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 $4^{9999} \bmod 19$.

(b) Compute $8^{7^{65}} \bmod 10$.

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 $a^n \pmod{p}$

(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))

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

$(p-1)^{-1} \cdots 3^{-1}\ 2^{-1}\ 1^{-1}\ 1\cdot 2\cdot 3\cdots(p-1) \equiv a^{p-1}(1\cdot 2\cdot 3\cdots(p-1)) \pmod p \Rightarrow 1 \equiv a^{p-1} \pmod p$

$(p-1)^{-1} \cdots 3^{-1}\ 2^{-1}\ 1$

$S = T$

$S = \{1, 2, 3, \cdots, p-1\} \qquad T = \{a, 2a, 3a, \cdots, (p-1)a\}$

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

$S = \{0, 1, 2, \cdots, p-1, p, p+1, \cdots, 2p, \cdots, 3p \cdots, 4p, \cdots (q-1)p, \cdots, p^2-1\}$

p #s s.t. $\gcd(\#, p) \neq 1$

$\boxed{p^2 - p}$

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

$\gcd(x, p^2) = 1 \Rightarrow x^{-1} \bmod p^2$ exists

$S' = \{1, 2, 3, \cdots, p-1, p+1, \cdots, 2p-1, 2p+1, \cdots, pp-1\}$

$|S'| = p(p-1) = p^2 - p$

$S' \qquad T' = \{a, 2a, 3a, \cdots, a(p-1), \cdots, a(p^2-1)\}$

$f(x) = ax \bmod p$ bijection whenever $\gcd(a, p) = 1$

$1\cdot 2\cdot 3\cdots(p-1)\cdots(p^2-1) \equiv a^{p(p-1)}\, 1\cdot 2\cdot 3\cdots(p-1)\cdots(p^2-1) \pmod p$

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

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?

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

(c) Calculate d.

(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'?

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

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

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

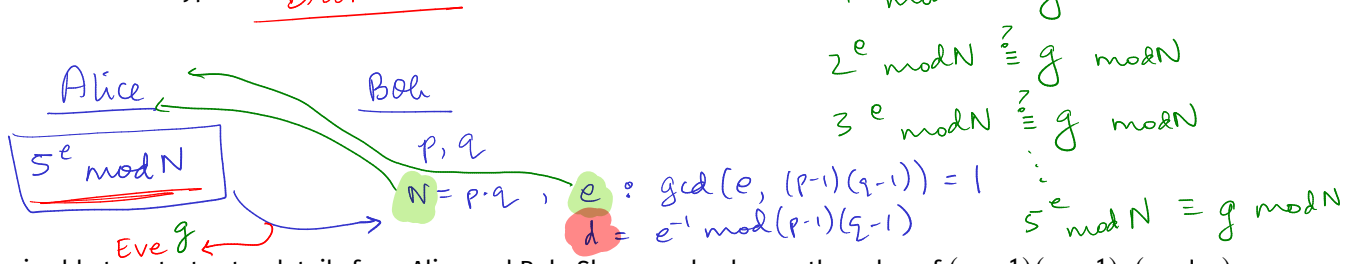
3. For all r not divisible by primes p or q, find some a and b such that

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

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. Broken

1-
2-
3-
4-
5-
6-



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

Fine $(p-1)(q-1) \equiv pq - q + 1 - p \equiv -q + 1 \pmod p$

$\Rightarrow$ Eve knows $q \bmod p$

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

Incorrect

$e^{-1} \bmod (p-1)(q-1)$ does not exist!

$m \in \{0, \ldots, pq-1\}$

HUGE 4096 bits 2048

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 $1 \le i \le d+1$.

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?

   exactly

   $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n$ ($a_n \neq 0$)

   $(p-1)p^n$

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

   p^{n+1}

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

   $(0,1), (1,2)$ $\quad n+1-2 = n-1$

   p^{n-1}

2. Let $n \ge 2$ 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 $(x-2)q(x) = xq(x-1)$.

   0 is a root of $q(x)$.

   $x = 0$ $\quad -2q(0) = 0 \quad q(x-1) = 0$

   $q(x) = (x-0)q_1(x) = xq_1(x)$

   $(x-2)xq_1(x) = x(x-1)q(x-1)$

   Let $x = 1$

   $(1-2)1q_1(1) = 0 \Rightarrow q_1(1) = 0 \Rightarrow 1$ is a root of $q_1(x)$.

   $q_1(x) = (x-1)q_2(x)$

   $(x-2)(x-1)xq_2(x) = x(x-1)(x-2)q_2(x-1)$

   q_2 has deg $\le n-2$

   $x \neq 0, x \neq 1, x \neq 2$

   $q_2(x) = q_2(x-1)$

   $n-1$ $\begin{cases} q_2(3) = q_2(2) \\ q_2(4) = q_2(3) \\ \vdots \\ q_2(n) = q_2(n-1) = c \end{cases}$

   $q_2(x) = c$

   $q(x) = xq_1(x) = x(x-1)q_2(x)$

   $= x(x-1)c$

S

$+ \quad \times \quad ()^{-1}$

"Field"

$v, u \in S$
$u+v \in S$
$u \times v \in S$

$0 \in S$
$u + 0 = u \quad \forall u \in S$
$1 \in S$
$u \times 1 = u \quad \forall u \in S$
$\forall u \in S \setminus \{0\}, \exists u^{-1} : u \times u^{-1} = 1$

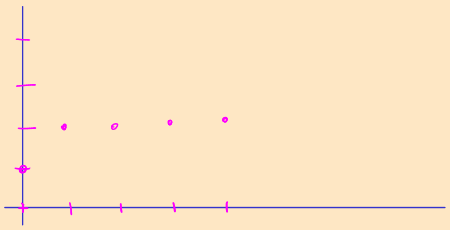
$2 \in \mathbb{Z}$
$2^{-1} = \frac{1}{2} \notin \mathbb{Z}$

$\mathbb{Z}_p \to p$ Galois field

$\mathbb{Z}_a$, a is not necessarily prime

$x^{11} \equiv x^4 \cdot x^7 \equiv x^7 \pmod 5$ (FLT)

$x^7 \to x^3$



mod 5

deg $\le d$ poly $\to d+1$

① $a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_d x^d \pmod p$

eval ↔ Lagrange Interp.

② $(x_0, y_0), (x_1, y_1), \cdots, (x_d, y_d)$

③ $a(x - r_1)(x - r_2) \cdots (x - r_d)$

$x^2 + 1, \; x \in \mathbb{R}$

$x \equiv a \pmod m$
$x \equiv b \pmod n$
$x \equiv c \pmod k$

$c\, mn\, ((mn)^{-1} \bmod k)$
$+ \; b\, mk\, ((mk)^{-1} \bmod n)$
$+ \; a\, nk\, ((nk)^{-1} \bmod m)$
$\equiv \; x \pmod{kmn}$

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.

   $(1,2)$, $(2,1)$, $(3,4)$ $\quad a + bx + cx^2 \pmod 7$

   (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?

   $p(x) = 2p_1(x) + p_2(x) + 4p_3(x)$

   (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 $c \in GF(7)$.

   $c(x-2)(x-3)$

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

   $p_1(1) = 1$

   $$c(1-2)(1-3) \equiv 1 \pmod 7$$
   $$\Rightarrow c \equiv (1-2)^{-1}(1-3)^{-1} \pmod 7$$
   $$p_1(x) \equiv 4x^2 + x + 3 \pmod 7$$

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

   $$p_2(x) \equiv (x-1)(x-3)(2-1)^{-1}(2-3)^{-1} \pmod 7$$
   $$p_3(x) \equiv (x-1)(x-2)(3-1)^{-1}(3-2)^{-1} \pmod 7$$

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

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

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 $P = Q$.

$D(x) = P(x) - Q(x) = 0$

$P(1) - Q(1) = 0$

$P(2) - Q(2) = 0$

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.

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?

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

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

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

   (e) Explain why this scheme is anonymous.

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?

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

(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.

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.