Lecture 12: Modular Arithmetic

http://book.imt-decal.org, Ch. 3.2

Introduction to Mathematical Thinking

March 7, 2019

Suraj Rampure

Announcements

number theory: integers

Recap

- Divisibility: $a|b$ → $b = ca$
- Division Algorithm: $a = dq + r$, where $0 \leq r < d$ $r \in \{0, 1, 2, \ldots d-1\}$
- Fundamental Theorem of Arithmetic: every positive integer has a unique prime factorization
- Canonical Representations $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ ($p_1, p_2, \ldots, p_k$: primes)
- GCD and LCM

Important takeaway:

- In the division algorithm, if we set $d = 4$, for example, it tells us all integers can be written in the form $4q$, $4q + 1$, $4q + 2$, or $4q + 3$

Common misconceptions:

1. $a|bc$ DOES NOT IMPLY $a|b$ or $a|c$ (e.g. $12|4 \cdot 9$, but 12 does not divide 4 or 9)
2. $a|b^n$ DOES NOT IMPLY $a|b$ (e.g. $12|6^2$, but 12 does not divide 6)

$$d = \gcd(a,b) \Longrightarrow \exists\, u, v \in \mathbb{Z} : au + bv = d$$

converse holds when $\gcd(a,b) = 1$

i.e. if $\exists\, u, v : au + bv = 1 \Longrightarrow \gcd(a,b) = 1$

Example

Prove that if $\gcd(a, c) = \gcd(b, c) = 1$, then $\gcd(ab, c) = 1$.

Hint: Use the fact that we can always find integers x, y such that $ax + by = \gcd(a, b)$.

$$ax + cy = 1$$
$$bx' + cy' = 1$$

WTS $ab \cdot \square + c \cdot \triangle = 1$

$$1 = (ax + cy)(bx' + cy') = abxx' + acxy' + bcx'y + c^2yy'$$

$$1 = ab(xx') + c(axy' + bx'y + cyy')$$

$\therefore \gcd(ab, c) = 1$.

Motivating Examples for Modular Arithmetic

Odd and Even

equivalent

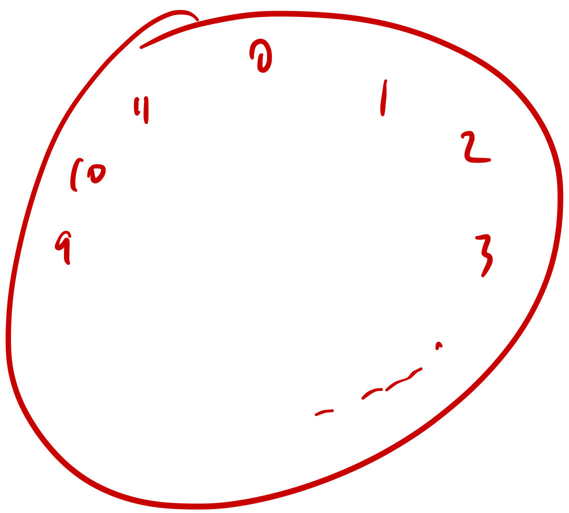
odd: remainder 1 when div by 2 — 7, 3, −13, 57... ≡ 1

even: remainder 0 " " 2 — 4, −16, 22, ... ≡ 0

e.g. $15 + 13 \cdot 22 \equiv 1 + 1 \cdot 0 \equiv 1 + 0 \equiv 1$

$15 + 73 \cdot 75 \equiv 1 + 1 \cdot 1 \equiv 2 \equiv 0$

Clocks



6:00, 8 hours later

→ 2 o'clock

$\{0, 1, 2, \ldots 11\}$

Formalization

We say

equivalent / congruent

$$a \equiv b \pmod{m}$$

if and only if

23 ≡ 2 mod 7

7 | 23 − 2

$$m|a-b$$

$a \equiv b \pmod{m}$ reads "a is equivalent to b, **modulo** m." a and b are equivalent modulo m if and only if they have the same remainder when divided when m. We can also represent this as $b = a + km, k \in \mathbb{Z}$.

19 ≡ 24 ≡ 4 ≡ 1004 mod 5

e.g. 23 = 2 + k · 7

3

When dealing with numbers modulo m, all integers can be reduced to one of

$$\{0, 1, 2, ..., m-1\}$$

This is the set of all possible remainders when dividing by m.

For example, consider the set of integers mod 3. All integers are equivalent to a number in the set $\{0, 1, 2\}$. For instance, under modulo 3, we have that $33 \equiv 0$ and $11 \equiv 2$.

Suppose that $a \equiv r \pmod{m}$. We can add any integer multiple of m to a, and the equivalence still holds, since the remainder when dividing by m doesn't change.

$-12 \equiv -7 \equiv -2 \equiv 3 \equiv 8 \equiv 13 \equiv 18 \equiv 23 \ldots \mod 5$

$a = mq + r$

$a + m = mq + r + m$

$a + m = m(q+1) + r$

Therefore, the following are all equivalent to a in modulo m:

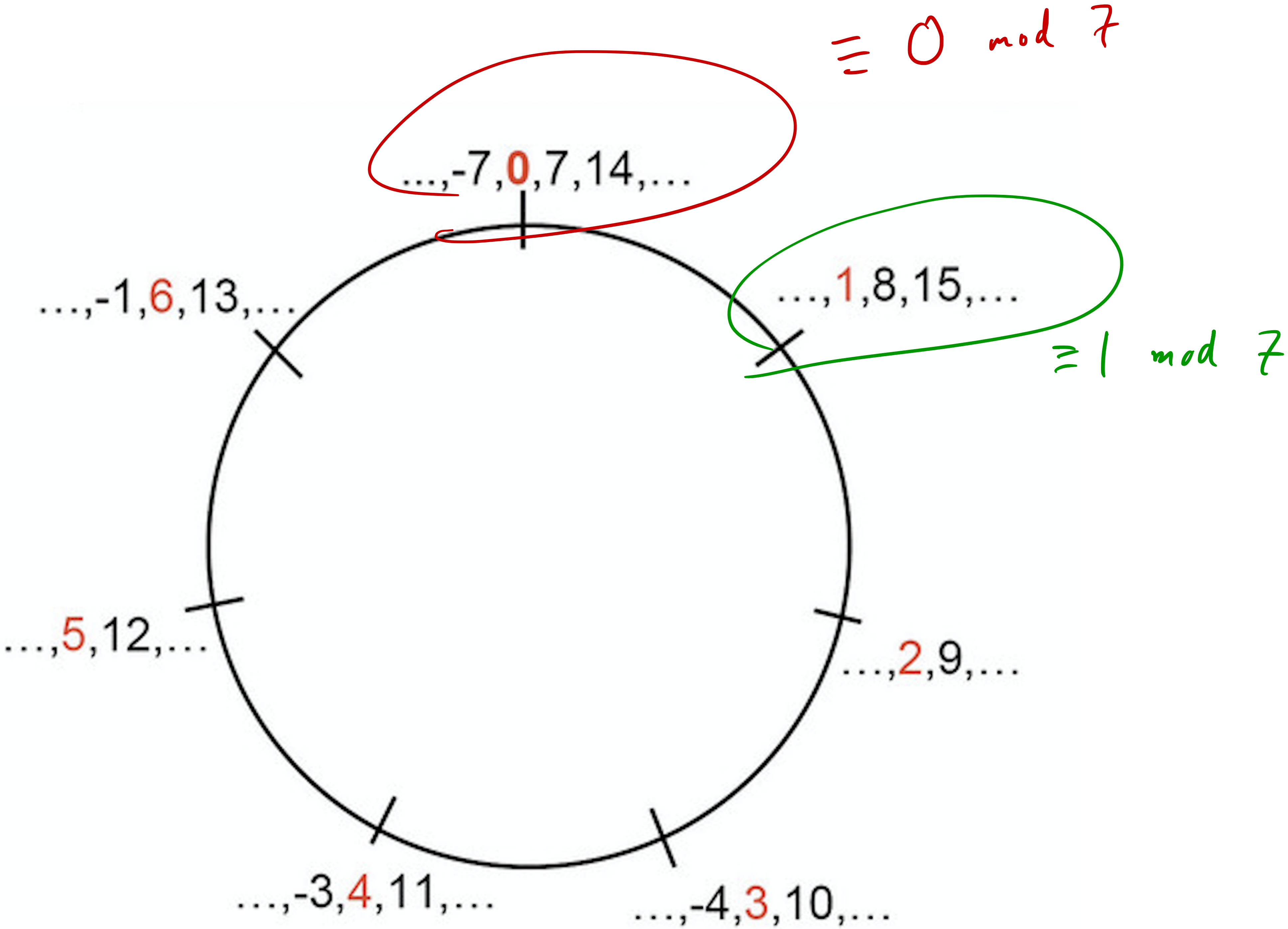
$$\{\ldots, a-2m, a-m, a, a+m, a+2m, \ldots\}$$

For example, all elements in the following set are equivalent to $3 \pmod{5}$, and can thus be "reduced" to 3:

$$\{\ldots, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\}$$

Note: This implies that negative integers also have equivalences in modular arithmetic, e.g. $-12 \equiv 3 \pmod{5}$

$5 \mid -12 - 3 \rightarrow -15 = k \cdot 5$, $k = -3$


≡ 0 mod 7
…,-7,0,7,14,…
…,1,8,15,…
≡ 1 mod 7
…,-1,6,13,…
…,5,12,…
…,2,9,…
…,-3,4,11,…
…,-4,3,10,…

Addition and Multiplication

$\mathbb{Z}/5\mathbb{Z} \longleftrightarrow \mathbb{Z}_5$: set of integers modulo 5

Suppose we want to simplify $13 + 14 \cdot 6 \pmod 5$. We could do the following:

$$13 + 14 \cdot 6 \equiv 13 + 84 \equiv 97 \equiv 2 \pmod 5$$

However, we could also simplify things first:

$$13 + 14 \cdot 6 \equiv 3 + 4 \cdot 1 \equiv 7 \pmod 5 \equiv 2 \pmod 5$$

or even

$$13 + 14 \cdot 6 \equiv -2 + 4 \cdot 1 \equiv 2 \pmod 5$$

$$-2 + (-1) \cdot 1 \equiv -3 \equiv 2 \pmod 5$$

Note, regardless of the order of simplification, the "standard form" result always remains the same.

In general, we have that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

Addition $$a + c \equiv b + d \pmod{m}$$

Multiplication $$a \cdot c \equiv b \cdot d \pmod{m}$$

$b = a + mk_1$
$d = c + mk_2$
$+$
$b + d = a + c + m(k_1 + k_2)$
$\square = \triangle + m\,\bigcirc$
Addition $\therefore \square \equiv \triangle$ mod m

Proof of the first rule:

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $b = a + mk_1$ and $d = c + mk_2$.

$$b + d = a + c + mk_1 + mk_2 = (a + c) + m(k_1 + k_2)$$

$$\Rightarrow b + d \equiv a + c \pmod{m}$$

Proof of the second rule: Exercise.

$$b = a + mk_1$$
$$d = c + mk_2$$

RTP $bd \equiv ac \mod m$,

i.e. $bd = ac + m\Delta$,

$\Delta \in \mathbb{Z}$

$$bd = (a + mk_1)(c + mk_2)$$

$$bd = ac + mak_2 + mk_1c + m^2k_1k_2$$

$$bd = ac + m(ak_2 + ck_1 + mk_1k_2)$$

$\therefore \quad bd \equiv ac \mod m$

$(x^a)^b = x^{ab}$

$15 = 3 \cdot 5$

$2^{15} = (2^3)^5$

Exponentiation

Suppose we want to evaluate $2^{15} \pmod 9$. We *could* find $2^{15} = 32768$, and divide this number by 9 and find the remainder, but there's a better way.

$$2^{15} = (2^3)^5$$

$(2 ** 15) \% 9 \rightarrow 8$

We can use the fact that $2^3 \equiv 8 \equiv -1 \pmod 9$:

$$(2^3)^5 \equiv (-1)^5 \equiv -1 \equiv 8 \pmod 9$$

Let's look at the following examples:

$11 = 10 + 1$

- $5^{11} \pmod{26}$ $\equiv (5^2)^5 \cdot 5 \equiv (-1)^5 \cdot 5 \equiv -5 \equiv 21 \bmod 26$ $= 2 \cdot 5 + 1$
- $23^9 \pmod{24}$ $\equiv (-1)^9 \equiv -1 \equiv 23 \bmod 24$

Exponentiation Technique: Repeated Squaring

Any integer can be written as the sum of powers of two (because any integer can be written in binary).

Suppose we want to consider $4^{26} \pmod{13}$. We can write $26 = 16 + 8 + 2$, implying that we can write 4^{26} as $4^{16} \cdot 4^8 \cdot 4^2$.

$$4^1 \equiv 4 \pmod{13}$$

$$4^2 \equiv 16 \equiv 3 \pmod{13}$$

$$4^8 \equiv (4^2)^4 \equiv 3^4 \equiv 81 \equiv 3 \pmod{13}$$

$$4^{16} \equiv (4^8)^2 \equiv 3^2 \equiv 9 \pmod{13}$$

Combining these results: $4^{26} \equiv 4^{16} \cdot 4^8 \cdot 4^2 \equiv 9 \cdot 3 \cdot 3 \equiv 27 \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod{13}$

Example

Determine $3^{37} \pmod{53}$.

$37 = 32 + 4 + 1$

$\Rightarrow 3^{37} = 3^{32} \cdot 3^{4} \cdot 3^{1}$

$3^{1} \equiv 3$

$3^{2} \equiv 9$

$3^{4} \equiv 9^{2} \equiv 81 \equiv 28$

$3^{8} \equiv 28^{2} \equiv$

$3^{16} \equiv$

$3^{32} \equiv$

$14^7 \equiv 14 \equiv 0 \mod 7$

Fermat's Little Theorem

Consider some prime p. Then, Fermat's Little Theorem states

$$a^p \equiv a \pmod{p}$$

Alternatively, if a is not a multiple of p, we can say

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

$\gcd(a, p) = 1$

$5^6 \equiv 1 \mod 7$

$25^{-6} \mod 7 \longrightarrow 1 \mod 7$

$5^9 \mod 7 \equiv (5^7)\cdot(5^2)$

$\equiv 5 \cdot 5^2 \equiv 5 \cdot 4 \equiv 20 \equiv -1 \equiv 6$

Modular arithmetic makes proofs that previously required induction or many cases relatively simple.

Example: Prove $11^n - 6$ is divisible by 5, $\forall n \in \mathbb{N}$.

$5 \mid 11^n - 6, \ \forall n \in \mathbb{N}$

$\Updownarrow$

$11^n - 6 \equiv 0 \bmod 5$

Before: Done by induction.

Base Case: $n = 1$: $11 - 6 = 5$, which is clearly divisible by 5.

Induction Hypothesis: Assume $11^k - 6$ is divisible by 5, for some arbitrary $k \in \mathbb{N}$ Equivalently, we can say that $5c = 11^k - 6$, for some $c \in \mathbb{N}$.

Induction Step:

$$11^{k+1} - 6 = 11^k \cdot 11 - 6 = (5c + 6) \cdot 11 - 6 = 5(11c + 12)$$

$$\therefore \ 5 \mid 11^k - 6 \Rightarrow 5 \mid 11^{k+1} - 6$$

Now:

$1^n - 1 \equiv 0$

$$11^n - 6 \equiv 1^n - 6 \equiv 1 - 6 \equiv -5 \equiv 0 \pmod 5$$

$11 \equiv 1 \bmod 5$

Example

Prove that any odd square is of the form $8k+1$, where k is an integer.

Chapter 3.2.

if n is odd, $n^2 \equiv 1 \mod 8$

1
3
5
7

$8c$	$8c+1$
$8c+2$	$8c+3$
$8c+4$	$8c+5$
$8c+6$	$8c+7$

Cancellation Law

In standard arithmetic, the cancellation property refers to the fact that, for any real numbers $a, b, c, c \neq 0$,

$$ac = bc$$

$$ac = bc \Rightarrow a = b$$

Does this hold in modular arithmetic?

$2 \cdot 6 \equiv 12 \equiv 0$

$4 \cdot 6 \equiv 24 \equiv 0$

mod $\underline{12}$

$ac \equiv bc \mod 5$

$\Rightarrow a \equiv b \mod 5$

$2 \cdot 6 \equiv 4 \cdot 6 \mod \underline{12}$

~~$2 \equiv 4$~~

inverse of 3, + : -3

$3 + (-3) = 0$

Division in Modular Arithmetic

In traditional, non-modular arithmetic, to solve the equation $3x = 14$, we would multiply both sides by the multiplicative inverse of 3, i.e. "divide by 3":

id_{add} : 0

id_{mult} : 1

$$3x = 14$$

$$3^{-1} \cdot 3x = 3^{-1} \cdot 14$$

$x = 3^{-1} \cdot 14 = \frac{1}{3} \cdot 14$

The *multiplicative inverse* of any non-zero real number x is defined such that

$$x \cdot x^{-1} = 1$$

In regular arithmetic, we have $x^{-1} = \frac{1}{x}$. However, with modular arithmetic, fractions no longer have meaning (remember, when dealing with numbers $\text{mod } m$, the only numbers that exist are $\{0, 1, 2, 3, ..., m-1\}$... there are no fractions in this list). **Now what?**

Modular Inverses

We say y is the modular inverse of x in $\mathrm{mod}\ m$ if

$$x \cdot y \equiv 1 \pmod{m}$$

This inverse may not necessarily exist, as we will see shortly.

For example: The inverse of 3 in $\mathrm{mod}\ 5$ is 2, because:

$$3 \cdot 2 \equiv 6 \equiv 1 \pmod{5}$$

However, the inverse of 10 in $\mathrm{mod}\ 12$ doesn't exist, because there is no solution to

$$10x \equiv 1 \pmod{12}$$

The problem of finding the inverse of a in $\bmod m$ reduces to finding integers x, y that satisfy the equation

$$ax + my = 1$$

This equation states that the product ax is 1 away from some multiple of y.
If we were to take "$\bmod m$" on both sides, we would end up with $ax \equiv 1 \pmod{m}$.
Here, x represents the inverse of a.

e.g. Inverse of 3 in $\bmod 5$:

$$3x + 5y = 1$$

$$3(2) + 5(-1) = 1 \Rightarrow 3^{-1} \equiv 2 \pmod{5}$$

How can we find x, y? For small numbers, Guess and Check. In general – extended Euclidean algorithm.

Inverse of 10 in $\mod 12$:

$$10x + 12y = 1$$

But, since 10 and 12 share factors:

$$5x + 6y = \frac{1}{2}$$

We want integer solutions for x, y. However, this equation implies that the sum of two integers is a fraction! Not possible.

Takeaway: The inverse of a in $\mod m$ exists **iff** $\gcd(a, m) = 1$.

Goal: Find integer solutions to $ax + my = 1$.

Euclid's GCD Algorithm:

```
def gcd(a, b):
        if b == 0:
                return a
    return gcd(b, a % b)
```

How can we use this to find x, y?