CS70 Discrete Mathematics and Probability Theory, Spring 2024

Midterm

7:00-9:00pm, 6 March 2024

Your First Name: **Your Last Name:**

SIGN Your Name: **Your SID Number:**

Your Exam Room:

Name of Person Sitting on Your Left:

Name of Person Sitting on Your Right:

Name of Person Sitting in Front of You:

Name of Person Sitting Behind You:

Instructions:

(a) *As soon as the exam starts,* **please write your student ID in the space provided at the top of every page!** *(We will remove the staple when scanning your exam.)*

(b) *There are 14 pages (2-sided) on the exam. Notify a proctor immediately if a page is missing.*

(c) *We will* **not** *grade anything outside of the space provided for a question (i.e., either a designated box if it is provided, or otherwise the white space immediately below the question).* **Be sure to write your full answer in the box or space provided!** *Scratch paper is provided on request; however, please bear in mind that nothing you write on scratch paper will be graded!*

(d) **The questions vary in difficulty, so if you get stuck on any question you are strongly advised to leave it and return to it later. In particular, you may find some of the later questions easier than some of the earlier ones.** *There is no penalty for incorrect answers.*

(e) *In the interests of fairness, proctors will* **not** *answer clarifying questions during the exam. If you believe there is an ambiguity or error in a problem, write down what you think is the most appropriate response and move on. Any legitimate such issues will be handled during grading.*

(f) *You may consult* **one two-sided "cheat sheet"** *of notes. Apart from that, you may not look at any other materials. Calculators, phones, computers, and other electronic devices are* **not** *permitted.*

(g) *You may use, without proof, theorems and lemmas that were proved in the notes and/or in lecture.*

(h) *You have 120 minutes: there are 10 questions on this exam worth a total of 105 points.*

[exam starts on next page]

1. Warm-Up Multiple Choice [2 points].

Bob is in court being tried for stealing a bag of diamonds. The judge says: "If Bob stole the diamonds, then he didn't do it alone." Bob's attorney says: "That is not true!" Assuming that the attorney is telling the truth, which of the following statements must be true? [*Shade one bubble; no justification; no penalty for incorrect answers.*] *2pts*

Bob stole the diamonds, and did so alone.

The judge's statement is of the form: $A \Rightarrow B$ where A is "Bob stole the diamonds" and B is "He did not do it alone". The attorney's (true) assertion is:

$$\neg(A \Rightarrow B) \equiv \neg(\neg A \vee B) \equiv A \wedge (\neg B)$$

from which the answer follows.

2. True/False [12 points].

Answer by shading the correct bubble; no justification; no penalty for incorrect answers.

TRUE FALSE

● ○ If the halting problem is computable, then pigs can fly. *2pts*

This is an implication $A \implies B$, where A is "The halting problem is computable" and B is "Pigs can fly." Since A is false, the implication must be true (no matter what B is!).

○ ● $\forall x(P(x) \Rightarrow Q(x))$ is logically equivalent to $\neg\exists x\big(\neg P(x) \wedge Q(x)\big)$. *2pts*

$\forall x(P(x) \Rightarrow Q(x)) \equiv \neg\neg\forall x(Q(x) \vee \neg P(x))$, which by de Morgan is equivalent to $\neg\exists x(\neg Q(x) \wedge P(x))$. Clearly this is not equivalent to $\neg\exists x\big(\neg P(x) \wedge Q(x)\big)$.

● ○ $Q(0) \wedge (\forall n \in \mathbb{N})\big([P(n) \Rightarrow Q(n+1)] \wedge [Q(n) \Rightarrow P(n)]\big) \Rightarrow (\forall n \in \mathbb{N})P(n)$. *2pts*

The conjunction of the two implications $P(n) \Rightarrow Q(n+1)$ and $Q(n+1) \Rightarrow P(n+1)$ is equivalent to $P(n) \Rightarrow P(n+1)$. Together with $P(0)$, this is equivalent to the principle of mathematical induction, so $\forall n \in \mathbb{N})P(n)$ holds.

○ ● $Q(0) \wedge (\forall n \in \mathbb{N})\big([P(n) \Rightarrow Q(n+1)] \wedge [Q(n) \Rightarrow P(n+1)]\big) \Rightarrow (\forall n \in \mathbb{N})P(n)$. *2pts*

Starting from $Q(0)$, we can deduce the following implications: $Q(0) \Rightarrow P(1) \Rightarrow Q(2) \Rightarrow P(3) \Rightarrow \ldots$. Thus we can only deduce that $P(n)$ holds for odd n, not for all n.

● ○ The following problem is computable: Given as input a decimal number x with a finite number n of digits, is x the first n digits of the decimal expansion of π? *2pts*

There are many ways (going back centuries) to approximate π to any desired number of digits using power series. A computer can solve this problem by doing that computation to n digits and checking against the input number x.

○ ● The following problem is computable: Given as input a program P and two strings x, y, does P output y on input x? *2pts*

If this problem Π were computable, we could solve the halting problem as follows. To test if a program P halts on input x, modify P to a new program P' that outputs a special symbol $\perp$ whenever it halts, and then give the input $(P', x, \perp)$ to Π.

[exam continues on next page]

3. Stable Matching T/F [10 points].

Answer by shading the correct bubble; no justification; no penalty for incorrect answers.

TRUE FALSE

● ○ In a stable matching instance, if we run the propose-and-reject algorithm twice, once with jobs proposing and once with candidates proposing, and candidate C is matched with job J in both cases, then C must be matched with J in every stable pairing. *2pts*

Since J is matched with C in the job-optimal pairing, J cannot be matched with a more preferred job in any stable pairing. Since J is matched with C in the candidate-optimal pairing (which is also the job-pessimal pairing), J cannot be matched with a less preferred job in any stable pairing. Hence J must be matched with C in any stable pairing.

● ○ In a stable matching instance with n jobs and n candidates, for any n, the job-optimal pairing may contain a pair (J, C) where J is C's least favorite job and C is J's least favorite candidate. *2pts*

Consider an instance in which each job $J_i \neq J$ puts candidate $C_i \neq C$ at the top of its list, and vice versa. Candidate C puts job J at the bottom of its list, and vice versa (and the rest of these lists are arbitrary). Then the only stable pairing is the set of pairs $\{(J_i, C_i)\}$ and (J, C), because any J_i or C_i not matched with its favorite partner will create a rogue couple.

The next three questions use the following terminology. In a stable matching instance, we call a job J and a candidate C an *ideal pair* if C is J's top-ranked candidate and J is C's top-ranked job. We call J, C a *hell pair* if C is J's bottom-ranked candidate and J is C's bottom-ranked job. And we call J, C *outcasts* if both J and C are ranked last by all other candidates and jobs, respectively.

TRUE FALSE

● ○ If J, C are an ideal pair, then they must be matched with each other in any stable pairing. *2pts*

Suppose in some pairing J is matched with some $C' \neq C$ (and therefore also J must be matched with some $J' \neq J$). Then J, C is a rogue couple so the pairing isn't stable.

● ○ If J, C are a hell pair, and J', C' are another hell pair, then it is not possible for J to be matched with C and J' with C' in the same stable pairing. *2pts*

Suppose some pairing contains both pairs (J, C) and (J', C'). Then J, C' (and also J', C is a rogue couple, because they prefer each other to their current partners (who are their least favorites).

● ○ If J, C are outcasts, then they must be matched with each other in any stable pairing. *2pts*

Suppose some pairing contains the pairs (J, C') and (J', C). Then C', J' is a rogue couple, because each prefers each other to their current partners (who are their least favorites). Hence every stable pairing must match J with C.

[exam continues on next page]

4. Logical Robot [10 points].

You've just unboxed your brand new personal assistance robot! As you flip through its user manual, you encounter the following propositional variables defining its behavior at a particular moment:

P: the robot is powered on
M: the robot is in motion
A: the robot's alarm system is activated
R: the robot is rerouting
S: the robot senses an obstacle in its path

(a) Express in logic: "The robot is not in motion unless it is powered on." *2pts*

$$\neg P \implies \neg M \qquad \text{(or equivalently } M \implies P\text{)}$$

The English statement above is equivalent to saying "If the robot is powered off then it is not in motion" which corresponds directly to the propositional logic form above. Note that it does not say whether or not the robot is in motion when it is powered on.

(b) Express in logic the *contrapositive* of the following statement: "If the robot is powered on, then it is either in motion or its alarm system is activated." *2pts*

The statement is $P \implies (M \vee A)$. Therefore the contrapositive is $(\neg M \wedge \neg A) \implies \neg P$.

(c) Now assume the following propositional forms are true (and ignore any statements in parts (a)–(b)): *4pts*

- $M \Rightarrow P$
- $(S \wedge A) \Rightarrow (\neg R \vee \neg P)$
- $(P \wedge M \wedge R) \Rightarrow S$
- $(P \wedge S) \Rightarrow (A \vee \neg M)$

If you also assume that the robot is in motion (M is true), what can you deduce about the values of R and S? [*Shade one bubble; no justification; no penalty for incorrect answers.*]

R is false & S could be either true or false.

This answer follows from the following set of inferences. First, note that M is true. Since $M \Rightarrow P$, therefore P is also true. Thus, the 2nd, 3rd, and 4th statements simplify to:

(i) $(S \wedge A) \Rightarrow \neg R$
(ii) $R \Rightarrow S$
(iii) $S \Rightarrow A$

Now consider a case split on the value of S.
If S is true, then so is A, by (iii), and therefore by (i), R is false.
If S is false, then by (ii), R must also be false. In either case R is false. We do not know, however, whether S is true or false; both values are possible.

(d) Later in the manual, you see the following predicates defining the robot's behavior at any given time $t \geq 0$: *2pts*

$L(t)$: the robot battery is low at time t $\quad C(t)$: the robot is charging at time t

Express in logic: "At all times t, if the robot battery is low at t, then there is some future time strictly later than t when it is charging."

$$\forall t \left(L(t) \implies \exists u \left[u > t \wedge C(u) \right] \right)$$

[exam continues on next page]

5. Spot the Errors [6 points].

Each of the induction proofs below contains a single fatal error. Shade the **single bubble** corresponding to the step in the proof that contains the error, and also explain the error **clearly and concisely** in the box provided. Do not attempt to write a lot of text—one sentence is typically enough! Points will be deducted for long-winded or imprecise answers.

(a) **Claim:** For all integers $n \geq 0$, we have $2^n = 1$. *3pts*

Proof:

◯ The base case $n = 0$ holds because $2^0 = 1$.

● For the inductive step, we write $n + 1 = i + j$ for two positive integers i, j with $i, j \leq n$.

◯ By strong induction, we may assume that the claim holds for i and j.

◯ Therefore, we have: $2^{n+1} = 2^i 2^j = 1 \times 1 = 1$.

◯ Hence the claim holds for $n + 1$.

The inductive step highlighted above claims that we can write $1 = i + j$ for two positive integers i, j. But this claim is not true when $n = 0$, since $n + 1 = 1$ cannot be written in this way! (In detail, this means that going from the base case $P(0)$ to $P(1)$ fails, so of course the whole induction fails.)

(b) **Claim:** The sum of the interior angles of any polygon with $n \geq 3$ vertices is $180(n - 2)$ degrees. *3pts*

Proof:

◯ The base case $n = 3$ claims that the sum of the interior angles of a triangle is 180 degrees, which we know is true.

◯ For the inductive step, assume the claim holds for a polygon with n vertices.

● Now extend this polygon to one with $n + 1$ vertices by "adding a triangle", i.e., by replacing one of its edges by two new edges and a vertex.

◯ The increase in the sum of interior angles is exactly the angles of the added triangle, which is 180 degrees.

◯ Thus the new angle sum is $180(n - 2) + 180 = 180((n + 1) - 2)$, so the claim holds also for a polygon with $n + 1$ vertices.

This is a classic case of "build-up error." Rather than claiming that any n-gon can be extended to an $(n+1)$-gon by adding a triangle, the inductive step has to start from an $(n+1)$-gon and argue that we can remove a triangle from it to obtain an n-gon. (This is in fact true, but it needs to be written that way and justified.)

[exam continues on next page]

6. Induction [10 points].

Prove parts (a) and (b) below by induction on n. Clearly label your base case and induction step for each part.

(a) Recall the Fibonacci numbers, defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Prove that $F_0^2 + F_1^2 + \ldots + F_n^2 = F_n F_{n+1}$ for all $n \geq 0$. *5pts*

We prove by induction on $n \geq 0$.
Base Case: Consider $n = 0$. LHS = $F_0^2 = 0$. RHS = $F_0 F_1 = 0 \cdot 1 = 0$ = LHS.
Induction Step: Assume the statement holds for $n = k$. We show that it holds for $n = k + 1$.
The induction hypothesis is $F_0^2 + F_1^2 + \ldots + F_k^2 = F_k F_{k+1}$.
For $n = k + 1$,

$$\begin{aligned} \text{LHS} &= F_0^2 + F_1^2 + \ldots + F_k^2 + F_{k+1}^2 \\ &= F_k F_{k+1} + F_{k+1}^2 \\ &= F_{k+1}(F_k + F_{k+1}) \\ &= F_{k+1} F_{k+2} \\ &= \text{RHS} \end{aligned}$$

from which the result follows. □

(b) Prove that $\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2$ for all $n \geq 1$. [HINT: You may use the fact that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.] *5pts*

Base Case: For $n = 1$, LHS = $1^3 = 1$. RHS = $1^2 = 1$ = LHS.
Induction Step: Assume the statement holds for $n = k$. We show that it holds for $n = k + 1$.
The induction hypothesis is $\sum_{i=1}^{k} i^3 = \left(\sum_{i=1}^{k} i\right)^2$.
Now consider $n = k + 1$.

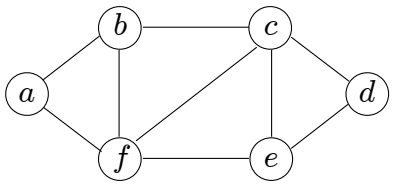
$$\begin{aligned} \text{LHS} &= \sum_{i=1}^{k+1} i^3 = \left(\sum_{i=1}^{k} i^3\right) + (k+1)^3 \\ &= \left(\sum_{i=1}^{k} i\right)^2 + (k+1)^3 \qquad \text{(by induction hypothesis)} \\ &= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \qquad \text{(using Hint)} \\ &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= (k+1)^2 \cdot \left(\frac{k^2}{4} + (k+1)\right) = (k+1)^2 \cdot \left(\frac{k^2 + 4k + 4}{4}\right) \\ &= \frac{(k+1)^2(k+2)^2}{2^2} \\ &= \left(\sum_{i=1}^{k+1} i\right)^2 = \text{RHS} \qquad \text{(using Hint again)} \end{aligned}$$

from which the result follows. □

7. Graphs [14 points].

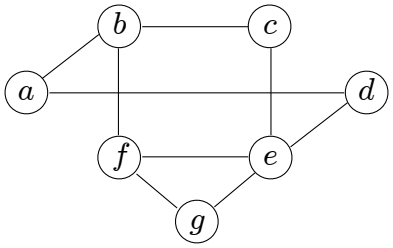
For parts (a) and (b), write your answer only in the box provided (no justification).

(a) Which one edge must be added to the following graph so that it contains an Eulerian tour? *2pts*



Answer: edge $\{b, e\}$. A graph contains an Eulerian tour if and only if all vertices have even degree. Here the only two odd-degree vertices are b, e, so we have to add the edge between them to make all degrees even.

(b) Which one vertex must be removed from the following graph so that it contains a Hamiltonian cycle? *2pts*
[Recall that a Hamiltonian cycle is a cycle that visits every vertex of a graph exactly once.]



Answer: vertex c. Note that removing c leaves the Hamiltonian cycle (a, b, f, g, e, d, a). To see that we must in fact remove c (and not some other vertex), note that any Hamiltonian cycle that includes c must include the path (b, c, e) because c has only these two neighbors. If we don't remove a then this path must actually extend to d, a, b, c, e (since a has only two neighbors), and at this point we are stuck. But we can't remove a since doing so would leave d with only one neighbor. So the only vertex we could possibly remove is c.

(c) Let T be a tree with n vertices. Suppose T has a vertex of degree k. Prove that T has at least k leaves. *4pts*

Suppose T has exactly ℓ leaves, which we will label $1, 2, \ldots, \ell$, and label the vertex of degree k by $\ell + 1$. Denoting by d_i the degree of vertex i, for $1 \leq i \leq n$, we have that

$$\sum_{i=1}^{n} d_i = 2(n-1), \tag{1}$$

since any tree with n vertices has $n-1$ edges. But we know that $d_1 = d_2 = \ldots = d_\ell = 1$ (the leaves), $d_{\ell+1} = k$, and $d_i \geq 2$ for all $\ell + 2 \leq i \leq n$ (since the other vertices are not leaves). Plugging these values into (1) gives

$$2(n-1) \geq \ell + k + 2(n - \ell - 1).$$

Simplifying this inequality gives $\ell \geq k$, which means that G has at least k leaves.

[exam continues on next page]

An alternative approach is the following. Let v denote the vertex of degree k, and let $v_1, \ldots, v_k$ denote its neighbors. If we remove v and the edges $\{v, v_i\}$ from T, we are left with k disjoint subtrees, each containing one of the v_i. Now each of these subtrees is either the single vertex v_i (which is then a leaf of T) or contains at least two leaves (which we proved in discussion), at least one of which is not v_i and is therefore a leaf of T. Hence T contains at least k leaves.

[exam continues on next page]

[Q7 continued]

(d) The *girth* of a graph G is the number of edges in a shortest cycle in G. (If G has no cycles then its girth is ∞.) Suppose that G is connected, has $n = 80$ vertices, $e = 135$ edges, and girth 5. Is G planar? Explain your answer carefully and show all your work. You may use Euler's theorem relating the numbers of vertices, edges and faces of planar graphs, provided you state it clearly. *6pts*

We start from Euler's formula: For any planar graph G, we have $f = e - v + 2$. Proceeding as in the proof of this formula (Theorem 5.2 in Note 5), we can write $\sum_i s_i = 2e$, where s_i denotes the number of sides of face i. Now the fact that G has girth 5 means that $s_i \geq 5$ for each i, and hence $5f \leq 2e$, or equivalently, $f \leq \frac{2e}{5}$. Plugging this into Euler's formula yields $e - v + 2 \leq \frac{2e}{5}$, which after rearranging is $3e \leq 5v - 10$. Finally, we see that this inequality is violated when we plug in $v = 80$, $e = 135$, meaning that the given graph G is not planar.

8. Modular Arithmetic and RSA [17 points].

(a) **Short answers.** Write your answer only in the box provided (no justification).

(i) Calculate $1! + 3! + 5! + \ldots + 99! \pmod{24}$. *2pts*

Answer: $7 \pmod{24}$. The key observation is that $24 = 4!$, which is a factor of all the terms in the sum except for the first two. Thus the sum is just $1! + 3! \pmod{24} = 7 \pmod{24}$.

(ii) Solve the equation $5x \equiv 7 \pmod{11}$. *2pts*

Answer: 8. We find the inverse of 5 mod 11, which is 9. (We can do this either by trial and error or using extended gcd.) Multiplying through by 5^{-1} we get $x = 5^{-1} \times 5 \times x = 5^{-1} \times 7 = 9 \times 7 = 8 \pmod{11}$.

(iii) What is the units digit of 7^{96} ? *2pts*

Answer: 1. Looking at the units digit of the first few powers of 7, we get $7, 9, 3, 1, 7, \ldots$, at which point the sequence must repeat. The sequence has period 4, so since $96 = 0 \pmod{4}$, we see that the units digit must be 1.

(iv) Suppose Bob implements RSA using the primes $p = 7$, $q = 11$ and $e = 11$. What is Bob's public key? *2pts*

Bob's public key is (N, e), where $N = pq$. So the key is $(77, 11)$.

(v) In the same scenario as part (iv), suppose Carol wants to send Bob the message $x = 3$. What encrypted value should Carol send to Bob? *2pts*

Answer: 47. Following the RSA protocol, if Carol's message is x then she should send to Bob the encrypted value $x^e \pmod{N}$, which in this case is $3^{11} \pmod{77}$. We can calculate this by noting that $3^4 = 81 = 4 \pmod{77}$, so $3^8 = 16 \pmod{77}$ and $3^{11} = 16 \times 27 = 432 = 47 \pmod{77}$.

(vi) Again in the same scenario as part (iv), suppose Bob receives from Carol the encrypted message $y = 47$. What was Carol's original message? *2pts*

Answer: 3. Again following RSA, to decrypt the received message y, Bob needs to compute $y^d \pmod{N}$, where $d = e^{-1} \pmod{(p-1)(q-1)} = 11^{-1} \pmod{60} = 11$ is his private key. So Bob computes $47^{11} \pmod{77}$. Fortunately, we don't actually need to do this computation since we know from part (v) that 47 is the encryption of the message 3. Hence, by the bijective property of RSA, we know that Bob must in fact obtain the value 3.

[exam continues on next page]

[Q8 continued]

(b) Nathan wants to prepare his favorite dish, the Tropical Trio Fruit Salad, a delicious mix of *lychee* (L), *mango* (M), and *passion fruit* (P). However, the local supermarket rarely stocks these exotic fruits. Based on Nathan's observations: *5pts*

- Lychees (L) are available every 5 days and were last seen in store 3 days ago;
- Mangoes (M) appear every 3 days and were last seen yesterday (1 day ago);
- Passion fruits (P) show up every 11 days and were last seen 2 days ago.

But there's a catch! The salad needs to be made the very day these fruits are purchased, in case they spoil. In how many days at the soonest will Nathan be able to buy on the same day all three fruits he needs? [HINT: One approach is to use the Chinese Remainder Theorem.]

Answer: 152 days. Call today Day 0. Let x be the first day on which all ingredients are simultaneously available. Then x must satisfy the following three equations:

$$\begin{aligned} x+3 &= 0 \pmod 5 \quad \text{i.e., } x = 2 \pmod 5 \\ x+1 &= 0 \pmod 3 \quad \text{i.e., } x = 2 \pmod 3 \\ x+2 &= 0 \pmod{11} \quad \text{i.e., } x = 9 \pmod{11} \end{aligned}$$

The fact that there is a unique such $x \pmod{165 = 3 \times 5 \times 11}$ follows from the Chinese Remainder Theorem, since $3, 5, 11$ are coprime. The automatic way to solve for x is to use the algorithm in the notes (and you are encouraged to try this). However, since these are fairly small numbers it is probably quicker to do it by brute force, as follows. Listing the positive numbers that are equal to $9 \pmod{11}$, we get $9, 20, 31, 42, 53, 64, 75, 86, 97, \ldots$. The ones that are equal to 2 (mod 5) are $42, 97, 152, \ldots$. Of these, the first that is equal to 2 (mod 3) is 152.

9. Polynomials, Secret Sharing, and ECCs [16 points].

A group of students are participating in a treasure hunt on an island. Here is what they are told:

- The treasure is hidden at coordinates (x, y), where $x, y \in \{0, 1, \ldots, p-1\}$ for a large prime number $p > 20$.
- There is a polynomial P of degree $d = 2$ such that $x = P(10) \pmod p$ and $y = P(20) \pmod p$.
- Several hints are spread across the island. On each hint is written an integer $2 \leq k \leq p-1$ and the corresponding value $0 \leq P(k) \leq p-1$ of the polynomial. No two hints contain the same integer k, and there are no hints with $k = 10$ or $k = 20$.

Without any hints, the treasure could be in any of p^2 locations (x, y) (since there are p choices for x, and p choices for y).
For parts (a)-(c), write your answer only in the box provided (no justification).

(a) How many hints do the students need to find in order to determine the exact location of the treasure? *2pts*

Answer: 3. Three points are required to uniquely specify a polynomial P of degree 2.

(b) The students have now found one hint. Given this information, in how many different locations (x, y) could the treasure still be? *2pts*

Answer: p^2. At this point the students know just one point $P(k)$ ($k \neq 10, 20$) on the degree-2 polynomial P. This information is still consistent with any two additional values $P(10)$ and $P(20)$, so the treasure could be at any of the p^2 positions.

(c) The students have now found two hints in total. In how many different locations (x, y) could the treasure still be? *2pts*

Answer: p. At this point the students know two points on the degree-2 polynomial P. Thus $P(10)$ may still take on any of the p possible values, but once it is known P (and therefore also $P(20)$) is completely specified.

(d) The students have found the following three hints: $P(0) = 5$, $P(1) = 5$, $P(3) = 11$. Find $P(x)$. *4pts*
[HINT: You do not know p, except for the fact that it is a large prime. In this example, you can deduce the coefficients of P without knowing p. Rather than using Lagrange interpolation, write $P(x) = ax^2 + bx + c$ and solve equations for a, b, c.]

Answer: $P(x) = x^2 - x + 5$. We need to interpolate to find P from the three given points $(0, 5), (1, 5), (3, 11)$, with all arithmetic mod a large prime p. We could use Lagrange interpolation, but it's easier here just to write down the equations and solve them directly, as suggested in the hint. Writing $P(x) = ax^2 + bx + c$, we get the following equations for the coefficients a, b, c:

$$\begin{aligned} c &= 5 \\ a + b + c &= 5 \\ 9a + 3b + c &= 11. \end{aligned}$$

The first equation immediately gives $c = 5$. Subtracting a multiple of 3 times the second equation from the third gives $6a - 2c = -4$, and hence $6a = 6$. Thus $a = 1$. (Note that we got lucky here and didn't need to know the inverse of 6 mod p, which is just as well since at this point we're not given p!) Finally, substituting back the values of a, c into the second equation gives $b = -1$. (Again, writing b as -1 (rather than as $p - 1$) means we don't need to know p.)

[exam continues on next page]

[Q9 continued]

(e) You are now given that $p = 89$. Use the polynomial P from part (d) to determine the location of the treasure. *2pts*

Answer: $(6, 29)$. We know that the coordinates of the treasure are (x, y), where $x = P(10) \pmod{89}$ and $y = P(20) \pmod{89}$. Thus we have $x = 100 - 10 + 5 = 95 = 6 \pmod{89}$, and $y = 400 - 20 + 5 = 385 = 29 \pmod{89}$.

For parts (f)-(g), write your answer only in the box provided (no justification).

(f) Now suppose that one of the hints may be incorrect. How many hints in total do the students need to determine whether one of their hints is incorrect? *2pts*

Answer: 4. Given four hints, the students can use any three of them to construct a unique degree-2 polynomial that passes through those hints. They then just need to check if the fourth point lies on that same polynomial: if so, then all the hints are correct, otherwise one of them is incorrect.

NOTE: Some students instead gave the answer 3, possibly based on the following reasoning. Given 3 points, the students can construct the unique polynomial Q through them, then evaluate $Q(10)$ and $Q(20)$, and finally visit the location $(Q(10, Q(20))$ and check if the treasure is there. If so, then all the hints are correct, and if not, then at least one of them is incorrect. This is not the solution we had in mind, and arguably it does "cheat" a bit by using the additional information of visiting a location, but we decided to award it full credit anyway.

(g) How many hints in total do the students need to find the correct polynomial, given that they have one incorrect hint (but don't know which one it is)? *2pts*

Answer: 5. The situation here is analogous to a noisy channel in which packets can be corrupted. The students need to obtain $n = 3$ correct hints in order to reconstruct their polynomial P. Suppose they are given m hints, $k = 1$ of which may be incorrect. Then we know from Berlekamp-Welch that, if the number of hints satisfies $m \geq n + 2k = 5$, then reconstruction is possible.

[exam continues on next page]

10. Countability [8 points].

Consider an infinite grid city, represented by $\mathbb{Z} \times \mathbb{Z}$, where the roads form a perfect grid pattern and each pair of integers (x, y) represents an intersection. A vehicle starts at the origin $(0, 0)$, pointing upwards. Then at each intersection, the vehicle can choose to drive straight, turn left or turn right. For example, it can first drive to either one of the $(-1, 0)$, $(0, 1)$ or $(1, 0)$ intersections. For each of the following sets, *determine whether the set is countable or uncountable, and give a one-sentence justification* by relating the set to specific examples or theorems covered in class.

(a) The set of all intersections $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that x and y are co-prime. *2pts*

Yes. It is a subset of $\mathbb{Z}^2$ which is countable, and so it is itself countable.

(b) The set of all possible finite routes the vehicle can take. *2pts*

Yes. A finite route can be encoded as a finite string using the alphabet $\{L, S, R\}$ (left, straight, right) and the set of finite ternary strings $\{L, S, R\}^*$ is countable. (For example by enumerating its elements in lexicographic order.)

(c) The set of all possible infinite routes the vehicle can take. *2pts*

No. An infinite route can be modeled as an infinite string using the alphabet $\{L, S, R\}$ (left, straight, right). We know that the set of infinite binary strings is uncountable (from lecture/notes), so our set of infinite ternary strings is also uncountable.

(d) At each intersection $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, there is a parking lot with $|x| + |y|$ parking spots. For example, at intersection $(-3, 7)$, there are $|-3| + |7| = 10$ parking spots. Is the set of all parking spots in the city countable? *2pts*

Yes. The set of parking spots at each intersection is finite, the set of all intersections $\mathbb{Z} \times \mathbb{Z}$ is countable, and a countable union of finite sets is countable.

More details: For a fixed intersection (a, b), there is a fixed finite number of parking spots ($|a|+|b|$). So the set of parking spots at any given intersection is finite. Since the set of all intersections is countable, the set of all parking spots, being a countable union of finite sets, is also countable. One way to go about enumerating them would be to start at $(0, 0)$, go to $(1, 0)$, count the one parking spot (spot 1), go to $(1, 1)$, count the two parking spots (spots 2, 3), go to $(1, 0)$, count the one parking spot (spot 4), go to $(-1, 1)$, count the two parking spots (spots 5, 6), etc, and keep iterating like this in an infinite spiral.

[End of exam!]