6.S096: Number Theory January 16, 2024

Lecture 1— Intro to Arithmetic

A. Anas Chentouf, M. Wacyl Meddour, Mohammed Ali Othman *Scribe:*

Mathematics is historically introduced as the study of numbers and shapes and how they intertwine with one another. In this class, we shall focus on the former and its relevance to the modern concepts of computer science.

For the first week, we shall cover some basic notions of elementary number theory [1] as well as some related concepts in computer science.

We will then re-express everything we have learned in the language of groups, before applying group theory to applications in cryptography, signal processing, and analytic number theory.

As a quick reminder of the notation and conventions that we will be using throughout the class: $\mathbb{N}$ denotes the set of natural numbers (integers ≥ 1), $\mathbb{Z}$ the set of all integers, $\mathbb{Q}$ the set of rational numbers, $\mathbb{R}$ the set of real numbers and $\mathbb{C}$ the set of complex numbers. We will also use positive to denote the property of being strictly greater than 0 [2].

1 Divisibility

Consider the natual numbers

$$1, \mathbf{2}, 3, \mathbf{4}, 5, \mathbf{6}, 7, \mathbf{8}, 9, \mathbf{10}, 11, \mathbf{12}, \ldots$$

You may recognize that bold numbers are called *even*, and the rest are *odd*. All even numbers are of the form $2k$ where k is some integer. Said number are called *multiples of* 2 and 2 is called a *divisor* of each of them. We may do a lot of reasoning about even and odd numbers, but we first generalize these concepts to the integers.

1.1 Divisors and Multiples

Definition 1.1: Divisibility

Given two integers a and b, where $a \neq 0$, we say that a *divides* b and write $a|b$ if there exists an integer k for which $b = a \cdot k$. In this case, we also say that b is a *multiple* of a.
If a does not divide b, we write $a \nmid b$.

[1] so no explicit use of abstract algebra (such as groups, rings, etc...)
[2] this comment is to distinguish from the positive definition used by some which includes 0

We can deduce many useful properties from this single definition.

Proposition 1.2

Given integers a, b, c, x, y where a is nonzero, the following relations hold:

1. $a|a$,
2. if $a|b$ then $a|bc$,
3. if $a|b$ and $a|c$ then $a|bx + cy$,
4. if $a|b$ and $b \neq 0$ then $|a| \leq |b|$.

You should try to convince yourself why these properties are true. They all follow from the basic definition of divisibility, and are powerful enough to solve some basic divisibility problems.

Example.

Find all natural numbers n for which n^2 is a multiple of $n + 2$.

Describing this in a mathematical language, this means that $n + 2|n^2$. Note that

$$\frac{n^2 - 4}{n + 2} = \frac{(n + 2)(n - 2)}{n + 2} \in \mathbb{Z},$$

and so if $n + 2$ divides n^2 if and only if

$$\frac{4}{n + 2} = \frac{-(n^2 - 4) + n^2}{n + 2} \in \mathbb{Z}.$$

This means that $n + 2$ is a divisor of 4, so we can find all possible values of n knowing that $n+2 \in \{-4, -2, -1, 1, 2, 4\}$, which gives us that $\{-6, -4, -3, -1, 0, 2\}$ are the values of n we are searching for.

1.2 Euclidean Division and the Greatest Common Divisor

We'll introduce a basic tool that has immense use in tackling questions regarding divisibility: Euclidean Division

Proposition 1.3: Euclidean Division

Let d be a positive integer. For any integer a, one can find unique integers q, r such that $0 \leq r < d$ and $a = qd + r$. In this case, q is called the *quotient* and r the *remainder* of a over d.

Proof. To prove existence, note that the ratio $\frac{a}{d}$ is enclosed between two successive integers, i.e there exists an integer q such that $q \leq \frac{a}{d} < q+1$. As such, $qd \leq a < qd+d$ and thus $0 \leq a - qd < d$. Setting $r = a - pd$, we indeed get that $a = qd + r$ with $0 \leq r < d$.

To prove uniqueness, assume that $qd + r = q'd + r'$. Then $d(q - q') = (r - r')$ and so $d|r - r'$, the difference of two integers in the interval $[0, r)$. The only this is possible is if they are both equal, and so $r = r'$ and hence $q = q'$. □

Note that d divides a if and only if the remainder r is equal to zero.

Definition 1.4

A *common divisor* of two integers a and b is an integer d such that $d|a$ and $d|b$.

Notice particularly that 1 and -1 are common divisors to every pair of integers. One can think of common divisors as a "scale" to how similar two numbers are, arithmetically speaking. Two numbers with the same common divisors are equal up to sign because of of Proposition 1.2 (iv).

Let us now talk about a special type of divisors that can be used to compare numbers : common divisors. us take a look at a natural notion that arises from the idea of common divisors.

Proposition 1.5: Greatest Common Divisor

Given two integers a and b not both 0, there exists a unique positive integer d satisfying the following conditions:
(i) d is a common divisor of a and b, i.e $d|a$ and $d|b$.
(ii) For every common divisor q of a and b we have that $q|d$.

This integer d is called the *greatest common divisor* of a and b, and is denoted by $\gcd(a, b)$.

Before proving the statement above, let us look at some examples and how the greatest common divisor can be useful. Say we want to compute the greatest common divisor of 250 and 30. Notice that if $d|250$ and $d|30$ then d must also divide the remainder when we divide 250 by 30 since it is equal to $250 - 8 \cdot 30 = 10$, and since 10 is a common divisor of 30 and 250, then $\gcd(250, 30) = 10$. What we just did is an example of the Euclidean algorithm - a systematic way of computing the

greatest common divisor of two numbers by repeated use of euclidean division.

Here is a sketched proof of why Proposition 1.5 is true. Let a and b be two integers not both 0. Notice that in the cases described above, the greatest common divisor always ended up being a result of (repeated) application of Proposition 1.2 (iii), which means that $\gcd(a, b)$ turned out to be a linear combination of a and b. This motivates us to look at possible linear combinations to extract the greatest common divisor.

Note that 1.2 (iii) implies that *any* common divisor d of a and b divides *any* linear combination of a and b. Hence if $\gcd(a, b)$ is indeed a linear combination of a and b, then it has to be the smallest positive one. This gives us another characterization of the greatest common divisor.

Proof of Proposition 1.5. Consider the set of linear combinations of a and b with integer coefficients $S = \{ax + by : x, y \in \mathbb{Z}\}$. Since a and b are not both 0, the set S contains infinitely many positive and negative elements. Let d be the smallest strictly positive element of S, and write $d = ax + by$. We claim that d satisfies the conditions of **Proposition 1.4**.

Since d is a linear combination of a and b, it's a multiple of every common divisor of a and b. So we just have to show that $d|a$ and $d|b$. Clearly, if either is 0, it's divisible by d. Now suppose that $a \neq 0$

Apply euclidean division and write $a = qd + r$ where $0 \leq r < d$ .We see that

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$$

which means that r is a linear combination of a and b, and yet it's smaller than d. By our assumption on d, this means r has to be 0 (since $r \geq 0$ and it can not be positive), so then $a = qd$ and $d|a$ as desired. By complete similarity, $d|b$ and this concludes the proof. □

As a consequence of this proof, we find ourselves with a very neat result concerning the greatest common divisor of two numbers a and b. Beyond its existence, we are also guaranteed that it's a linear combination of a and b.

Theorem 1.6: Bézout's Theorem

Given two integers a and b not both 0, there exists integers x and y such that

$$\gcd(a, b) = ax + by.$$

Moreover, $\gcd(a, b) = 1$ if and only if $ax + by = 1$ for some integers x and y.

The second part of the theorem follows from the fact that if $ax + by = 1$ then $\gcd(a, b)|1$ so it has to be 1. This result will be extensively used later on, so it's a good thing to keep it in mind!

To conclude, we look at some interesting properties of the greatest common divisor which will be useful later on.

Proposition 1.7: Properties of GCD

Given integers a, b, and c, the following properties hold:

1. $\gcd(a, 0) = |a| = \gcd(a, a)$
2. $\gcd(a, b) = \gcd(a, b - ac)$
3. If c is a common divisor of a and b, then $\gcd(a, b) = c$ if and only if $\gcd\left(\frac{a}{c}, \frac{b}{c}\right) = 1$. Particularly speaking, $\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$
4. $\gcd(ca, cb) = c\gcd(a, b)$

Proof. The first property follows from the fact that $0|a$ and $a|a$.
For the second, note that if $d|a$ and $d|b$ then $d|b - ac$. Similarly speaking, if $d|a$ and $d|b - ac$ then $d|b = (b - ac) + ac$. Thus pairs (a, b) and $(a, b - ac)$ have the same common divisors and hence the same greatest common divisors. In particular this tells that if we apply euclidean division $a = qd + r$, then $\gcd(a, d) = \gcd(d, r)$
To prove the third property, suppose $\gcd(a, b) = c$. By Bézout, there exists x, y such that $ax + by = c$, and so $\frac{a}{c}x + \frac{b}{c}y = 1$. Hence $\gcd\left(\frac{a}{c}, \frac{b}{c}\right) = 1$. The converse follows by applying the Bézout argument in the reverse direction.
For the last property, not that $c\gcd(a, b)$ divides both ca and cb, so the result follows by the previous property. □

To showcase these properties, let us consider the following example.

Example.

> Suppose that Timmy gets a haircut every 54 days, while John gets a haircut every 30 days. Knowing that today they both got a haircut, when will be the next time that this happens?
>
> Let the 0^{th} day being the first day Timmy and John met at the barber, the 1^{st} day being the day after that, and so on. Mathematically speaking, Timmy and John will get a haircut on the n^{th} day whenever $30|n$ and $54|n$, respectively. For them to get a haircut on the same day, both conditions have to be satisfied, and so we search for the least common multiple of 30 and 54. It does not take too long to convince oneself that the answer is 270 days.

Naturally though, one may wonder what happens when changing the numbers in the problem, meaning switching 54 for an arbitrary positive integer a, and 30 for another positive integer b. Is there a systematic way to find the solution?
The answer is yes, and it turns out that this number is closely related to the greatest common divisor. This means that the first day they get a haircut together is the smallest number which is both divisible by a and b.

Such a number is called the *Least Common Multiple* of a and b and is denoted by $\operatorname{lcm}(a, b)$. It shares loads of properties with the greatest common divisor, the most notable of which is that

$$\operatorname{lcm}(a, b) \gcd(a, b) = ab$$

for all integers a and b.

Proposition 1.8

For any integers a, b which are not both zero, the relation $\operatorname{lcm}(a, b) \gcd(a, b) = ab$ holds.

Proof. Note that $a \gcd(a, b)$ and $b \gcd(a, b)$ both divide ab, or alternatively, that a and b both divide $\frac{ab}{\gcd(a,b)}$. By definition, this means that $\operatorname{lcm}(a, b)|\frac{ab}{\gcd(a,b)}$. By Bézout, we may write $\gcd(a, b) = ax + by$ for some integers x, y, and so

$$\gcd(a, b) \operatorname{lcm}(a, b) = a \operatorname{lcm}(a, b)x + b \operatorname{lcm}(a, b)y.$$

Since ab divides both terms on the right hand side, it must divide the left hand side. Hence, ab and $\gcd(a, b) \operatorname{lcm}(a, b)$ are positive integers which divide each other, so they are equal. □

1.3 Euclidean Algorithm

So far, we have tackled the question of existence of the greatest common divisor as well as some of its properties. In this section, we will provide the traditional way of computing the greatest common divisor, known as the Euclidean Algorithm.

Euclidean division is the basic step in the Euclidean Algorithm, and can help us compute the greatest common divisor as follows: The greatest common divisor of two integers a and b is the *last non-zero remainder* in a chain of Euclidean Divisions generated from a and b via the Euclidean Algorithm, where each transition step applies Euclidean division $\gcd(a, b) = \gcd(b, a - qb)$.

Let us look at an example of this. Say we want to compute 1581 and 612. Applying Euclidean Division multiple times in a row, each time dividing the prior divisor by the remainder we got, we get the following:

$$\begin{aligned} 1581 &= 612 \cdot 2 + 357 \\ 612 &= 357 \cdot 1 + 255 \\ 357 &= 255 \cdot 1 + 102 \\ 255 &= 102 \cdot 2 + 51 \\ 102 &= 51 \cdot 2 + 0 \end{aligned}$$

As we can see from the example above, to pass from a line to another we divide the previous divisor by the remainder we got, and repeat until we get a zero remainder. From this, we can conclude that $\gcd(1581, 612) = 51$ since 51 is the last non-zero remainder. But why is that?

To make sense of this, we first need to confirm that this process terminates. The remainders form a strictly decreasing sequence of nonnegative integers, which means it eventually has to become zero. The last non-zero remainder is the greatest common divisor of our two initial numbers follows from Proposition 1.7 (ii). An extensive application of this property tells us the following:

$$\gcd(612, 1581) = \gcd(612, 1581 - 2 \cdot 612) = \gcd(612, 357).$$

Particularly speaking, one can see that the greatest common divisor of the divided number and the divisor (the two red numbers) is *preserved* at each line. In that

sense, we can see that:

$$\gcd(612, 1581) = \gcd(357, 612) = \gcd(255, 357) = \ldots = \gcd(102, 51).$$

Since the last remainder is 0, $51|102$ and thus $\gcd(612, 1581) = 51$, as desired.

There is nothing special about the numbers chosen here, and this algorithm works for all other positive integers. You will have a chance to code this algorithm in the upcoming pset.

2 Primes and Factorization

In the previous section, we used the tools of arithmetic (particularly divisibility) to classify numbers. An important special case with regards to divisibility, and many other arithmetic properties, arises when considering the prime numbers.

2.1 Primes and Infinity

Definition 2.1: Primes

A positive integer is said to be *prime* if it has exactly 2 positive divisors (namely 1 and itself).
Any positive integer with more than 2 positive divisors is called *composite*.

Primes are the building blocks of natural numbers, one such way is the result of the Fundamental Theorem of Arithmetic. Despite their simple definition, primes are mysterious objects that are still studied to this day. Many mathematicians devoted their lives to understanding them and finding patterns in their distribution. With the recent development of computer science, our capacity to both compute primes and prime divisors of numbers increased drastically. The largest confirmed prime known currently has 24 million digits. ♡♡♡ Anas: [cite this]

Notice particularly speaking that 1 is NOT a prime, but rather what we call a *unit*. The two units of integer are 1 and -1.

Proposition 2.2: Properties of Primes

Let p be a prime number and let n, m be positive integers.

1. The number n can be expressed as the product (possible empty) of primes.
2. If $p \nmid n$ then $\gcd(n, p) = 1$.
3. If $p|mn$ then $p|m$ or $p|n$.

Proof. We will prove the first result by induction. We can see that the statement is true for 1 (vacuously) and for 2 and 3 which are primes. Suppose that the result holds for $2, \dots n-1$. If n is not a prime then $n = ab$ where $a \geq 2$ and $b \geq 2$. Since both a and b are at least 2 but strictly less than n, they are both a product of primes, so n is indeed a product of primes. This type of reasoning is called *induction* which can be viewed as a "recursion of proofs".

For the second result, note that $\gcd(n, p)|p$ so $\gcd(n, p) = 1$ or $\gcd(n, p) = p$. In the first case $p \nmid n$ and in the second case $p \mid n$ and vice-versa.

Finally, assume that $p \nmid m$. Then by the previous result $\gcd(p, m) = 1$, and so by Bézout there exist x, y such that $px + my = 1$. Multiplying by n we get that $npx + nym = n$. Since $p|mn$ and $p|p$ then p divides the left hand side, so it also divides the right hand side. Hence $p|n$, as desired. □ □

As a conclusion of the proposition above, we get that every positive integer greater than 1 has at least one prime divisor. This fact can help us prove a rather interesting yet quite antique result on prime numbers.

Theorem 2.3: Euclid

There exists infinitely many prime numbers.

Proof. Suppose otherwise, and let $p_1 < p_2, < p_n$ denote the set of all prime numbers. Consider the number $N = p_1 p_2 \dots p_n + 1$. Clearly $N > p_n > 1$ for all i, and so it is not prime but it has a prime divisor. However, if $p_i|N$ then $p_i|1 = N - p_1 \cdots, p_i \cdots p_n$, contradiction. □

From a computational point of view, the problems of computing primes and checking if a number is prime have both been pondered for many years. There are multiple algorithms to check if a number is prime. The easiest one can think of has complexity $O(n)$ where we check if a number between 2 and $n-1$ divides n. We can

do slightly better though by noticing that checking from 2 to $\sqrt{n}$ is enough. Such processes are called *primality tests*, and will be discussed in the last lecture.

We will conclude this subsection by noticing that **Proposition 2.2** (iii) can be generalized as follows. The proof is left as an exercise for the reader.

Proposition 2.4

Let a, b, c be integers such that $a|bc$. If $\gcd(a, b) = 1$, then $a|c$.

2.2 Fundamental Theorem of Arithmetic

The following theorem concerning primes is of capital importance in number theory. In fact, it is so important that it was given the rather peculiar name of fundamental theorem of arithmetic. It encompasses perfectly why primes represent the DNA of integers, and why information about primes can recover information about integers themselves.

Theorem 2.5: Fundamental Theorem of Arithmetic

Let $n \geq 2$ be a positive integer. Then n can be written uniquely as a product of primes, i.e there exists unique primes $p_1, \dots p_k$ (up to reordering) for which $n = p_1 p_2 \dots p_k$.

Before proving this theorem, let us make sure to understand what it states exactly. What we are saying here is that every integer $n \geq 2$ can be written as a product of certain fixed primes in one and only one way up to reordering. The last sentence means that the primes are the same but their order is irrelevant because multiplication is commutative (i.e $ab = ba$).

Let us look at some examples of what this theorem states. For example, we can see that $628 = 2 \cdot 2 \cdot 157$ where every factor here is prime. What this theorem guarantees to us is that this is the *unique* way to write 628 as a product of primes up to reordering, meaning that any prime p that could appear in such a factorization of 628 is either 2 or 157, and that the number of 2's is always 2 and the number of 157's is always 1. As such, the only other possible ways to write 628 as a product of primes are $628 = 2 \cdot 157 \cdot 2 = 157 \cdot 2 \cdot 2$ which are the same up to order.

Proof. We already know from Proposition 2.2 (i) that n can be written as a product of primes. As such, we simply have to show the uniqueness of this expression up to reordering.

Suppose that $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_s$ for primes $p_1, \dots, p_k, q_1, \dots, q_s$. We then get that $p_1 | q_1 q_2 \dots q_s$. By Proposition 2.2 (iii), we get that $p_1 | q_i$ for some $1 \leq i \leq s$. Since both p_1 and q_i are prime, we get that $p_1 = q_i$. We can reorder the q_i's so that $p_1 = q_1$, and hence we get that $p_2 p_3 \dots p_k = q_2 q_2 \dots q_s$. By an inductive argument (descent) recursive argument, we can get that after reordering $p_2 = q_2$, $p_3 = q_3$, etc... and that $k = s$. This concludes the uniqueness part of the argument. □

To showcase the power of the fundamental theorem of arithmetic, let us go back to the greatest common divisor. Suppose that a and b are two positive integers. We now know that we can write them uniquely as a product of primes. Since these primes may not be unique, we can regroup them by how many times they appear and write our integers as product of prime powers with distinct bases. Furthermore, we can assume that our exponents can be 0 which enables us to work with the same primes for both a and b.

$$a = p_1 p_2 \dots p_s \longmapsto a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}; \alpha_i \geq 0$$
$$b = p_1 p_2 \dots p_t \longmapsto a = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}; \beta_i \geq 0$$

For example, if we want to compute $\gcd(90, 12)$ we can write $90 = 2 \cdot 5 \cdot 3 \cdot 3$ as $90 = 2^1 \cdot 5^1 \cdot 3^2$ and $12 = 2 \cdot 2 \cdot 3$ as $12 = 2^2 \cdot 3^1 \cdot 5^0$. Notice that we only include the primes that divide either of 90 or 12 in both factorization. Finally, by **??** (iv) :

$$\gcd(90, 12) = \gcd(2^1 \cdot 5^1 \cdot 3^2, 2^2 \cdot 3^1 \cdot 5^0) = 2^1 \cdot 3^1 \cdot 5^0 \cdot \gcd(2^0 \cdot 5^1 \cdot 3^1, 2^1 \cdot 3^0 \cdot 5^0) = 6$$

The reason we know that $\gcd(2^0 \cdot 5^1 \cdot 3^1, 2^1 \cdot 3^0 \cdot 5^0) = 1$ without even computing both elements is that they have **no common prime factors**. This is because we extract the minimum power for each prime dividing either of our elements. Here is a formal proof of the validity of this procedure.

Proposition 2.6: GCD From Prime Factorization

Let a and b be two positive integers such that $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ where $p_1, p_2, \dots, p_k$ are primes and $\alpha_i, \beta_i \geq 0$. Then :

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)}$$

Proof:
For $1 \leq i \leq k$, let $c_i = \min(\alpha_i, \beta_i)$ By **Proposition 1.6** (iv) :

$$\begin{aligned}
\gcd(a,b) &= \gcd(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}) \\
&= p_1^{c_1} p_2^{c_2} \dots p_k^{c_k} \gcd(p_1^{\alpha_1 - c_1} p_2^{\alpha_2 - c_2} \dots p_k^{\alpha_k - c_k}, p_1^{\beta_1 - c_1} p_2^{\beta_2 - c_2} \dots p_k^{\beta_k - c_k}) \\
&= p_1^{c_1} p_2^{c_2} \dots p_k^{c_k} \\
&= p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)}
\end{aligned}$$

Notice that $\gcd(p_1^{\alpha_1 - c_1} p_2^{\alpha_2 - c_2} \dots p_k^{\alpha_k - c_k}, p_1^{\beta_1 - c_1} p_2^{\beta_2 - c_2} \dots p_k^{\beta_k - c_k}) = 1$ because both sides share no common prime factor since either $\alpha_i - c_i = 0$ or $\beta_i - c_i = 0$ (because c_i is either one or the other). $\square$

3 Modular Arithmetic

As discussed before, we can analyze numbers by categorizing them depending on their behavior with respect to the usual arithmetic operations. We initially categorized numbers by looking at divisors and multiples of a certain fixed integer d. But some numbers are neither a divisor, nor a multiple of d. Despite this, we can still categorize them depending on their *remainder* after Euclidean division by d.

To explain what I mean, let us look at a very basic example. The difference between 7am and 7pm is very clear for a human being. However, for a usual 12-hour clock, there is absolutely no difference between them since they both point to the same number in the clock, i.e 7. Similarly, whether we are the 26'th of December, 2023, the 19'th or even the 12'th, we will always be a Tuesday. This is because our two numbers differ by a multiple of 7.

Motivated by these two examples, we are willing to categorize numbers based on this aspect. Fixing a positive integer d, we will throw two numbers in the same bin if they differ by a multiple of d. Notice first that this categorize *all* integers, since every integer is in the same bin as its remainder after Euclidean division by d. Because of this, we have exactly d bins, one for each possible remainder. Finally, notice that multiples of d have remainder 0 and are all categorized in the same bin. As such, this is a generalization of our initial idea to categorize integers.

This whole process is at the core of *modular arithmetic*, which happens to be the study of integers through these bins that they fit into, as well as to see how bins relate to one another. Let us look at the math behind this process.

3.1 Basic Definitions

We start with some basic definitions.

Definition 3.1: Congruence

Fix a positive integer n. We say that two integers a and b are congruent modulo n if $n|a-b$, and we write $a \equiv b \pmod{n}$

Note that this is equivalent to saying there exists an integer k such that $a = b+kn$ This definition is motivated by what we discussed above: We throw two integers in the same bin if they differ by a multiple of d, like we threw 26 and 12 into the "Tuesday" bin because they differ by a multiple of 7, in this case 14. Here are some properties of congruence:

Proposition 3.2: Properties of Congruence

Let n be a positive integer, and let a,b and c be integers.
(i) $a \equiv a \pmod{n}$
(ii) $a \equiv b \pmod{n}$ is equivalent to $b \equiv a \pmod{n}$
(iii) $a \equiv b \pmod{n}$ is equivalent to $a + c \equiv b + c$
(iv) $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$
(v) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

These properties are simply restatement of the basic definitions and properties of divisibility. For example, you can prove the third one by noticing that $a \equiv b \pmod{n}$ means $n|a - b$ meaning that $n|(a + c) - (b + c)$ and as such $a + c \equiv b + c \pmod{n}$ and vice-versa. We encourage the reader to try and prove the rest of these properties.

The first interesting property of congruence is compatibility. If we view it as "equality", we already know that we can add to both sides the same number and that the "equality" would remain valid by **??Proposition 3.2** (iii). What if instead of adding the same number, we add two *congruent* numbers ? If congruence is supposed to mimic equality, then the resulting two expressions should also be congruent. This turns out to be the case, and it represents a fundamental property of modular arithmetic.

Proposition 3.3: Compatibility

Fix a positive integer n and let a, b, c, d be positive integers such that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then:
(i) $a + b \equiv c + d \pmod{n}$
(ii) $ab \equiv cd \pmod{n}$

Despite compatibility of addition and multiplication, exponentiation is not compatible with congruence. For example, $2 \equiv 7 \pmod{5}$ yet $3^2 \not\equiv 3^7 \pmod{5}$. Be careful with this one! We will develop tools in future lectures to better understand exponentiation.

Proof of Proposition 3.3:

(i) We know there exists j, k such that $a = c + jn$ and $b = d + kn$, So adding both equations gives $a+b = c+d+jn+kn = c+d+n(j+k)$ therefore $a+b \equiv c+d \pmod{n}$, as desired.

(ii) Again write $a = c + jn$ and $b = d + kn$ and this time multiply the two equations. We get

$$ab = cd + ckn + jdn + jkn^2 = cd + n(ck + dj + jkn)$$

thus $ab \equiv cd \pmod{n}$. □

The practical beauty of compatibility is that it makes size irrelevant in modular arithmetic: Why should we bother working with huge numbers when we can work with their remainders mod n ? Indeed, if today we are Monday, I can assure to you that it will be a Saturday in $6^{12344321} - 1$ days. Why ?

Recall that $6^{12344321}$ is simply $6 \cdot 6 \cdots 6$ multiplied 12344321 times. But, since $6 \equiv -1 \pmod{7}$, then that expression is the same as $(-1) \cdot (-1) \cdot (-1) \ldots$ by a repeated application of **Proposition 3.3** (ii). As such, $6^{12344321} - 1 \equiv (-1)^{12344321} - 1 \equiv -2 \pmod{7}$. So the effect of going forward in time $6^{12344321} - 1$ days, when viewed from the perspective of days of the week, is the same effect as going backward in time 2 days. Since today we are Monday, then two days ago was a Saturday.

So now we know how to add, multiply and subtract bins: We just take random elements of the concerned bins (called representatives), do our operation, then consider the bin of the result. Compatibility guarantees that no matter what representatives we chose, we will always end up in the same bin at the end. For example, if we want to add the bin of 2 and the bin of 3 mod 7, we can see that $2+3 = 5$ mod 7 so the result would be the bin of 5. If we pick other representatives, say 9 and 17, then $17 + 9 = 26 \equiv 5 \pmod{7}$, and as such we end up in the same bin again.

Now one may ask, what about division ? If $a \equiv b \pmod{n}$ and $d | \gcd(a, b)$, it **does not hold** in general that $\frac{a}{d} \equiv \frac{b}{d} \pmod{n}$. For example, $12 \equiv 18 \pmod{6}$ yet $4 \not\equiv 6 \pmod{6}$. Particularly speaking, that means that **we cannot in general cancel a common factor in congruences**, and that **Proposition 3.2** (iv) is a strict implication.

Despite this, we can find some circumstances in which division may be possible. For example, suppose that $a \equiv b \pmod{n}$ and that d is a positive integer s.t $d|a, d|b$ and $d|n$. Then, it is true that $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. Indeed, going back to our definition of congruence, this means that $a = b + nk$ for some integer k, and hence that $\frac{a}{d} = \frac{b}{d} + \frac{n}{d}k$.

3.2 Inverses and Wilson's Theorem

We continue on our quest to divide within congruences. We know that, given integers a, b, c and a positive integer n, then $ca \equiv cb \pmod{n}$ means that $n|c(a-b)$. Imagine for a second that $\gcd(n, c) = 1$. This means that no prime factor of n appears in c whatsoever. As such, since $n|c(a-b)$, they must all appear in $a-b$. Hence, $n|a-b$ and $a \equiv b \pmod{n}$. The conclusion is that we can cancel a common factor for as long as it is *coprime* to n, i.e, its greatest common divisor with n is 1. We can formalize this in the following proposition:

Proposition 3.4: Inverses

Let n be a positive integer, and let a be an integer such that $\gcd(a, n) = 1$ (such an integer will now be called coprime to n). Then there exists an integer b such that $ab \equiv 1 \pmod{n}$. b is called an *inverse* of a mod n. Moreover, all inverses of a mod n are congruent.

Proof:

Since $\gcd(a, n) = 1$, there exists b, c such that $ab + cn = 1$ by Bézout's Theorem. Hence $n|1 - ab$ and thus $ab \equiv 1 \pmod{n}$, as desired. Moreover, suppose that b and b' are inverses of a mod n. Then $ab \equiv ab' \equiv 1 \pmod{n}$. Multiplying by b on both sides we get that $bab' \equiv b \pmod{n}$ but since $ba \equiv 1 \pmod{n}$ then $b' \equiv b \pmod{n}$. □

What this theorem is saying is that if some bin is coprime to n then we can find another bin such that their "product" is the bin containing 1. This result is quite interesting and can lead to some interesting conclusions. For example, we can see that every non-zero bin has an inverse modulo p where p is prime. Indeed, every integer between 1 and $p-1$ is coprime to p, so all their respective bins have inverses. However, 0 does not have an inverse mod p, which is evident since $0k \equiv 0 \pmod{p}$ for every k.

This line of thought can make us wonder the following: What numbers are their own inverses? This basically means that we want to solve $x^2 \equiv 1 \pmod{n}$ for some fixed positive integer n. Unfortunately, this is not as easy as taking a square root : We do not know that square roots are compatible with congruences (and in fact, they are not).

Let us look at the following example. Pick $n = 20$. Then $1^2 \equiv 1 \pmod{20}$, $19^2 \equiv (-1)^2 \equiv 1 \pmod{20}$ AND $11^2 = 121 \equiv 1 \pmod{20}$. Since $1, 11$ and 19 are in distinct bins, we have found three solutions to this equation. The reason that

"simply taking the square root" does not work here is that the idea behind taking the square root in real numbers comes from factoring. Indeed, to solve $x^2 = 1$, we notice that this means that $x^2 - 1 = 0$ i.e $(x-1)(x+1) = 0$, and hence either $x - 1 = 0$ or $x + 1 = 0$.

Does this work in congruences? We indeed get that $(x-1)(x+1) \equiv 0 \pmod{n}$ if $x^2 \equiv 1 \pmod{n}$, but does this means that either $x-1$ or $x+1$ is 0 mod n ? Not necessarily. Indeed, if n is not prime, one can find $a, b < n$ such that $ab = n$. Then, neither a nor b is 0 mod n but their product is. If we restrict ourselves to primes, then it turns out to be true. Indeed, if $p|(x-1)(x+1)$ then $p|(x-1)$ or $p|x+1$ so that $x \equiv \pm 1 \pmod{p}$. So, modulo primes, the only "bins" whose inverse is themselves are 1 and $p-1$'s bins. This results in the following interesting theorem:

Theorem 3.5: Wilson's Theorem

Let $n \geq 2$ be a positive integer. Then n is a prime number if and only if $(n-1)! \equiv -1 \pmod{n}$.

Let us recall that $(n-1)!$ is the product of all integers from 1 to $n-1$, i.e $(n-1)! = (n-1) \cdot (n-2) \cdot (n-3) \ldots 2 \cdot 1$. The reason why this works is as follows. If n is not prime, then one can find $1 < a < n$ such that $a|n$. But a appears in $(n-1)!$ so it also divides $(n-1)!$. Hence, if $n|(n-1)!+1$ then $a|(n-1)!+1$ which would mean that $a|1$ which is clearly impossible. So the only integers satisfying this have to be primes.
One question remains: Why would primes satisfy this? The answer: Inverses ! Suppose that n is prime. By definition, this means that $1, \ldots, n-1$ are coprime to n. As such, they all have an inverse. By compatibility, this inverse is also between 1 and $n-1$. As such, we can pair up the numbers between 1 and $n-1$ into pairs of inverses that multiply down to 1. We have to be careful with this reasoning however, some numbers may be their own inverses. But this only happens with 1 and $n-1$. As such, we can deduce that the integers $2, 3, \ldots, n-2$ can be paired up into pairs of inverse that multiply to 1. Here is how the proof goes:

Proof of Theorem 3.5

Suppose that $n \geq 2$ is not prime. Then one can find a such that $1 < a < n$ and $a|n$ by definition. Thus, if $n|(n-1)!+1$ then since $a|(n-1)!+1$, but $a|(n-1)!$ so that $a|1$, contradiction. So n has to be prime.

Similarly, if n is prime, then $1, 2, \ldots, n-1$ are coprime to n, and only 1 and $n-1$ are their own inverses in that set. So one can pair up the numbers $2, 3, \ldots, n-2$

into pairs of inverses that multiply to 1 mod n. Hence:

$$(n-1)! \equiv 1 \cdot (2 \cdot 3 \ldots (n-2)) \cdot (n-1) \equiv 1 \cdot (n-1) \equiv -1 \pmod{n}$$

□

Wilson's Theorem is interesting in the sense that it's a total categorization of primes. From this perspective, it's a primality test that "never misses". It can also help us find a formula for $\pi(x)$ or for the n'th prime. However, these formulas and properties are unpractical due to how difficult and time-consuming it is to compute $(n-1)!$ in general. The same problem applies to the primality test using Wilson's theorem, which is considerably less efficient than the usual "check until square-root" algorithm.

3.3 Chinese Remainder Theorem (CRT)

We will end this section by discussing the Chinese Remainder Theorem. This results concerns the existence of certain "bins" modulo nm that have certain chosen remainders modulo n and modulo m, where m and n are coprime integers. To showcase what I mean, suppose we have a certain number of apples n that is no more than 35. We know that if we group those apples by 5, we are left with 2 apples, and if we group them by 7, we are left with 3 apples. What could that number n be ?

Mathematically, we want an integer $1 \leq n \leq 35$ for which $n \equiv 2 \pmod{5}$ and $n \equiv 3 \pmod{7}$. It is not too hard to see that $n = 17$ is the only solution to such a problem. However, it is important to see that if we allow integers beyond 35, we get a whole lot of solutions :

$$17, 52, 87, 122, \ldots$$

All these solutions are congruent to 17 modulo 35, and since 17 satisfies the condition, then it makes sense that all numbers congruent to 17 modulo 35 satisfy the condition because $35 = 5 \cdot 7$. For example, $87 = 17 + 35 \cdot 2 = 17 + 2 \cdot 5 \cdot 7$. Since the term added to 17 is divisible by both 5 and 7, it does not affect the equation when taken modulo 5 or 7.

This is precisely the statement of the Chinese remainder theorem. Given two coprime integers m and n, we can find a unique *residue class* (meaning a bin) modulo mn that is congruent to whatever we want modulo m and n. As we shall see later, the condition that m and n are coprime is essential. For example, there is no integer n that is 1 mod 2 and 2 mod 6, since the first condition implies n is odd while the second implies n is even. This problem occurs because $\gcd(2, 6) = 2 > 1$.

Theorem 3.6: Chinese Remainder Theorem

Let n and m be coprime positive integers $\gcd(n, m) = 1$, and let a and b be arbitrary integers. Consider the following system of congruences with unknown $x \in \mathbb{Z}$:

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

The solutions of this system form a unique residue class modulo mn.

What we are saying here is that all solutions of the two congruences above are in the same "bin" modulo mn, and that similarly, all elements of that bin are solutions to the system.

To prove CRT, we will make use of the following handy lemma:

Lemma 3.7

Let m, n, x be integers satisfying $m|x$, $n|x$ and $\gcd(m, n) = 1$. Then $mn|x$.

Proof: Since $m|x$ we can write $x = mk$ for $k \in \mathbb{Z}$. Thus, $n|mk$. But $\gcd(n, m) = 1$ and thus $n|k$ by **Proposition 2.4**. So $k = nk'$ for $k' \in \mathbb{Z}$. Multiplying by m we get $mk = nmk'$ and thus $x = nmk'$ and $nm|x$, as desired.

Proof of Theorem 3.6:

We will first exhibit a solution y to the system of congruences above making use of inverses. Then, we wil show that every element congruent to y mod mn is a solution. Finally, we'll show that every solution is congruent to y mod mn. Since $\gcd(m, n) = 1$, one can find integers u and v such that $mu + nv = 1$ by Bézout's Theorem, i.e :

$$mu \equiv 1 \pmod{n}$$
$$nv \equiv 1 \pmod{m}$$

Let $y = amu + bnv$. Then :

$$y \equiv amu \equiv a \pmod{n}$$
$$y \equiv bnv \equiv b \pmod{m}$$

So y is a valid solution, and hence solutions to this system always exist. Further-

more, let x be any integer such that $x \equiv y \pmod{mn}$. Then $x = y + nmk$ for $k \in \mathbb{Z}$ by definition. Thus : $x \equiv y \pmod{n}$ and $x \equiv y \pmod{m}$ because mnk is 0 mod n and mod m. Hence x is also a valid solution.

Finally, if x is a solution to the system of congruences, then $x \equiv a \equiv y \pmod{n}$ and $x \equiv b \equiv y \pmod{m}$ and thus $n|x-y$ and $m|x-y$. By **Lemma 3.7**, $nm|x-y$ hence $x \equiv y \pmod{mn}$.

So the set of solutions to this system of congruences is a unique residue class mod mn. □

It is important to understand that what we did in the proof was to first exhibit a solution y, then show that every element congruent to y mod mn is also a solution, and vice-versa that every solution is congruent to y mod mn. By doing so, we ensure that the set of solutions to the system of congruences above is the set of all integers congruent to y mod mn.

The Chinese Remainder Theorem can help us reduce multiple system of congruences into a unique congruence. It appears as a stepping stone to prove many theoretical results across mathematics, as well as a practical way to recover integers given some information on their residuals. The Chinese Remainder Theorem also holds for arbitrarily long systems of congruences for as long as the modulis are **pairwise** coprime. For example, if we want to find all integers n congruent to 2 mod 3, to 3 mod 5 and to 6 mod 7, then since $3, 5, 7$ are pairwise coprime, CRT ensures that the solutions are of the form $n = a + 3 \cdot 5 \cdot 7k$ where $k \in \mathbb{Z}$ and a is a fixed solution. For example, we can see that 83 satisfies all congruences above, so that the solutions are exactly the integers of the form $83 + 105k$, $k \in \mathbb{Z}$.

So CRT reduces the problem to finding only one solution for our system of congruences. This is not always easy, however, and may require loads of computations. The proof of CRT gives us a way of recovering one solution by computing the coefficients u and v for which $mu + nv = 1$ that exist by Bézout's Theorem. These can be recovered by "rolling back" the Euclidean Algorithm.