Lecture 6: Primality and Modular Arithmetic

http://book.imt-decal.org, Ch. 3 (in progress)

Introduction to Mathematical Thinking

October 15th, 2018

Suraj Rampure

Announcements

- Lecture is on Monday this week; Wednesday will be taking up the midterm
- Midterm solutions will be posted by then, midterm grades by the weekend
- Homework 6 out by Wednesday, due a week from today

Today: Introduction to Number Theory. Formalizing a lot of concepts we've seen over the past few weeks, and also introducing Modular Arithmetic. Textbook section isn't quite ready yet, but the slides are pretty comprehensive.

$x = 3k + 0$

$x = 3k + 1$

$x = 3k + 2$

Division Algorithm

If n, d are positive integers such that $n \geq d$, then it is possible to find non-negative integers q, r such that $n = dq + r$, where $r < d$. If $r = 0$, we can say $d|n$.

n: dividend

d: divisor

q: quotient

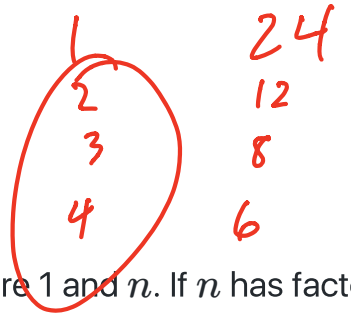
r: remainder

Divide 25 by 7

I get 3, R 4

$25 = 7 \cdot 3 + 4$

24



Primality

We say an integer $n > 1$ is **prime** if its only factors are 1 and n. If n has factors other than 1 and itself, then we say it is **composite**. The number 1 is neither prime nor composite.

- As we saw in HW 5: there are infinitely many primes (no largest, but the smallest is 2)
- To check if n is prime: we could check every integer from 2 to $n - 1$... any easier way?

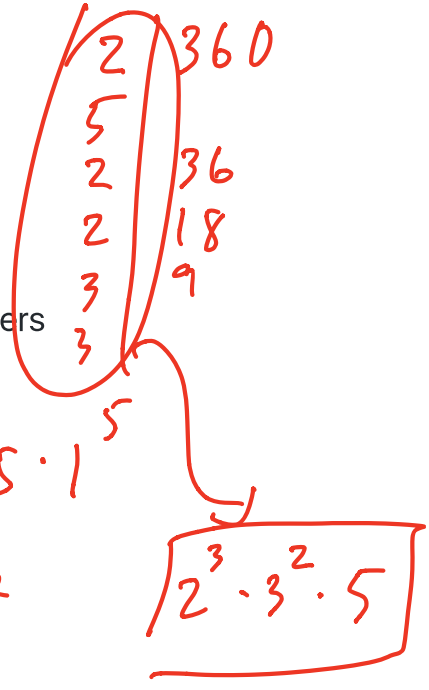
Sieve of Erathosenes

could also just check until $\lfloor \sqrt{n} \rfloor$

Fundamental Theorem of Arithmetic

The fundamental theorem of arithmetic says two things:

1. Any integer greater than 1 can be written as a product of prime numbers
2. This prime factorization is unique



$5 \cdot 1^2$ $5 \cdot 1^3$ $5 \cdot 1^4$ $5 \cdot 1^5$

→ we don't count 1 to be prime

Example: What is the smallest number whose digits multiply to 10,000?

$10^4 = 2^4 \cdot 5^4$

$\frac{20}{2^2 \cdot 5}$

225
45

22225555
44555
285555
255558

GCDs and LCMs

Recall, $\gcd(a, b)$ refers to the greatest common divisor between a, b and $\text{lcm}(a, b)$ refers to the lowest common multiple between a, b.

Suppose we have $a = p_1^{c_1} \cdot p_2^{c_2} \cdot \ldots \cdot p_n^{c_n}$ and $b = p_1^{d_1} \cdot p_2^{d_2} \cdot \ldots \cdot p_n^{d_n}$. Then:

$$\gcd(a, b) = p_1^{min(c_1,d_1)} \cdot p_2^{min(c_2,d_2)} \cdot \ldots \cdot p_n^{min(c_n,d_n)}$$

$$\text{lcm}(a, b) = p_1^{max(c_1,d_1)} \cdot p_2^{max(c_2,d_2)} \cdot \ldots \cdot p_n^{max(c_n,d_n)}$$

For example: $a = 1200 = 2^4 \cdot 3 \cdot 5^2$ and $b = 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

$$\gcd(1200, 2520) = 2^{min(4,3)} \cdot 3^{min(1,2)} \cdot 5^{min(2,1)} \cdot 7^{min(0,1)} = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 120$$

$$\text{lcm}(1200, 2520) = 2^{max(4,3)} \cdot 3^{max(1,2)} \cdot 5^{max(2,1)} \cdot 7^{max(0,1)} = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 25200$$

Introduction to Modular Arithmetic

Suppose the clock reads 5, and you want to know the time in 13 hours. You wouldn't say 18, you would say 6. When we deal with a clock, the only numbers we care about are $\{0, 1, 2, 3, 4, ...11\}$.

all possible remainders when dividing by 12

Formally, we say $a \pmod m$ is the remainder when a is divided by m. i.e. if $a = dq + r$, then $a \pmod d \equiv r$.

equivalent

$b - a = km$

Another definition:

$$a \equiv b \pmod m \Rightarrow m \mid a - b \Rightarrow b = a + km, k \in \mathbb{Z}$$

$a \equiv b \pmod m$ reads "a and b are equivalent, modulo m." This also means they have the same remainder when divided by m.

mod 5 : {0, 1, 2, 3, 4}

When dealing with numbers $\mod m$, the set of all integers can be reduced to one of the numbers $\{0, 1, 2, ..., m-1\}$.

Suppose we have the number $a \mod m$. The following are all equivalent to a in modulo m:

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

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

all have rem. 3 when divided by 5

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

- This implies that negative integers also have equivalences in modular arithmetic, e.g. $-12 \equiv 3 \pmod 5$
- It is always true that $n + k \equiv k \pmod n$; we will use this often in simplifying arithmetic

$a + mK \pmod m \equiv a \mod m$

Attendance

https://tinyurl.com/larriors

$\ldots, -7, -2, 3, 8, 13, 18, 23, 28, \ldots$

Arithmetic Operations in $\mod m$

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

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

$m \mid a-b \rightarrow m \mid b-a$

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

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

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

Proof of the first rule:

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $b = a + mk_1$ and $d = c + mk_2$. $b-a = mk_1$ $k_1, k_2 \in \mathbb{Z}$

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

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

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

Proof of the second rule: On HW 6!

Key takeaway: We can make simplifications as we go.

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

Exponentiation

$15 = 3 \cdot 5$

$\ldots, -10, -1, 8, 17, 26, \ldots$

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.

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

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

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

$11 = 2 \cdot 5 + 1$

Other examples:

$$5^{11} \pmod{26} \equiv (5^2)^5 \cdot 5 \equiv (-1)^5 \cdot 5 \equiv -5 \pmod{26} \equiv 21 \pmod{26}$$

$$23^9 \pmod{24} \equiv (-1)^9 \equiv -1 \equiv 23 \pmod{24}$$

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 $4^{16} \cdot 4^8 \cdot 4^2$.

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

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

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

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

Combining these results:

$$4^{26} \equiv 4^{16} \cdot 4^8 \cdot 4^2 \equiv 3 \cdot 4 \cdot 3 \equiv 12 \cdot 3 \equiv (-1) \cdot 3 \equiv -3 \pmod{13}$$

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

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 $c \in \mathbb{N}$.

$11^k = 5c + 6$

Induction Step:

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

some integer

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

Now:

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

Division in Modular Arithmetic

$A^{-1}Ax = A^{-1}b$

$x = A^{-1}b$

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":

$$3x = 14$$

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

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 $\mod m$, 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 $\mod m$ if

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

$3x \equiv 1 \mod 5$

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

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

$3^{-1} \equiv 2 \mod 5$

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

$2^{-1} \equiv 3 \mod 5$

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

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

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

$x \equiv a^{-1} \mod m$

$$ax + my = 1$$

This equation states that the product ax is 1 away from some multiple of y.
If we were to take "$\mod m$" 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 $\mod 5$:

$3(-3) + 5(2) = 1$

$3^{-1} \equiv -3 \equiv 2 \mod 5$

$$3x + 5y = 1$$

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

How can we find x, y? For small numbers, Guess and Check. In general – Euclid's Extended GCD Algorithm (will get practice with this on HW).

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** $\gcd(a, m) = 1$. More formal proof of this in the homework.

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?

Will explore more on homework, and discussion next week.