CS 70 Discrete Mathematics and Probability Theory
Fall 2022 Satish Rao and Babak Ayazifar

# HW 05

Due: Saturday, 10/1, 4:00 PM
Grace period until Saturday, 10/1, 6:00 PM

## Sundry

Before you start writing your final homework submission, 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.)

**Solution:** I worked alone on this problemset.

## 1 RSA Practice

Consider the following RSA schemes and solve for asked variables.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key $d$? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encode your answer from part (**??**) to check its correctness.

**Solution:**

(a) $d \equiv e^{-1} \pmod{(p-1)(q-1)}$, so $d \equiv 9^{-1} \pmod{40}$. Given that $9 \cdot 9 = 81 \equiv 1 \pmod{40}$, we have that $d \equiv 9^{-1} \equiv \boxed{9} \pmod{40}$.

(b) $4^d \equiv x \pmod{pq} \implies 4^9 \equiv x \pmod{55}$. Splitting 4 into 5 and 11 gives us $4^9 \equiv 4 \pmod 5$ and $4^9 \equiv 4^{-1} \cdot 4^{10} \equiv 3 \cdot 1 \equiv 3 \pmod{11}$. From the Chinese Remainder Theorem, the number that is equivalent to $4 \pmod 5$ and $3 \pmod{11}$ must exist, and simple hand computation reveals that it is $x = \boxed{14}$.

(c) $x^e \pmod{pq} = 14^9 \pmod{55}$ can be split into $14^9 \equiv 4^9 \pmod 5$ and $14^9 \equiv 3^9 \pmod{11}$. We find that $4^9 \equiv 4 \pmod 5$ and $3^9 \equiv 3^{-1} 3^{10} \equiv 4 \cdot 1 \equiv 4 \pmod{11}$. Clearly, the encrypted value must be $4 \pmod{55}$, which is what the receiver is given to get.

## 2 Tweaking RSA

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and $p$ is prime. Similar to the original method, for any message $x \in \{0, 1, \dots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose $e$ and $d$ in the encryption and decryption function, respectively. Prove that the message $x$ is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve now compute $d$ in the decryption function? If so, by what algorithm?

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where $p, q, r$ are all prime). Explain how you can do so, and include a proof of correctness showing that $D(E(x)) = x$.

**Solution:**

(a) We can pick any prime number $e \in [1, N-2]$ and let $d \equiv e^{-1} \pmod{N-1}$. If $y = x^e \pmod{N}$, then $D(y) \equiv (x^e)^d \pmod{N} \equiv x^{ed} \pmod{N}$. Because $d \equiv e^{-1} \pmod{N-1}$, we have that $ed \equiv 1 \pmod{N-1}$, so $x^{ed} \equiv x \pmod{N}$ from Fermat's Little Theorem.

(b) However, Eve can also use Fermat's Little Theorem Eve can easily find that $d \equiv e^{-1} \pmod{N-1}$, since $ed \equiv 1 \pmod{N-1}$.

(c) For three primes $p, q, r$, we can still find $x^e \pmod{N}$ pretty easily for a prime $e$ and we can find $d \equiv e^{-1} \pmod{(p-1)(q-1)(r-1)}$, so $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$. From Fermat's Little Theorem on $p, q, r$ we find that

$$\begin{aligned} x^{ed} &\equiv x \pmod{p} \\ x^{ed} &\equiv x \pmod{q} \\ x^{ed} &\equiv x \pmod{r}. \end{aligned}$$

We can directly find from these relations that $x^{ed} \equiv x \pmod{pqr}$, or in other words, that $D(E(x)) = x$.

## 3 Secret Sharing

Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted, and we know that:

- Two TAs together should be able to access the answers
- Three Readers together should be able to access the answers
- One TA and one Reader together should also be able to access the answers

Design a Secret Sharing scheme to make this work.

**Solution:** Create two polynomials over the reals $p, q$ with degree 1 and one polynomial with $r$ with degree 2. Furthermore, let $p, q, r$ all have the same constant term $s$.

Give each TA a different share of $p$ and each reader a different point of $q$. Then, all TA's together can pool their shares to find $p$, and all readers together can pool their shares to find $r$, but if any TA or reader disagreed, then $p$ and $q$ will remain inaccessible.

Also give every TA an identical share of $q$ and every reader another identical share of $q$. Then, both a TA and a reader's consent are needed to unlock $q$.

# 4 Trust No One

Gandalf has assembled a fellowship of eight peoples to transport the One Ring to the fires of Mount Doom: four hobbits, two humans, one elf, and one dwarf. The ring has great power that may be of use to the fellowship during their long and dangerous journey. Unfortunately, the use of its immense power will eventually corrupt the user, so it must not be used except in the most dire of circumstances. To safeguard against this possibility, Gandalf wishes to keep the instructions a secret from members of the fellowship. The secret must only be revealed if enough members of the fellowship are present and agree to use it.

Gandalf has hired your services to help him come up with a secret sharing scheme that accomplishes this task, summarized by the following points:

- There is a party of four hobbits, two humans, an elf, and a dwarf, and a secret message that must remain unknown to everyone if not enough members of the party agree.
- A group of people consisting of at least two people from different people classes and at least one people class that is fully represented (i.e., has all members present) can unlock the secret of the ring.

A few examples: only four hobbits agreeing to use the ring is not enough to know the instructions. One human and three hobbits is not enough. However, all four hobbits and one human agreeing is enough. Both humans and the dwarf agreeing is enough.

**Solution:** We use a polynomial $P$ of degree 2 with a secret $s$, so we would need 3 shares to find $s$.

Give each hobbit the share $(1, P(1))$, and then give them each a distinct share for a polynomial $P_1$ of degree 3 with secret $P(2)$. Then, all four hobbits will need to agree to find $(2, P(2))$.

Repeat the scheme for humans similarly; give each human the share $(3, P(3))$, and then give them each a distinct share of a polynomial $P_2$ of degree 1 with secret $P(4)$. Then, both humans will need to agree to find $(4, P(4))$.

Finally, give the dwarf two shares $(5, P(5)), (6, P(6))$ and give the elf two shares $(7, P(7)), (8, P(8))$.

Now, we claim that this satisfies the criteria. If the dwarf or elf agrees along with some member of a different people class, we will have at least $2+1=3$ points, enough to unlock $s$.

If neither the dwarf nor the elf agrees, we will need 3 shares among the humans and hobbits. If only part of the hobbits and part of the humans agree, they will together only have 2 share $(1, P(1))$ and $(3, P(3))$ because all humans or all hobbits would need to agree to unlock the third point (either $P(2)$ or $P(4)$). If either all humans agree or all hobbits agree, we would be able to unlock either $P(2)$ or $P(4)$, necessarily giving us three shares of $P$ to find $s$. □

## 5 Lagrange? More like Lamegrange.

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

(a) 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) 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) 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) 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?

**Solution:**

(a) We would get the polynomial $y = y_0$.

(b)

$$\begin{aligned} f_1(x) &= f_0(x) + a_1(x - x_0) \\ \implies f_1(x_1) &= y_0 + a_1(x_1 - x_0) \\ \implies y_1 &= y_0 + a_1(x_1 - x_0) \\ \implies y_1 - y_0 &= a_1(x_1 - x_0) \\ \implies a_1 &= \boxed{\frac{y_1 - y_0}{x_1 - x_0}}. \end{aligned}$$

(c) Using similar logic to the previous part,

$$\begin{aligned} f_2(x) &= f_1(x) + a_2(x - x_0)(x - x_1) \\ \implies y_2 &= y_0 + \frac{y_1 - y_0}{x_1 - x_0}(x_2 - x_0) + a_2(x_2 - x_0)(x_2 - x_1) \\ \implies y_2 - y_0 &= \frac{y_1 - y_0}{x_1 - x_0}(x_2 - x_0) + a_2(x_2 - x_0)(x_2 - x_1) \\ \implies \frac{y_2 - y_0}{x_2 - x_0} &= \frac{y_1 - y_0}{x_1 - x_0} + a_2(x_2 - x_1) \\ \implies \frac{y_2 - y_0}{x_2 - x_0} - \frac{y_1 - y_0}{x_1 - x_0} &= a_2(x_2 - x_1) \\ \implies a_2 &= \boxed{\frac{y_2 - y_0}{(x_2 - x_0)(x_2 - x_1)} - \frac{y_1 - y_0}{(x_1 - x_0)(x_2 - x_1)}}. \end{aligned}$$

(d) To prevent things from getting messy, we express $a_{i+1}$ in terms of $f_i$. Note that we can recover previous $f_i$ recursively.

$$\begin{aligned} f_{i+1}(x) &= f_i(x) + a_{i+1} \prod_{j=0}^{i} (x - x_j) \\ f_{i+1}(x_{i+1}) - f_i(x_{i+1}) &= a_{i+1} \prod_{j=0}^{i} (x_{i+1} - x_j) \\ \boxed{\frac{y_{i+1} - f_i(x_{i+1})}{\prod_{j=0}^{i} (x_{i+1} - x_j)}} &= a_{i+1}. \end{aligned}$$

# 6 Equivalent Polynomials

This problem is about polynomials with coefficients in $\mathrm{GF}(q)$ for some prime $q \in \mathbb{N}$. We say that two such polynomials $f$ and $g$ are *equivalent* if $f(x) = g(x)$ for every $x \in \mathrm{GF}(q)$.

(a) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 5 that is equivalent to $f(x) = x^5$ over $\mathrm{GF}(5)$; then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 1 + 3x^{11} + 7x^{13}$ over $\mathrm{GF}(11)$.

(b) Prove that whenever $f(x)$ has degree $\geq q$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< q$.

**Solution:**

(a) From Fermat's Little Theorem, $f(x) = x^5 = \boxed{x}$ in $\mathrm{GF}(5)$ and $g(x) = 1 + 3x^{11} + 7x^{13} = \boxed{1 + 3x + 7x^3}$ in $\mathrm{GF}(11)$.

(b) Again using Fermat's, we have that $a^q \equiv a \pmod{q}$. Therefore, in $\mathrm{GF}(q)$ we have $x^q \equiv x \pmod{q}$, so any term of $f(x)$ with degree $mq + n$ with $n < q$ will be equivalent to the same term but with power $n$. Therefore, all polynomials $f(x)$ with degree $\geq q$ will have an equivalent polynomial of degree $< q$, which can be obtained by reducing the exponents via Fermat's for each term.

# 7 The CRT and Lagrange Interpolation

Let $n_1, \dots n_k$ be pairwise co-prime, i.e. $n_i$ and $n_j$ are co-prime for all $i \neq j$. The Chinese Remainder Theorem (CRT) tells us that there exist solutions to the following system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} && (1)\\ x &\equiv a_2 \pmod{n_2} && (2)\\ &\vdots && (\vdots)\\ x &\equiv a_k \pmod{n_k} && (k) \end{aligned}$$

and all solutions are equivalent $\pmod{n_1 n_2 \cdots n_k}$. For this problem, parts (a)-(c) will walk us through a proof of the Chinese Remainder Theorem. We will then use the CRT to revisit Lagrange interpolation.

(a) We start by proving the $k = 2$ case: Prove that we can always find an integer $x_1$ that solves $(1)$ and $(2)$ with $a_1 = 1, a_2 = 0$. Similarly, prove that we can always find an integer $x_2$ that solves $(1)$ and $(2)$ with $a_1 = 0, a_2 = 1$.

(b) Use part (a) to prove that we can always find at least one solution to $(1)$ and $(2)$ for any $a_1, a_2$. Furthermore, prove that all possible solutions are equivalent $\pmod{n_1 n_2}$.

(c) Now we can tackle the case of arbitrary $k$: Use part (b) to prove that there exists a solution $x$ to $(1)$-$(k)$ and that this solution is unique $\pmod{n_1 n_2 \cdots n_k}$.

(d) For polynomials $p_1(x)$, $p_2(x)$ and $q(x)$ we say that $p_1(x) \equiv p_2(x) \bmod q(x)$ if $p_1(x) - p_2(x)$ is of the form $q(x) \times m(x)$ for some polynomial $m(x)$.

Define the polynomials $x - a$ and $x - b$ to be co-prime if they have no common divisor of degree $1$. Assuming that the CRT still holds when replacing $x, a_i$ and $n_i$ with polynomials (using the definition of co-prime polynomials just given), show that the system of congruences

$$\begin{aligned} p(x) &\equiv y_1 \pmod{(x - x_1)} && (1')\\ p(x) &\equiv y_2 \pmod{(x - x_2)} && (2')\\ &\vdots && (\vdots)\\ p(x) &\equiv y_k \pmod{(x - x_k)} && (k') \end{aligned}$$

has a unique solution $\pmod{(x - x_1) \cdots (x - x_k)}$ whenever the $x_i$ are pairwise distinct. What is the connection to Lagrange interpolation?

Hint: To show that a unique solution exists, you may use the fact that the CRT has a unique solution when certain properties are satisfied.

**Solution:**

(a) We want $x \equiv 0 \pmod{n_1}$ and $x \equiv 1 \pmod{n_2}$, which means that $qn_2 - 1 \equiv 0 \pmod{n_1}$ for some $q$, or in other words, $qn_2 \equiv 1 \pmod{n_1}$. Because $n_1$ and $n_2$ are coprime, there must exist such $q$. □

(b) We know from part (a) that there is a solution for $p \equiv 1 \pmod{n_1}, p \equiv 0 \pmod{n_2}$ and that there is a solution for $q \equiv 1 \pmod{n_2}, q \equiv 0 \pmod{n_1}$.

Then, note that a solution $x = a_1 p + a_2 q$ must have a residue of $a_1(1) + a_2(0) \equiv a_1 \pmod{n_1}$ and a residue of $a_1(0) + a_2(1) \equiv a_2 \pmod{n_2}$.

Now, we prove that this solution is unique. Let $x, y$ both have residues $a_1 \pmod{n_1}, a_2 \pmod{n_2}$. Then, $x = u_1 n_1 + a_1 = v_1 n_2 + a_2, y = u_2 n_1 + a_1 = v_2 n_2 + a_2$. Subtracting the two yields $y - x = (u_2 - u_1)n_1 = (v_2 - v_1)n_2$, which means their difference is both divisible by $n_1$ and by $n_2$. Therefore, the difference $y - x$ must be divisible by $n_1 n_2$, meaning $y - x \equiv 0 \pmod{n_1 n_2}$ or $y \equiv x \pmod{n_1 n_2}$. □

(c) We can modify part (a) for general $k$; instead of checking $x \equiv 1 \pmod{n_1}, x \equiv 0 \pmod{n_2}$, we can check for $x \equiv 1 \pmod{n_1}, x \equiv 0 \pmod{n_j}$ for $j \neq 1$. This would result in $qn_i - 1 \equiv 0 \pmod{\prod_{j=2}^{k} n_j}$, which would still necessarily have a valid $q$ because all $n_i$ are coprime, so there is an inverse of $n_i$ modulo $\prod_{j=2}^{k} n_j$.

Similarly to part (b), we can use the information from the previous paragraph to find values $b_i$ for which $b_i \equiv 1 \pmod{x_n}$ and $b_i \equiv 0 \pmod{n_j}$ for all $j \neq i$ in the range $[1,k]$. Then, we can simply find a valid $x$ through

$$x = \sum_{i=1}^{k} a_i b_i.$$

Once again, we must check that this $x$ is unique modulo $\prod_{i=1}^{k} n_i = N$. Let $x, y$ both have the same residues modulo $n_i$ for all $i \in [1,k]$. Then, $y - x$ must be divisible by $n_i$ for all $i \in [1,k]$ by the same logic as in part (b) extended to $k$ moduli, so $y - x \equiv 0 \pmod{N}$ and $x \equiv y \pmod{N}$. □

(d) As we are given that CRT works as normal within a polynomial ring, we simply have to prove that $x - x_i$ are all relatively prime for pairwise distinct $x_i$.

Assume for the sake of contradiction that $x - a | x - b$ for $a \neq b$. Then, $k(x - a) = x - b$ for constant $k$ because $x - a$ and $x - b$ both have degree 1. To set the constant term equal, we would have $k = \frac{b}{a}$, meaning that we would need $x - b = \frac{b}{a}x - b$. This only holds when $\frac{b}{a} = 1$, or $a = b$, a contradiction.

Therefore, as all $x_i$ are pairwise distinct, every modulus is relatively prime, so the system of congruences must have a unique solution $p(x)$ by CRT. □