COMPSCI 250:Introduction to Computation

Lecture #12: Divisibility and Primes
David Mix Barrington and Ghazaleh Parvini
2 October 2023

Divisibility and Primes

- Introduction to Number Theory
- An Application: Hashing With Open Addressing
- Do Incredibly Large Naturals Even Exist?
- Primes and Prime Factorization
- The Sieve of Eratosthenes
- Congruences and Congruence Classes

The Hasse Diagram Theorem

- The **Hasse Diagram Theorem** says that any finite partial order is the “path-below” relation of some Hasse diagram, and the “path-below” relation of any Hasse diagram is a partial order.
- The second of these two statements is easy to prove -- we just have to check that the path-below relation is reflexive, antisymmetric, and transitive.
- The text proves the first statement -- we’ll prove it later using mathematical induction.

Idea of the Proof

- Suppose we have a partial order on a finite set X. We'll outline a way to draw a Hasse diagram for X.
- We first show that X must have a **minimal element**, which is some element a such that $\forall b: R(b, a) \rightarrow (a = b)$ is true.
- Then we recursively make a Hasse diagram for the partial order we get by removing a from X.

Idea of the Proof

- This recursion is grounded (as we recall from COMPSCI 187) because the recursive call is always to a smaller set.
- The base case is when the set is empty.
- Given the Hasse diagram for $X \setminus \{a\}$, we add a point for element a back in at the bottom.
- We draw new lines up from a to any element b such that no element c satisfies R(a, c) and R(c, b) except for c = a or c = b.

Introduction to Number Theory

- We've defined the **natural numbers** to be the non-negative integers {0, 1, 2, 3,...}. **Number theory** is the branch of mathematics that deals with the naturals.
- We'll define properties of the naturals using quantifiers, starting from basic predicates like $x = y$, $x \leq y$, $x + y = z$, and $x \cdot y = z$. We will give *definitions* of the naturals and these predicates and prove the properties from them.

Introduction to Number Theory

- Because **counting** is a fundamental human activity, and the naturals are an abstraction of counting, number theory has a long history.
- We'll see results originally proved in ancient Greece and in medieval China. But there are easily stated questions in number theory to which no one knows the answer.
- Remember that naturals, and integers in general, are different from `int`s.

Application: Hashing

- In data structures courses we studied **hashing**, where a large address space is mapped into a smaller space called a **hash table**.
- The mapping from address space to hash table cannot be one-to-one, and we have a problem if it fails to be one-to-one on the address values that we actually use.
- A **collision** is when two relevant addresses are mapped to the same hash address.

Application: Hashing

- One way of computing a hash address is to divide the original address by the size s of the hash table and let the remainder, in the range from 0 to s - 1, be the hash address.

- One way to deal with collisions, called **open addressing**, has us look at new hash addresses if the first hash address h is full -- we look at h + k, h + 2k, h + 3k,... until we find an empty space in the table.

- If k = 1, we will find an open space if one exists. What about for other values of k?

Incredibly Large Naturals

- Some questions of number theory involve ridiculously large naturals. For example, the **Goldbach Conjecture** says that every even natural greater than 2 is the sum of two prime numbers.

- It is known that if this fails, it fails on a very large number (greater than 10^{18} according to Wikipedia). One paper in theoretical computer science treats all input sizes up to $\exp^*(20)$ (a tower of twenty two-to-the operations) as a special case.

Incredibly Large Naturals

- If naturals exist in order to count sets, what about naturals that are too big to denote any set of material objects in the universe?
  Or numbers so big that no computer could ever name them?

- We say in mathematics that given any property of naturals, either a natural with that property exists or it doesn’t.
  This is something of an article of faith.

Provability in Number Theory

- Logicians have shown that given any proof system for number theory, one of two things must happen. (This is **Gödel's Theorem**.)
- Either the system is able to prove false statements (it is **unsound**), or there are statements that are *true, but not provable in the system* (it is **incomplete**).
- There is some question about what it means for an unprovable statement to be true.

Prime Numbers

- We'll begin now with the foundations of number theory. The first concept, of one natural **dividing** another, was in our last lecture. We defined the division relation D so that $D(x, y)$ means $\exists z: x \cdot z = y$.

- A **prime number** is a natural, greater than 1, that is divided *only by itself and 1*.
  In symbols, we say
  $P(x) \leftrightarrow (x > 1) \land \forall y: D(y, x) \rightarrow (y = 1 \lor y = x)$.

Composite Numbers

- Numbers greater than 1 that are not prime are called **composite**.
  A composite x can be written as $y \cdot z$ where both y and z are greater than 1.
- By convention, we say that 0 and 1 are neither prime nor composite.
- A composite number can be **factored**, and its factors can also be factored if they are composite.

Clicker Question #1

- Which of the following statements *is not* true?
- (a) Every natural ending in 5, in decimal notation, is composite.
- (b) No prime number is a perfect square.
- (c) If n is any natural with $n > 5$, $n^2 - 5n + 6$ is composite.
- (d) There exists exactly one set of three consecutive odd numbers that are prime.

Not the Answer

Clicker Answer #1

- Which of the following statements *is not* true?
- (a) Every natural ending in 5, in decimal notation, is composite. 5 itself is prime!
- (b) No prime number is a perfect square. factors as x times x, $1 = 1^2$ is not prime
- (c) If n is any natural with $n > 5$, $n^2 - 5n + 6$ is composite. factors as $(n-2)(n-3)$
- (d) There exists exactly one set of three consecutive odd numbers that are prime. 3, 5, 7

Prime Factorizations

- If we keep factoring the factors of our original composite number as long as we can, we reach a point where all our factors are prime.

- For example, $504 = 2\cdot252 = 2\cdot6\cdot42 = 2\cdot6\cdot2\cdot21 = 2\cdot2\cdot3\cdot2\cdot7\cdot3$.

- Or we could have made other choices: $504 = 126\cdot4 = 63\cdot2\cdot4 = 9\cdot7\cdot2\cdot4 = 3\cdot3\cdot7\cdot2\cdot4 = 3\cdot3\cdot7\cdot2\cdot2\cdot2$. We have the same prime factors (and the same number of each) in a different order.

Prime Factorizations

- We can be a bit more systematic about factoring by first taking out 2’s until the number is odd, then taking out as many 3’s as we can, then as many 5’s, and so on.
- This can be coded as either an iterative or a recursive algorithm.
- Doing this by hand means lots of tests for divisibility, which can be aided by tricks that are described in Excursion 3.2 of the text.

Clicker Question #2

- Factor the number 2100 completely. How many factors do you get, and how many *different* factors? (For example 20 = 2·2·5 has three factors, and two different factors.)
- (a) six factors, four different factors
- (b) seven factors, three different factors
- (c) seven factors, four different factors
- (d) nine factors, four different factors

Not the Answer

Clicker Answer #2

- Factor the number 2100 completely. How many factors do you get, and how many *different* factors? (For example 20 = 2·2·5 has three factors, and two different factors.)
- (a) six factors, four different factors
  2·2·3·5·5·7
- (b) seven factors, three different factors
- (c) seven factors, four different factors
- (d) nine factors, four different factors

Primality Testing

- If we are trying to factor x, and we fail to find any number between 1 and x that divides x, we have shown that x is prime.

- This is the **trial division** method to test for primality. We can improve its efficiency by only testing trial divisors up to the **square root** of x. (Why is this all right?)

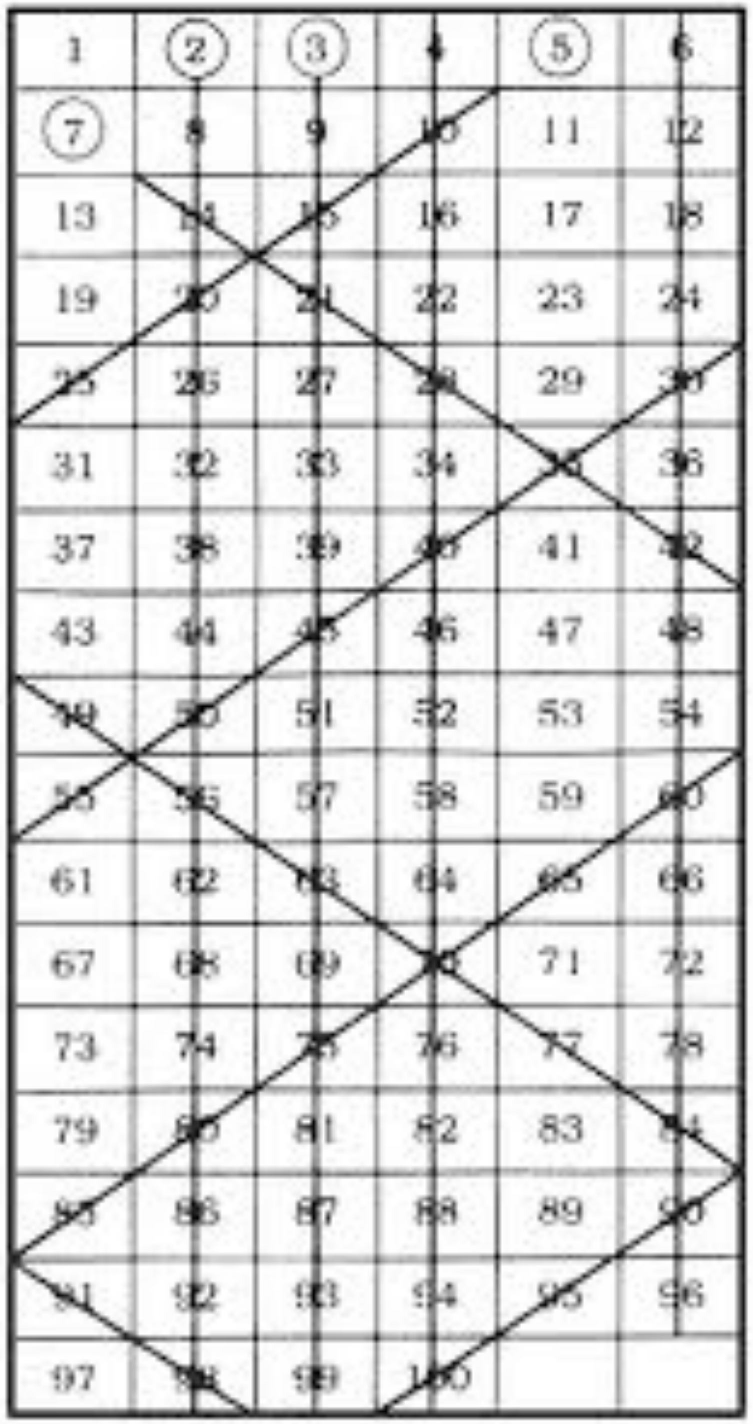
- Testing a 100-digit number this way would be horrible even with a computer, as the square root of a 100-digit number has about 50 digits.

Primality Testing

- Is there a better way to test whether a large number is prime?
- In practice, we do this with a **randomized algorithm**. There is a property of numbers a < n that *no* a’s have if n is prime, and *most* a’s have if n is composite. We try many random a’s, and either prove n to be composite or build up confidence that n is prime.
- There’s a practical algorithm that gets a guaranteed answer, but it is slower than the randomized test.

The Sieve of Eratosthenes

- The ancient Greeks developed a system to simultaneously test all the numbers in a given range for primality.
- The picture lists all the numbers from 1 through 100.

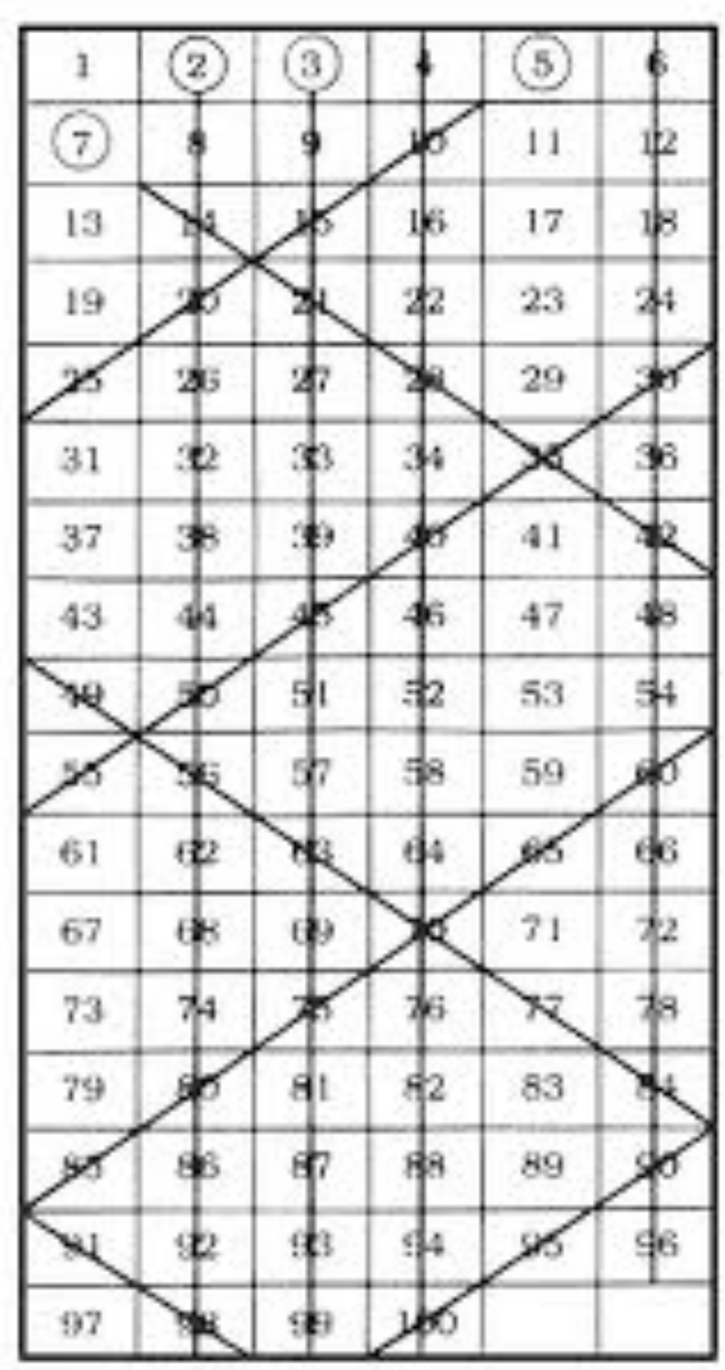


1	2	3	~~4~~	5	~~6~~
7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~
19	~~20~~	~~21~~	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~
43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	~~50~~	~~51~~	~~52~~	53	~~54~~
~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~
67	~~68~~	~~69~~	~~70~~	71	~~72~~
73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~
79	~~80~~	~~81~~	~~82~~	83	~~84~~
~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~
97	~~98~~	~~99~~	~~100~~		

Image from Ivars Peterson, *The Mathematical Tourist*

The Sieve of Eratosthenes

- We identify 2 as prime and cross out all its multiples. We do the same for 3, 5 and 7. The next prime, 11, is bigger than the square root of 100, so we don't need to check it.
- 25 of these 100 naturals are prime. They get rarer as we go on.
- Note that after 2 and 3, every prime is one more or one less than a multiple of 6.



1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100		

Image from Ivars Peterson, *The Mathematical Tourist*

Congruences and Classes

- We have one more major definition in number theory. Recall that the parity relation P, where P(x, y) means that x and y are both odd or both even, is an equivalence relation.

- We can write this using the Java % operation, in which x % y is the remainder when x is divided by y.
  P(x, y) is true if and only if x % 2 == y % 2.
  Equivalently, P(x, y) is true if 2 divides x - y (or else y - x, whichever is a natural).

Congruences and Classes

- If P(x, y) is true we also say that x and y are **congruent modulo 2**.
- In general x and y are **congruent modulo k** if x % k == y % k, or equivalently if k divides x - y or y - x. For example, 3 and 17 are congruent modulo 7.
- For another example, two naturals are congruent modulo 10 if and only if they have the same last digit.

Clicker Question #3

- Which of the following statements *is true*?
- (a) No two of 2^1, 2^2, 2^3, and 2^4 are congruent to one another modulo 5.
- (b) 23 and 45 are congruent, modulo 7.
- (c) If a natural is congruent to 3, modulo 9, then it is composite.
- (d) If p and q are distinct primes, then p could be congruent to 0 modulo q.

Not the Answer

Clicker Answer #3

- Which of the following statements *is true*?
- (a) No two of 2^1, 2^2, 2^3, and 2^4 are congruent to one another modulo 5. 2(2), 4(4), 8(3), 16(1)
- (b) 23 and 45 are congruent, modulo 7. 23%7 == 2, 45%7 == 3
- (c) If a natural is congruent to 3, modulo 9, then it is composite. 3 is prime with this property
- (d) If p and q are distinct primes, then p could be congruent to 0 modulo q. Can't be a multiple

Congruence Classes

- Remember that any **equivalence relation** on a set A divides A into **equivalence classes**, where the class [a] of an element a is the set {b: R(a, b)}.
- Congruence modulo k is an equivalence relation, and we refer to the equivalence classes of this relation as the **congruence classes modulo k**.

Congruence Classes

- For example, the two congruence classes of the parity relation P are the set of even numbers and the set of odd numbers.

- [0] = [114] = {0, 2, 4, 6,…} and [1] = [9843] = {1, 3, 5, 7,…}, for congruence modulo 2.

- Periodic processes in the real world or in computing can be modeled with the system of **modular arithmetic** we will begin studying in our next lecture.

Congruence Classes Mod 4

- Similarly the equivalence relation of congruence mod 4 divides **N** into four equivalence classes:

0,4,8,12,16,20,…
1,5,9,13,17,21,…
2,6,10,14,18,22,…
3,7,11,15,19,23,…

- As we'll see next lecture, the class of the product of two numbers a and b depends only on the class of a and the class of b.
- For example, the product of any two numbers in the class of 3 is in the class of 1.

Congruence Classes Mod 4

0,4,8,12,16,20,…
1,5,9,13,17,21,…
2,6,10,14,18,22,…
3,7,11,15,19,23,…

- There are no prime numbers in the class of 0, and only one prime in the class of 2, 2 itself.
- In Discussion #4 (Section 3.4), we will show that there are an infinite number of primes, and then that there are an infinite number of primes in the class of 3. (There are also an infinite number in the class of 1, but this is a bit harder to prove.)