An Introductory Guide to Number Theory

For an Undergraduate Course in Number Theory

Cheyenne Ward

Fall 2024

Contents

1 Introduction

Number Theory studies the properties and relationships of integers, focusing on concepts like divisibility, primes, modular arithmetic, and the Fundamental Theorem of Arithmetic. Primes, as the indivisible units of integers, distinguish themselves from composites and act as the building blocks for algorithms and theorems such as Fermat's Little Theorem and the Chinese Remainder Theorem. These concepts allow us to solve congruences, compute greatest common divisors, and factor numbers. With applications in cryptography, coding theory, and computational algorithms, Number Theory provides tools to understand and work with the structure of integers.

2 Definitions

Note: Not all of the listed definitions are used in this guide but are still important for the reader to know. It is encouraged that the reader studies them.

2.1 Divides

Let $a, b \in \mathbb{Z}$. We say a divides b (written $a \mid b$) if there exists an integer n such that $b = a \cdot n$.

2.1.1 Examples

Case when the definition works:
Let $a = 3, b = 12$. By the definition we get the following equation:

$$12 = 3 \cdot n \text{ for some } n \in \mathbb{Z}.$$

A little bit of algebraic manipulation of the equation or an educated guess may lead you to believe $n = 4$. Aha! Since $4 \in \mathbb{Z}$, a does in fact divide b (represented as $a \mid b$).

Now let's see a case where the definition does not work: Let $a = 5, b = 7$. By the definition of divides we get the following equation:

$$7 = 3 \cdot n \text{ for some } n \in \mathbb{Z}.$$

You might choose to use some algebra to get $n = \frac{7}{3}$. However, remember that n should exist in $\mathbb{Z}$. Since $\frac{7}{3}$ is not an integer, our value for n does not work and $a \nmid b$.

2.2 Well-Ordered

A set S is well-ordered if every subset of S has a least element.
Well-Ordering Principle (Axiom): A nonempty set of positive integers has a least element.

2.2.1 Examples

Consider the set $\mathbb{N}$. We will take the following subset: $\{3, 9, 27\}$. This subset has a least element 3.

Let's look at another subset of $\mathbb{N}$: $\{1, 2, 4\}$. This set also has a least element 1.

You may be able to see that for every element $a \in \mathbb{N}$, $a \leq a + 1$ where $a \geq 0$. Thus every subset of $\mathbb{N}$ will have a least element therefore the set of natural numbers is well-ordered.

At this moment we encourage the reader to think of a set that is not well-ordered.

Consider the set $\mathbb{Z}$. This set contains negatives and it is not difficult to find a subset that does not have a least element.

That is the subset (which we will denote as S) of negatives: $\{-1, -2, -3, -4, -5, ...\}$ which continues infinitely. Here, for every $a \in S$ there exists an integer b such that ba. Therefore S does not contain a least element and $\mathbb{Z}$ is ot well-ordered.

2.3 Common Divisor

Given $a, b \in \mathbb{Z}$, and not both are zero, we say d is a common divisor of a and b if $d|a$ and $d|b$.
The largest of the common divisors of a and b is called the greatest common divisor of a and b, written gcd(a,b).

2.3.1 Examples

Let $a = 4, b = 8$. We want to find a $d \in \mathbb{Z}$ such that $d \mid a$ and $d \mid b$. We will take an educated guess that $d = 2$. We can check our guess using the definition of divides:

Let $4 = 2 \cdot n$ for some $n \in \mathbb{Z}$ and let $8 = 2 \cdot m$ for some $m \in \mathbb{Z}$. Solving for each variable we get $n = 2$ and $m = 4$. Since $2, 4 \in \mathbb{Z}$, $d \mid a$ and $d \mid b$ thus d is a common divisor of a and b.

Is d the largest common divisor? We will revisit this question later in the section titled The Euclidean Algorithm.

Now let us examine a case when a and b do not have a common divisor. Let $a = 12, b = 2$ and $d = 3$. Using the definition of divides we can see that $12 = 3 \cdot n$ for $n = 4$. However solving for m in $2 = 3 \cdot m$ gives us $m = \frac{2}{3}$ which is not in $\mathbb{Z}$ thus $d \nmid b$ even though $d \mid a$ thus d is NOT a common divisor of a and b.

2.4 Relatively Prime

When $\gcd(a, b) = 1$, we say that a and b are relatively prime or coprime.

2.4.1 Examples

Please refer to the section titled The Euclidean Algorithm before proceeding with the examples!

Let $a = 8, b = 9$. The Euclidean Algorithm produces:

$$9 = 8 \cdot 1 + 1$$
$$1 = 1 \cdot 1 + 0$$

The last non-zero remainder here is 1 thus $\gcd(8, 9) = 1$ and 8 and 9 are relatively prime.

Refer to the section The Euclidean Algorithm to see example where the remainder is not 1 and thus $\gcd(a, b) \neq 1$.

2.5 Congruent Modulo

Let a, b and n be integers with $n \geq 2$. We say $a \cong b \pmod{n}$ if $n \mid (a - b)$.

2.5.1 Examples

A case where this works:
Let $a = 15$, $b = 7$, and $n = 4$. We first Compute $a - b$:

$$a - b = 15 - 7 = 8$$

We then check if $4 \mid 8$. This is true when $n = 2$ when solving for $8 = 4 \cdot n$ for some $n \in \mathbb{Z}$.

A case where this does not work:
Let $a = 14$, $b = 9$, and $n = 4$. We first Compute $a - b$:

$$a - b = 14 - 9 = 5$$

We then check if $4 \mid 5$. This is not true as $n = \frac{5}{4} \notin \mathbb{Z}$ when solving for $5 = 4 \cdot n$ for some $n \in \mathbb{Z}$.

2.6 Prime Number

A positive integer p greater than 1 is called prime if the only positive integer divisors of p are 1 and p itself.

2.6.1 Examples

Theorem 12 gives a method to use to show that a number is prime however, here we use smaller numbers that where telling if it is prime is more trivial.

Let $p = 6$. The divisors of 6 are $\{1, 2, 3, 6\}$. Since 6 has divisors other than 1 and itself, 6 is not prime.

Let $p = 3$. The divisors of 3 are $\{1, 3\}$. Since 3 the only divisors of 3 are 1 and itself, 3 is prime!

2.7 Mersenne Prime

A prime number of the form $2^n - 1$, for some $n \in \mathbb{N}$ is called a Mersenne Prime.

2.7.1 Examples

Let $n = 3$. We begin by computing $2^n - 1$:

$$2^3 - 1 = 8 - 1 = 7$$

The divisors of 7 are $\{1, 7\}$. Since the only divisors of 7 are 1 and itself, 7 is prime and $2^3 - 1 = 7$ is a Mersenne Prime.

Let $n = 4$. We begin by computing $2^n - 1$:

$$2^4 - 1 = 16 - 1 = 15$$

The divisors of 15 are $\{1, 3, 5, 15\}$. Since 15 has divisors other than 1 and itself, 15 is prime and $2^4 - 1 = 15$ is not a Mersenne Prime.

2.8 Fermat Prime

A prime number of the form $2^{2^k} + 1$, for some $k \in \mathbb{N}$ is called a Fermat Prime.

2.8.1 Examples

Let $k = 2$. We begin by computing $2^{2^k} + 1$:

$$2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$$

The divisors of 17 are $\{1, 17\}$. Since the only divisors of 17 are 1 and itself, 17 is prime, and $2^{2^2} + 1 = 17$ is a Fermat Prime.

Let $k = 4$. We begin by computing $2^{2^k} + 1$:

$$2^{2^4} + 1 = 2^{16} + 1 = 65,536 + 1 = 65,537$$

The divisors of $65,537$ include numbers other than 1 and itself, so $65,537$ is not a prime number. Therefore, $2^{2^4} + 1 = 65,537$ is not a Fermat Prime.

2.9 Order of a modulo n

Let $a, n \in \mathbb{N}, n \geq 2$ where $\gcd(a, n) = 1$. The smallest natural number k such that $a^k \cong 1($ mod n is called the order of a modulo n and is denoted $\text{ord}_n(a)$.

2.10 Examples

Let $a = 2$, $n = 5$, and $\gcd(a, n) = 1$.

We compute powers of a modulo n:

$$2^1 = 2 \to 2 = 2 \mod 5 \; 2^2 = 4 \to 4 = 4 \mod 5 \; 2^3 = 8 \to 8 \mod 5 = 3 \; 2^4 = 16 \to 16 \mod 5 = 1$$

The smallest k such that $2^k \cong 1 \pmod 5$ is $k = 4$. Thus, $\text{ord}_5(2) = 4$

Let $a = 2$, $n = 4$, and $\gcd(a, n) \neq 1$.

We compute powers of a modulo n:

$$2^1 = 2 \to 2 = 2 \mod 4$$
$$2^2 = 4 \to 4 = 0 \mod 4$$
$$2^3 = 8 \to 8 \mod 4 = 0$$
$$2^4 = 16 \to 16 \mod 4 = 0$$

Since $\gcd(a, n) \neq 1$, the condition for the order to be defined does not hold. Thus, the order of a modulo n is **not defined**.

2.11 Involving Euler θ - function

For a natural number n, the Euler θ - function, $\theta(n)$, is equal to the number of natural numbers less than or equal to n that are relatively prime with n.

2.11.1 Examples

Let $n = 6$. We determine $\theta(6)$ by finding the natural numbers less than or equal to 6 that are relatively prime to 6.

The numbers less than or equal to 6 are:

$$1, 2, 3, 4, 5, 6$$

We check the gcd of each number with 6:

$$\begin{aligned}
&\gcd(1,6) = 1 \quad \text{(relatively prime)} \\
&\gcd(2,6) = 2 \quad \text{(not relatively prime)} \\
&\gcd(3,6) = 3 \quad \text{(not relatively prime)} \\
&\gcd(4,6) = 2 \quad \text{(not relatively prime)} \\
&\gcd(5,6) = 1 \quad \text{(relatively prime)} \\
&\gcd(6,6) = 6 \quad \text{(not relatively prime).}
\end{aligned}$$

The numbers that are relatively prime to 6 are:

$$1, 5$$

Thus, $\theta(6) = 2$.

Let $n = 1$. By definition, $\theta(n)$ counts the natural numbers less than or equal to n that are relatively prime to n.

The only number less than or equal to 1 is:

$$1$$

The $\gcd(1, 1) = 1$, which satisfies the relatively prime condition. However, the Euler θ-function is typically undefined for $n = 1$ because it is not meaningful to apply the concept of "relative primality" to the number 1 itself in this context.

Thus, $\theta(1)$ is **not defined**.

3 Theorems

Here we state key theorems the reader may encounter in a Number Theory course at the Undergraduate level. In the section Application of Some Theorems. Although all the theorems listed may not be covered in the section previously mentioned, the reader is still encouraged to review them.

3.1 Theorem 1

Let a, q, b, r and k be integers. If $a = bq + r$ and if $k|a$ and $k|b$, then $k|r$.

3.2 Theorem 2

Let a, q, b, r and k be integers with a and b not both zero. If $a = bq+r$, then $\gcd(a, b) = \gcd(b, r)$.

3.3 Theorem 3: Bezout's Theorem

For all integers a and b (not both zero), there exist integers x and y such that $\gcd(a, b) = a \cdot x + b \cdot y$.

3.4 Theorem 4: On a Linear Diophantine Equation Having Solution

A Linear Diophantine Equation $ax + by = c$ has a solution (infinitely many) if and only if $\gcd(a, b)|c$.

3.5 Theorem 5

For any integers a and b, not both zero, there exist integers x and y such that $ax + by = \gcd(a, b)$.

3.6 Theorem 6

Given integers a, b and c, where $c \neq 0$ and a and b are not both zero, there exists integers x and y such that $ax + by = c$ if and only id $\gcd(a, b)|c$.

3.7 Theorem 7

For $a, b, n \in \mathbb{Z}$ with $n \geq 2$, we have $a \cong b(\mod n)$ if and only if a and b have the same remainder when divided by n.

3.8 Theorem 8

Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}$ with $n \geq 2$. If $a \cong b(\mod n)$ and $c \cong d(\mod n)$, then:

$$\text{(i) } a \cdot c \cong b \cdot d(\mod n)$$
$$\text{(ii) } a + c \cong b + d(\mod n)$$

3.9 Theorem 9

Let a, b, n be integers with $n \geq 2$. Then $ax \cong b(modn)$ has a solution if and only if there exist integers x and y such that $ax + ny = b$ (if and only if $\gcd(a, n)|b$)

3.10 Theorem 10: The Chinese Remainder Theorem (CRT)

Let $n_1, n_2, ..., n_r$ be possible integers such that $\gcd(n_i, n_j) = 1$, for all $i \neq j$. Then the system of linear congruences:

$$x \cong a_1(modn_1)$$
$$x \cong a_2(modn_2)$$
$$x \cong a_r(modn_r)$$

has a simultaneous solution, which is unique modulo the integer $N = n_1 \cdot n_2 \cdot ... \cdot n_r$.

3.11 Theorem 11

For all integers a and n, with $n \geq 2$, $a \cong -(n - a)(\mod n)$.

3.12 Theorem 12

An integer $n1$ is prime if and only if, for all primes $p\sqrt{n}$, we have that $p \nmid n$.

3.13 Theorem 13: The Fundamental Theorem of Arithmetic (FTA)

Every natural number greater than 1 is either a prime or a composite. If it is composite then it can be expressed as a finite product of powers of prime numbers. This product is unique up to the order of the prime power of factors.

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m}, p_1 p_2 p_m.$$

3.14 Theorem 14

Let $X, Y, N \in \mathbb{Z}$. Then X is a solution to $X \cong y(\mod N)$, where $N = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_n^{e_n}, p_1 = \prod_{i=1}^{n} p_i^{e_i}$ if and only if X satisfies the system

$$X \cong Y(\mod p_1^{e_1})$$
$$X \cong Y(\mod p_2^{e_2})$$
$$X \cong Y(\mod p_n^{e_n}).$$

3.15 Theorem 15

Let $a, n \in \mathbb{N}, n \geq 2$ and $\gcd(a, n) = 1$. Then there exists $k \in \mathbb{N}$ such that $a^k \cong 1(\mod n)$.

3.16 Theorem 16

Let $a, n \in \mathbb{N}, n \geq 2$ and $\gcd(a, n) = 1$ and let $k = \text{ord}_n(a)$. Then $a^1, a^2, ..., a^k$ are all incongruent $(\mod n)$.

3.17 Theorem 17

If $a, n \in \mathbb{N}, n \geq 2$ and $\gcd(a, n) = 1$ and $k = \text{ord}_n(a)$. Then, for all $m \in \mathbb{N}$, a^m is congruent to exactly one of $a^1, a^2, ..., a^k$.

3.18 Theorem 18

Let $a, n \in \mathbb{N}, n \geq 2$ and $\gcd(a, n) = 1$ and $k = \text{ord}_n(a)$. Then $a^m \cong 1(\mod n)$ if and only if $k \mid m$.

3.19 Theorem 19

If $\gcd(a, n) = 1$, then $\text{ord}_n(a) \leq n$.

3.20 Theorem 20: Fermat's Little Theorem

For $a \in \mathbb{Z}$ and p prime with $p \nmid a$, $a^{p-1} \cong 1(\mod p)$.

3.21 Theorem 21

Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, and let $a \in \mathbb{Z}$. If $x \cong a(\mod n)$ and $x \cong a(\mod m)$, then $x \cong a(\mod m \cdot n)$.

3.22 Theorem 22: Euler's Theorem

$a^{\theta(n)} \cong 1(\mod n)$.

3.23 Theorem 23:

If p and q are distinct primes, then $\theta(p \cdot q) = (p-1)(q-1)$.

4 The Division Algorithm

The division algorithm says for $a, b \in \mathbb{Z}$, where $b > 0$, we can always write $a = q \cdot b + r$, for some integers q and r, where $0 \leq rb$. Moreover, given a and b, there is only one pair q and r (q: quotient and r: remainder) which satisfy these constraints.

Example: Let $a = -34, b = 6$. Applying the division algorithm produces:

$$-24 = 6 \cdot -6 + 2 \text{ where -6 is quotient and 2 is the remainder.}$$

5 The Euclidean Algorithm

The Euclidean Algorithm is an extension of the The Division Algorithm where we continue until $r = 0$. When $r = 0$ there are no more common divisors between a and b thus the greatest common divisor of a and b is the last non-zero remainder of a and b.

Example: Let $a = 12, b = 8$. Applying the euclidean algorithm produces:

$$12 = 8 \cdot 1 + 4$$
$$8 = 4 \cdot 2 + 0$$

Example from section Common Divisor:

Let $a = 4, b = 8$. Using the euclidean algorithm we get: $8 = 4 \cdot 2 + 0$

Here we only need one step for the euclidean algorithm thus $\gcd(a, b) = 4$ (the divisor).

6 Application of Some Theorems

6.1 Problem 1

Find a solution in the canonical complete residue system modulo $6 \cdot 11 \cdot 17$ to the following:

$$x \cong 5 \pmod 6$$
$$x \cong 4 \pmod 1)1$$
$$x \cong 3 \pmod 1)7$$

Solution:
We begin by examining the modulos $6, 11, 17$. Since every pair of these is coprime, we can apply the chinese remainder theorem to this problem.

$$n = 6 \cdot 11 \cdot 17 = 1122$$
$$N_1 = \tfrac{n}{6} = 187, N_2 = \tfrac{n}{11} = 102, N_3 = \tfrac{n}{7} = 66$$
$$187x_1 \cong 1 \pmod 6 \rightarrow x_1 = 1$$
$$102x_2 \cong 1 \pmod 1)1 \rightarrow x_2 = 4$$
$$66x_3 \cong 1 \pmod 1)7 \rightarrow x_3 = 8$$
$$x = (1 \cdot 5 \cdot 187) + (4 \cdot 4 \cdot 102) + (8 \cdot 3 \cdot 66) = 4151$$

Since $4151 \cong 785 \bmod 1122$, $x = 785$ is a solution.

6.2 Problem 2

Find all solutions (if any exist) in the ccrs_{301} to the following linear congruence:

$$140x \cong 133 \pmod 3)01$$

Solution:

If solutions did exist to the linear congruence $140x \cong \bmod 43$, then the greatest common divisor (gcd) would divide 133.
Since the euclidean algorithm reduces the numbers until their remainder is 0 thus preserving the gcd of these two numbers up until this point, we can use it to find the greatest common

divisor of 140 and 301:

$$301 = 140 \cdot 2 + 21$$

$$140 = 21 \cdot 6 + 14$$

$$21 = 14 \cdot 1 + 7$$

$$14 = 7 \cdot 2 + 0$$

Here we see the gcd of 140 and 301 is 7.

By Bezouts Identity, we can express $\gcd(140, 301)$ as $140x - 301y = 133$. To make this equation easier to work with we will reduce it to $20x - 43y = 19$ by dividing the left-hand side (LHS) and right-hand side (RHS) by 7. We make note of our slope here: $20/43$ where 43 is the distance between solutions.

We will now use the Extended Euclidean Algorithm on the reduced equation to get the values for x and y:

$$43 = 20 \cdot 2 + 3 \rightarrow 3 = 43 - 20 \cdot 2$$

$$20 = 3 \cdot 6 + 2 \rightarrow 2 = 20 - 3 \cdot 6$$

$$3 = 2 \cdot 1 + 1 \rightarrow 1 = 3 - 2 \cdot 1$$

$$43 = 20 \cdot 2 + 3 \rightarrow 3 = 43 - 20 \cdot 2$$

The equations to the right of the arrows are the equation for the remainder of the equation to the left of the arrow.

Here, we see that the greatest common divisor of 20 and 43 is 1. We now substitute the equations to the right of the arrows into each other then scale by 19 to get a particular solution. From here, we start at -285 and keep adding 43 to it until we get a number larger than 301 to see all of the numbers between 0 and 301. These numbers will be the solutions.

$$2 = 20 - (43 - 20 \cdot 2) \cdot 6$$

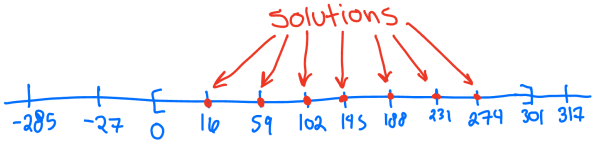
$$2 = (13)(20) - (43)(6)$$

$$1 = (43) - (20)(2) - (13)(20) - (43)(6)$$

$$1 = (-15)(20) - (43)(7)$$

$$19[1 = (-15)(20) - (43)(-7)]$$

$$19 = (20)(-285) - (43)(-133)$$



6.3 Problem 3

Find the units digit of 3^{100} by using Fermat's Little Theorem

Solution:

We begin by noting that the units digit of 3^{100} is the same as $3^{100} \mod 10$. Thus, by Fermat's Little Theorem, let $a = 3$ and $p = 5$. Since $3^4 \cong 1 \pmod 5$, we can simplify:

$$3^{100} \cong (3^4)^{25} \cong 1^{25} \cong 1 \pmod 5.$$

Next, we consider $3^{100} \mod 2$. Since 3 is odd, any power of 3 remains odd. Therefore:

$$3^{100} \cong 1 \pmod 2.$$

Now, we have the system of congruences:

$$3^{100} \cong 1 \pmod 5, \quad 3^{100} \cong 1 \pmod 2.$$

By the **Chinese Remainder Theorem**, since 2 and 5 are coprime, there exists a unique solution modulo 10. Let x represent $3^{100} \mod 10$. Then we solve the following system:

$$x \cong 1 \pmod 5, \quad x \cong 1 \pmod 2.$$

To combine these, let $x = 5k + 1$ (from $x \cong 1 \pmod 5$). Substitute this into the second congruence:

$$5k + 1 \cong 1 \pmod 2.$$

Simplify modulo 2:

$$5k \cong 0 \pmod 2.$$

Since $5 \cong 1 \pmod 2$, this reduces to:

$$k \cong 0 \pmod 2.$$

Thus, $k = 2m$ for some integer m. Substituting back, we get:

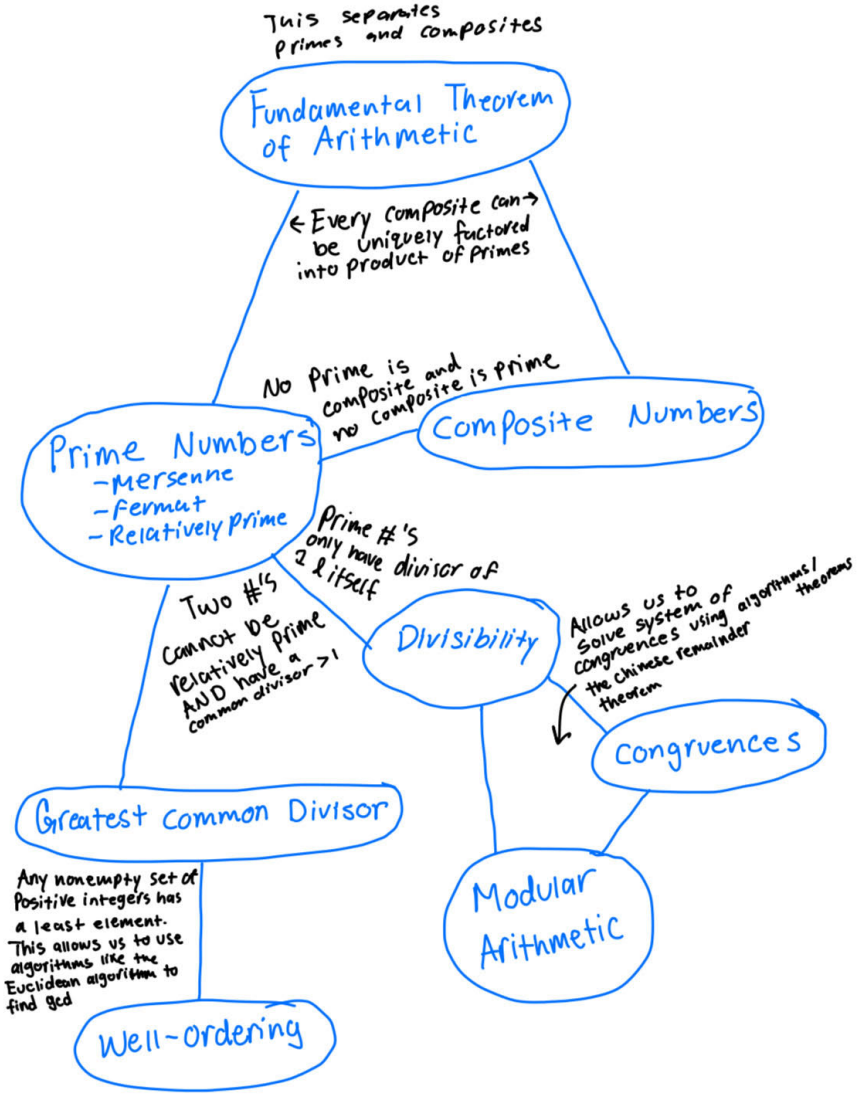
$$x = 5(2m) + 1 = 10m + 1.$$

This shows:

$$x \cong 1 \pmod{10}.$$

Therefore, $3^{100} \cong 1 \pmod{10}$, and the units digit of 3^{100} is 1:

A Mind Map


This separates primes and composites
Fundamental Theorem of Arithmetic
Every composite can be uniquely factored into product of primes
No Prime is composite and no composite is prime
Prime Numbers
-Mersenne
-Fermat
-Relatively prime
Composite Numbers
Prime #'s only have divisor of 2 & itself
Two #'s cannot be relatively prime AND have a common divisor >1
Divisibility
Allows us to solve system of congruences using algorithms/theorems the Chinese remainder theorem
Congruences
Greatest common Divisor
Any nonempty set of positive integers has a least element. This allows us to use algorithms like the Euclidean algorithm to find gcd
Well-ordering
Modular Arithmetic

References

[1] David Burton, *Elementary Number Theory*, 7th edition.