Introduction to Number Theory

Number Theory is the branch of mathematics that studies the properties of the integers.

For example: prime numbers, Fibonacci numbers, continued fractions, ...

We'll discuss some of these properties of integers, and then apply them to the Fibonacci numbers.

Introduction to Number Theory

The first property we'll discuss is **divisibility**.

We know:

$$3 \cdot 5 = 15$$

We say that the number 15 is the **product** of the **factors** 3 and 5.

In particular, **3 is a factor of 15**. We write this as:

$$3 \mid 15$$

We say that "**3 divides 15**"

Introduction to Number Theory

So, the notation

$$x \mid y$$

means that "x divides y."

But more specifically, it means there is another integer k so that

$$x \cdot k = y.$$

Remember: $3 \mid 15$, so what is k?

$$3 \cdot 5 = 15, \quad \text{so} \quad k = 5.$$

$x \mid y$ means $x \cdot k = y$ for some integer k.

True/False:

1. $4 \mid 20$ — TRUE, since $4 \cdot 5 = 20$
2. $3 \mid 46$ — FALSE, since $3 \cdot 15 = 45$ and $3 \cdot 16 = 48$
3. $17 \mid 17$ — TRUE, since $17 \cdot 1 = 17$
4. $12 \mid 6$ — FALSE, since $12 \cdot \frac{1}{2} = 6$ but $\frac{1}{2}$ is NOT an integer.
5. $5 \mid 137,560$ — TRUE, since ???

Some properties of divisibility

NOTE:

- In order for $x \mid y$, then it must be true that $x \leq y$.
- For any number x, $1 \mid x$.
- For any number x, $x \mid x$.

We call 1 and x the **trivial divisors** of x, and usually ignore these when talking about divisors.

Some properties of divisibility

Suppose we know that x, y and z are three numbers so that

$$x \mid y \quad \text{and} \quad y \mid z.$$

Is it true that $x \mid z$??

Example:

$$4 \mid 12 \quad \text{and} \quad 12 \mid 24$$

Is it true that $4 \mid 24$?? YES! (Since $4 \cdot 6 = 24$).

Some properties of divisibility

Theorem

Suppose we know that x, y and z are three numbers so that

$$x \mid y \quad \text{and} \quad y \mid z.$$

Then it is also true that $x \mid z$.

Some properties of divisibility

Suppose we know that x is a number that divides both y and z:

$$x \mid y \quad \text{and} \quad x \mid z.$$

Is it true that $x \mid y + z$??

Example:

$$7 \mid 21 \quad \text{and} \quad 7 \mid 35$$

Is it true that $7 \mid 56$?? YES! (Since $7 \cdot 8 = 56$).

Some properties of divisibility

Theorem

Suppose we know that x, y and z are three numbers so that

$$x \mid y \quad \text{and} \quad x \mid z.$$

Then it is also true that $x \mid y + z$.

Divisibility of the Fibonacci numbers

Recall the Fibonacci numbers:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots$$

Some of them are even. That is, some are divisible by 2:

$$2 \mid 2 \qquad 2 \mid 8 \qquad 2 \mid 34 \qquad 2 \mid 144 \qquad 2 \mid 610 \ldots$$

Divisibility of the Fibonacci numbers

Recall the Fibonacci numbers:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots$$

Some of them are even. That is, some are divisible by 2:

$$2 \mid 2 \qquad 2 \mid 8 \qquad 2 \mid 34 \qquad 2 \mid 144 \qquad 2 \mid 610 \ldots$$

Divisibility of the Fibonacci numbers

Two divides every third Fibonacci number!!

But 2 is the third Fibonacci number!!

So, every third Fibonacci number is divisible by the third Fibonacci number (2).

Theorem

If $3 \mid n$, *then* $F_3 \mid F_n$.

Divisibility of the Fibonacci numbers

Recall the Fibonacci numbers:

$$\ldots, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584,$$

$$4181, 6765, 10946, 17711, \ldots$$

Some of them are divisible by three.

$$3 \mid 3 \qquad 3 \mid 21 \qquad 3 \mid 144 \qquad 3 \mid 987 \qquad 3 \mid 6765\ldots$$

Divisibility of the Fibonacci numbers

Recall the Fibonacci numbers:

$$\ldots, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584,$$

$$4181, 6765, 10946, 17711, \ldots$$

Some of them are divisible by three.

$$3 \mid 3 \qquad 3 \mid 21 \qquad 3 \mid 144 \qquad 3 \mid 987 \qquad 3 \mid 6765 \ldots$$

Divisibility of the Fibonacci numbers

Three divides every fourth Fibonacci number!!

But 3 is the fourth Fibonacci number!!

So, every fourth Fibonacci number is divisible by the fourth Fibonacci number (3).

Theorem

If $4 \mid n$, *then* $F_4 \mid F_n$.

Divisibility of the Fibonacci numbers

Recall the Fibonacci numbers:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584,$$

$$4181, 6765, 10946, 17711, \ldots$$

Some of them are divisible by 5:

$$5 \mid 5 \qquad 5 \mid 55 \qquad 5 \mid 610 \qquad 5 \mid 6765 \ldots$$

Divisibility of the Fibonacci numbers

Recall the Fibonacci numbers:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584,$$

$$4181, 6765, 10946, 17711, \ldots$$

Some of them are divisible by 5:

$$5 \mid 5 \qquad 5 \mid 55 \qquad 5 \mid 610 \qquad 5 \mid 6765 \ldots$$

Divisibility of the Fibonacci numbers

Five divides every fifth Fibonacci number!!

But 5 happens to be the fifth Fibonacci number!!

So, every fifth Fibonacci number is divisible by the fifth Fibonacci number (5).

Theorem

If $5 \mid n$, *then* $F_5 \mid F_n$.

Divisibility of the Fibonacci numbers

Recall the Fibonacci numbers:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584,$$

$$4181, 6765, 10946, 17711, 28657, 46368, \ldots$$

Some of them are divisible by 8:

$$8 \mid 8 \qquad 8 \mid 144 \qquad 8 \mid 2584 \qquad 8 \mid 46368 \ldots$$

Divisibility of the Fibonacci numbers

Recall the Fibonacci numbers:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584,$$

$$4181, 6765, 10946, 17711, 28657, 46368, \ldots$$

Some of them are divisible by 8:

$$8 \mid 8 \qquad 8 \mid 144 \qquad 8 \mid 2584 \qquad 8 \mid 46368 \ldots$$

Divisibility of the Fibonacci numbers

Eight divides every sixth Fibonacci number!!

But 8 happens to be the sixth Fibonacci number!!

So, every sixth Fibonacci number is divisible by the sixth Fibonacci number (8).

Theorem

If $6 \mid n$, *then* $F_6 \mid F_n$.

Divisibility of the Fibonacci numbers

This is actually true for all positive integers k:

Theorem

If $k \mid n$, *then* $F_k \mid F_n$.

Example:

$$F_{27} = 196,418$$

Since $9 \mid 27$, then $F_9 \mid F_{27}$.

That is, $34 \mid 196,418$.

Divisibility of the Fibonacci numbers

Theorem

If $k \mid n$, *then* $F_k \mid F_n$.

Example:

$$F_{46} = 1,836,311,903$$

Since $23 \mid 46$, then $F_{23} \mid F_{46}$.

That is, $28,657 \mid 1,836,311,903$

Divisibility of the Fibonacci numbers

Example: Find seven factors of $F_{48} = 4,807,526,976$.

Since 2, 3, 4, 6, 8, 12, 16, 24 all divide 48, then

$$F_2 = 1 \qquad F_3 = 2$$

$$F_4 = 3 \qquad F_6 = 8$$

$$F_8 = 21 \qquad F_{12} = 144$$

$$F_{16} = 987 \qquad F_{24} = 46368$$

All of these Fibonacci numbers must divide F_{48} !!

Introduction to Number Theory

We've talked about the **divisors** of an integer:

x **is a divisor of** y if there is an integer k so that

$$x \cdot k = y$$

Shorthand notation:

$$x \mid y.$$

Introduction to Number Theory

We can list several divisors of any positive integer:

$$36 = 4 \cdot 9$$

$$36 = 6 \cdot 6$$

$$36 = 2 \cdot 18$$

$$36 = 2 \cdot 2 \cdot 3 \cdot 3$$

Which is better?

Introduction to Number Theory

If we just want to find any two divisors, there may be many ways to do so.

We'd like to be able to find a list of divisors in such a way that the same list is always found.

Instead of looking for any divisors, let's agree to find all prime divisors of a number.

Introduction to Number Theory

Example:

$$120 = 12 \cdot 10 = 3 \cdot 4 \cdot 2 \cdot 5 = 3 \cdot 2 \cdot 2 \cdot 2 \cdot 5$$

Or,

$$120 = 2 \cdot 60 = 2 \cdot 6 \cdot 10 = 2 \cdot 2 \cdot 3 \cdot 2 \cdot 5$$

We get the same **prime factors**, even though we didn't start with the same initial pair of divisors.

Introduction to Number Theory

In fact, this will always be true !!

Theorem (The Fundamental Theorem of Arithmetic)

Every positive integer can be written in a unique way as the product of prime divisors.

Introduction to Number Theory

So, suppose we take any (large) integer.

No matter how we start, we will always end up with the same list of prime divisors that multiply to that large number.

Example:

$$6765 = 5 \cdot 1353 = 5 \cdot 3 \cdot 451 = 3 \cdot 5 \cdot 11 \cdot 41$$

Introduction to Number Theory

Example:

$$18,200 = 182 \cdot 100 = 2 \cdot 91 \cdot 10 \cdot 10 = 2 \cdot 7 \cdot 13 \cdot 2 \cdot 5 \cdot 2 \cdot 5$$

There's a better way to keep track of these...

$$18,200 = 2^3 \cdot 5^2 \cdot 7 \cdot 13$$

Let's always agree to write the **prime factorization** in order of lowest primes to highest primes.

A "new" property of integers.

We know how to find the divisors of any number.

If we're given two numbers, there will be divisors that are common to both numbers.

For example, 24 and 28 have common divisors of 2, 4.

4 is the largest number that is a divisor of both 24 and 28.

A "new" property of integers.

Definition

For any two integers x and y, the **greatest common divisor** is the largest number that is a divisor of both x and y.

Example: the greatest common divisor of 24 and 28 is 4.

Notation:

$$\gcd(24, 28) = 4$$

A "new" property of integers.

Finding the gcd is not always this easy, though.

But, we have steps to follow in order find it:

1. List the prime factors of each number.
2. Then list all prime factors that are common to each number.
3. The product of these common prime factors is the greatest common divisor.

A "new" property of integers.

Example: Find $\gcd(1540, 18200)$.

$$1540 = 154 \cdot 10 = 11 \cdot 14 \cdot 2 \cdot 5 = 11 \cdot 2 \cdot 7 \cdot 2 \cdot 5$$

$$1540 = 2^2 \cdot 5 \cdot 7 \cdot 11$$

$$18,200 = 2^3 \cdot 5^2 \cdot 7 \cdot 13$$

Common factors: $2 \cdot 2 \cdot 5 \cdot 7 = 140$

Therefore,

$$\gcd(1540, 18200) = 140.$$

A "new" property of integers.

Example: Find $\gcd(231, 260)$.

$$231 = 3 \cdot 7 \cdot 11$$

$$260 = 2^2 \cdot 5 \cdot 13$$

Common factors: none! (Not true: 1 is always a common factor)

Therefore,

$$\gcd(231, 260) = 1.$$

We say that 231 and 260 are **relatively prime**, since the greatest common divisor is 1.

A "new" property of integers.

Definition

Two numbers x and y are **relatively prime** if $\gcd(x, y) = 1$.

An interesting fact:

Theorem

Consecutive Fibonacci numbers are relatively prime.

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots$$

$\gcd(F_n, F_m) = ???.$

Speaking of Fibonacci numbers....

Let's take two Fibonacci numbers and find their g.c.d.

$$F_{12} = 144 \quad \text{and} \quad F_{15} = 610$$

$$144 = 12 \cdot 12 = 2^4 \cdot 3^2 \qquad 610 = 2 \cdot 5 \cdot 61$$

$$\gcd(F_{12}, F_{15}) = \gcd(144, 610) = 2$$

$\gcd(F_n, F_m) = ???.$

Let's take two more Fibonacci numbers and find their g.c.d.

$$F_{20} = 6765 \quad \text{and} \quad F_{25} = 75025$$

$$6765 = 3 \cdot 5 \cdot 11 \cdot 41 \qquad 75025 = 5^2 \cdot 3001$$

$$\gcd(F_{20}, F_{25}) = \gcd(6765, 75025) = 5$$

$\gcd(F_n, F_m) = ???.$

Let's take another pair of Fibonacci numbers and find their g.c.d.

$$F_{21} = 10946 \quad \text{and} \quad F_{28} = 317811$$

$$10946 = 2 \cdot 13 \cdot 421 \qquad 317811 = 3 \cdot 13 \cdot 29 \cdot 281$$

$$\gcd(F_{21}, F_{28}) = \gcd(10946, 317811) = 13$$

$\gcd(F_n, F_m) = ???.$

Let's take one more pair of Fibonacci numbers and find their g.c.d.

$$F_{13} = 233 \quad \text{and} \quad F_{26} = 121393$$

$$233 \text{ is prime;} \qquad 121393 = 233 \cdot 521$$

$$\gcd(F_{13}, F_{26}) = \gcd(233, 121393) = 233$$

$\gcd(F_n, F_m) = ???.$

Our examples so far:

$$\gcd(F_{12}, F_{15}) = \gcd(144, 610) = 2 = F_3 = F_{\gcd(12,15)}$$

$$\gcd(F_{20}, F_{25}) = \gcd(6765, 75025) = 5 = F_5 = F_{\gcd(20,25)}$$

$$\gcd(F_{21}, F_{28}) = \gcd(10946, 317811) = 13 = F_7 = F_{\gcd(21,28)}$$

$$\gcd(F_{13}, F_{26}) = \gcd(233, 121393) = 233 = F_{13} = F_{\gcd(13,26)}$$

Is there a pattern?

Theorem

The greatest common divisor of two Fibonacci numbers is another Fibonacci number. In particular,

$$\gcd(F_n, F_m) = F_{\gcd(m,n)}$$

Example:

$$\gcd(102334155, 832040) = \gcd(F_{40}, F_{30}) = F_{\gcd(30,40)} = F_{10} = 55$$

Theorem

The greatest common divisor of two Fibonacci numbers is another Fibonacci number. In particular,

$$\gcd(F_n, F_m) = F_{\gcd(m,n)}$$

Example:

$$\gcd(6765, 46368) = \gcd(F_{20}, F_{24}) = F_{\gcd(20,24)} = F_4 = 3$$

What we've seen today:

Theorem

If $k \mid n$, *then* $F_k \mid F_n$.

Theorem

The greatest common divisor of two Fibonacci numbers is another Fibonacci number. In particular,

$$\gcd(F_n, F_m) = F_{\gcd(m,n)}$$