4 FLT, CRT, AND RSA

Computer Science Mentors 70

Feb 22 - Feb 27
Spring 2021

Amogh Gupta, Sylvia Jin, Aekus Bhathal, Abinav Routhu, Debayan Bandyopadhyay
Roast us here: *https://tinyurl.com/csm70-feedback20*

1 Fermat's Little Theorem

Claim [Note 7, Page 1]: For any prime p and any $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$

Proof: See appendix.

1. (a) Compute $4^{9999} \bmod 19$.

Solution: By Fermat's little theorem, since $\gcd(4, 19) = 1$, we see that $a^{p-1} = 4^{18} \equiv 1 \bmod 19$. Then by long division, we see that $9999/18 = 555.5$ so $9999 \equiv 9 \pmod{18}$ (or since 9999 is a multiple of 9 but not a multiple of 2, secretly using CRT!), $9999 \equiv 9 \bmod 18$, so $4^{9999} \equiv 4^9 \equiv 4^{2^3} 4 \equiv 5 \cdot 4 \equiv 1 \bmod 19$.

(b) Compute $8^{7^{6^5}} \bmod 10$.

Solution: There are 2 approaches here: doing arithmetic on the last digit, or using CRT mod 2 and 5.
Last digit: Writing out the last digit for a few powers, we see that the pattern repeats after 4, with the pattern being $8, 4, 2, 6, 8, 4, \ldots$. Then we need to find what the exponent of 8 is mod 4, in order to find which one the last digit is. We see that $7 \equiv -1 \bmod 4$, and the exponent of 7 is even, so $7^{6^5} \equiv 1 \bmod 4$ so we look at the digits which corresponds to $1 \bmod 4$, which is 8.
CRT: 8 is even so the overall quantity is $0 \bmod 2$, while by FLT, $8^4 \equiv 1 \bmod 5$ so we now need to find what the exponent is mod 4. $7 \equiv -1 \bmod 4$ so 7 raised to an even power is $1 \bmod 4$, and 6^5 is even, which means $7^{6^5} \equiv 1 \bmod 4$ which means that $8^{7^{6^5}} \bmod 5 \equiv 8^1 \equiv 3 \bmod 5$. Since we have $8^{7^{6^5}} \equiv 0 \bmod 2$, $8^{7^{6^5}} \equiv 3 \bmod 3$, by CRT the final result is $8 \bmod 10$.

2. In this question, we prove the existence of n such that $a^n \equiv 1 \pmod{p}$ when p is a prime and a is not evenly divisible by p.

(a) Prove that there are at most $p-1$ different values for $a^n \pmod{p}$

Solution: Under modulus p, there can be at most p different values for any expression. However, since a is not a multiple of p, $a^n \not\equiv 0 \pmod{p}$, so we are left with at most $p-1$ different values.

(b) Argue that there must be some i, j such that $a^i \equiv a^j \pmod{p}$ (hint: use the result from part (a))

Solution: There are p different powers of a and $p-1$ possible values modulo p, so by the Pigeonhole Principle $a^i \equiv a^j \pmod{p}$ for some $1 \leq i < j \leq p$

(c) Use part (b) to prove that there exists some n such that $a^n \equiv 1 \pmod{p}$

Solution: $p \mid a^j - a^i$, or equivalently $p \mid a^i(a^{j-i} - 1)$. Since a is not divisible by p, it is relatively prime to p, so $p \mid a^{j-i} - 1$, and $a^{j-i} \equiv 1 \pmod{p}$. Thus, we have found such an n (specifically $n = j - i$).

3. In this question, we will try to prove a variant Fermat's Little Theorem for numbers $\pmod{p^2}$.

   (a) How many integers $x, 0 \leq x \leq p^2 - 1$ are there such that $\gcd(x, p^2) = 1$? What is true about this set of integers?

   Solution: Because p is prime, p^2 only shares factors with multiples of p. This means that the elements which are *not* coprime to p^2 are $0, p, 2p, \ldots, (p-1)p$. There are p^2 total elements in the range $0 \leq x \leq p^2 - 1$, and we've listed the p elements which are *not* coprime. Thus, there are $p^2 - p = p(p-1)$ elements which are coprime to p^2. We can say that these elements have a multiplicative inverse $\bmod p^2$.

   (b) Prove that if $\gcd(a, p) = 1$, then $a^{p(p-1)} \equiv 1 \pmod{p^2}$.

   Solution: Consider the set of numbers x that satisfy the condition from part a; call it S. If we multiply this set of elements by a, an element which is coprime to p (and therefore to p^2), then we get a set of numbers, S' which look like $a, 2a, \ldots, (p^2 - 1)a$. But, we can recall from question 3 that multiplying a set of elements coprime to p^2 by a coprime number is a bijection, so the set of numbers that we get is exactly the same, $S = S'$ (even though the sequence may have them in a different order). Thus, we can multiply the elements in both sets together and they should be equal. Multiplying all the elements in S gives a product, which we can call P. Multiplying all the elements in S' gives the same product multiplied by $p(p-1)$ copies of a, or $a^{p(p-1)}P$. Thus, we have $a^{p(p-1)}P = P \pmod{p^2}$. Notice that P is the product of numbers that have multiplicative inverses; this means that P itself has an inverse. Multiplying both sides by the inverse of P yields $a^{p(p-1)} = 1 \pmod{p}$.

2 RSA

1. **RSA-BC123 [Practice Bank]**
   Bob would like to receive messages from Alice via RSA.

   (a) He chooses 2 primes, $p = 7$ and $q = 11$. What is N?

   Solution: $N = pq = (7)(11) = 77$

   (b) He chooses $e = 7$. To what number is e relatively prime?

   Solution: e must be relatively prime to $(p-1)(q-1) = 60$.

   (c) Calculate d.

   Solution: $d = e^{-1} \bmod (p-1)(q-1) = 7^{-1} \bmod 60 = 43$

   (d) Imagine Alice wants the send Bob a message $x = 30$. She applies her encryption function $E(x)$ to 30. What is the encrypted message x'?

   Solution: $E(x) = x^e \bmod N \rightarrow 30^7 \bmod 77 = 2$

   (e) What is the result of Bob applying his decryption function $D(x')$?

   Solution: $D(x') = (x')^d \bmod 77 = 2^{43} \bmod 77 = 30$

2. **Prove the correctness of RSA.**
   Hint: Proving RSA amounts to showing that given $d = e^{-1} \bmod (p-1)(q-1)$:

$$(x^e)^d = x \bmod N \qquad \forall x \in \{0, 1, 2, \ldots, N-1\}$$

Solution:

$$\begin{aligned}(x^e)^d &= x \bmod N \qquad \forall x \in \{0, 1, 2, \ldots, N-1\} \\ (x^e)^d - x &= x^{1+(p-1)(q-1)k} - x \bmod N \\ &= x(x^{(p-1)(q-1)k} - 1) \bmod N\end{aligned}$$

Now, we will show that the last expression is divisible by both p and q by FLT.

Case 1: $x \bmod p = 0$:

$$x(x^{(p-1)(q-1)k} - 1) = 0(0^{(p-1)(q-1)k} - 1) = 0 \bmod p$$

Case 2: $x \bmod p \neq 0$:

$$\begin{aligned}x(x^{(p-1)(q-1)k} - 1) &= x((x^{(p-1)})^{(q-1)k} - 1) \bmod p \\ x(1-1) &= 0 \bmod p\end{aligned}$$

A symmetric argument works for q. If the expression is divisible by both p and q, then it is divisible by $pq = N$. Thus,

$$\begin{aligned}x(x^{(p-1)(q-1)k} - 1) &= 0 \bmod N \\ (x^e)^d &= x \bmod N\end{aligned}$$

3. For all r not divisible by primes p or q, find some a and b such that

$$r^{(p-1)(q-1)} - ap - bq \equiv 0 \pmod{pq}$$

Solution: First, we do some groundskeeping to tidy up the equation

$$r^{(p-1)(q-1)} \equiv ap + bq \pmod{pq} \tag{1}$$

Let's denote the left side of the equation LHS and the right side RHS. First, we work on the LHS.

Recall that the product of exponents x^{yz} can be rewritten in two forms $(x^y)^z$ and $(x^z)^y$. Hence,

$$\begin{aligned}r^{(p-1)(q-1)} &= (r^{p-1})^{q-1} \\ &= (r^{q-1})^{p-1}\end{aligned}$$

Now, we apply FLT:

$$(r^{p-1})^{q-1} \equiv 1^{q-1} \equiv 1 \pmod{p}$$
$$(r^{q-1})^{p-1} \equiv 1^{p-1} \equiv 1 \pmod{q}$$

Now, we can treat the LHS as an unknown. Since p and q are prime and thus coprime, we can now apply CRT to find $r^{(p-1)(q-1)} \mod pq$:

$$r^{(p-1)(q-1)} \equiv (1)pp_q^{-1} + (1)qq_p^{-1} \pmod{pq}$$

Hence, we find that $a = p_q^{-1}$ and $b = q_p^{-1}$ satisfies (1) for all r not divisible by p or q (here p_q^{-1} is the modular inverse of $p \mod q$ and q_p^{-1} is the modular inverse of $q \mod p$).

4. In each of the following examples, Alice and Bob wish to send messages to one another and eve wishes to intercept the message. RSA is either used incorrectly (yields an incorrect result), is used correctly but can be broken, or is both correct and can not be broken. Select the option that best applies and explain. Assume that p, q are prime and Bob publishes the public key $(N = pq, e)$

   (a) Eve, Alice, and Bob share a menu. Bob asks Alice what dish she wants, and Alice responds with the name of the dish using standard RSA encryption.

   Solution: *Broken*. Since there are a finite number of options, Eve can just guess-and-check. Eve knows the public key that Bob will release in order to receive Alice's message, so now Eve can just encrypt all menu items using e and see which one matches Alice's encrypted message, which she can publicly see.

   (b) Eve is able to extort extra details from Alice and Bob. She now also knows the value of $(p-1)(q-1) \pmod{p}$

   Solution: *Correct*. Eve's goal is to compute $(p-1)(q-1)$ so that she is able to find $d = e^{-1} \mod (p-1)(q-1)$.

   Given $(p-1)(q-1) \equiv pq - p - q + 1 \equiv -q + 1 \pmod{p}$, Eve can find $q \pmod{p}$. But this simply isn't enough information since rewriting $q = kp + m$ where m is known introduces another variable k. Using the only other information we have about p and q, $N = pq = kp^2 + mp$.

   Now, to solve for k, Eve would have to be able to efficiently factor $p(q-m)$, which we know is a hard, otherwise she can also efficiently factor pq.

   (c) Bob selects e where e is coprime to N but not coprime to $(p-1)(q-1)$.

   Solution: *Incorrect*. RSA works only if e is coprime to $(p-1)(q-1)$ so that there exists $d = e^{-1} \pmod{(p-1)(q-1)}$.

   It is possible for e to be coprime with N but not with $(p-1)(q-1)$. For instance, if $p = 5$ and $q = 7$, choose $e = 4$. Now, there is no multiplicative inverse such that $4d \equiv 1 \pmod{4 \cdot 6}$.

3 Polynomials

[Note 8, Page 1]
Property 1: A non-zero polynomial of degree d has at most d roots.
Property 2: Given $d+1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, with all the x_i distinct, there is a unique polynomial $p(x)$ of degree (at most) d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

1. In this problem, consider all polynomials to be over GF(p), where $p > n$ for all the n defined in the problems.

   (a) How many distinct degree n polynomials are there?

   Solution: A degree n polynomial must be of the form $a_n x^n + a_n x^{n-1} \cdots + a_1 x + a_0$, where $a_n \neq 0$, and each a_i is taken from GF(p) (or in other words, from 0 to $p-1$), and a polynomial is determined uniquely by its coefficients. Thus, we have $p-1$ choices for a_n and p choices for $a_0, a_1, \ldots, a_{n-1}$, giving $\boxed{(p-1)p^n}$ such polynomials.

   (b) How many distinct polynomials $p(x)$ of degree at most n are there?

   Solution: We follow the same solution as in part (a), but now there are p choices for a_n, since a_n can be 0. We thus get $\boxed{p^{n+1}}$ polynomials.

   (c) How many distinct polynomials of degree at most n are there such that $p(0) = 1$ and $p(1) = 2$?

   Solution: A polynomial of degree at most n is uniquely determined by the values of the polynomial at $n+1$ points (for example, $p(0), p(1), \ldots, p(n-1), p(n)$). We have p choices for the values of $p(2), p(3), \ldots, p(n-1), p(n)$ (since they can taken on any value from 0 to $p-1$), and these values combined with the $p(0)$ and $p(1)$ uniquely determine a polynomial, so there are $\boxed{p^{n-1}}$ such polynomials.

2. Let $n \geq 2$ be a positive integer, and let p be a prime greater than n. Find all polynomials $q(x)$ of degree at most n in GF(p) such that $(x-2)q(x) = xq(x-1)$.

   Solution: First, we plug in $x = 0$, giving that $-2q(0) = 0$. Thus, $q(0) = 0$, so 0 is a root of $q(x)$. Then q has a factor of x, so $q(x) = xq_1(x)$ and $q(x-1) = (x-1)q_1(x-1)$ for some polynomial q_1 in GF(p). Then we have that $(x-2)xq_1(x) = x(x-1)q_1(x-1)$.

   Next, we plug in $x = 1$. Then $-1q_1(1) = 0$, so $q_1(1) = 0$. Thus, q_1 has a factor of $x-1$, so $q_1(x) = (x-1)q_2(x)$ and $q_1(x-1) = (x-2)q_2(x-1)$. Substituting in, we get $(x-2)x(x-1)q_2(x) = x(x-1)(x-2)q_2(x-1)$. Moreover, note that q_2 has degree at most $n-2$.

   Suppose that x is not equal to 0, 1 or 2. Then $q_2(x) = q_2(x-1)$. Thus, we conclude that $q_2(2) = q_2(3) = \cdots = q_2(n) = c$, where c is some constant. Note that we have $n-1$ values of the polynomial q_2, which has degree at most $n-2$. Thus, there is a unique polynomial that satisfies these equations; specifically, the constant polynomial $q_2(x) = c$.

   Thus, we conclude that $q(x) = xq_1(x) = x(x-1)q_2(x) = cx(x-1)$ for some constant c in GF(p).

4 Lagrange Interpolation

1. In this question, we want to demonstrate the intuition behind the Lagrange interpolation technique.

   Let $p(x)$ be a polynomial of degree 2 over GF(7). Suppose $p(1) = 2$, $p(2) = 1$ and $p(3) = 4$. We would like to find the coefficient representation for p.

   (a) Suppose we had polynomials, p_1, p_2, and p_3, of degree 2 satisfying the following properties:

   $$p_1(1) = 1, \quad p_1(2) = 0, \quad p_1(3) = 0$$
   $$p_2(1) = 0, \quad p_2(2) = 1, \quad p_2(3) = 0$$
   $$p_3(1) = 0, \quad p_3(2) = 0, \quad p_3(3) = 1$$

   How can we express p in terms of p_1, p_2, and p_3?

   Solution: $p = 2p_1 + p_2 + 4p_3$.

   (b) Now let's actually find the coefficient representation of p_1. To start off with, show that p_1 must have the form $c(x-2)(x-3)$ for some constant $c \in GF(7)$.

   Solution: We know that p_1 has zeros 2 and 3 so it must have $(x-2)(x-3)$ as factors. Since it is degree 2, it must be of the form $c(x-2)(x-3)$.

   (c) What is the value of c? What is the coefficient representation of p_1?

   Solution: We must multiply $(x-2)(x-3)$ by a constant factor that will make it equalled to 1 at $x = 1$. Thus we must take the multiplicative inverse of $(1-2)(1-3) = 2 \mod 7$. This turns out to be 4. Thus, $c = 4$, and expanding shows that the coefficient representation of p_1 is $4x^2 + x + 3$.

   (d) Now find p_2 and p_3 using the same method.

   Solution: $p_2 = 6x^2 + 4x + 4$, $p_3 = 4x^2 + 2x + 1$

   (e) Using what we've done so far, find p

   Solution: $p = 2(4x^2 + x + 3) + (6x^2 + 4x + 4) + 4(4x^2 + 2x + 1) = 2x^2 \mod 7$

   (f) Do you see how this relates to CRT?

   Solution: Lagrange interpolation is similar to CRT, where instead of taking numbers modulo some different n_i, we take polynomials modulo polynomials $x - n_i$.

2. Suppose that P and Q are degree n polynomials such that $P(1) = Q(1), \cdots, P(n+1) = Q(n+1)$. Show that $P = Q$.

   Solution: By Lagrange Interpolation, a degree at most n polynomial is determined by its value at $n+1$ points. Thus, we conclude that P and Q must be the same.

3. Let p be a degree 2 polynomial in GF(7) that goes through the points (1, 2), (2, 1), and (3, 4). Find p.

Solution: Using Lagrange interpolation:

$$p(x) = 2 * \frac{(x-2)(x-3)}{(1-2)(1-3)} + 1 * \frac{(x-1)(x-3)}{(2-1)(2-3)} + 4 * \frac{(x-1)(x-2)}{(3-1)(3-2)}$$

$$p(x) = x^2 - 5x + 6 - x^2 + 4x - 3 + 2x^2 - 6x + 4$$

$$p(x) = 2x^2 - 7x + 7$$

$$p(x) = 2x^2 (\mathrm{mod} 7)$$

To do this with coefficients, we have the system of equations:

$$p(1) \equiv a_2 + a_1 + a_0 \equiv 2 \mod 7$$

$$p(2) \equiv 4a_2 + 2a_1 + a_0 \equiv 1 \mod 7$$

$$p(3) \equiv 9a_2 + 3a_1 + a_0 \equiv 2a_2 + 3a_1 + a_0 \equiv 4 \mod 7$$

This is a system of 3 equations with 3 variables that can be solved (painfully) to get the same answer.

5 Secret Sharing

1. (SU19 MT2) A group of 23 officials are voting on whether to pass a law. All the officials need to vote in favor of the law for it to pass. To make the voting fair, they want to use an anonymous secret-sharing scheme, such that other members of the group cannot see what an official voted for (unless the vote is unanimous, which makes determining this trivial). Suppose there is a third party who will pick a degree d polynomial $P(x)$ in $GF(23)$, give each official a point $(i, P(i))$, and be able to confirm if a guessed polynomial is correct or not (but not reveal the polynomial itself).

   (a) What should degree d be for this scheme? Why?

   Solution: 22, so that we need 23 correct and unique points to reconstruct the polynomial.

   (b) If official i wants to vote in favor of the law, what must they do?

   Solution: They should send in the point $(i, P(i))$.

   (c) If official i wants to vote against the law, what must they do?

   Solution: They should send in the point (i, q) such that $q \not\equiv P(i) (\text{mod} 23)$ to prevent everyone from having that correct point to interpolate the polynomial.

   (d) Explain why $P(x)$ can be recovered with a unanimous vote, and cannot be recovered otherwise.

   Solution: All 23 correct points are needed to recover the 22-degree polynomial. If some people voted against the law, their points will not be a part of $P(x)$, so an incorrect polynomial will be recovered.

   (e) Explain why this scheme is anonymous.

   Solution: All our third party is able to do is tell us if the interpolated polynomial is correct ($P(x)$) or not. If we get the incorrect polynomial, we do not have any information to deduce which of the provided points actually deviated from the correct polynomial.

2. **Encoding Graphs**

Let's say that we want to encode **simple** graphs on n vertices as polynomials and send it over a channel. We label the vertices of a graph G from $0 \ldots n-1$. We create some mapping $X : F_n \to F_n$ that maps each vertex label to its corresponding vertex's degree in G. We send G along a channel by transferring points $(i, X(i))$. Answer the following questions:

(a) Find the polynomial that encodes a K_n complete graph. Is this polynomial unique to this type of graph? In other words, does this polynomial only represent the K_n graph?

Solution: The polynomial that represents this graph is going to be $P(x) = n - 1$ because every node has degree $n - 1$. This is unique because the only graphs where every vertex is of degree $n - 1$ are K_n graphs.

(b) Assume that n is even. Find the polynomial that encodes a $K_{\frac{n}{2},\frac{n}{2}}$ bipartite graph

Solution: We know that each vertex in a $K_{\frac{n}{2},\frac{n}{2}}$ bipartite has degree $\frac{n}{2}$, so the polynomial is going to be $P(x) = \frac{n}{2}$.

(c) Is it always the case that there is a unique graph for every polynomial encoded this way? If yes, prove so; if not, provide a counterexample.

Solution: No. Think about the graph on 6 vertices where each vertex has a degree of 2. You can have a simple cycle on all 6 vertices or have two separate K_3 subgraphs.

6 Appendix

Proof of Fermat's Little Theorem: Let S denote the set of non-zero integers mod p, i.e., $S = \{1, 2, \ldots, p-1\}$. Consider the sequence of numbers $a, 2a, 3a, \ldots, (p-1)a \bmod p$. We already saw in the previous Lecture Note that, whenever $\gcd(p, a) = 1$ (i.e., p, a are coprime, which certainly holds here since p is prime) these numbers are all distinct. Therefore, since none of them is zero, and there are $p-1$ of them, they must include each element of S exactly once. Therefore, the set of numbers

$$S' = \{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$$

is exactly the same as S (just in a different order)!
Now suppose we take the product of all numbers in S, mod p. Clearly, this product is

$$1 \times 2 \times \cdots \times (p-1) = (p-1)! \mod p. \tag{2}$$

On the other hand, what if we take the product of all the numbers in S'? Clearly this is

$$a \times 2a \times \cdots \times (p-1)a = a^{p-1}(p-1)! \mod p. \tag{3}$$

But from our observation in the previous paragraph that the sets of numbers in S and in S' are exactly the same (mod p), the products in (2) and (3) must in fact be equal mod p. Hence we have

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod p. \tag{4}$$

Finally, since p is prime, we know that every non-zero integer has an inverse mod p, and therefore $(p-1)!$ has an inverse mod p. Hence we can multiply both sides of (4) by the inverse of $(p-1)!$ to get $a^{p-1} \equiv 1 \pmod p$, as required.