CS 70 Discrete Mathematics and Probability Theory
Fall 2026 Hug, Sabin

DIS 3

Chinese Remainder Theorem

Modular Arithmetic Intro II

Note 6

Euclid's GCD Algorithm: An algorithm to find $\gcd(x,y)$ efficiently, using the following two identities:

- $\gcd(x,y) = \gcd(y,x)$
- $\gcd(x,y) = \gcd(y, x \bmod y)$

Extended Euclid's GCD Algorithm: An extension to Euclid's GCD algorithm allowing us to find coefficients a and b such that $ax + by = \gcd(x,y)$. Note that if $\gcd(x,y) = 1$, then the equation $ax + by = \gcd(x,y) = 1$ tells us that (a,x) are inverses in $\pmod{y}$ and (b,y) are inverses in $\pmod{x}$.

Chinese Remainder Theorem: Given a system of k modular equations $x \equiv a_i \pmod{n_i}$, for various constants a_i and coprime moduli n_i, there exists a *unique* solution x defined as follows:

$$x \equiv \sum_{i=1}^{k} a_i b_i \pmod{N}$$

$$b_i = \left(\frac{N}{n_i}\right)\left(\left(\frac{N}{n_i}\right)^{-1} \bmod n_i\right)$$

$$N = \prod_{i=1}^{k} n_i$$

1 Music Video

Note 6

Xander, a music artist, is wrapping up his latest single, "Remainders Everywhere."

(a) Xander decides to run a choreography contest for his new song. The three finalists (Alice, Bob, and Candy) have very different rhythms for their choreographies though! Alice created her dance in groups of 3 beats with a 2 beat extra finale at the end. Bob's submission is 5 beat groups with a 1 beat finale. Candy's is 11 beat groups and has a 7 beat finale. If all submissions perfectly match the song, what is the smallest possible number of beats in Xander's original song?

(b) Now that Xander's music video and choreography is ready, he wants to send the final result to his mentor Yonathan to take a look. But, he needs to avoid letting the song fall into the hands of his fans, who are eagerly waiting a leak. So, Xander decides to use the RSA cryptosystem to send it to Yonathan. Using primes $p = 11$ and $q = 17$, he uses a public key of $(N, e) = (187, 7)$. What should their private key be?

2 Sparsity of Primes

Note 6

A prime power is a number that can be written as p^i for some prime p and some positive integer i. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

Hint: This is a Chinese Remainder Theorem problem. We want to find n such that $(n+1)$, $(n+2)$, $\ldots$, *and* $(n+k)$ *are all not powers of primes. We can enforce this by saying that* $n+1$ *through* $n+k$ *each must have two distinct prime divisors. In your proof, you can choose these prime divisors arbitrarily.*

3 Debugging the Chinese Remainder Theorem

Note 6

Suppose we want to solve the system

$$x \equiv 2 \pmod 5, \quad x \equiv 3 \pmod 7, \quad x \equiv 4 \pmod 9.$$

Since 5, 7, and 9 are pairwise coprime, we can use the Chinese Remainder Theorem with

$$N = 5 \cdot 7 \cdot 9 = 315.$$

Recall that in the CRT construction, each b_i should satisfy

$$b_i \equiv 1 \pmod{n_i}$$

and

$$b_i \equiv 0 \pmod{n_j}$$

for every $j \neq i$.

A student computes

$$b_1 = 126, \quad b_2 = 90, \quad b_3 = 280.$$

(a) Check each of b_1, b_2, and b_3 against the required CRT properties. Which value, if any, is incorrect? Explain why the incorrect value fails.

(b) Compute a correct replacement for the incorrect value.

(c) Using the corrected values of b_1, b_2, and b_3, find the solution x modulo 315. Verify that your answer satisfies all three original congruences.

4 Euclid's Gallons

Note 6

You have two jugs that hold a and b gallons, a tap with unlimited water, and no markings on the jugs. The only moves allowed are: fill a jug to the top, empty a jug completely, or pour one jug into the other until the first is empty or the second is full. The goal is to end with exactly t gallons in one of the jugs.

(a) (Famous one!) With a 3 gallon and a 5 gallon jug, get exactly 4 gallons. Write out your moves. Then count how many times you filled each jug and emptied each jug, and try to write an equation that must hold for your solution.

(b) Call pouring from one jug into another "pumping a into b." In one round of pumping, we fill the a jug and pour it into the b jug. If the b jug fills up before the a jug is empty, empty the b jug and pour the leftover from the a jug into it. Every round starts and ends with the a jug empty. Try pumping 3 into 5 for a few rounds and keep track of how much the 5 jug holds after each round.

Now suppose $\gcd(a,b) = 1$ and $0 < t < b$. Show that the b jug holds exactly t gallons after some round, and give a formula for which round this happens on.

(c) You have a 7 gallon and a 12 gallon jug and need 5 gallons. Use the extended Euclidean algorithm to find how many rounds it takes to pump 7 into 12. Then find how many rounds it takes to pump 12 into 7 (same procedure with the roles swapped: fill the 12 jug, pour into the 7 jug, empty the 7 jug when it fills). Which would you rather do?

(d) With a 6 gallon and a 9 gallon jug, can you measure 4 gallons? Explain.

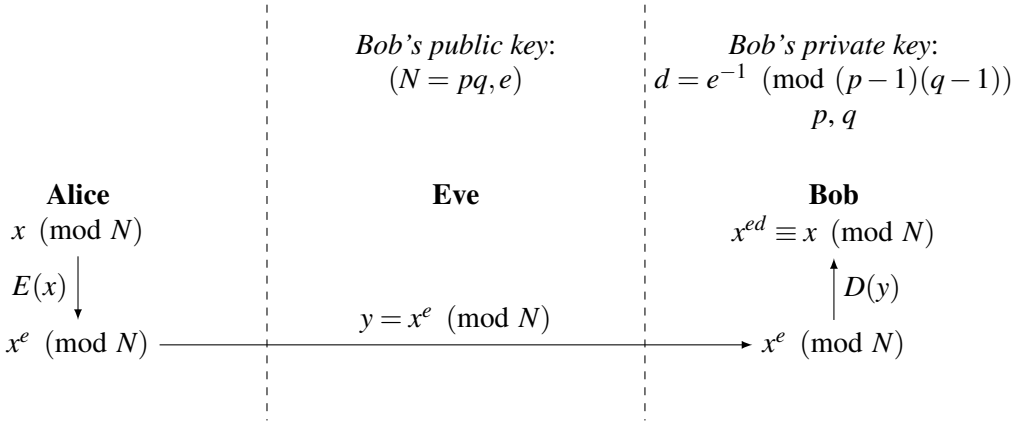
RSA

RSA Intro

Note 7

Fermat's Little Theorem: For all primes p, $a^{p-1} \equiv 1 \pmod{p}$ if $a \neq 0$. An equivalent version of the statement (still assuming p is prime) is $a^p \equiv a \pmod{p}$ for all a.

RSA Scheme: A cryptographic scheme that allows communication over insecure channels via public-key encryption. Alice encrypts her message x with Bob's public key, ensuring that only Bob (with his private key) can decrypt it, which prevents Eve from eavesdropping.



5 RSA for Concert Tickets

Note 7

Alice wants to tell Bob her concert ticket number, m, which is an integer between 0 and 100 inclusive. She wants to tell Bob over an insecure channel that Eve can listen in on, but Alice does not want Eve to know her ticket number.

(a) Bob announces his public key $(N = pq, e)$, where N is large (512 bits). Alice encrypts her message using RSA. Eve sees the encrypted message, and figures out what Alice's ticket number is. How did she do it?

(b) Alice decides to be a bit more elaborate. She picks a random number r that is 256 bits long, so that it is too hard to guess. She encrypts that and sends it to Bob, and also computes rm, encrypts that, and sends it to Bob. Eve is aware of what Alice did, but does not know the value of r. How can she figure out m? (You may assume that r is coprime to N.)

6 RSA with Multiple Keys

Note 7

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(N_1, e), \ldots, (N_k, e)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

Further, in all of the subparts, you may assume that Eve knows the details of the modified RSA schemes (i.e. Eve knows the format of the N_i's, but not the specific values used to compute the N_i's).

(a) Suppose Eve sees the public keys $(p_1q_1, 7)$ and $(p_1q_2, 7)$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently. Think of p_1, q_1, q_2 as massive 1024-bit numbers. Assume p_1, q_1, q_2 are all distinct and are valid primes for RSA to be carried out.

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(p_1q_1, 3)$, $(p_2q_2, 3)$, and $(p_3q_3, 3)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above. Assume $p_1, p_2, p_3, q_1, q_2, q_3$ are all distinct and are valid primes for RSA to be carried out.

(c) Let's say the secret x was not changed ($e = 3$), so they used the same public keys as before, but did not transmit different messages. How can Eve figure out x?