Multiplicative Functions

Lecture 5

Justin Stevens

Outline

Fibonacci Numbers

The Fibonacci numbers show up in many unexpected situations and have many beautiful properties. We present a motivating example:

Example 1. Consider a board of length n. How many ways are there to tile this board with squares (length 1) and dominos (length 2)?

Let the number of tilings of an n-board be $f(n)$. We calculate $f(4)$:

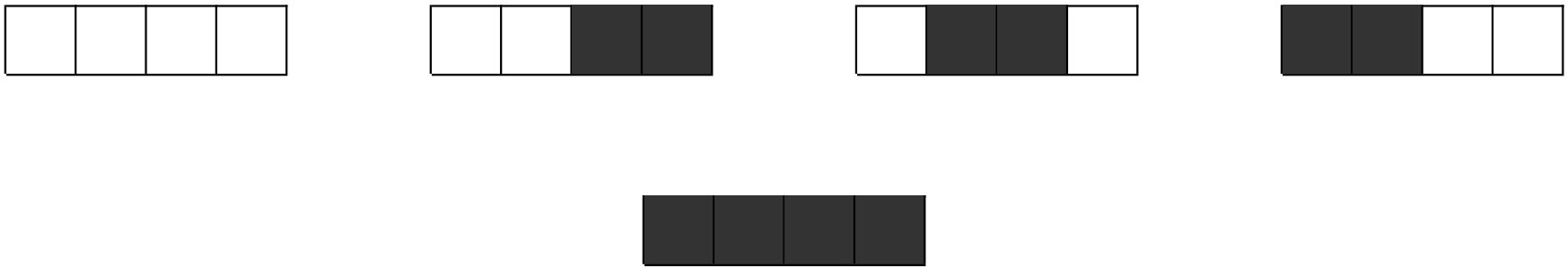


Table 1: The five tilings of a 4-board

Hence $f(4) = 5$. For larger values of n, we need a different strategy.

Fibonacci Numbers 2

Observe that if an n-board begins with a square, then we have to tile an $n-1$ board. However, if the n-board begins with a domino, then we have to tile an $n-2$ board. Therefore,

$$f(n) = f(n-1) + f(n-2).$$

We see that $f(1) = 1$ and $f(2) = 2$, therefore we can compute:

$$\begin{aligned} f(3) &= f(2) + f(1) = 2 + 1 = 3 \\ f(4) &= f(3) + f(2) = 3 + 2 = 5 \\ f(5) &= f(4) + f(3) = 5 + 3 = 8. \end{aligned}$$

The only difference between this and the Fibonacci numbers are that the latter begins with an extra 1. Therefore, $f(n) = \boxed{F_{n+1}}$. Using this n-tiling, we can prove several identities regarding Fibonacci numbers.

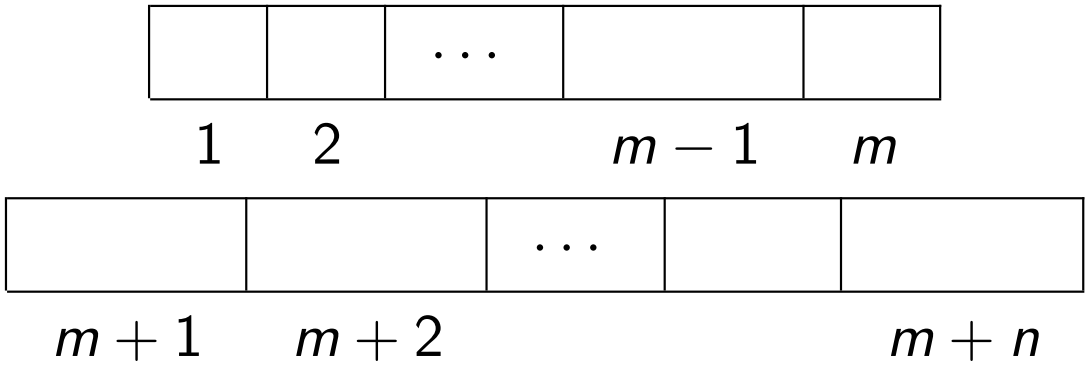
Property

Example 2. Show that $f(m+n) = f(m)f(n) + f(m-1)f(n-1)$.

The left-hand side is simply the number of tilings of an $(m+n)$-board.

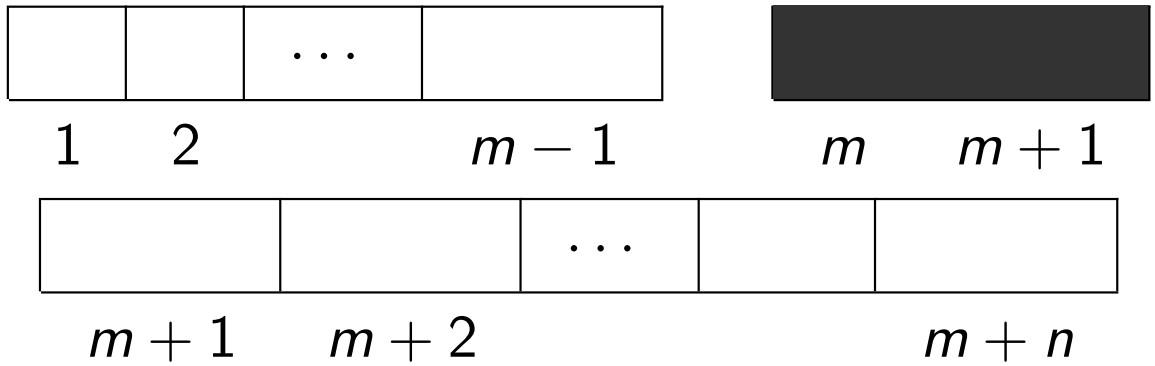
For the right-hand side, we have two cases:

- If there is no domino at square m, we have $f(m)f(n)$ tilings:



Sum Property

- If there is a domino at square m, we have $f(m-1)f(n-1)$ tilings:



Hence, $f(m+n) = f(m)f(n) + f(m-1)f(n-1)$.

Substituting $m = a$ and $n = b-1$ gives the Fibonacci identity

$$F_{a+b} = F_{a+1}F_b + F_aF_{b-1}.$$

Other Properties

The below properties can all be proved using the tiling method:

- $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$.
- $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$.
- $F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_n F_{n+1}$.
- $F_{n+1} = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots$.

Try them out yourself!

Fibonacci Divisibility

Example. Prove that $F_m \mid F_{mq}$ for all natural q.

We use induction. For $q = 1$, $F_m \mid F_m$. For $q = 2$,

$$F_{2m} = F_{m+1}F_m + F_mF_{m-1}.$$

Fibonacci Divisibility

Example. Prove that $F_m \mid F_{mq}$ for all natural q.

We use induction. For $q = 1$, $F_m \mid F_m$. For $q = 2$,

$$F_{2m} = F_{m+1}F_m + F_mF_{m-1}.$$

Suppose the statement is true for $q = k$, implying that $F_m \mid F_{mk}$.

Fibonacci Divisibility

Example. Prove that $F_m \mid F_{mq}$ for all natural q.

We use induction. For $q = 1$, $F_m \mid F_m$. For $q = 2$,

$$F_{2m} = F_{m+1}F_m + F_mF_{m-1}.$$

Suppose the statement is true for $q = k$, implying that $F_m \mid F_{mk}$. We show it holds for $q = k + 1$. From the identity with $a = mk$ and $b = m$,

$$F_{mk+m} = F_{mk+1}F_m + F_{mk}F_{m-1}.$$

Fibonacci Divisibility

Example. Prove that $F_m \mid F_{mq}$ for all natural q.

We use induction. For $q = 1$, $F_m \mid F_m$. For $q = 2$,

$$F_{2m} = F_{m+1}F_m + F_mF_{m-1}.$$

Suppose the statement is true for $q = k$, implying that $F_m \mid F_{mk}$. We show it holds for $q = k + 1$. From the identity with $a = mk$ and $b = m$,

$$F_{mk+m} = F_{mk+1}F_m + F_{mk}F_{m-1}.$$

Since $F_m \mid F_{mk}$ (hypothesis), $F_m \mid F_{mk+m}$ by the linear combination theorem. Hence, the statement is proven for $q = k + 1$.

Fibonacci GCD 1

Example. Show that consecutive Fibonacci numbers are relatively prime.

Fibonacci GCD

Example. Show that $\gcd(F_n, F_m) = F_{\gcd(n,m)}$.

Write $n = mq + r$ using the division algorithm. Using the Fibonacci identity,

Fibonacci GCD

Example. Show that $\gcd(F_n, F_m) = F_{\gcd(n,m)}$.

Write $n = mq + r$ using the division algorithm. Using the Fibonacci identity,

$$F_n = F_{mq+r} = F_{mq+1}F_r + F_{mq}F_{r_1}.$$

Fibonacci GCD

Example. Show that $\gcd(F_n, F_m) = F_{\gcd(n,m)}$.

Write $n = mq + r$ using the division algorithm. Using the Fibonacci identity,

$$F_n = F_{mq+r} = F_{mq+1}F_r + F_{mq}F_{r_1}.$$

Since $F_m \mid F_{mq}$, we can subtract multiples of F_m using Euclidean algorithm:

$$\gcd(F_n, F_m) = \gcd(F_{mq+1}F_r + F_{mq}F_{r-1}, F_m) = \gcd(F_{mq+1}F_r, F_m).$$

Fibonacci GCD

Example. Show that $\gcd(F_n, F_m) = F_{\gcd(n,m)}$.

Write $n = mq + r$ using the division algorithm. Using the Fibonacci identity,

$$F_n = F_{mq+r} = F_{mq+1}F_r + F_{mq}F_{r_1}.$$

Since $F_m \mid F_{mq}$, we can subtract multiples of F_m using Euclidean algorithm:

$$\gcd(F_n, F_m) = \gcd(F_{mq+1}F_r + F_{mq}F_{r-1}, F_m) = \gcd(F_{mq+1}F_r, F_m).$$

Finally, $\gcd(F_{mq+1}, F_m) = 1$ since consecutive Fibonacci numbers are relatively prime:

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

Fibonacci GCD

Example. Show that $\gcd(F_n, F_m) = F_{\gcd(n,m)}$.

Write $n = mq + r$ using the division algorithm. Using the Fibonacci identity,

$$F_n = F_{mq+r} = F_{mq+1}F_r + F_{mq}F_{r_1}.$$

Since $F_m \mid F_{mq}$, we can subtract multiples of F_m using Euclidean algorithm:

$$\gcd(F_n, F_m) = \gcd(F_{mq+1}F_r + F_{mq}F_{r-1}, F_m) = \gcd(F_{mq+1}F_r, F_m).$$

Finally, $\gcd(F_{mq+1}, F_m) = 1$ since consecutive Fibonacci numbers are relatively prime:

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

For example, if $n = 182$ and $m = 65$, $\gcd(182, 65) = 13$ and

$$\gcd(F_{182}, F_{65}) = \gcd(F_{65}, F_{52}) = \gcd(F_{52}, F_{13}) = F_{13}.$$

Fibonacci GCD

Example. Show that $\gcd(F_n, F_m) = F_{\gcd(n,m)}$.

Write $n = mq + r$ using the division algorithm. Using the Fibonacci identity,

$$F_n = F_{mq+r} = F_{mq+1}F_r + F_{mq}F_{r_1}.$$

Since $F_m \mid F_{mq}$, we can subtract multiples of F_m using Euclidean algorithm:

$$\gcd(F_n, F_m) = \gcd(F_{mq+1}F_r + F_{mq}F_{r-1}, F_m) = \gcd(F_{mq+1}F_r, F_m).$$

Finally, $\gcd(F_{mq+1}, F_m) = 1$ since consecutive Fibonacci numbers are relatively prime:

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

For example, if $n = 182$ and $m = 65$, $\gcd(182, 65) = 13$ and

$$\gcd(F_{182}, F_{65}) = \gcd(F_{65}, F_{52}) = \gcd(F_{52}, F_{13}) = F_{13}.$$

The conclusion is equivalent to $\gcd(F_n, F_m) = F_{\gcd(n,m)}$.

Outline

Modular Inverses

Theorem. Prove that the inverse of a mod m exists iff $\gcd(a, m) = 1$.

Modular Inverses

Theorem. Prove that the inverse of a mod m exists iff $\gcd(a, m) = 1$.

Proof.

By Bezout's theorem, there exists integers x and y such that

$$ax + my = 1$$

if and only if $\gcd(a, m) = 1$.

Modular Inverses

Theorem. Prove that the inverse of a mod m exists iff $\gcd(a, m) = 1$.

Proof.

By Bezout's theorem, there exists integers x and y such that

$$ax + my = 1$$

if and only if $\gcd(a, m) = 1$. Taking this equation mod m, we see that $ax \equiv 1 \pmod{m}$. □

Method

Example 3. Solve $39x \equiv 1 \mod 100$ by finding integers satisfying $39x_0 + 100y_0 = 1$.

Method

Example 4. Solve $39x \equiv 1 \mod 100$ by finding integers satisfying $39x_0 + 100y_0 = 1$.

Solution. We use the Euclidean algorithm:

$$\begin{aligned}
100 &= 39 \cdot 2 + 22 && 1 = 16 \cdot \underline{100} - 41 \cdot \underline{39} && \uparrow \\
39 &= 22 \cdot 1 + 17 && 1 = -9 \cdot \underline{39} + 16 \cdot \underline{22} && \uparrow \\
22 &= 17 \cdot 1 + 5 && 1 = 7 \cdot \underline{22} - 9 \cdot \underline{17} && \uparrow \\
17 &= 5 \cdot 3 + 2 && 1 = -2 \cdot \underline{17} + 7 \cdot \underline{5} && \uparrow \\
5 &= 2 \cdot 2 + 1 \quad \Longrightarrow && 1 = \underline{5} - 2 \cdot \underline{2} && \uparrow
\end{aligned}$$

Therefore $(x_0, y_0) = (-41, 16)$, hence $x \equiv -41 \equiv \mathbf{59} \pmod{100}$.

Method

Example 5. Solve $39x \equiv 1 \mod 100$ by finding integers satisfying $39x_0 + 100y_0 = 1$.

Solution. We use the Euclidean algorithm:

$$\begin{aligned}
100 &= 39 \cdot 2 + 22 && 1 = 16 \cdot \underline{100} - 41 \cdot \underline{39} && \uparrow \\
39 &= 22 \cdot 1 + 17 && 1 = -9 \cdot \underline{39} + 16 \cdot \underline{22} && \uparrow \\
22 &= 17 \cdot 1 + 5 && 1 = 7 \cdot \underline{22} - 9 \cdot \underline{17} && \uparrow \\
17 &= 5 \cdot 3 + 2 && 1 = -2 \cdot \underline{17} + 7 \cdot \underline{5} && \uparrow \\
5 &= 2 \cdot 2 + 1 \quad \Longrightarrow && 1 = \underline{5} - 2 \cdot \underline{2} && \uparrow
\end{aligned}$$

Therefore $(x_0, y_0) = (-41, 16)$, hence $x \equiv -41 \equiv \mathbf{59} \pmod{100}$. Observe the pair $(59, -23)$ also satisfies the equation. This hints at a general solution.

Linear Diophantine Equations

Theorem. For coprime a and b, all integer solutions to $ax + by = c$ are

$$(x, y) = (x_0 + bk, y_0 - ak),\ k \in \mathbb{Z},$$

where (x_0, y_0) is a particular solution.

Linear Diophantine Equations

Theorem. For coprime a and b, all integer solutions to $ax + by = c$ are

$$(x, y) = (x_0 + bk, y_0 - ak),\ k \in \mathbb{Z},$$

where (x_0, y_0) is a particular solution.

All integer solutions of $2x + 5y = 1$ are $(x, y) = (-2 + 5k, 1 - 2k)$.

Solving Linear Congruences

Example. Solve the linear congruence $7x \equiv 3 \pmod{34}$.

Solving Linear Congruences

Example. Solve the linear congruence $7x \equiv 3 \pmod{34}$.
We begin by observing that $7^{-1} \equiv 5 \pmod{34}$. Muliplying by 3:

$$x \equiv 3 \cdot 7^{-1} \equiv 3 \cdot 5 \equiv \mathbf{15} \pmod{34}.$$

Corollary. The congruence $ax \equiv c \mod m$ is solved by

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

for $\gcd(a, m) = 1$.

Cancellation Law

Theorem. Prove that if $ca \equiv cb \pmod{m}$, then $a \equiv b \pmod{m/d}$, where $d = \gcd(c, m)$.

We begin by observing that by the definition of modulos,

$$ca \equiv cb \pmod{m} \iff m \mid ca - cb \iff c(a - b) = mk.$$

Cancellation Law

Theorem. Prove that if $ca \equiv cb \pmod{m}$, then $a \equiv b \pmod{m/d}$, where $d = \gcd(c, m)$.
We begin by observing that by the definition of modulos,

$$ca \equiv cb \pmod{m} \iff m \mid ca - cb \iff c(a - b) = mk.$$

Since $d = \gcd(c, m)$, we write $c = dr$ and $m = ds$ where $\gcd(r, s) = 1$:

Cancellation Law

Theorem. Prove that if $ca \equiv cb \pmod{m}$, then $a \equiv b \pmod{m/d}$, where $d = \gcd(c, m)$.
We begin by observing that by the definition of modulos,

$$ca \equiv cb \pmod{m} \iff m \mid ca - cb \iff c(a - b) = mk.$$

Since $d = \gcd(c, m)$, we write $c = dr$ and $m = ds$ where $\gcd(r, s) = 1$:

$$dr(a - b) = dsk \iff r(a - b) = sk.$$

Cancellation Law

Theorem. Prove that if $ca \equiv cb \pmod{m}$, then $a \equiv b \pmod{m/d}$, where $d = \gcd(c, m)$.
We begin by observing that by the definition of modulos,

$$ca \equiv cb \pmod{m} \iff m \mid ca - cb \iff c(a - b) = mk.$$

Since $d = \gcd(c, m)$, we write $c = dr$ and $m = ds$ where $\gcd(r, s) = 1$:

$$dr(a - b) = dsk \iff r(a - b) = sk.$$

Therefore, $s \mid r(a - b)$. By Euclid's Lemma, since $s \mid a - b$.

Cancellation Law

Theorem. Prove that if $ca \equiv cb \pmod{m}$, then $a \equiv b \pmod{m/d}$, where $d = \gcd(c, m)$.
We begin by observing that by the definition of modulos,

$$ca \equiv cb \pmod{m} \iff m \mid ca - cb \iff c(a - b) = mk.$$

Since $d = \gcd(c, m)$, we write $c = dr$ and $m = ds$ where $\gcd(r, s) = 1$:

$$dr(a - b) = dsk \iff r(a - b) = sk.$$

Therefore, $s \mid r(a - b)$. By Euclid's Lemma, since $s \mid a - b$.

For instance, $3x \equiv 3 \pmod{9} \implies x \equiv 1 \pmod{3}$.

No Solutions

Example. Show that the congruence $5x \equiv 3 \pmod{10}$ has no solutions.

No Solutions

Example. Show that the congruence $5x \equiv 3 \pmod{10}$ has no solutions. From the definition of modulos, we see that

$$5x \equiv 3 \pmod{10} \iff 10 \mid 5x - 3 \iff 5x - 3 = 10y$$

for some integer y. However, this implies that $5(x - 2y) = 3$, contradiction.

No Solutions

Example. Show that the congruence $5x \equiv 3 \pmod{10}$ has no solutions. From the definition of modulos, we see that

$$5x \equiv 3 \pmod{10} \iff 10 \mid 5x - 3 \iff 5x - 3 = 10y$$

for some integer y. However, this implies that $5(x - 2y) = 3$, contradiction.

Theorem. $ax \equiv c \mod m$ has solutions if and only if $\gcd(a, m) \mid c$.

Proof of Linear Congruence Theorem

Theorem. $ax \equiv c \mod m$ has solutions if and only if $\gcd(a, m) \mid c$.

Proof of Linear Congruence Theorem

Theorem. $ax \equiv c \mod m$ has solutions if and only if $\gcd(a, m) \mid c$.

Assume that the congruence has solutions. Then, observe that

$$ax \equiv c \pmod{m} \iff m \mid ax - c \iff ax - c = my.$$

Proof of Linear Congruence Theorem

Theorem. $ax \equiv c \mod m$ has solutions if and only if $\gcd(a, m) \mid c$.

Assume that the congruence has solutions. Then, observe that

$$ax \equiv c \pmod{m} \iff m \mid ax - c \iff ax - c = my.$$

Since $\gcd(a, m) \mid a$ and $\gcd(a, m) \mid m$, we must have $\gcd(a, m) \mid b$.

Proof of Linear Congruence Theorem

Theorem. $ax \equiv c \mod m$ has solutions if and only if $\gcd(a, m) \mid c$.

Assume that the congruence has solutions. Then, observe that

$$ax \equiv c \pmod{m} \iff m \mid ax - c \iff ax - c = my.$$

Since $\gcd(a, m) \mid a$ and $\gcd(a, m) \mid m$, we must have $\gcd(a, m) \mid b$.

We now show that if $\gcd(a, m) \mid b$, then there are solutions. Let $d = \gcd(a, m)$, therefore, there exists relatively prime integers a_1 and m_1 such that $a = da_1$ and $m = dm_1$.

Proof of Linear Congruence Theorem

Theorem. $ax \equiv c \pmod{m}$ has solutions if and only if $\gcd(a, m) \mid c$.

Assume that the congruence has solutions. Then, observe that

$$ax \equiv c \pmod{m} \iff m \mid ax - c \iff ax - c = my.$$

Since $\gcd(a, m) \mid a$ and $\gcd(a, m) \mid m$, we must have $\gcd(a, m) \mid b$.

We now show that if $\gcd(a, m) \mid b$, then there are solutions. Let $d = \gcd(a, m)$, therefore, there exists relatively prime integers a_1 and m_1 such that $a = da_1$ and $m = dm_1$. Furthermore, since $d \mid b$, there exists an integer b_1 such that $b = db_1$. We now rewrite:

$$da_1x \equiv db_1 \pmod{dm_1} \iff a_1x \equiv b_1 \pmod{m_1}.$$

Proof of Linear Congruence Theorem

Theorem. $ax \equiv c \pmod{m}$ has solutions if and only if $\gcd(a, m) \mid c$.

Assume that the congruence has solutions. Then, observe that

$$ax \equiv c \pmod{m} \iff m \mid ax - c \iff ax - c = my.$$

Since $\gcd(a, m) \mid a$ and $\gcd(a, m) \mid m$, we must have $\gcd(a, m) \mid b$.

We now show that if $\gcd(a, m) \mid b$, then there are solutions. Let $d = \gcd(a, m)$, therefore, there exists relatively prime integers a_1 and m_1 such that $a = da_1$ and $m = dm_1$. Furthermore, since $d \mid b$, there exists an integer b_1 such that $b = db_1$. We now rewrite:

$$da_1x \equiv db_1 \pmod{dm_1} \iff a_1x \equiv b_1 \pmod{m_1}.$$

This congruence has a solution, namely $x \equiv b_1 a_1^{-1} \pmod{m_1}$.

Example

Example. Find all solutions to the congruence $18x \equiv 30 \pmod{42}$.

Example

Example. Find all solutions to the congruence $18x \equiv 30 \pmod{42}$.
We can divide the congruence by $\gcd(18, 42) = 6$:

$$3x \equiv 5 \pmod{7}.$$

Example

Example. Find all solutions to the congruence $18x \equiv 30 \pmod{42}$.
We can divide the congruence by $\gcd(18, 42) = 6$:

$$3x \equiv 5 \pmod{7}.$$

Listing numbers that are 5 mod 7, namely $5, \mathbf{12}, 19$, $x \equiv 4 \pmod{7}$:

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}.$$

Example

Example. Find all solutions to the congruence $18x \equiv 30 \pmod{42}$.
We can divide the congruence by $\gcd(18, 42) = 6$:

$$3x \equiv 5 \pmod{7}.$$

Listing numbers that are 5 mod 7, namely $5, \mathbf{12}, 19$, $x \equiv 4 \pmod{7}$:

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}.$$

Wrapping Up

Theorem. For integers a and b, let $d = \gcd(a, b)$. If (x_0, y_0) is a particular solution of the Diophantine equation $ax + by = c$, then the general solution is given by

$$(x, y) = (x_0 + \frac{b}{d} \cdot k, y_0 - \frac{a}{d} \cdot k),\ k \in \mathbb{Z}.$$

Corollary. The linear congruence $ax \equiv c \pmod{m}$ has $d = \gcd(a, m)$ mutually incongruent solutions if $d \mid c$.

Chicken Mcnugget Theorem

Definition. Let $a_1, a_2, \cdots, a_n$ be relatively prime positive integers. Consider the set

$$S = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n,\ x_i \geq 0\}.$$

The largest positive integer that is non-representable is called the *Frobenius number* of the set and is denoted $g(a_1, a_2, \cdots, a_n)$.

Chicken Mcnugget Theorem

Definition. Let $a_1, a_2, \cdots, a_n$ be relatively prime positive integers. Consider the set

$$S = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n,\ x_i \geq 0\}.$$

The largest positive integer that is non-representable is called the *Frobenius number* of the set and is denoted $g(a_1, a_2, \cdots, a_n)$.

Observe that if the restriction $x_i \geq 0$ was not in place, then S would simply contain multiples of $\gcd(a_1, a_2, \cdots, a_n)$ by generalized Bezout's theorem. Furthermore, if the numbers $a_1, a_2, \cdots, a_n$ are not relatively prime, then the answer is infinity.

Chicken Mcnugget Theorem

Definition. Let $a_1, a_2, \cdots, a_n$ be relatively prime positive integers. Consider the set

$$S = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n,\ x_i \geq 0\}.$$

The largest positive integer that is non-representable is called the *Frobenius number* of the set and is denoted $g(a_1, a_2, \cdots, a_n)$.

Observe that if the restriction $x_i \geq 0$ was not in place, then S would simply contain multiples of $\gcd(a_1, a_2, \cdots, a_n)$ by generalized Bezout's theorem. Furthermore, if the numbers $a_1, a_2, \cdots, a_n$ are not relatively prime, then the answer is infinity.

Theorem. For relatively prime positive integers a and b,

$$g(a, b) = ab - a - b.$$

Proof Part 1

Theorem. For coprime a and b, $g(a, b) = ab - a - b$.

Proof Part 1

Theorem. For coprime a and b, $g(a, b) = ab - a - b$.

For the sake of contradiction, assume that for nonnegative integers x and y,

$$ab - a - b = ax + by.$$

Proof Part 1

Theorem. For coprime a and b, $g(a, b) = ab - a - b$.

For the sake of contradiction, assume that for nonnegative integers x and y,

$$ab - a - b = ax + by.$$

Taking mod a gives $by \equiv -b \pmod{a} \implies y \equiv -1 \pmod{a}$.

Proof Part 1

Theorem. For coprime a and b, $g(a, b) = ab - a - b$.

For the sake of contradiction, assume that for nonnegative integers x and y,

$$ab - a - b = ax + by.$$

Taking mod a gives $by \equiv -b \pmod{a} \implies y \equiv -1 \pmod{a}$. Similarly, $ax \equiv -a \pmod{b} \implies x \equiv -1 \pmod{b}$.

Proof Part 1

Theorem. For coprime a and b, $g(a, b) = ab - a - b$.

For the sake of contradiction, assume that for nonnegative integers x and y,

$$ab - a - b = ax + by.$$

Taking mod a gives $by \equiv -b \pmod{a} \implies y \equiv -1 \pmod{a}$. Similarly, $ax \equiv -a \pmod{b} \implies x \equiv -1 \pmod{b}$. We see that

$$ax + by \geq a(b-1) + b(a-1) = 2ab - a - b > ab - a - b.$$

Therefore, $ab - a - b$ is non-representable, and $g(a, b) \geq ab - a - b$.

Proof Part 2

Theorem. For coprime a and b, $g(a, b) = ab - a - b$.

Take any number $M > ab - a - b$ and consider $ax + by = M$. By Bezout's theorem, we know there exists integers x_0 and y_0 such that $ax_0 + by_0 = 1$.

Multiplying by M gives $aMx_0 + bMy_0 = M$. Therefore, for an integer k, the solutions to the diophantine equation are parametized by

$$(x, y) = (Mx_0 + kb, My_0 - ka).$$

We desire to find a solution such that x and y nonnegative. By the division algorithm, we can choose k such that $0 \leq x \leq b - 1$. For this specific x,

$$ax + by = M > ab - a - b \implies b(y + 1) > a(b - 1 - x) \geq 0,$$

therefore y is also nonnegative. Hence, every integer $M > ab - a - b$ is representable.

Extension

Example. There are $(a-1)(b-1)/2$ non-representable integers.

We try an example with $a = 12$ and $b = 5$.

Extension

Example. There are $(a-1)(b-1)/2$ non-representable integers.

We try an example with $a = 12$ and $b = 5$.

(0)	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

Extension

Example. There are $(a-1)(b-1)/2$ non-representable integers.

We try an example with $a = 12$ and $b = 5$.

(0)	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

Observe that all the numbers above the multiples of 5 are non-representable. For every $0 \leq j \leq a-1$, let m_j be the smallest nonnegative solution to

$$ax + j \equiv 0 \pmod{b}.$$

In the above example, $m_0 = 0, m_1 = 2$, $m_2 = 4$, $m_3 = 1$, $m_4 = 3$, and so forth. Clearly, there are m_j non-representable integers in each column.

Extension Part 2

Consider the multiples of b, $\{0, b, 2b, 3b, \cdots, (a-1)b\}$. I claim that every member of this set lies in a different column. Indeed, if for some integers s and t, $bs \equiv bt \pmod{a}$, then since $\gcd(a, b) = 1$, $s \equiv t \pmod{a}$.

Extension Part 2

Consider the multiples of b, $\{0, b, 2b, 3b, \cdots, (a-1)b\}$. I claim that every member of this set lies in a different column. Indeed, if for some integers s and t, $bs \equiv bt \pmod{a}$, then since $\gcd(a, b) = 1$, $s \equiv t \pmod{a}$.

For each m_j, let $am_j + j = bn_j$. We see that n_j takes on the values $0, 1, 2, 3, \cdots, a-1$, each exactly once. Summing over the circled numbers:

Extension Part 2

Consider the multiples of b, $\{0, b, 2b, 3b, \cdots, (a-1)b\}$. I claim that every member of this set lies in a different column. Indeed, if for some integers s and t, $bs \equiv bt \pmod{a}$, then since $\gcd(a, b) = 1$, $s \equiv t \pmod{a}$.

For each m_j, let $am_j + j = bn_j$. We see that n_j takes on the values $0, 1, 2, 3, \cdots, a-1$, each exactly once. Summing over the circled numbers:

$$\sum_{j=0}^{a-1} (am_j + j) = \sum_{j=0}^{a-1} (bn_j)$$

$$a\sum_{j=0}^{a-1} m_j + \sum_{j=0}^{a-1} j = b\sum_{j=0}^{a-1} n_j$$

$$\sum_{j=0}^{a-1} m_j = \frac{(a-1)(b-1)}{2}.$$

Since the left hand side is the number of non-representable integers, our proof is complete.

Outline

Divisors of a Number

Theorem. If $n = p_1^{k_1} p_2^{k_2} \cdots p_k^{k_r}$, then the positive divisors of n are of the form

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},\ 0 \leq a_i \leq k_i.$$

Example 6. (AIME) Compute the probability that a randomly chosen divisor of 10^{99} is an integer multiple of 10^{88}.

Solution to AIME problem

Example 7. (AIME) Compute the probability that a randomly chosen divisor of 10^{99} is an integer multiple of 10^{88}.

Solution to AIME problem

Example 8. (AIME) Compute the probability that a randomly chosen divisor of 10^{99} is an integer multiple of 10^{88}.

Solution. The divisors of $10^{99} = 2^{99} \cdot 5^{99}$ are of the form $d = 2^a \cdot 5^b$ where $0 \leq a, b \leq 99$. Hence, 10^{99} has $100 \cdot 100$ divisors. If d is a multiple of 10^{88}, then $88 \leq a, b \leq 99$. Hence, there are $12 \cdot 12$ divisors that are multiples of 10^{88}. The desired probability is $\frac{12 \cdot 12}{100 \cdot 100} = \frac{9}{625}$.

Tau and Sigma

Definition. $\tau(n)$ is the number of positive divisors of n and $\sigma(n)$ is the sum of those divisors.
For $n = 12$, $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$ and $\tau(12) = 6$.

Theorem. If $n = p_1^{k_1} p_2^{k_2} \cdots p_k^{k_r}$, then the number and sum of positive divisors of n are

$$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1).$$

$$\sigma(n) = \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1} \right) \cdots \left(\frac{p_k^{k_r+1} - 1}{p_k - 1} \right).$$

Proof of Formulas

Proof.

Let d be an arbitrary divisor of n, so $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where $0 \leq a_i \leq k_i$. For each prime, we have $k_i + 1$ choices for the exponent of p_i. Hence,

$$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1).$$

Furthermore, each divisor of n appears exactly once in the product

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}\right) \cdots$$

Therefore, applying the geometric series formula

$$1 + p_1 + p_1^2 + \cdots + p_1^{k_1} = \frac{p_1^{k_1+1} - 1}{p_1 - 1}$$

the result follows for $\sigma(n)$. □

Tau and Sigma Problems

Example 9. The cells in a jail are numbered from 1 to 100 and their doors are activated from a central button. The activation opens a closed door and closes an open door. Starting with all the doors closed the button is pressed 100 times. When it is pressed the k-th time the doors that are multiples of k are activated. Which doors are open at the end?

Example 10. Show that the product of the divisors of a number n is $n^{\tau(n)/2}$.

Jail Cell Solution

Solution. The number 100 seems arbitrary, so we try the problem for a jail with 10 cells. We create a table of which jail cells are activated each time we press the button:

Buttons \ Jail Cells	1	2	3	4	5	6	7	8	9	10
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	X	✓	X	✓	X	✓	X	✓	X	✓
3	X	X	✓	X	X	✓	X	X	✓	X
4	X	X	X	✓	X	X	X	✓	X	X
5	X	X	X	X	✓	X	X	X	X	✓
6	X	X	X	X	X	✓	X	X	X	X
7	X	X	X	X	X	X	✓	X	X	X
8	X	X	X	X	X	X	X	✓	X	X
9	X	X	X	X	X	X	X	X	✓	X
10	X	X	X	X	X	X	X	X	X	✓
	1	2	2	3	2	4	2	4	3	4

Jail Cell Solution 2

Indeed, door n will be activated when the button is pressed the d-th time if and only if $d \mid n$. Therefore, the number of activations is equal to the number of positive divisors of n, or $\tau(n)$.

Jail Cell Solution 2

Indeed, door n will be activated when the button is pressed the d-th time if and only if $d \mid n$. Therefore, the number of activations is equal to the number of positive divisors of n, or $\tau(n)$.

We therefore wish to find when $\tau(n)$ is odd. By our formula, we see that

$$\tau(n) = \prod (k_i + 1).$$

If $\tau(n)$ is odd, then every term in the product must be too, therefore, k_i must be even. Hence, every exponent in the prime factorization of n is even, and n must be a perfect square.

Jail Cell Solution 2

Indeed, door n will be activated when the button is pressed the d-th time if and only if $d \mid n$. Therefore, the number of activations is equal to the number of positive divisors of n, or $\tau(n)$.

We therefore wish to find when $\tau(n)$ is odd. By our formula, we see that

$$\tau(n) = \prod (k_i + 1).$$

If $\tau(n)$ is odd, then every term in the product must be too, therefore, k_i must be even. Hence, every exponent in the prime factorization of n is even, and n must be a perfect square.

For the original problem, the open cells are $1, 4, 9, 16, 25, 36, 49, 64, 81, 100$.

Product of Divisors of n

Example 11. Show that the product of the divisors of a number n is $n^{\tau(n)/2}$.

Solution. Let d be an arbitrary divisor of n so that $n = dd'$. We therefore see that

$$\prod_{d|n} d \cdot \prod_{d'|n} d' = n^{\tau(n)}.$$

As d ranges through the divisors, d' does the same in reverse order. Hence, $\prod_{d|n} d = \prod_{d'|n} d'$:

$$\left(\prod_{d|n} d\right)^2 = n^{\tau(n)} \implies \prod_{d|n} d = n^{\tau(n)/2}.$$

Multiplicative Function Definition

After studying these functions, we introduce multiplicative functions.

Definition. A function f is **multiplicative** if whenever $\gcd(a, b) = 1$,

$$f(ab) = f(a)f(b).$$

Multiplicative Function Definition

After studying these functions, we introduce multiplicative functions.

Definition. A function f is **multiplicative** if whenever $\gcd(a, b) = 1$,

$$f(ab) = f(a)f(b).$$

By induction, if $n_1, n_2, n_3, \cdots, n_r$ are pairwise relatively prime, then

$$f(n_1 n_2 \cdots n_r) = f(n_1)f(n_2)\cdots f(n_r).$$

Hence, if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorzation of a number,

$$f(n) = f(p_1^{k_1})f(p_2^{k_2})\cdots f(p_r^{k_r}).$$

Multiplicative Function Definition

After studying these functions, we introduce multiplicative functions.
Definition. A function f is **multiplicative** if whenever $\gcd(a, b) = 1$,

$$f(ab) = f(a)f(b).$$

By induction, if $n_1, n_2, n_3, \cdots, n_r$ are pairwise relatively prime, then

$$f(n_1 n_2 \cdots n_r) = f(n_1)f(n_2) \cdots f(n_r).$$

Hence, if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorzation of a number,

$$f(n) = f(p_1^{k_1})f(p_2^{k_2}) \cdots f(p_r^{k_r}).$$

Therefore, we only evaluate multiplicative functions up to prime powers.
Also, since $f(a \cdot 1) = f(a) \cdot f(1)$, so we must have $f(1) = 1$ if $f \neq 0$.

Multiplicative Function Definition

After studying these functions, we introduce multiplicative functions.
Definition. A function f is **multiplicative** if whenever $\gcd(a, b) = 1$,

$$f(ab) = f(a)f(b).$$

By induction, if $n_1, n_2, n_3, \cdots, n_r$ are pairwise relatively prime, then

$$f(n_1 n_2 \cdots n_r) = f(n_1)f(n_2) \cdots f(n_r).$$

Hence, if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorzation of a number,

$$f(n) = f(p_1^{k_1})f(p_2^{k_2}) \cdots f(p_r^{k_r}).$$

Therefore, we only evaluate multiplicative functions up to prime powers. Also, since $f(a \cdot 1) = f(a) \cdot f(1)$, so we must have $f(1) = 1$ if $f \neq 0$.

f is completely multiplicative if $f(ab) = f(a)f(b)$ for all natural a, b. For example, the functions $\mathrm{id}(n) = n$ and 1 are completely multiplicative.

Sum of Divisors of Multiplicative Function

Theorem. If f is a multiplicative function and F is defined as

$$F(n) = \sum_{d|n} f(d),$$

then F is also multiplicative.

Corollary. τ and σ are multiplicative functions since $\tau(n) = \sum_{d|1} 1$ and $\sigma(n) = \sum_{d|n} d$.

Proof

Proof.

Let m and n be relatively prime integers, so $F(mn) = \sum_{d|mn} f(d)$. Since $d \mid mn$, we decompose d into $d = d_1 d_2$ such that $d_1 \mid m$ and $d_2 \mid n$. We hence have

$$\begin{aligned} F(mn) &= \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m} \sum_{d_2|m} f(d_1) f(d_2) \\ &= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) \\ &= F(m)F(n). \end{aligned}$$

ω and Ω

Two other functions worth mentioning are $\omega(n)$ and $\Omega(n)$. $\omega(n)$ counts the number of distinct prime divisors of n and $\Omega(n)$ counts with multiplicity. In other words,

$$\omega(n) = \sum_{p|n} 1, \quad \Omega(n) = \sum_{p|n} v_p(n).$$

For instance, $400 = 2^4 \cdot 5^2$, so $\omega(400) = 2$ and $\Omega(540) = 4 + 2 = 6$.

Definition. A function f is **additive** if $f(ab) = f(a) + f(b)$ whenever $\gcd(m, n) = 1$.

Example 12. Show that $\omega(n)$ is an additive function and $2^{\omega(n)}$ is multiplicative.

Proof of Additivity

Example. Show that $\omega(n)$ is an additive function and $2^{\omega(n)}$ is multiplicative.

Proof.

Let $a = \prod_{1 \leq i \leq r} p_i^{e_i}$ and $b = \prod_{1 \leq j \leq s} p_j^{f_j}$. Since $p_i \neq q_j$, we see that

$$ab = \prod_{1 \leq i \leq r} p_i^{e_i} \cdot \prod_{1 \leq j \leq s} p_j^{f_j}$$

has $r + s$ distinct prime factors. Hence, $\omega(ab) = r + s = \omega(a) + \omega(b)$. Furthermore, since $\omega(n)$ is additive, $f(n) = 2^{\omega(n)}$ is multiplicative:

$$f(ab) = 2^{\omega(ab)} = 2^{\omega(a)+\omega(b)} = 2^{\omega(a)}2^{\omega(b)} = f(a)f(b).$$

A Weird Identity

Example. Prove the identity $\tau(n^2) = \sum_{d|n} 2^{\omega(d)}$.

Solution. From our theorem, we see that the right hand side is a multiplicative function.

A Weird Identity

Example. Prove the identity $\tau(n^2) = \sum_{d|n} 2^{\omega(d)}$.

Solution. From our theorem, we see that the right hand side is a multiplicative function. Furthermore, for coprime a and b with $a = \prod_{1 \leq i \leq r} p_i^{e_i}$, $b = \prod_{1 \leq j \leq s} q_j^{f_j}$, we see that

$$\tau((ab)^2) = \prod_{1 \leq i \leq r} (2e_i + 1) \cdot \prod_{1 \leq j \leq s} (2f_j + 1) = \tau(a^2)\tau(b^2).$$

A Weird Identity

Example. Prove the identity $\tau(n^2) = \sum_{d|n} 2^{\omega(d)}$.

Solution. From our theorem, we see that the right hand side is a multiplicative function. Furthermore, for coprime a and b with $a = \prod_{1 \leq i \leq r} p_i^{e_i}$, $b = \prod_{1 \leq j \leq s} q_j^{f_j}$, we see that

$$\tau((ab)^2) = \prod_{1 \leq i \leq r} (2e_i + 1) \cdot \prod_{1 \leq j \leq s} (2f_j + 1) = \tau(a^2)\tau(b^2).$$

Hence, $\tau(n^2)$ is also multiplicative. Therefore, we only need to show the identity for $n = p^k$:

A Weird Identity

Example. Prove the identity $\tau(n^2) = \sum_{d|n} 2^{\omega(d)}$.

Solution. From our theorem, we see that the right hand side is a multiplicative function. Furthermore, for coprime a and b with $a = \prod_{1 \le i \le r} p_i^{e_i}$, $b = \prod_{1 \le j \le s} q_j^{f_j}$, we see that

$$\tau((ab)^2) = \prod_{1 \le i \le r} (2e_i + 1) \cdot \prod_{1 \le j \le s} (2f_j + 1) = \tau(a^2)\tau(b^2).$$

Hence, $\tau(n^2)$ is also multiplicative. Therefore, we only need to show the identity for $n = p^k$:

$$\tau(n^2) = \tau(p^{2k}) = 2k + 1$$

$$\sum_{d|n} 2^{\omega(d)} = 2^{\omega(1)} + 2^{\omega(p)} + 2^{\omega(p^2)} + \cdots + 2^{\omega(p^k)} = 2k + 1.$$

A Weird Identity

Example. Prove the identity $\tau(n^2) = \sum_{d|n} 2^{\omega(d)}$.

Solution. From our theorem, we see that the right hand side is a multiplicative function. Furthermore, for coprime a and b with $a = \prod_{1 \le i \le r} p_i^{e_i}$, $b = \prod_{1 \le j \le s} q_j^{f_j}$, we see that

$$\tau((ab)^2) = \prod_{1 \le i \le r} (2e_i + 1) \cdot \prod_{1 \le j \le s} (2f_j + 1) = \tau(a^2)\tau(b^2).$$

Hence, $\tau(n^2)$ is also multiplicative. Therefore, we only need to show the identity for $n = p^k$:

$$\tau(n^2) = \tau(p^{2k}) = 2k + 1$$
$$\sum_{d|n} 2^{\omega(d)} = 2^{\omega(1)} + 2^{\omega(p)} + 2^{\omega(p^2)} + \cdots + 2^{\omega(p^k)} = 2k + 1.$$

The second equation follows since $\omega(1) = 1$ and $\omega(p^j) = 1$.