CS 70 Discrete Mathematics and Probability Theory
Summer 2019 James Hulett and Elizabeth Yang

HW 3

Due: July 14, 2019 at 11:59 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Squared RSA

(a) (10 points) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where a is coprime to p, and p is prime. (Hint: Try to mimic the proof of Fermat's Little Theorem from the notes.)

(b) (10 points) Now consider the RSA scheme: the public key is $(N = p^2q^2, e)$ for primes p and q, with e relatively prime to $p(p-1)q(q-1)$. The private key is $d = e^{-1} \pmod{p(p-1)q(q-1)}$. Prove that the scheme is correct for x relatively prime to both p and q, i.e. $x^{ed} \equiv x \pmod{N}$.

2 Breaking RSA (15 points)

Eve is not convinced she needs to factor $N = pq$ in order to break RSA. She argues: "All I need to know is $(p-1)(q-1)$... then I can find d as the inverse of e mod $(p-1)(q-1)$. This should be easier than factoring N." Prove Eve wrong, by showing that if she knows $(p-1)(q-1)$, she can easily factor N (thus showing finding $(p-1)(q-1)$ is at least as hard as factoring N). Assume Eve has a friend Wolfram, who can easily return the roots of polynomials over $\mathbb{R}$ (this is, in fact, easy).

3 Lagrange? More like Lamegrange.

In this problem, we walk you through an alternative to Lagrange interpolation.

(a) (5 points) Let's say we wanted to interpolate a polynomial through a single point, (x_0, y_0). What would be the polynomial that we would get? (This is not a trick question.)

(b) (5 points) Call the polynomial from the previous part $f_0(x)$. Now say we wanted to define the polynomial $f_1(x)$ that passes through the points (x_0, y_0) and (x_1, y_1). If we write $f_1(x) = f_0(x) + a_1(x - x_0)$, what value of a_1 causes $f_1(x)$ to pass through the desired points?

(c) (5 points) Now say we want a polynomial $f_2(x)$ that passes through (x_0, y_0), (x_1, y_1), and (x_2, y_2). If we write $f_2(x) = f_1(x) + a_2(x - x_0)(x - x_1)$, what value of a_2 gives us the desired polynomial?

(d) (5 points) Suppose we have a polynomial $f_i(x)$ that passes through the points (x_0, y_0), ..., (x_i, y_i) and we want to find a polynomial $f_{i+1}(x)$ that passes through all those points and also (x_{i+1}, y_{i+1}). If we define $f_{i+1}(x) = f_i(x) + a_{i+1} \prod_{j=0}^{i} (x - x_j)$, what value must a_{i+1} take on?

4 Error-Correcting Polynomials

(a) (5 points) Alice has a length 8 message to Bob. There are 2 communication channels available. When n packets are fed through channel A, the channel will only deliver 5 packets (picked at random). Similarly, channel B will only deliver 5 packets (picked at random), but it will also corrupt (change the value) of one of the delivered packets. Each channel will only work if at least 10 packets are sent through it. Using each of the 2 channels once, how can Alice send the message to Bob?

(b) (5 points) Alice wishes to send a message to Bob as the coefficients of a degree 2 polynomial P. For a message $[m_1, m_2, m_3]$, she creates polynomial $P = m_1x^2 + m_2x + m_3$ and sends 5 packets: $(0, P(0)), (1, P(1)), (2, P(2)), (3, P(3)), (4, P(4))$. However, Eve interferes and changes one of the values of a packet before it reaches Bob. If Bob receives

$$(0,3), (1,0), (2,3), (3,0), (4,3),$$

and knows Alice's encoding scheme and that Eve changed one of the packets, can he still figure out what the original message was? If so find it as well as the x-value of the packet that Eve changed, if not, explain why he can not. (Work in mod 11.)

(c) (5 points) Alice decides that putting the message as the coefficients of a polynomial is too inefficient for long messages because the degree of the polynomial grows quite large. Instead, she decides to encode the message as values in a degree 2 polynomial. For a 5 length message $[m_0, m_1, m_2, m_3, m_4]$, she creates a degree 2 polynomial P such that $P(0) = m_0, P(1) = m_1, P(2) = m_2, P(3) = m_3, P(4) = m_4$. (Alice makes sure to choose her message in such a way that it can be encoded in a polynomial of degree 2.) She then sends the length 5 message directly to Bob as 5 packets: $(0, m_0), (1, m_1), (2, m_2), (3, m_3), (4, m_4)$. Eve again interfere and changes the value of a packet before it reaches Bob. If Bob receives $(0,0), (1,3), (2,0), (3,3), (4,0)$ and knows Alice's encoding scheme and that Eve changed one of the packets, can he still figure out what the original message was? If so find it as well as the x-value of the packet that Eve changed, if not, explain why he can not. (Work in mod 11.)

(d) (10 points) After getting tired of decoding degree 2 polynomials, Bob convinces Alice to send messages using a degree 1 polynomial instead. To be on the safer side, Alice decides to continue to send 5 points on the polynomial even though it is only degree 1. She encodes and sends a length 5 message in the same way as part (c) (except using a degree 1 polynomial). Eve however, decides to change 2 of the packets. After Eve interferes, Bob receives $(0,-3),(1,-1),(2,x),(3,-3),(4,5)$. If Alice sent $(0,-3),(1,-1),(2,1),(3,3),$ $(4,5)$, for what values of x will Bob not be able to uniquely determine the Alice's message? (Assume Bob knows that Eve changed 2 of the packets and **work in mod 13.**)

5 Berlekamp-Welch Algorithm

In this question we will send the message $(m_0,m_1,m_2) = (4,3,2)$ of length $n = 3$. We will use an error-correcting code for $k = 1$ general error, doing arithmetic over GF(5).

(a) (5 points) Construct a polynomial $P(x) \pmod 5$ of degree at most 2, so that

$$P(0) = 4, \qquad P(1) = 3, \qquad P(2) = 2.$$

What is the message (c_0,c_1,c_2,c_3,c_4) that is sent?

(b) (5 points) Suppose the message is corrupted by changing c_0 to 0. Set up the system of linear equations in the Berlekamp-Welch algorithm to find $Q(x)$ and $E(x)$.

(c) (5 points) Assume that after solving the equations in part (b) we get $Q(x) = -x^2 + 4x$ and $E(x) = x$. Show how to recover the original message from Q and E.

6 Countability Practice

(a) (10 points) Prove or disprove: The set of increasing functions $f : \mathbb{N} \to \mathbb{N}$ (i.e., if $x \geq y$, then $f(x) \geq f(y)$) is countable.

(b) (10 points) Prove or disprove: The set of decreasing functions $f : \mathbb{N} \to \mathbb{N}$ (i.e., if $x \geq y$, then $f(x) \leq f(y)$) is countable.

(c) (5 points) Is a set of disks in $\mathbb{R}^2$ such that no two disks overlap necessarily countable or possibly uncountable? [A disk is a region in the plane of the form $\{(x,y) \in \mathbb{R}^2 : (x-x_0)^2 + (y-y_0)^2 \leq r^2\}$, for some $x_0, y_0, r \in \mathbb{R}$, $r > 0$.]
(Hint: Try to relate it to something we know that's countable, such as $\mathbb{Q} \times \mathbb{Q}$)

(d) (5 points) Is a set of circles in $\mathbb{R}^2$ such that no two circles overlap necessarily countable or possibly uncountable? [*Hint*: A circle is a subset of the plane of the form $\{(x,y) \in \mathbb{R}^2 : (x-x_0)^2 + (y-y_0)^2 = r^2\}$ for some $x_0, y_0, r \in \mathbb{R}$, $r > 0$. The difference between a circle and a disk is that a disk contains all of the points in its interior, whereas a circle does not.]