 1 \equiv -1 \pmod p$.

Proof 2. **Bézout's lemma:** Let $k \in \{1, 2, \ldots, p-1\}$. Since p is prime, $GCD(k, p) = 1$ for all k. By Bézout's identity[3] we know that there are integers a, b such that $ak + bp = 1$. Taking modulus with p gives us that $ak = 1 \pmod{p}$ thus $a \mod p \in \{1, 2, \ldots, p-1\}$ is a multiplicative inverse of k. Due to the Bézout's identity equation, we know that this is inverse is unique since what we did for k we could do for a to get the same equation which would imply that k is the inverse of a. So multiplicative inverses are paired or $a = k$. The latter happens iff $k^2 - 1$ is divisible by p which implies that $k \equiv \pm 1 \pmod{p}$. As before, all other numbers pair up and result in 1, except for $p-1$ which causes the factorial to be $-1 \mod p$.

Proof 3. **The bijective inverse function:** Use the fact that for each $x \in \{1, 2, \ldots, p-1\}$ there is a unique y such that $xy \equiv 1 \pmod{p}$. Define $y = f(x)$ to such that $x \cdot f(x) \equiv 1 \pmod{p}$. Since multiplication is commutative, $y = f(x) \implies x = f(y)$. If $f(x) = f(x') = y$ then $xy = x'y \implies x = x' \mod p$ since $GCD(y, p) = 1$, so each x must map to a distinct y. As before, $f(x) = x => x^2 = 1 => x = \pm 1 \pmod{p}$ so $x = 1$ and $x = p-1$ are the only values that map to themselves under the function f. This function is onto (it maps to each value in $\{1, \ldots, p-1\}$). To see this, assume otherwise, so there is some y for which is no x such that $f(x) = y$. However, consider the product of y with each other element in $\{2, \ldots, p-2\}$ (we already know that y is not 1 or $p-1$). There are $p-3$ products and

Proof 4. **Roots of polynomials:** Consider the polynomial $g(x) = x(x-1)(x-2)\cdots(x-(p-1))$. Its degree is $p-1$, due to the leading term x^{p-1} and the constant term is $(p-1)!$. It has $p-1$ roots: $1, 2, \ldots, p-1$. Consider the polynomial $h(x) = x^{p-1} - 1$ which also has degree $p-1$ and leading term x^{p-1}. It is also known that this has the same $p-1$ roots via Fermat's little theorem. If we consider $f(x) = g(x) - h(x)$ it has degree at most $p-2$ since the leading terms cancel out. However, since all of $1, 2, \ldots, p-1$ are roots of both $g(x)$ and $h(x)$ they must be roots of $f(x)$ as well. However, a $p-2$ degree polynomial cannot have $p-1$ roots so $f(x)$ must be zero everywhere and in particular $f(0) = (p-1)! - 1 \equiv 0 \pmod{p}$ which proves the required result.

6. Find all positive integers n such that $3^n - n^2$ is divisible by 5.

$$f(n) = 3^n \mod 5 = 3^{4k+r} \mod 5 = \begin{cases} 3 & r = 1 \\ 4 & r = 2 \\ 2 & r = 3 \\ 1 & r = 0 \end{cases}$$

$$g(n) = n^2 \mod 5 = \begin{cases} 1 & n \mod 5 = 1 \\ 4 & n \mod 5 = 2 \\ 4 & n \mod 5 = 3 \\ 1 & n \mod 5 = 4 \\ 0 & n \mod 5 = 0 \end{cases}$$

For $3^n - n^2$ to be divisible by 5, we need $3^n \equiv n^2 \pmod{5}$. This happens whenever $f(n) = g(n)$ which can only happen when $f(n) \in \{1, 4\}$. This happens when $n \mod 4 = 2$ and $n \mod 5 \in \{2, 3\}$ or when $n \mod 4 = 0$ and $n \mod 5 \in 1, 4$.

We only need to consider numbers upto 20 since $20k + r \equiv r \pmod{5}$ and $20k + r \equiv r \pmod{4}$

[3] If GCD(x, y) = d, then there are integers m, n such that $xm + ny = d$.

so once we characterize the numbers upto 20 for which $3^n - n^2$ is divisible by 5, adding multiples of 20 to those numbers will continue to ensure divisibility by 5.

For $n \in \{0, 1, \ldots, 19\}$, $n \mod 4 = 2$ happens when $n \in [2, 6, 10, 14, 18]$ and taking $\mod 5$ on these n gives us, in order $[2, 1, 0, 4, 3]$. So only 2 and 18 are valid candidates.

Similarly, for $n \equiv 0 \pmod 4$ and $n \mod 5 \in \{1, 4\}$ the number must be in both $\{0, 4, 8, 12, 16\}$ and in $\{1, 4, 6, 9, 11, 14, 16, 19\}$ which implies that $n \in \{4, 16\}$.

Thus, the set of all positive integers n such that $3^n - n^2 \equiv 0 \pmod 5$ is $\{n | n \mod 20 \in \{2, 4, 16, 18\}\}$.

■

Problem 5 (Recurrences Practice)

Solve the following recurrences:

1. $T(n) = 3T(n/2) + n^2$
2. $T(n) = 4T(n/2) + n^2$
3. $T(n) = T(n/2) + 2^n$
4. $T(n) = 16T(n/4) + n$
5. $T(n) = 2^n T(n/2) + n^n$
6. $T(n) = 2T(n/2) + n \lg n$
7. $T(n) = 2T(n/2) + n/\log n$
8. $T(n) = 2T(n/4) + n^{0.51}$
9. $T(n) = 0.5T(n/2) + 1/n$
10. $T(n) = 16T(n/4) + n!$
11. $T(n) = \sqrt{2}T(n/2) + \log n$
12. $T(n) = 3T(n/2) + n$
13. $T(n) = 3T(n/3) + \sqrt{n}$
14. $T(n) = 4T(n/2) + cn$
15. $T(n) = 3T(n/4) + n \log n$
16. $T(n) = 3T(n/3) + n/2$
17. $T(n) = 6T(n/3) + n^2 \log n$
18. $T(n) = 4T(n/2) + n/\log n$
19. $T(n) = 7T(n/3) + n^2$
20. $T(n) = 4T(n/2) + \log n$

Solution:

1. $T(n) = 3T(n/2) + n^2$

   Master theorem: $a = 3, b = 2, c = 2, c_{crit} = \log_2 3 < c$. $T(n) = \Theta(n^2)$.

2. $T(n) = 4T(n/2) + n^2$

   Master theorem: $a = 4, b = 2, c = 2, c_{crit} = \log_2 4 = 2 = c$. $T(n) = \Theta(n^2 \log n)$.

3. $T(n) = T(n/2) + 2^n$

   $T(n) = 2^n$ since the critical exponent will be smaller than some polynomial which will be smaller than the exponential which implies that the exponential will dominate.

4. $T(n) = 16T(n/4) + n$

   Master theorem: $a = 16, b = 4, c = 1, c_{crit} = \log_4 16 = 2 > c$. $T(n) = \Theta(n^2)$.

5. $T(n) = 2^n T(n/2) + n^n$

   Master theorem does not apply since the number of subproblems is not constant.

6. $T(n) = 2T(n/2) + n \lg n$

   Master theorem: $a = 2, b = 2, c = 1, k = 1, c_{crit} = \log_2 2 = 1 = c$. $T(n) = \Theta(n \log^2 n)$.

7. $T(n) = 2T(n/2) + n/\log n$

   Master theorem: $a = 2, b = 2, c = 1, k = -1, c_{crit} = \log_2 2 = 1 = c$. $T(n) = \Theta(n \log\log n)$.

8. $T(n) = 2T(n/4) + n^{0.51}$

   Master theorem: $a = 2, b = 4, c = 0.51, c_{crit} = \log_4 2 = 0.5 < c$. $T(n) = \Theta(n^{0.51})$.

9. $T(n) = 0.5T(n/2) + 1/n$

   Master theorem does not apply since cannot have less than 1 subproblem.

10. $T(n) = 16T(n/4) + n!$

    $T(n) = n!$ since the critical exponent will be smaller than some polynomial which will be smaller than the factorial which implies that the factorial will dominate.

11. $T(n) = \sqrt{2}T(n/2) + \log n$

    Master theorem: $a = \sqrt{2}, b = 2, c = 0, k = 1, c_{crit} = \log_2 2^{1/2} = 1/2 > c$. $T(n) = \Theta(\sqrt{n})$.

12. $T(n) = 3T(n/2) + n$

    Master theorem: $a = 3, b = 2, c = 1, c_{crit} = \log_2 3 > c$. $T(n) = \Theta(n^{\lg 3})$.

13. $T(n) = 3T(n/3) + \sqrt{n}$

    Master theorem: $a = 3, b = 3, c = 1/2, c_{crit} = \log_3 3 = 1 > c$. $T(n) = \Theta(n)$.

14. $T(n) = 4T(n/2) + cn$

    Master theorem: $a = 4, b = 2, c = 1, c_{crit} = \log_2 4 = 2 > c$. $T(n) = \Theta(n^2)$.

15. $T(n) = 3T(n/4) + n \log n$

    Master theorem: $a = 3, b = 4, c = 1, k = 1, c_{crit} = \log_4 3 < c$. $T(n) = \Theta(n \log n)$.

16. $T(n) = 3T(n/3) + n/2$

    Master theorem: $a = 3, b = 3, c = 1, c_{crit} = \log_3 3 = c$. $T(n) = \Theta(n \log n)$.

17. $T(n) = 6T(n/3) + n^2 \log n$

    Master theorem: $a = 6, b = 3, c = 2, k = 1, c_{crit} = \log_3 6 < c$. $T(n) = \Theta(n^2 \log n)$.

18. $T(n) = 4T(n/2) + n/\log n$

    Master theorem: $a = 4, b = 2, c = 1, k = -1, c_{crit} = \log_2 4 > c$. $T(n) = \Theta(n^2)$.

19. $T(n) = 7T(n/3) + n^2$

    Master theorem: $a = 7, b = 3, c = 2, c_{crit} = \log_3 7 < c$. $T(n) = \Theta(n^2)$.

20. $T(n) = 4T(n/2) + \log n$

    Master theorem: $a = 4, b = 2, c = 0, k = 1, c_{crit} = \log_2 4 > c$. $T(n) = \Theta(n^2)$.

■

Problem 6 (Divide and Destroy)

Given a length n array $A[1 \ldots n]$, describe an $O(\log n)$ algorithm for the following:

(a) A is a circular sorted array, that is, an array which is sorted and then rotated by k indices such that $A[1 \dots k-1]$ and $A[k \dots n]$ are both sorted and concatenating $A[k \dots n] \circ A[1 \dots k-1]$ would return an overall sorted array. Find the value k by which A was rotated.

(b) A is a unimodal array, that is, an array in which $A[1 \dots k]$ is sorted in ascending order and $A[k \dots n]$ is sorted in descending order so that $A[k]$ forms a unique peak/mode in the array. Find the index of an input number x.

(c) A is a sorted array, where all numbers occur twice except a number x which occurs only once. Find the index of x.

[***Hint**: You've already seen divide and destroy algorithms for searching.*]

Solution:

All of these can be solved by using binary search like ideas, that is, you perform some comparison like operation using the middle index of the input array, discard half the array, and then recurse on the remaining half. In each subpart: in each step we do constant work, remove half the input and recurse on the remaining half. Thus, $T(n) = T(n/2) + 1 = \Theta(\lg n)$.

(a) Finding the rotation value k in a circular sorted array.

Note that the number of indices k that A is rotated by is also the index where the minimum element will end up at after rotation. Further note that the minimum element has the unique property that both its neighboring elements are greater than it. Lastly note that a subarray $A[i \dots j]$ contains k iff it is not sorted, that is, iff $A[j] < A[i]$. We modify binary search using these ideas.

Let our input be $A[L \dots M \dots R]$, so that we keep track of the leftmost index L, the rightmost index R, and the middle index M. If $A[M-1] > A[M] < A[M+1]$, then M is the index of interest. If not, then recurse in the left subarray if $A[L] > A[M]$ and into the right subarray if $A[L] < A[M]$.

(b) A is a unimodal array.

Let M be the middle index in the array. If $A[M-1] < A[M] > A[M+1]$ then M is the peak element and we're done. If $A[M] < A[M+1]$ the index M is part of the increasing part and the peak is to the right. Otherwise the peak is to the left. This takes $O(\log n)$ time.

Once the peak has been found, then we know that the sub-arrays to the left and right are both sorted. We run a binary search in each spending another $O(\log n)$ time on each. The overall time complexity remains $O(\log n)$.

(c) A has all numbers except one occurring twice.

Property: In all arrays like this, assuming 0 indexing, before the unique element, the indices of a pairs will have parity (even, odd) while after the unique element indices of pairs will have parity (odd, even).

The algorithm behaves similar to a binary search, however, you do not compare the value in the array to a target value, instead you check whether neighboring even–odd indices in the array have the same value. If they do, then every number before that index were repeated twice and the unique number is to the right, so you recurse on the right half. If these indices differ, then at some point to the left of the current index, the unique number occurred and shifted the

repeated pairs from being in even-odd indices to being in odd-even indices, so you recurse on the left half of the array.

Alternate approach uses another property:
Property: For an array to have every element repeated twice except for one unique element, the length of the array must be odd.

Look at the middle element and its two neighbors, if they're all distinct, then the middle element is the unique element. If not, then consider the pair in these three elements and split the array into two excluding this pair. The unique element must be on the side that will have an odd length after the pair is excluded. The side which has an even length cannot have the unique element due to the property we described above. Recurse on the side containing the element.

■