CS 70 Discrete Mathematics and Probability Theory
Summer 2018 Sinho Chewi and Vrettos Moulos

HW 3

Due: July 6, 2018 at 10 PM

Sundry

Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of homework party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

Please copy the following statement and sign next to it:

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

1 Bijections

Let n be an odd number. Let $f(x)$ be a function from $\{0,1,\ldots,n-1\}$ to $\{0,1,\ldots,n-1\}$. In each of these cases say whether or not $f(x)$ is necessarily a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

(a) $f(x) = 2x \pmod{n}$.

(b) $f(x) = 5x \pmod{n}$.

(c) n is prime and

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ x^{-1} \pmod{n} & \text{if } x \neq 0. \end{cases}$$

(d) n is prime and $f(x) = x^2 \pmod{n}$.

2 Solution for $ax \equiv b \pmod{m}$

In the notes, we proved that when $\gcd(m,a) = 1$, a has a unique multiplicative inverse, or equivalently $ax \equiv 1 \pmod{m}$ has exactly one solution x (modulo m). This proof also implies that when $\gcd(m,a) = 1$, there is a unique solution to $ax \equiv b \pmod{m}$, where x is the unknown variable.

Now consider the equation $ax \equiv b \pmod{m}$, when $\gcd(m,a) > 1$.

(a) Let $\gcd(m,a) = d$. Prove that $ax \equiv b \pmod{m}$ has a solution (that is, there exists an x that satisfies this equation) if and only if $b \equiv 0 \pmod{d}$. (Hint: If $b \equiv 0 \pmod{d}$, we can get a useful equation by dividing the equation $ax \equiv b \pmod{m}$ by d.)

(b) Let $\gcd(m,a) = d$. Assume $b \equiv 0 \pmod{d}$. Prove that $ax \equiv b \pmod{m}$ has exactly d solutions (modulo m).

(c) Solve for x: $77x \equiv 35 \pmod{42}$.

3 Squared RSA

(a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where a is relatively prime to p and p is prime.

(b) 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, i.e. $x^{ed} \equiv x \pmod{N}$. You may assume that x is relatively prime to both p and q.

(c) Prove that this scheme is at least as hard to break as normal RSA; that is, prove that if this scheme can be broken, normal RSA can be as well.

4 Breaking RSA

(a) 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).

(b) When working with RSA, it is not uncommon to use $e = 3$ in the public key. Suppose that Alice has sent Bob, Carol, and Dorothy the same message indicating the time she is having her birthday party. Eve, who is not invited, wants to decrypt the message and show up to the party. Bob, Carol, and Dorothy have public keys $(N_1, e_1), (N_2, e_2), (N_3, e_3)$ respectively, where $e_1 = e_2 = e_3 = 3$. Furthermore assume that N_1, N_2, N_3 are all different. Alice has chosen a number $0 \leq x < \min\{N_1, N_2, N_3\}$ which indicates the time her party starts and has encoded it via the three public keys and sent it to her three friends. Eve has been able to obtain the

three encoded messages. Prove that Eve can figure out x. First solve the problem when two of N_1, N_2, N_3 have a common factor. Then solve it when no two of them have a common factor. Again, assume Eve is friends with Wolfram as above.

Hint: The concept behind this problem is the Chinese Remainder Theorem: Suppose $n_1, ..., n_k$ are positive integers, that are pairwise co-prime. Then, for any given sequence of integers $a_1, ..., a_k$, there exists an integer x solving the following system of simultaneous congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Furthermore, all solutions x of the system are congruent modulo the product, $N = n_1 \cdots n_k$. Hence: $x \equiv y \pmod{n_i}$ for $1 \leq i \leq k \iff x \equiv y \pmod{N}$.

5 Fermat's Little Theorem

Fermat's Little Theorem states that for any prime p and any $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$. Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

6 How Many Polynomials?

Let $P(x)$ be a polynomial of degree at most 2 over GF(5). As we saw in lecture, we need $d+1$ distinct points to determine a unique d-degree polynomial. (Note that for the purposes of this problem we consider two polynomials to be distinct if they return different values for any input.)

(a) Assume that we know $P(0) = 1$, and $P(1) = 2$. Now we consider $P(2)$. How many values can $P(2)$ have? How many distinct polynomials are there?

(b) Now assume that we only know $P(0) = 1$. We consider $P(1)$, and $P(2)$. How many different $(P(1), P(2))$ pairs are there? How many different polynomials are there?

(c) How many different polynomials of degree at most d over GF(p) are there if we only know k values, where $k \leq d$?

7 Secret Sharing with Spies

An officer stored an important letter in her safe. In case she is killed in battle, she decides to share the password (which is a number) with her troops. However, everyone knows that there are 3 spies among the troops, but no one knows who they are except for the three spies themselves. The 3 spies can coordinate with each other and they will either lie and make people not able to open the safe, or will open the safe themselves if they can. Therefore, the officer would like a scheme to share the password that satisfies the following conditions:

- When M of them get together, they are guaranteed to be able to open the safe even if they have spies among them.
- The 3 spies must not be able to open the safe all by themselves.

Please help the officer to design a scheme to share her password. What is the scheme? What is the smallest M? Show your work and argue why your scheme works and any smaller M couldn't work. (The troops only have one chance to open the safe; if they fail the safe will self-destruct.)

8 Berlekamp-Welch Algorithm with Fewer Errors

In class we derived how the Berlekamp-Welch algorithm can be used to correct k general errors, given $n+2k$ points transmitted. In real life, it is usually difficult to determine the number of errors that will occur. What if we have less than k errors?

Suppose Alice wants to send 1 message to Bob and wants to guard against 1 general error. She decides to encode the message with $P(x) = 4$ (on GF(7)) such that $P(0) = 4$ is the message she want to send. She then sends $P(0), P(1), P(2) = (4,4,4)$ to Bob.

(a) Suppose Bob receives the message $(4,5,4)$. Without performing Gaussian elimination explicitly, find $E(x)$ and $Q(x)$.

(b) Now, suppose there were no general errors and Bob receives the original message $(4,4,4)$. Show that the $Q(x), E(x)$ that you found in part (a) still satisfies $Q(i) = r_i E(i)$ for all $i = 0,1,2$.

(c) Show that $E(x) = x$, $Q(x) = 4x$ is another possible set of polynomials that satisfies $Q(i) = r_i E(i)$ for all $i = 0,1,2$.

(d) Suppose you're actually trying to decode the received message $(4,4,4)$. Based on what you showed in the previous two parts, can you predict what will happen during row reduction when you try to solve for the unknowns?

(e) As you showed in the previous part, when there are less than k errors and Bob actually receives $n+2k$ packets, there will be multiple possible $Q(x)$ and $E(x)$ polynomials. Prove that no matter what the solution of $Q(x)$ and $E(x)$ are, the recovered $P(x)$ will always be the same.