Z. Abel, B. Chapman, E. Demaine
revised Tuesday 12th March, 2024

Lecture 09: Modular Arithmetic

1 Quick Followup from Last Week

Proposition 1. *For all integers a and b, the common divisors of a and b are precisely the common divisors of a and $b-a$.*

Proof. Suppose d is a common divisor of a and b. Let x, y be integers such that $dx = a$ and $dy = b$. Then $d(y-x) = b-a$, so d is also a common divisor of a and $b-a$.
Conversely, suppose d is a common divisor of a and $b-a$. Let x, y be integers such that $dx = a$ and $dz = b-a$. Then $d(x+z) = b$, so d is also a common divisor of a and b. □

Theorem 2 (Bezout's Identity + The Pulverizer)**.** *For any integers a, b, there exist integers s, t such that $\gcd(a,b) = as + bt$. We can compute s, t from a, b using the Pulverizer.*

Corollary 3. *A number can be written as an i.l.c. of a, b IFF it is a multiple of $\gcd(a,b)$.*

Proof. Let $g = \gcd(a,b)$. Every ilc of a, b is divisible by g. Conversely, we know $g = sa + tb$ for some s, t by Bezout, so every multiple of g (say kg) can be written as $(ks)a + (kt)b$ and is therefore an ilc of a, b. □

2 Towards Modular Arithmetic

- What is even+odd? (odd)
- What is the last digit of 357×994? (8, b/c $7 \times 4 = 28$)
- It is curently 3pm. What time will it be in 49 hours? (4pm, b/c 49h is 1h more than 2 full days)
- Today is Tuesday. What day of the week will it be in 10 days? (Friday, b/c 10 days is 3 more than a week.)
- What day of the week will it be 100 days from now? What computation do you need to do? ($\text{rem}(100, 2) = 2$, so Tues+2=Thurs)

These are all familiar examples of Modular Arithmetic. When working modulo n, the theme is "ignore multiples of n, just focus on remainders".

Even/Odd: remainder when dividing by 2. Weekday: remainder when dividing by 7. Last digit: remainder when dividing by 10. Hour: remainder when dividing by 12 or 24 (if we care about am/pm).

Often called clock arithmetic, because we're familiar with ignoring multiples of 12 or 24 when telling time.

Definition 1. *We say $a \equiv_n b$ (pronounced "a is congruent to b mod n") IFF $n \mid a - b$.*

Note: more standard notation for $a \equiv_n b$ is $a \equiv b \bmod n$ or $a \equiv b \pmod{n}$. However, this notation can invite confusion (explained later), so we suggest sticking to the $a \equiv_n b$ notation until you are familiar with modular arithmetic.

We'd like to consider a and b "the same" when their difference is a multiple of n.

For example, there are only 5 different "values" when looking mod 5:

$$
\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}
$$

For a general number k, which group will it belong to? Just look at $k \operatorname{rem} 5$. If we write $k = 5q + r$, then $k \equiv_5 r$, because $k - r = 5q$.

Recall the Division Theorem:

Theorem 4. *For all pairs of integers n, d with $d > 0$, there exists a* unique *pair of integers q, r where $n = qd + r$ and $0 \le r < d$. The number $q = n \operatorname{div} d$ is the* quotient*, and $r = n \operatorname{rem} d$ is the* remainder*.*

When working mod n, a number k is always congruent to its remainder (sometimes called its *residue*): if $k = nq + r$, then $n \mid nq = k - r$, so $k \equiv_n r$. Claim: the n remainders $0, 1, \ldots, n-1$ represent all the possible "groupings" (called *residue classes* or *equivalence classes*) mod n.

Theorem 5. *$a \equiv_n b$ if and only if $(a \operatorname{rem} n) = (b \operatorname{rem} n)$.*

Proof. If $(a \operatorname{rem} n) = (b \operatorname{rem} n) = r$ then $a = nq + r$ and $b = nq' + r$ for some q, q'. So $a - b = n(q - q')$ which is a multiple of n, so $a \equiv_n b$.

Conversely, suppose $a \equiv_n b$, so $a - b = nk$ for some k. Write $b = qn + r$ where $0 \le r \le n - 1$, so $r = (b \operatorname{rem} n)$. Then $a = b + nk = (k + q)n + r$. Since $0 \le r \le n - 1$, $k + q$ and r are the unique values guaranteed by the Division Theorem, i.e., r also equals $a \operatorname{rem} n$. □

So the n different remainders when dividing by n divide $\mathbb{N}$ into n different groups, identified by their remainders. Can think of $0, 1, \ldots, n-1$ as the only possible values mod n, and all other numbers are congruent to one of these.

3 Interlude: Confusing Notation

3.1 Remainder

Remainder can be notated as $a \operatorname{rem} n$ aka $\operatorname{rem}(a, n)$ aka $a \bmod n$. Recall that n is always positive, but a can be pos or neg.

Many languages have the modulo operator $a\%n$ which generally behaves like our rem, but not always!! By our def, $a \operatorname{rem} n$ is always nonnegative, even when a is negative: $(-43\%10) = 7$. Python and Mathematica agree with us. But many *other* languages think negative a values should have negative remainders: $(-43\%10) = -3$. Javascript and C/C++, for example. And some have both, with two different names, e.g., CoffeeScript (% vs %%), Lisp (mod vs rem), Fortran (mod vs modulo), Haskell (mod vs rem).

For this class, any version of remainder we use will always mean the *nonnegative* one.

Similarly, $a//n$ is commonly used programming notation for integer division, but languages disagree on which way to round. We always round *down*.

3.2 Two meanings for mod

Confusing notation: $a \bmod n$ is commonly used for $\operatorname{rem}(a, n)$. Confusing! What does $a = b \bmod n$ mean? Does it mean $a \equiv b \bmod n$? Or does it mean $a = (b \bmod n)$, i.e., $a = b \operatorname{rem} n$?

Difference: $a \bmod n$ is a function, with a single definite value, namely $a \operatorname{rem} n$. Always between 0 and $n - 1$.

But $a \equiv b \bmod n$ is a relationship between two quantities. Neither needs to be between 0 and $n - 1$. E.g., $12 \equiv 17 \bmod 5$ is a true statement. Their remainders are $(12 \bmod 10) = 2$ and $(17 \bmod 5) = 2$.

4 Putting the Arithmetic in Modular Arithmetic

The simple statement even+odd=odd says something profound: "no matter which even number and odd number we add, the result is always odd". This generalizes: "if we pick *any* number $a \equiv_5 3$ and *any* number $b \equiv_5 4$, adding them will always produce a number $a + b \equiv_5 7$. (Could also write this as $a + b \equiv_5 2$.)

Theorem 6. *If $a \equiv_n b$, then for any c,*

1. $a + c \equiv_n b + c$,
2. $ac \equiv_n bc$,
3. $a - c \equiv b - c$, *and*
4. $c - a \equiv c - b$.

Proof. By definition of $\equiv_n$, $n \mid a - b$.

1. $(a+c)-(b+c) = a-b$, so $n \mid (a+c)-(b+c)$. Therefore, $a+c \equiv_n b+c$.
2. $ac - bc = (a-b)c$, a multiple of $a-b$, so $n \mid ac-bc$. Therefore, $ac \equiv_n bc$.
3. $(a-c)-(b-c) = a-b$, so $n \mid (a-c)-(b-c)$. Therefore, $a-c \equiv_n b-c$.
4. $(c-a)-(c-b) = b-a$, a multiple of $a-b$, so $n \mid b-a$. Therefore, $c-a \equiv_n c-b$.

□

When adding or multiplying or subtracting, can replace a by anything it is congruent to mod n, without changing the result mod n.

True for the **base** of exponents as well:

Theorem 7. *If $x \equiv_n y$, then for any $k \geq 1$, $x^k \equiv_n y^k$.*

Proof. This is just repeated multiplication, so we proceed by induction on k.

- IH: $P(k) := x^k \equiv_n y^k$
- Base case ($k = 1$): this is the theorem assumption.
- IS: Assume that $x^{k-1} \equiv_n y^{k-1}$. Then

$$\begin{aligned} x^k &\equiv_n x^{k-1} \cdot x \\ &\equiv_n y^{k-1} \cdot x && \text{(previous theorem, taking } a = x^{k-1}, b = y^{k-1}, \text{ and } c = x) \\ &\equiv_n x \cdot y^{k-1} && \text{(commutativity)} \\ &\equiv_n y \cdot y^{k-1} && \text{(previous theorem, taking } a = x, b = y, \text{ and } c = y^{k-1}) \\ &\equiv_n y^k \end{aligned}$$

- By induction, for all $k \geq 1$, $x^k \equiv_n y^k$.

□

Warning: The same is *not* true for the exponent k. E.g., $1 \equiv_5 6$, but $2^1 \not\equiv_5 2^6$ (they have remainders 2 and 4, respectively).

Let's see an example: What are the last two digits of

$$x := 11335^{11111}(6 + 7799^{5000})?$$

That's the same as asking for $x \operatorname{rem} 100$.

General strategy: replace intermediate calculations with their remainders, as early and often as we can. This helps us work with smaller numbers.

First of all,

$$x \equiv_{100} 35^{11111}(6 + 99^{5000}).$$

(Not allowed to just reduce the exponents mod 100.) For the right exponent, $99 \equiv_{100} -1$, so $99^{5000} \equiv_{100} (-1)^{5000} \equiv_{100} 1$. For the left term, look for a pattern:

$$\begin{aligned} 35^1 &\equiv_{100} 35 \\ 35^2 &\equiv_{100} 25 \\ 35^3 &\equiv_{100} 25 \cdot 35 \equiv_{100} 75 \\ 35^4 &\equiv_{100} 75 \cdot 35 \equiv_{100} 25. \end{aligned}$$

Will continue bouncing between 25 and 75. So $35^{11111} \equiv_{100} 75$. We find $x \equiv_{100} 75 \cdot (6+1) \equiv_{100} 25$, so this must be the remainder.

5 Division

Addition, Subtraction, Multiplication, and *bases* of exponents can be substituted mod n (but not the exponents).

Can we divide mod n? Suppose $3x \equiv_6 3$. Can we "divide both sides by 3" and conclude that $x \equiv_6 1$? No. (Consider e.g.: $3 \times 5 \equiv_6 3$.)

A *multiplicative inverse* of x, denoted x^{-1}, is a number you can multiply x by to get 1. In $\mathbb{R}$, the multiplicative inverse of 3 is $3^{-1} = 1/3$, because $3 \cdot 1/3 = 1$. If "1/3" made sense mod 6, then we could multiply both sides by 1/3 to conclude that $5 \equiv_6 1$. So 3 doesn't have a multiplicative inverse mod 6.

When do mod n inverses exist for a number a?

Theorem 8. *a has an inverse mod n IFF* $\gcd(a, n) = 1$.

Proof. a has an inverse mod n IFF exists b such that $ab \equiv_n 1$ IFF exists b and q such that $ab - 1 = nq$ (i.e. $ab - nq = 1$) IFF 1 is a linear combination of a and n IFF $\gcd(a, n) = 1$. □

Corollary 9. *If p is prime and $a \not\equiv_p 0$, then a has an inverse mod p.*

Proof. $\gcd(a, p)$ must be p (if $p \mid a$) or 1 (only other factor of p). Now apply previous result. □

Having a multiplicative inverse means we "can cancel from both sides" or "divide" by that amount. E.g., 7 and 13 are inverses of each other mod 30. If we know $7x \equiv_{30} 14$ can we conclude that $x \equiv 2 \bmod 30$? Instead of dividing, let's multiply both sides by 13:

$$\begin{aligned} 7x &\equiv_{30} 14 \\ 13 \cdot 7x &\equiv_{30} 13 \cdot 14 \\ 91x &\equiv_{30} 182 \\ x &\equiv_{30} 2 \end{aligned}$$

So yes, since 7 has a multiplicative inverse, we can "cancel it from both sides".

What about $7x \equiv_{30} 12$? This time, we cannot "cancel" in the usual way, but we can still multiply by 13:

$$\begin{aligned} 7x &\equiv_{30} 12 \\ 13 \cdot 7x &\equiv_{30} 13 \cdot 12 \\ 91x &\equiv_{30} 156 \\ x &\equiv_{30} 6 \end{aligned}$$

Important fact:

Theorem 10 (Fermat's Little Theorem)**.** *If p is prime and $a \not\equiv_p 0$, then $a^{p-1} \equiv_p 1$.*

(Not to be confused with Fermat's **Last** Theorem. Very different, much harder.)

Proof. Idea: look at numbers $a, 2a, 3a, \ldots, (p-1)a$. Claim this is the same as $1, 2, 3, \ldots, (p-1)$ mod p, possibly in jumbled order. E.g., $p = 7$, $a = 3$, $3, 6, 9, 12, 15, 18 \equiv_7 3, 6, 2, 5, 1, 4$.

None are 0 mod p, so there are only $p-1$ possible remainders. Enough to show there are no duplicates. $ai \equiv_p aj$ implies $i \equiv_p j$, because a has a multiplicative inverse mod p! No two of the numbers $1, 2, \ldots, p-1$ are equiv mod p, so no duplicates.

Now, since both sets are same mod p, their product is congruent mod p:

$$(p-1)! \cdot a^{p-1} \equiv_p (p-1)!.$$

And since $\gcd((p-1)!, p) = 1$, we know $(p-1)!$ has an inverse mod p, so we can cancel it: $a^{p-1} \equiv_p 1$. Hooray! □

We saw earlier that we cannot reduce exponents mod n when doing arithmetic mod n. However, if n is prime, FLT gives us a way to reduce exponents anyway; we reduce mod $n-1$ instead of mod n.

6 Some Simple Applications of Modular Arithmetic

Theorem 11. *A number is divisible by 9 IFF its sum of digits is divisible by 9.*

Proof. Say $n = \sum_{i=0}^{k} d_i 10^i$. Note that $10^i \equiv_9 1^i \equiv_9 1$, so $\sum_{i=0}^{k} d_i 10^i \equiv_9 \sum_{i=0}^{k} d_i \cdot 1$.

We get a stronger result! $\mathrm{rem}(n, 9) = \mathrm{rem}(s(n), 9)$. The divisibility trick is just checking whether both sides are 0. □

Another application: ISBN numbers, $(a_1, \ldots, a_{10})$. Can think of the first 9 digits as the actual number, while the 10th digit is a checksum, where $a_1 + 2a_2 + 3a_3 + \cdots + 10a_{10} \equiv_{11} 0$. Given first 9 digits, how do we know a 10th digit exists? Because 10 has a multiplicative inverse mod 11. (Note however, that if this last digit should be 10, then the number is not a valid ISBN.)

Can prove that if a single digit gets copied wrong, the check won't come out to 0 mod 11. Similarly, if two adjacent unequal digits are swapped, check won't come out to 0 mod 11.

Similar ideas are used in other error-correcting scenarios, e.g., redundant memory storage, RAID. A simple hypothetical strategy: have first two disks store bits b_1 and b_2, while the third disk stores $b_3 := (b_1 \oplus b_2)$. If 2nd disk fails, can recover b_2 as $b_1 \oplus b_3$. ($\oplus$ denotes addition mod 2, or parity.)