SAMS 2023 WEEK 4: MODULAR ARITHMETIC AND RSA ENCRYPTION

Please keep this packet and bring it with you to class every day this week to work on. This packet will not be collected, but I encourage you to use our google group (linked on our course webpage) to post questions and solutions. A list of mini projects is included at the end of this worksheet. I'll ask groups to select a project topic no later than Wednesday, and to give a short (5-10 minute presentation) at the beginning of class this Friday.

Definitions and Theorems

The following definitions and theorems will be introduced during lecture, and will be needed for this week's problem set. Note that a *definition* is some explanation of the meaning of a word. A *theorem* is some statement which has been demonstrated to be true.

Definition 1. Let n be a positive integer. We say that integers a and b are CONGRUENT MODULO n if $n \mid (a-b)$. Equivalently, a is congruent to b modulo n if there exists an integer k so that

$$a = nk + b.$$

In this case, we write $a \equiv b (\mathrm{mod}\, n)$.

Definition 2. Let a be an integer. Then the MULTIPLICATIVE INVERSE OF a MODULO n, if it exists, is the integer a^{-1} so that

$$aa^{-1} \equiv 1 (\mathrm{mod}\, n).$$

Note that a^{-1} is unique if we choose it so that $0 \leq a^{-1} < n$.

RSA Encryption. In this scenario, Bob would like to send a secret message to Alice, which he has encoded as an integer m.

STEP 1: KEY CREATION (ALICE). Alice chooses two secret primes p and q. She then chooses any integer e called the *encryption exponent* satisfying

$$\gcd(e, (p-1)(q-1)) = 1.$$

Alice publishes $N = pq$ and e.

STEP 2: MESSAGE ENCRYPTION (BOB). Bob uses the public key (N, e) that Alice published in Step 1 to compute

$$c \equiv m^e (\mathrm{mod}\, N).$$

Bob then sends c back to Alice. Note that Bob's message m must satisfy $0 \leq m < N$ for the message to be decrypted successfully.

STEP 3: MESSAGE DECRYPTION (ALICE).

Alice computes the inverse of e modulo $(p-1)(q-1)$, say $d = e^{-1} (\mathrm{mod}\, (p-1)(q-1))$ and computes

$$c^d (\mathrm{mod}\, N).$$

We will observe that $c^d \equiv m (\mathrm{mod}\, N)$ and so Alice has successfully decrypted Bob's message.

Problem Set

Complete as many problems from the list below as you have time and interest for. Feel free to skip around as you'd like, and to work on your own or with your group as you prefer. If you generally prefer to work on your own, I encourage you to discuss at least two problems together with your group. I suggest you keep a notebook or binder for this course to store your solutions. There is also scratch paper available at the front of the class for you to use at any time.

P1. Determine which of the following congruences are true.

a) $14 \equiv 2 (\mathrm{mod}\, 12)$

b) $74 \equiv -1 (\mathrm{mod}\, 5)$

c) $74 \equiv -1 (\mathrm{mod}\, 7)$

d) $544 \equiv 16 (\mathrm{mod}\, 13)$

e) $-177 \equiv 3 (\mathrm{mod}\, 15)$

f) $70 \equiv 45 (\mathrm{mod}\, 22)$

P2. Let a and b be integers with $a \equiv b (\mathrm{mod}\, n)$ and $c \equiv d (\mathrm{mod}\, n)$.

a) Show that $a + c \equiv (b + d) (\mathrm{mod}\, n)$.

b) Show that $ac \equiv bd (\mathrm{mod}\, n)$.

P3. Explain why $n \mid a$ implies that $a \equiv 0 (\mathrm{mod}\, n)$. Conversely, explain why $a \equiv 0 (\mathrm{mod}\, n)$ implies that $n \mid a$.

P4. Find the multiplicative inverse of the following integers for the given modulus, if it exists. If it doesn't exist, explain why not.

a) $a = 3$ modulo $n = 7$

b) $a = 2$ modulo $n = 6$

c) $a = 2$ modulo $n = 21$

d) $a = 1$ modulo n for any integer n

e) $a = -1$ modulo n for any integer n

f) $a = n$ modulo n for any integer n

P5. Use the RSA algorithm described above to send a "secret number" to one of your groupmates without your other groupmates intercepting it. Note that all groupmates will need to create their own public keys.

a) What are some of the difficulties you ran into implementing the RSA algorithm?

b) Suppose that Eve is able to guess your primes p and q. How do you think Eve could intercept your private message?

Additional Problems

The problem set below requires methods and background we won't necessarily cover in our course. If you've seen proof methods before, or want some extra challenge, feel free to play with these!

A1. In this problem, we'll derive the following divisibility test.

Theorem 1. A positive integer n is divisible by 3 *if and only if* the sum of the digits of n is divisible by 3. That is, *if* a positive integer is divisible by 3, then the sum of the digits of n is also divisible by 3. *And conversely* if the sum of the digits of n is divisible by 3, then n is divisible by 3.

a) Let's start by checking to see if Theorem 1 holds for several examples.

(i) Observe that the following integers are divisible by 3, and the sum of their digits is also divisible by 3

$$13452, 279, 1020.$$

(ii) Choose a few integers whose digits *do not* sum to an integer divisible by 3. Check that they are not divisible by 3.

b) Next, let's use modular arithmetic to show that 13452 is divisible by 3 without using a calculator.

(i) Find integers a_0, a_1, a_2, a_3, a_4 so that

$$13452 = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + a_3 10^3 + a_4 10^4.$$

(ii) Check that $10 \equiv 1 (\mathrm{mod}\, 3)$.

(iii) Using P2 (b), convince yourself that we also have

$$10^2 \equiv 1 (\mathrm{mod}\, 3) \text{ and } |10^3 \equiv 1 (\mathrm{mod}\, 3).$$

(iv) Use P2 and the previous part to show that

$$13452 \equiv (a_0 + a_1 + a_2 + a_3 + a_4) \mathrm{mod}\, 3.$$

(v) Check that $a_0 + a_1 + a_2 + a_3 + a_4 \equiv 0 (\mathrm{mod}\, 3)$. Conclude from the previous part that $13452 \equiv 0 (\mathrm{mod}\, 3)$.

(vi) Using P3 to conclude that $3 \mid 13452$.

c) Finally, let's show that Theorem 1 holds for any integer. Our proof will follow similarly to the example in the previous part. Throughout, let n be any fixed integer.

(i) Explain how we know that there are integers $a_0, a_1, \ldots, a_k$ so that

$$n = a_0 + a_1 10^1 + a_2 10^2 + \cdots + a_k 10^k.$$

(ii) Explain how we know that $10^k \equiv 1 (\mathrm{mod}\, 3)$ for any integer k.

(iii) Using P2 and the previous part, observe that

$$n \equiv (a_0 + a_1 + \cdots + a_k) (\mathrm{mod}\, 3).$$

(iv) Suppose that $3 \mid n$. Use the previous part to show that

$$n \equiv 0 (\mathrm{mod}\, 3).$$

Conclude that $3 \mid n$.

(v) Conversely, suppose that $3 \mid (a_0 + a_1 + \cdots + a_k)$. Show that $3 \mid n$.

A2. Use a similar process to P3 to show the following.

Theorem 2. A positive integer is divisible by 9 if and only if the sum of its digits are divisible by 9.

A3. Lookup some other divisibility tests. You should be able to find them for the following integers: 2, 3, 5, 7, 11 and 13. You don't need to prove any of these, but it might be satisfying to check them for a few examples.

Mini Projects

Work with your group to select a topic from the list below that looks interesting to investigate. Only one topic may be covered by each group, and sign ups will be on a first come first serve basis. My only instruction for your presentations is to tell us something interesting about what you investigated in a way you're proud of. Your presentations should last about 5 minutes, but please make sure to take **no longer than 10 minutes**. There are no requirements, grades, or judgment for this assignment. Engage with it as much as is interesting to you!

Topics.

1. **Primitive Roots.** Some things you might investigate: What is a primitive root modulo a prime p? Give some examples. What do we know about how to find a primitive root of a given modulus?

2. **The Enigma Machine.** Some things you might investigate: What was the purpose of this machine? What was the historical significance? Can you say anything about how this encoded messages? Who was able to break the enigma machine? What was the significance of this?

3. **Alan Turing.** Some things you might investigate: Who was he? What was he best known for? What was his relation to the Enigma machine?

4. **Ancient Cryptography** Give a survey of cryptosystems from various cultures throughout history.

5. **History of RSA**. Some things you might investigate: Who was RSA named after? When was it created? Lookup the classification of cryptographic algorithms as munitions under the International Traffic in Arms Regulations. What was the social response to this regulation? Looking up "crypto wars" may be helpful.

6. **Diffie-Hellman**. We'll see the Diffie-Hellman key exchange next week. Some things you might investigate: Who were Diffie and Hellman? What were they best known for? I believe theirs was the first public key cryptosystem, is this true? Why was that significant?