Lec 15: Modular Arithmetic

Prof. Adam J. Aviv

GW

CSCI 1311 Discrete Structures I
Spring 2023

Congruence Modulo 3

Define the relation T on $\mathbb{Z}$, such that forall integers m and n

$$m \, T \, n \iff 3 \mid (m - n)$$

Show that T is reflexive, symmetric, and transitive, and is thus a equivalence relation.

Equivalence class modulo 3

- Reflexive: $m \, T \, m \implies 3 \mid (m - m) \implies 3 \mid 0$ which is true
- Symmetric: We must show that if $m \, T \, n$ then $n \, T \, m$. By definition of the relation and divides, $m \, T \, n \implies 3 \mid (m - n)$. So there must exists a k such that $3k = (m - n)$. If we multiply both sides by -1, then $3(-k) = n - m$. Let $k' = -k$, and $3k' = (n - m)$ which means that $3 \mid (n - m)$ and $n \, T \, m$.
- Transitive: We must show that if $m \, T \, n$ and $n \, T \, p$ then $m \, T \, p$. Using the same argument as before, if $m \, T \, n$ and $n \, T \, p$ there must exists r and s such that $3r = m - n$ and $3s = n - p$. If we add those two equations, $3r + 3s = m - n + n - p$, and then $3(r + s) = m - p$. Let $k = (r + s)$, and we have $3k = (m - p)$. So $3 \mid (m - p)$ and $m \, T \, p$.

Modulo congruence

Definition

Let m and n be integers and let d be a positive integer. We say that m is congruent to n modulo d and write

$$m \equiv n \pmod{d}$$

if, and only if,

$$d \mid (m - n)$$

More formally,

$$m \equiv n \pmod{d} \iff d \mid (m - n)$$

Modular Equivalences

If a,b, and n are integers with $n > 1$, we can desribe modular equivalence of a and b modulo n in any of the following ways:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$ (or $a \equiv_n b$)
3. $\exists k, a = b + kn$
4. a and b have the same (non-negative) remainder when divided by n
5. $a \bmod n = b \bmod n$

Exercise: congruence modulo n is a equivalence relation

For any integer $n > 1$, the congruence modulo n defines an equivalence relation. Show that for any integer a and b, $a \equiv b \pmod{n}$ is symmetric, reflexive and transitive.

What are all the equivalence classes for congruence modulo n?

Modular Arithmetic

Modular arithmetic is performing standard operations (addition, subtraction, multiplication) under a modulo, and because of the small set of equivalence classes, there are some interesting properties.

Modular Arithmetic

Let a, b, c, d and n be integers where $n > 1$. Suppose,

$$a \equiv c \pmod{n} \quad \wedge \quad b \equiv d \bmod n$$

Then

1. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$ for all integers m

Equivalence under multiplication

Multiplication Equivalence

If a, b, c, d and n are integers with $n > 1$ and

$$a \equiv c \pmod{n} \quad \wedge \quad b \equiv d \bmod n$$

then $ab \equiv cd \pmod{n}$

Proof.

If $a \equiv c \pmod{n}$ and $b \equiv_n d \pmod{n}$ then exists r and s such that $a = c + rn$ and $b = d + sn$. So

$$\begin{aligned} ab &= (c + rn)(d + sn) \\ &= cd + crn + rn + rnsn \\ &= cd + n(cr + r + rsn) \end{aligned}$$

Let $k = (cr + r + rsn)$, so $ab = cd + nk$. By definition of congruence modulo n, $ab \equiv cd \pmod{n}$ □

Exercise

Prove that

$(a + b) \equiv (c + d) \pmod n$

$(a - b) \equiv (c - d) \pmod n$

Multiplication before or after modulo

Corollary 1

Let a, b, and n are integers where $n > 1$, then

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod n$$

Corollary 2

Let a be an integer and m and n are integers where $n > 1$ and $m \geq 1$, then

$$a^m \equiv [(a \bmod n)^m] \pmod n$$

Exercise

Compute the following results

$(29 \cdot 30) \bmod 5$

$(42 \cdot 11)^3 \bmod 4$

$17^8 \bmod 3$

GCD: Greatest Common Denominator

Definition

The greatest common denominator (or GCD) of two positive integers a and b is largest integer value n such that $n \mid a$ and $n \mid b$, and we would say that the $gcd(a, b) = n$

Euclid's algorithm for $gcd(a, b)$:

1. Check if b is 0, if it is, then $gcd(a, 0) = a$ and we're done.
2. If $b > 0$, then let $r = a \bmod b$
3. Repeat (1), now computing $gcd(b, r)$ (so a is b, and b is r)

Compute $gcd(330, 156)$

Linear combination of integers

Definition

An integer d is said to be a linear combination of integers a and b if, and only if, there exists integers s and t such that $as + bt = d$.

Theorem (GCD as a Linear Combination)

For all integers a and b, not both zero, if $d = gcd(a, b)$, then there exists integers s and t such that $as + bt = d$.

Relative Prime and Linear Combinations

Definition

Two positive integers a and b are relatively prime if $gcd(a, b) = 1$. That is, they share no common divisors.

Corollary: Linear Combination of Relative Primes

If a and b are relatively prime (that is $gcd(a, b) = 1$), then there exists integers s and t such that $as + bt = 1$

Inverse Modulo

Corollary: Existence of Inverse Modulo n

For all integers a and n, if $gcd(a, n) = 1$, then there exists an integer s such that $as \equiv 1 \pmod{n}$. The integer s is called the inverse of a modulo n.

Proof.

By Corollary of Linear Combinations of Relatively Primes, there exists a s and t such that

$$
\begin{aligned}
as + nt &= 1 \\
as &= 1 - nt \\
as &= 1 + (-t)n
\end{aligned}
$$

By definition of congruence modulo n

$$as \equiv 1 \pmod{n}$$

□

Implications of Inverse Modulo

An inverse allows us to cancel out a value, like a^{-1} is the inverse of a. This is critical operation for cryptography.

Note we can only guarantee that an inverse exists if value and the modulo are relatively prime, but if the modulo is prime (or the product of two primes) than it should be relatively prime with all numbers except itself (or the two primes)

Find the inverse of the following numbers modulo 3

- 7
- 8
- 13

RSA Cryptography

One of the most important discoveries in cryptography is based on properties of modular arithmetic and modular inverses.

Rivest, Shamir, and Adleman.

Asymmetric, Public Key Cryptography

Asymmetric (or Public Key) Cryptography is a cryptographic procedure by which each party has a public encryption key that is known to every one and a private decryption key that is secret to them.

If Alice wants to send a message to Bob, Alice would encrypt the message with Bob's public key and send the resulting cipher text to Bob who decrypts the message using his private key.

The security is guaranteed by computational bounds. It is nearly impossible to determine (compute) a private key given the public key.

RSA Equations

Let p and q be primes, then we can find positive integers d and e such that d is the inverse to e modulo $(p-1)(q-1)$.

The public key is e and $n = pq$ — note that we release n, the multiplication of the two primes, but not the primes themselves.

The private key is d (the private exponent) and the values of p and q (the prime pair).

$$\underbrace{\boxed{C = M^e \bmod pq}}_{\text{Encryption}} \qquad \underbrace{\boxed{M = C^d \bmod pq}}_{\text{Decryption}}$$

Example RSA Encryption

Let's label the English alphabet as $A = 1, B = 2, C = 3, \ldots, Z = 26$, and public key is $n = 55$ and $e = 3$.

We can encrypt the message "HI" by encrypting each letters, "H"$= 8 = M_0$ and "I"$= 9 = M_1$.

$$C_0 = 8^3 \bmod 55 = 256 \bmod 55 = 17$$

$$C_1 = 9^3 \bmod n = 729 \bmod n = 14$$

Example RSA decryption (1)

To decrypt we need the secret exponent d for p and q. In our example, $p = 11$ and $q = 5$, so $(p-1)(q-1) = 40$. The positive inverse of $e = 3$ is $d = 27$ modulo 40.

$$M_0 = C_0^{27} \bmod 55 = 17^{27} \bmod 55$$

This may seem really difficult to compute, but since its under a modulo, we can solve it by taking successive powers.

Example RSA decryption (2)

$$\begin{aligned}
17 \bmod 55 &= 17 \bmod 55 & & = 17\\
17^2 \bmod 55 &= 17^2 \bmod 55 & = 17^2 \bmod 55 & = 14\\
17^4 \bmod 55 &= (17^2 \bmod n)^2 \bmod 55 & = (14)^2 \bmod 55 & = 31\\
17^8 \bmod 55 &= (17^4 \bmod n)^2 \bmod 55 & = (31)^2 \bmod 55 & = 26\\
17^{16} \bmod 55 &= (17^8 \bmod n)^2 \bmod 55 & = (26)^2 \bmod 55 & = 16
\end{aligned}$$

$$\begin{aligned}
17^{27} \bmod 55 &= 17^{16+8+2+1} \bmod 55\\
&= (17^{16} \cdot 17^8 \cdot 17^2 \cdot 17) \bmod 55\\
&= (16 \cdot 26 \cdot 14 \cdot 17) \bmod 55\\
&= ((16 \cdot 26) \bmod 55) \cdot ((14 \cdot 17) \bmod 55) \bmod 55\\
&= (31 \cdot 18) \bmod 55\\
&= 8 = \text{“H”}
\end{aligned}$$

Exercise

Decrypt $C_1 = 14$ with $pq = 55$ and $d = 27$.

Encrypt “GO” with $pq = 55$ and $e = 3$.