CS70 Summer 2018 — Solutions to Homework 3

Sung Hyun Harvey Woo, SID 24190408, `CS70`

July 6, 2018

Collaborators: Dylan Hwang (dylanhwang@berkeley.edu), Allison Wang (awang24@berkeley.edu), Michael Hillsman (mhillsman@berkeley.edu)

Sundry

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. — Sung Hyun Harvey Woo

1. Bijections

(a) Bijection.
Given any odd n, the greatest common divisor of 2 and n will be equal to 1 since n will be in the form of $2k+1$ for an integer k. Given that $gcd(2,n) = 1$, we can safely say that $f(x)$ is a bijection.

(b) Not necessarily a bijection.
A counter example would be if $n = 5$, in which case, the gcd of 5 and 5 will be 5, and $f(x)$ will equal 0 for all values of x.

(c) Bijection.
The problem states that $f(x)$ is equal to 0 when x is 0 and the multiplicative inverse when x is not zero. This indicates that there exists a multiplicative inverse for all values from 1 to $n-1$. We know that the size of the input set is equal to the size of the output set mod n, therefore, pulling from the lecture, if we prove that $f(x)$ is injective, then $f(x)$ would be bijective. We can prove injection if we show that $(\forall a, b) f(a) = f(b) \implies a = b$. Since n is prime, given two values a and b, if f(a) is equal to f(b), we know that a has to be equal to b since the multiplicative inverse is unique in mod n and the mutiplicative inverse of the multiplicative inverse is equal to the original number. As for $x = 0$, the only value x that can have $f(x) = 0$ is the value $x = 0$, so if $f(a) = f(b) = 0$, this means that a and b can only be 0, meaning $a = b$. Therefore, we know that $f(x)$ is injective and thus it is a bijection.

(d) Not necessarily a bijection.
A counter example would be when the value of x is -1 and 1. -1 is $n-1$ (mod n), and 1 is 1 (mod n), however, the $f(-1) = 1$ (mod n) and $f(1) = 1$ (mod n). Two different values of the same mod space map to the same value and therefore this is not necessarily a bijection.

2. Solution for $ax \equiv b$ (mod m)

(a) We can prove the statement if we prove it for both the forwards and backwards direction.
$ax \equiv b$ (mod m) has a solution $\implies b \equiv 0$ (mod m)
$ax - b \equiv 0$ (mod m) and since we know that $gcd(a,m) = d$, and $d > 1$, we know that $m|ax$ though d.
We also know that $m|ax - b$. Since $m|ax$, we know that in order for $m|ax - b$ to be true, m has to divide b, and therefore $ax \equiv b$ (mod m)

$b \equiv 0$ (mod m) $\implies ax \equiv b$ (mod m) has a solution

$$ax \equiv b \text{ (mod m) and } gcd(a,m) = d \tag{1}$$

$$gcd(\frac{a}{d}, \frac{m}{d}) = 1 \tag{2}$$

$$\frac{a}{d}x \equiv \frac{b}{d} \text{ (mod} \frac{m}{d}) \tag{3}$$

Since $gcd(\frac{a}{d}, \frac{m}{d}) = 1$, we know that there is a solution for $ax \equiv b$ (mod m). We proved it for both the forward and backward direction, so we know that this claim holds.

(b) We already know from part 2.a that if $b \equiv 0$ (mod d), then $ax \equiv b$ (mod m) has a solution of the form $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. Given this equation we can list all the solutions to this equation by putting this in the form of any arbitrary solution a, since each solution has to be of the form

$$x = a + \frac{m}{d}k \text{ for an integer k} \tag{4}$$

If we assume that two solutions of the form above are written as the following :

$$a_1 = a + \frac{m}{d}k_1 \qquad\qquad a_2 = a + \frac{m}{d}k_2 \tag{5}$$

Then, we can show conditions for when they are equal in modulus m

$$a + \frac{m}{d}k_1 \equiv a + \frac{m}{d}k_2 \text{ (mod m)} \tag{6}$$
$$\frac{m}{d}k_1 \equiv \frac{m}{d}k_2 \tag{7}$$
$$(\frac{m}{d}k_1) - (\frac{m}{d}k_2) \equiv 0 \tag{8}$$
$$\frac{m}{d}(k_1 - k_2) = ml \text{ for some integer l} \tag{9}$$
$$\frac{1}{d}(k_1 - k_2) = l \tag{10}$$
$$(k_1 - k_2) = dl \tag{11}$$
$$(k_1 - k_2) \equiv 0 \text{ (mod d)} \tag{12}$$

This shows us that the only way two solutions are equal mod m is if k_1 and k_2 are equal in mod d, meaning that we can have a bound on how many k values are available for a solution. Since they are in modulus d, the only values available for k is 0 to $d - 1$, proving that there are only d solutions.

(c)

$$77x \equiv 35 \text{ (mod 42)} \tag{13}$$
$$11x \equiv 5 \text{ (mod 6)} \tag{14}$$
$$5x \equiv 5 \text{ (mod 6)} \tag{15}$$
$$5 * 5x \equiv 5 * 5 \text{ (mod 6)} \tag{16}$$
$$x \equiv 1 \text{ (mod 6)} \tag{17}$$
$$\tag{18}$$

First we divide the whole congruence expression by 7 since we know that all coefficients and the mod are also divisible by 7, and from there we convert 11 (mod 6) into 5 (mod 6). From there, we figure out that the multiplicative inverse of 5 (mod 6) is 5, so we multiply both sides by 5 and get that the solution is $x = 6k + 1$ (mod 42)

3. Squared RSA

(a) We can begin to prove this claim by showing that $a^{p(p-1)}$ is equal to a to the power of $\varphi(p^2)$. p is prime and therefore $\varphi(p)$ is simply equal to $p - 1$ however, p^2 is not prime. Since p is

prime there are no other factors that divide p^2 except for p itself. So, the multiples of p, $0, p, 2p, 3p, ..., p(p-1)$ divide p^2, meaning that $\varphi(p^2)$ is equal to $p^2 - p$. From here we need to prove that $a^{\varphi(p)}$ is is equal to 1 mod p^2. Using Euler's theorem proven in note 7a, we can show that if $a \in (\mathbb{Z}/m\mathbb{Z})^X$, which we know is true since a cannot be a multiple of p, since it is relatively prime to p, then $a^{p(p-1)} = a^{\varphi(p^2)} \equiv 1$ (mod m).

(b) We have public key $(N = p^2q^2, e)$ and $d = e^{-1}$ (mod $p(p-1)q(q-1)$). To decode the encrypted message we have:

$$x^{ed} = x^{p(p-q)q(q-1)k+1} \text{ for an integer k} \tag{19}$$
$$= x^{p(p-1)q(q-1)k} * x \equiv x \text{ (mod N)} \tag{20}$$
$$x(x^{p(p-1)q(q-1)k} - 1) \equiv 0 \text{ (mod N)} \tag{21}$$

If we show that $x(x^{p(p-1)q(q-1)k} - 1) \equiv 0$ in both mod p^2 and in mod q^2, we can show that it will be equivalent to 0 mod $N(= p^2q^2)$ (taken from the proof of RSA, and the Chinese Remainder Theorem)

$$x(x^{p(p-1)q(q-1)k} - 1) \equiv 0 \text{ (mod } p^2) \tag{22}$$
$$x^{p(p-1)} \equiv 1 \text{ (mod } p^2) \tag{23}$$
$$x(1^{q(q-1)k} - 1) \equiv 0 \text{ (mod } p^2) \tag{24}$$
$$x(1-1) \equiv 0 \text{ (mod } p^2) \tag{25}$$
$$0 \equiv 0 \text{ (mod } p^2) \tag{26}$$
$$\tag{27}$$

From part a if this question, we know that $x^{p(p-1)} \equiv 1$ (mod p^2), given that p is prime. We can substitute this value into the original equation giving us $x(1^{q(q-1)k} - 1)$ which then we can reduce to show that 0 is congruent to 0, proving the original equation. We can prove the exact same thing using the exact same steps for mod q^2. We know that x^{ed} is divisible by p^2 and also by q^2, which means that it is also divisible by N. Thus we prove that $x(x^{p(p-1)q(q-1)k} - 1) \equiv 0$ (mod N).

(c) In normal RSA, you are given N and e to which all you need is the (primes) p and q values of $N = pq$ to break RSA since through those values you can figure out the private key. We have already shown that for high bit numbers, there are no efficient algorithms to factor a large number such as N. Similarly, for this squared RSA, $N = p^2q^2$, which from Eve's point of view, you can reduce to $\sqrt{N} = pq$. However, from here Eve would still have to factor a large N into prime factors p and q, making it at least as hard to break as normal RSA.

4. Breaking RSA

(a) We assume that Eve already knows the value of $(p-1)(q-1)$ which we will denote as M for simplicity. Knowing M gives her not only M, but because $(p-1)(q-1) = pq - p - q - 1$, she can find out the value of $-p-q$ by substituting in M, and pq, which she knows since the public key is N(=pq). Since we have a Wolfram who can return the roots of polynomials, we can figure out the roots of a polynomial that has roots p and q ($f(x) = (x-p)(x-q) = x^2 - px - qx + pq = x^2 + (-p-q)x + pq$). Eve already knows the values of pq and $(-p-q)$, therefore she can give the polynomial to Wolfram, and she will then have the values of p and q.

(b) Case 1: Two of N_1, N_2, N_3 have a common factor.
Two of the N values for the three public keys have a common factors. Since the N value is a product of primes p and q, we can see then that the two N values will have a common prime factor. We can find the the shared prime factor by finding the two N values whose GCD is not equal to 1. If we find p, we can divide the two N values by p to get their respective q values, giving us knowledge of both p and q, and thus breaking RSA.

Case 2: No Two of N_1, N_2, N_3 have a common factor.
We can break this instance of RSA by using the Chinese Remainder Theorem. We know that no two of the three N values share a common factor, meaning that they are relatively prime, so we can utilize CRT to find out the values of m^e in the encrypted messages. All values of e is equal to 3, so the encrypted message would be:

$$E(m_1) = m^{e_1} \pmod{N_1} \tag{28}$$
$$E(m_2) = m^{e_2} \pmod{N_2} \tag{29}$$
$$E(m_3) = m^{e_3} \pmod{N_3} \tag{30}$$
$$\tag{31}$$

Here we substitute 3 for each value of e and then put in in a form where we can use CRT to get a number that would satisfy all three conditions.

$$m^3 \equiv a \pmod{N_1} \tag{32}$$
$$m^3 \equiv b \pmod{N_2} \tag{33}$$
$$m^3 \equiv c \pmod{N_3} \tag{34}$$
$$\tag{35}$$

for integers a, b, c

Then, we can solve it such that we have a number $m^3 \equiv k \pmod{N_1N_2N_3}$, that satisfies conditions stated above. Since m has to be smaller than all three N values, that means that m^3 will be smaller than $N_1N_2N_3$, so we know that $m^3 = k$. Consequently, we can simply take the cube root of k to get m.

In either case, Eve can figure out the message.

5. Fermat's Little Theorem

(a) Given $\forall n \in \mathbb{N}, n^7 - n \equiv 0 \pmod{42}$, we can prove that this is valid if we prove that it is divisible by the factors of 42, which are 2,3 and 7, $(42 = 2 * 3 * 7)$. We can rewrite the expression as $n^7 - n = 42k$. If we can prove that this function is true for mod 2, 3, and 7, referencing the proof for RSA, we can prove that the expression holds for mod 42 since if a number can be written as $2k, 3l,$ and $7j$, it can be written as $2k * 3l * 7j = 42klj$ for some integer k, l, and j. The Chinese Remainder Theorem can also be use to prove the previous claim. Since 2, 3, and 7 are all prime numbers, we can use Fermat's little theorem.

Case 1: Mod 2

$$n^7 - n = 42k \pmod{2} \tag{36}$$

Since 2 is prime, we know that any n is congruent to 1 mod p using Fermat's Little Theorem. Using this information we have $n^7 - n = 1^7 - 1 = 1 - 1 = 0$. Therefore, we know that $n^7 - n \equiv 0 \pmod 2$.

Case 2: Mod 3

$$n^7 - n = 42k \pmod 3 \tag{37}$$

3 is also prime and therefore we know that $n^3 \equiv n \pmod 3$ using Fermat's Little Theorem. Using the same logic as before we have $(n^3)^2 * n - n = (n)^2 * n - n = n - n = 0$. Therefore, we know that $n^7 - n \equiv 0 \pmod 3$.

Case 3: Mod 7

$$n^7 - n = 42k \pmod 7 \tag{38}$$

7 is also prime and therefore we know that $n^7 \equiv n \pmod 7$ using Fermat's Little Theorem. Directly substituting this in, we have $n^7 - n = n - n = 0$. Therefore, we know that $n^7 - n \equiv 0 \pmod 7$.

We have proven that $n^7 - n \equiv 0 \pmod{\text{p}}$ for when p is equal to 2, 3, 7. Therefore we can prove that it holds for when p is equal to 42, thus $\forall n \in \mathbb{N}, n^7 - n \equiv 0 \pmod{42}$.

6. How Many Polynomials?

(a) 5, 5
Since the polynomial of degree 2 is over GF(5), P(2) can only be one of the values from GF(5), therefore it can have 5 values. Since the degree of the polynomial is 2, 3 points on the graph are needed to find P(x). Since P(0) and P(1) already have values and P(2) can have 5 different values, there are 5 different polynomials that P(x) can be.

(b) 25
If only P(0) is fixed, we have P(1) and P(2) each of which can take on 5 different values in GF(5). Since 3 points on the graph are required to find P(x), there are 25(=5*5) different combinations of P(1) and P(2) values, meaning that there are 25 different polynomials that P(x) can be.

(c) p^{d+1-k}
If the degree of P(x) is at most d over GF(p). Each of the points can take on p values, from 0 to $(p-1)$. $(d+1)$ points on the graph P(x) is required to determine a polynomial of degree at most d. Therefore, we can determine the number of total possible polynomials to be p^{d+1}. However, in this case, because we already know k values, that are fixed, all we need to know are $(d+1-k)$ points/values. this means that there are p^{d+1-k} possible polynomials for when we only know k values.

7. Secret Sharing with Spies

The secret sharing can be solved using polynomials and error correction. The basic idea behind the scheme would be to use polynomials and construct a degree $M-1$ polynomial such that the officer can give 1 point on the graph to each of her M soldiers. However, since we have 3 spies, who

can provide the wrong values such that it would give the wrong password, we know that there is the possibility of 3 errors. We need a system that would not allow the three spies with three values to find out the password, and one that would still work regardless of the three errors.

We can start with a degree 3 polynomial, since it requires 4 values to find, and therefore we can rule out the possibility of the three spies getting the password on their own. We can see this as requiring 4 values/soldiers, with the possibility of 3 errors. We need to find a minimum value M for which this system would work. We know from error correction that if we have at most k errors and need to transmit n packets, we can ensure that n packets will arrive by sending n + 2k packets. So if we plug in $n = 4$ and $k = 3$, we get $4 + (2 * 3) = 10$. So, using this method we can get the correct password with a minimum of 10 people even if we have 3 spies that provide an incorrect value.

8. Berlekamp-Welch Algorithm with Fewer Errors

(a) $Q(x) = 4x - 4$

If Bob received (4, 5, 4), we know that the degree of the Error locator polynomial is 1, and that the degree of Q is also 1 since it is equal to the sum of the degree of P and E. So, we have the following system of equations.

$$Q(x) = b_1 x + b_0 \tag{39}$$
$$E(x) = x + a_0 \tag{40}$$

We substitute in the values for $i = 0, 1, 2$:

$$b_0 = 4(0 + a_0) \tag{41}$$
$$b_1 + b_0 = 5(1 + a_0) \tag{42}$$
$$2b_1 + b_0 = 4(2 + a_0) \tag{43}$$

Using the first $b_0 = 4a_0$

$$b_1 + b_0 = 5 + 5a_0 \tag{44}$$
$$b_1 - 5 = a_0 \tag{45}$$

Also,

$$2b_1 + b_0 = 8 + 4a_0 \tag{46}$$
$$2b_1 + 4a_0 = 8 + 4a_0 \tag{47}$$
$$b_1 = 4 \tag{48}$$

We know that $b_1 = 4$, which leads to $a_0 = -1$, and also $b_0 = -4$ Since we know all the coefficients, We know that our $E(x) = x - 1$ and that $Q(x) = 4x - 4$.

(b) Case 1: $i = 0$ and $P(0) = 4$

$$Q(0) = r_0 E(0) \tag{49}$$
$$4(0) - 4 = 4 * (0 - 1) \tag{50}$$
$$-4 = -4 \tag{51}$$
$$\tag{52}$$

Case 2: $i = 1$ and $P(1) = 4$

$$Q(1) = r_1 E(1) \tag{53}$$
$$4(1) - 4 = 4 * (1 - 1) \tag{54}$$
$$0 = 0 \tag{55}$$
$$\tag{56}$$

Case 3: $i = 2$ and $P(2) = 4$

$$Q(2) = r_2 E(2) \tag{57}$$
$$4(2) - 4 = 4 * (2 - 1) \tag{58}$$
$$4 = 4 \tag{59}$$
$$\tag{60}$$

Q(x) and E(x) derived from part 8.a is still valid for these cases.

(c) We know that $Q(x) = P(x)E(x)$, so if you substitute in our Q and E function, we get the same function of P(x) as the original P(x):

$$4x = P(x) * x \tag{61}$$
$$P(x) = 4 \tag{62}$$

For the values $i = 0, 1, 2$, we have : 4x = P(x)* x
Case 1: $i = 0$ and $P(0) = 4$

$$4(0) = 4 * 0 \tag{63}$$

Case 2: $i = 1$ and $P(1) = 4$

$$4(1) = 4 * 1 \tag{64}$$

Case 3: $i = 2$ and $P(2) = 4$

$$4(2) = 4 * 2 \tag{65}$$

(d) When we try to solve it using row reduction to solve the system of equations, given a received message with no errors, you will get three equations that will be linearly dependent and therefore there will be a free variable, indicating that there will be multiple solutions for the system of equations.

(e) Even if there are less than k errors, and we have different Q(x), E(x) polynomials, we can still prove that P(x) will always be the same. From the lecture we have a proof for for the uniqueness of the solution to the linear system. If we let Q and E be any solution to the linear system, we know that $Q(i) = R_i * E(i)$ for all $n + 2k$ values of i. Since there are at most k errors, that means that we have at least $n + k$ values of i that satisfy $Q(i) = P(i)E(i)$. $Q(x)$ and $P(i)E(i)$ is of degree n+k-1. Since we have at least $n+k$ values to figure out an equation of degree n+k-1, we can still solve the system of equations to figure out the coefficients and thus figure out P(x), which will be the same regardless of how many errors (fewer than k) occur.