Counting sets of functions (Ch 12)

Goal: Given 2 sets X, $|X| = m$, and Y, $|Y| = n$ we want to know how many different functions we can have between X an Y.

Example: $X = \{1, 2\}$, $Y = \{a, b, c\}$
we have 3^2 possible functions $f: X \to Y$ (why?)

Def'n: Given two sets X and Y, the set of functions from X to Y is denoted

$$F(X, Y).$$

Proposition: Let X and Y be finite sets with $|X| = m$, $|Y| = n$, then the number of functions $X \to Y$ is n^m.

Proof: By induction on m (exercise).

The idea is that for each $x \in X$ there are n possibilities for $f(x)$ among the elements of Y. As there are m elements of X, the total number of possibilities is $n \times n \times \cdots \times n = n^m$.

So, now that we know the number of functions in $F(X,Y)$, what about the number of injections? bijections? surjections?

Proposition: Let X and Y be non-empty sets with $|X| = m$, $|Y| = n$, then the number of injections in $F(X,Y)$ is $n(n-1)\cdots(n-m+1)$.

$n(n-1)\cdots(n-m+1)$ called falling factorial

injections in $F(X,Y)$ denoted $\mathrm{Inj}(X,Y)$

Notice that $(n)_m := n(n-1)\cdots(n-m+1)$

$$= \begin{cases} n! & \text{when } m = n \\ 0 & \text{when } m > n \\ \frac{n!}{(n-m)!} & \text{when } m \leq n. \end{cases}$$

Proof: Again, by induction on m (exercise).

Defn: Given a set X, a bijection $X \to X$ is called a permutation of X.

Corollary: Given a set X, $|X| = n > 0$, the number of permutation of X is $n!$.

Proof: Every injection between two sets of equal cardinality is a bijection (by a previous theorem (Th. 11.1.7).)
So we can apply the above prop. on $|Inj(X,Y)|$ to $|Inj(X,X)|$ and obtain that the number of permutations in $(n)_n = n!$.

Counting sets of subsets:

Recall $\mathcal{P}(X) = \{A \mid A \subseteq X\}$.

Proposition: If X is a set, then

$$|\mathcal{P}(X)| = 2^{|X|}$$

Idea of Proof: $\forall x \in X$, x either belongs or doesn't belong to a subset of X (2 possibilities for each x). There are $|X|$ elements of X, so $2 \times 2 \times \cdots \times 2 = 2^{|X|}$ subsets.

Proof: exercise.

Definition: Given a set X and a non-neg. integer r, we denote

$$\mathcal{P}_r(X) = \{A \mid A \subseteq X, |A| = r\}.$$

Example: If $X = \{1,2,3\}$, then

$$\mathcal{P}_0(X) = \{\emptyset\}$$
$$\mathcal{P}_1(X) = \{\{1\}, \{2\}, \{3\}\}$$
$$\mathcal{P}_2(X) = \{\{1,2\}, \{1,3\}, \{2,3\}\}$$
$$\mathcal{P}_3(X) = \{\{1,2,3\}\} = \{X\}.$$
$$\mathcal{P}_r(X) = \emptyset, \quad r \geq 4.$$

Definition: We define the binomial coefficient

$$\binom{n}{r} := |\mathcal{P}_r(X)| \quad \text{where } |X| = n$$

Example: From our previous example

$\binom{3}{0} = 1$, $\binom{3}{1} = 3$, $\binom{3}{2} = 3$, $\binom{3}{3} = 1$,

$\binom{3}{r} = 0$ when $r \geq 4$.

Proposition: When n & r are non-neg. integer

(i) $\binom{n}{r} = 0$ if $r > n$

(ii) $\binom{n}{0} = 1$, $\binom{n}{1} = n$, $\binom{n}{n} = 1$

(iii) $\binom{n}{r} = \binom{n}{n-r}$ when $0 \leq r \leq n$

Proof of (iii): $\exists$ a bijection

$$\mathcal{P}_r(X) \longrightarrow \mathcal{P}_{n-r}(X)$$

which maps $A \longmapsto A^c$ when $A \subseteq X$.

so $|\mathcal{P}_r(X)| = |\mathcal{P}_{n-r}(X)|$

and $\binom{n}{r} = \binom{n}{n-r}$.

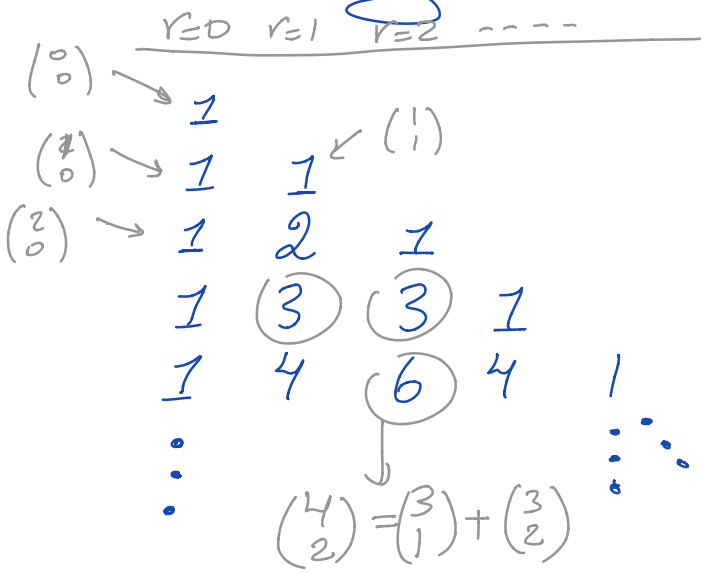
Evaluating binomial coefficients:

Proposition: Let n, r be integers s.t. $1 \le r \le n$, then

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

Visualization: Pascal's triangle

$n = 0$
$n = 1$
$n = 2$
$n = 3$
$n = 4$



A better way to compute binomial coefficients:

Theorem:

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

The Binomial Theorem:

$$\forall a, b \in \mathbb{R} \text{ and } n \in \mathbb{Z}^{\geq 0}$$

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

$$= a^n + \cdots + \binom{n}{i} a^{n-i} b^i + \cdots + b^n$$

Examples: • $(a+b)^2 = \binom{2}{0} a^2 b^0 + \binom{2}{1} a^1 b^1 + \binom{2}{2} a^0 b^2$

$$= a^2 + 2ab + b^2$$

• $(a+b)^3 = \binom{3}{0} a^3 b^0 + \binom{3}{1} a^2 b^1 + \binom{3}{2} a^1 b^2 + \binom{3}{3} a^0 b^3$

$$= a^3 + 3a^2 b + 3ab^2 + b^3$$

Proof of Binomial theorem: By induction (exercise).

Corollary: $\sum_{i=0}^{n} \binom{n}{i} = 2^n$

Proof: set $a = b = 1$ in binomial thm.

Ch 13: Number Systems

Recall the properties that numbers satisfy with respect to addition & multiplication; namely:

Commutativity, associativity, distributativity ($a(b+c) = ab+ac$), subtraction, division, (as well as having a zero and unit (1) element).

Definition: A rational number q, is a number that can be represented as a fraction $\frac{a}{b}$ where $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$. In other words q satisfies $\boxed{bq = a}$.

(A better definition of the rationals involves the concept of equivalence relations, which we may (or may not) have time to cover).

Proposition: Two fractions $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ (with $a_1, a_2 \in \mathbb{Z}$, $b_1, b_2 \in \mathbb{Z} \setminus \{0\}$) both represent the rational number q if and only if $a_1 b_2 = a_2 b_1$.

Proof: Exercise

Defn: We say the fraction $\frac{a}{b}$ is in lowest terms when a & b are coprime.

Defn:
- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
- $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$

sum & product of fractions

Do these definitions lead to well-defined addition & multiplication of rationals? That is, if q is represented by $\frac{a_1}{b_1}$ & $\frac{a_2}{b_2}$ and p is represented by $\frac{c_1}{d_1}$ & $\frac{c_2}{d_2}$ is the rational represented by $\frac{a_1}{b_1} + \frac{c_1}{d_1}$ the same as the rational rep. by $\frac{a_2}{b_2} + \frac{c_2}{d_2}$? What about for multiplication?

Proposition: Addition & multiplications of rationals is well-defined.

Proof: Our goal is to show that

$\frac{a_1}{b_1} + \frac{c_1}{d_1}$ and $\frac{a_2}{b_2} + \frac{c_2}{d_2}$ represent the same rational.

That is, we want to show that

$\frac{a_1 d_1 + c_1 b_1}{b_1 d_1}$ and $\frac{a_2 d_2 + c_2 b_2}{b_2 d_2}$ represent the same rational. This in turn means that we want to show that

$$(a_1 d_1 + b_1 c_1)\, b_2 d_2 = (a_2 d_2 + c_2 b_2)\, b_1 d_1.$$

But we know that $a_1 b_2 = a_2 b_1$ & $c_1 d_2 = c_2 d_1$ (why?).

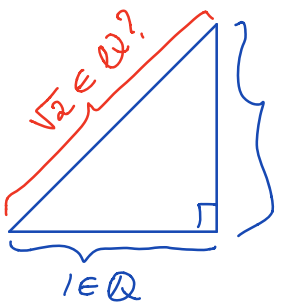
So now,

$$\begin{aligned}(a_1 d_1 + b_1 c_1)\, b_2 d_2 &= a_1 b_2 d_1 d_2 + c_1 d_2 b_1 b_2 \\ &= a_2 b_1 d_1 d_2 + c_2 d_1 b_1 b_2 \\ &= (a_2 d_2 + c_2 b_2)\, b_1 d_1,\end{aligned}$$

as desired.

(The proof for $\times$ is similar) exercise!

The irrationality of $\sqrt{2}$:



(Recall that $\sqrt{2}$ is the real number that satisfies $x^2 = 2$.)

Theorem: There does not exist a rational number q such that $q^2 = 2$.

Proof: We will proceed by contradiction. Suppose $\exists\, a \in \mathbb{Z}$, $b \in \mathbb{Z} - \{0\}$, such that $\left(\frac{a}{b}\right)^2 = 2$.

Suppose further that a/b is in lowest terms.

Now, $\left(\frac{a}{b}\right)^2 = 2 \iff \frac{a^2}{b^2} = 2 \iff a^2 = 2b^2$ (as $b \neq 0$)

As b^2 is an integer, a^2 must be even.

Now, a is either even or odd. Suppose by way of contradiction that a is odd, so $a = 2k+1$ for some $k \in \mathbb{Z}$.

Then $a^2 = 4k^2 + 4k + 1 = 2(\underbrace{2k^2 + 2k}_{\in \mathbb{Z}}) + 1$ is odd, a contradiction.

So, having proved that

$$(a^2 \text{ is even}) \Rightarrow (a \text{ is even})$$

we can now write $a = 2a_1$ for some $a_1 \in \mathbb{Z}$.

So $\underbrace{(2a_1)}_{a}{}^2 = 2b^2$,

and $b^2 = 2a_1^2$. So b^2, hence b, is even. So we showed that

$$a \text{ and } b \text{ are both even.}$$

But we had assumed a & b are co-prime, a contradiction. So our, initial assumption, that there is a rational q with $q^2 = 2$ is false.

A short discussion of real numbers

Representation: $x \in \mathbb{R}^{\geq 0}$ can be represented by an infinite decimal

$$a_0 . a_1 a_2 \cdots a_i \cdots \quad \text{where } a_i \in \mathbb{Z}^+ \text{ and } 0 \leq a_i \leq 9 \text{ for } i \geq 1.$$

Observation 1: (Set of finite decimals) $\subseteq \mathbb{Q}$.

Proof:

$$\begin{aligned} a_0 . a_1 \cdots a_n &= a_0 + \frac{a_1}{10} + \cdots + \frac{a_n}{(10)^n} \\ &= \frac{a_0 10^n + a_1 \cdot 10^{n-1} + \cdots a_n}{(10)^n} \in \mathbb{Q}. \end{aligned}$$

Def'n: An infinite decimal $a_0 . a_1 a_2 \cdots$ represents the real number a when

$$a_0 . a_1 a_2 \cdots a_n \leq a \leq a_0 . a_1 a_2 \cdots a_n + \frac{1}{10^n} \quad \forall n \in \mathbb{Z}^+$$

(You'll see a better def'n in 140A).

Example: Consider the infinite decimal

$$x = 0.999\ldots99\ldots$$
$$=: 0.\overline{9} \quad \text{(shorthand notation)}$$

From our definition

$$x = 0.\overline{9} \Leftrightarrow \left(\forall n \in \mathbb{Z}^+ : 0.\underbrace{99\cdots9}_{n} \leq x \leq 0.\underbrace{9\cdots9}_{n} + \frac{1}{10^n}\right).$$

$$\Leftrightarrow \left(\forall n \in \mathbb{Z}^+ : \ 1 - \frac{1}{10^n} \leq x \leq 1\right)$$

$$\Leftrightarrow \left(\boxed{\forall n \in \mathbb{Z}^+ : \ 0 \leq 1 - x \leq \frac{1}{(10)^n}}\right).$$

As $1-x \geq 0$, either $1-x = 0$ or $1-x > 0$.
Suppose $1-x > 0$, then $\exists k \in \mathbb{Z}^+$ such that $\boxed{1-x > \frac{1}{10^k}}$ (why?), but this contradicts the fact that $1-x \leq \frac{1}{10^n}\ \forall n$, so our assumption $1-x > 0$ is false.
Thus $1-x = 0$, and $\boxed{x = 1}$!

example: $0.999\ldots$
$0.12757575\ldots$

Fact: Recurring Decimals correspond exactly to the rationals

Chapter 14: Counting infinite sets

Recall: For finite sets, we say $|A| = |B|$ if there is a bijection $f: A \to B$.

We can extend this definition to arbitrary (not necessarily finite sets).

Example: $\boxed{|\mathbb{Z}| = |\mathbb{Z}^{\geq}|}$

proof: Let $f: \mathbb{Z} \to \mathbb{Z}^{\geq}$ be given by $f(n) = \begin{cases} 2n, & n \geq 0 \\ -2n-1, & n < 0 \end{cases}$

(example: $f(0)=0$, $f(-1)=1$, $f(1)=2$, $f(-2)=3$, $f(2)=4, \ldots$)

and note that f is a bijection (why?)

Example: $|\mathbb{Z}| = |\mathbb{Z}^+|$

Proof: Let $f: \mathbb{Z} \to \mathbb{Z}^+$ be given by

$$f(n) = \begin{cases} -2n, & n < 0 \\ 2n+1, & n \geq 0 \end{cases}$$

so $f(0) = 1$, $f(-1) = 2$, $f(1) = 3$, $f(2) = 4$, ... and note that f is a bijection (why?).

We say a set X is enumerable (or denumerable) if $\exists$ a bijection $f: \mathbb{Z}^+ \to X$

(Equivalently $\exists$ a bijection $X \to \mathbb{Z}^+$)

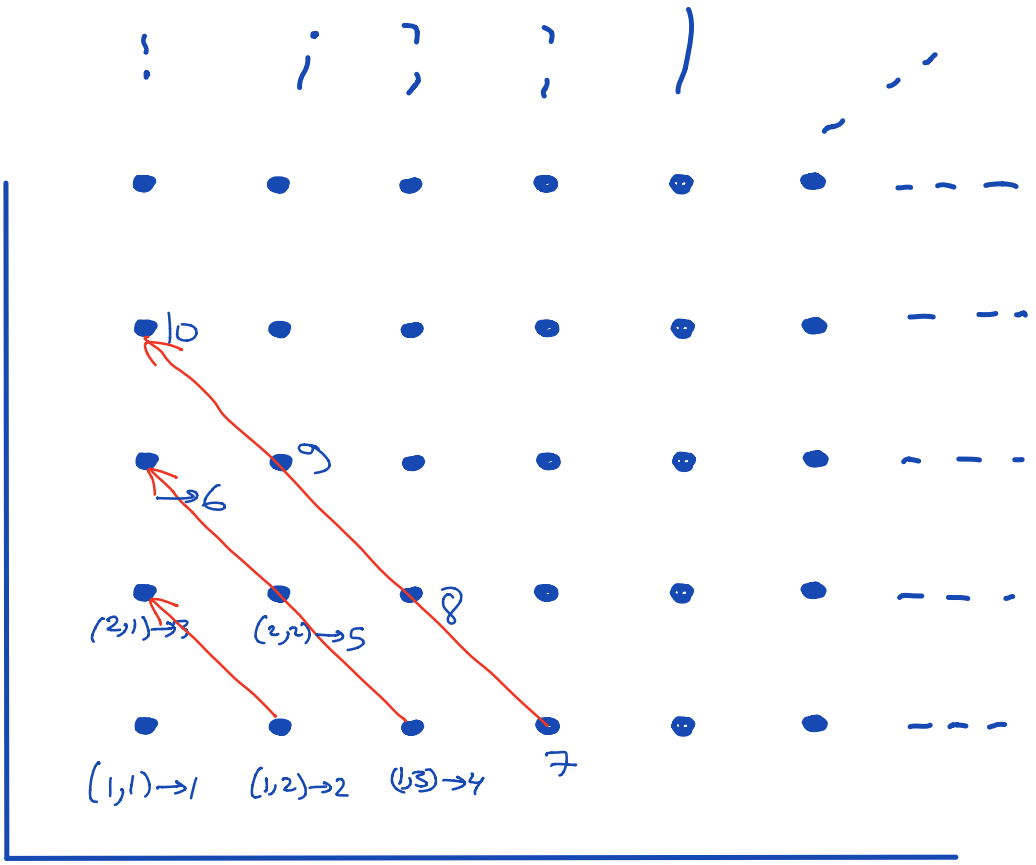
Def'n

Essentially, we are saying that we can count (enumerate) every element of X once and only once (and we use all the elements of $\mathbb{Z}^+$ to do it).

Def'n: A set X is countable if it is finite or enumerable.

Example: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is enumerable.

"Proof": Here is a bijection from $\mathbb{Z}^+ \times \mathbb{Z}^+$ to $\mathbb{Z}^+$



Question: Are all sets countable?

Answer: No! There are uncountable sets!

Our main tool to prove this is the following theorem, due to Cantor.

Theorem: For any set X (finite or infinite), there is no surjection

$$f: X \longrightarrow P(X).$$

Proof: Suppose, by way of contradiction that

$$f: X \longrightarrow P(X)$$

is surjective.

Then, every $A \in P(X)$ satisfies $f(a) = A$ for some $a \in X$.

Specifically, this is true for

$$A = \{ x \in X \mid x \notin f(x) \}$$

(Remember $f(x)$ is a set.)

Now, consider $a \in X$ s.t. $f(a) = A$. Either

(1) $a \in A \Rightarrow a \notin f(a) = A$, a contradiction

or (2) $a \notin A \Rightarrow a \in f(a) = A$, a contradiction.

Thus f cannot be a surjection. ∎

Corollary: $P(\mathbb{Z}^+)$ is not countable.

Proof: No bijection from $\mathbb{Z}^+ \to P(\mathbb{Z}^+)$ by the theorem above. ∎

Theorem: The set of real numbers $\mathbb{R}$ is uncountable.

"Proof": (Cantor's diagonalization argument)

For $\mathbb{R}$ (which is infinite) to be countable, there has to be a bijection $f: \mathbb{Z}^+ \to \mathbb{R}$.

We will show that $\exists x \in \mathbb{R}$, $x \neq f(a)$ for any $a \in \mathbb{Z}^+$, so f is not surjective (hence not bijective).

To that end, let

$$f(1) = a_{10} . a_{11} a_{12} a_{13} \cdots$$
$$f(2) = a_{20} . a_{21} a_{22} a_{23} \cdots$$
$$f(3) = a_{30} . a_{31} a_{32} a_{33} \cdots$$
$$\ddots$$
$$f(m) = a_{m0} . a_{m1} a_{m2} a_{m3} \cdots a_{mm} \cdots$$

where the $f(m)$'s do not end in trailing 9's.

Let $x \in \mathbb{R}$ be the number represented by

$$0 . b_1 b_2 b_3 \cdots b_m \cdots$$

where $b_m = \begin{cases} 1 & \text{if } b_{mm} = 0 \\ 0 & \text{otherwise.} \end{cases}$

Notice that x does not end in trailing zeros and that $x \neq f(m) \; \forall m \in \mathbb{Z}^+$ so f is not surjective.

The Division Theorem (Ch. 15)

Theorem: $\forall a, b \in \mathbb{Z}$, $b > 0$, there is a unique $q, r \in \mathbb{Z}$ where $b > r \geq 0$ and $a = bq + r$.

(q: quotient, r: remainder)

Proof: (1) Existence:

b q r

The case $b = 1$ is trivial as $a = 1 \cdot a + 0$.

So consider $b > 1$ and let

$$A = \{n = a - bq \mid q \in \mathbb{Z}, n \geq 0\}$$

Note that $A \neq \emptyset$ because

if $a \geq 0$, $a - 0 \cdot b \in A$

if $a < 0$, $a - ab = a(1-b) \in A$. ($a < 0$, $1 - b < 0$)

So, A is a set of non-negative integers and it therefore has a minimum, r with $r = a - bq$ for some $q \in \mathbb{Z}$.

so $\boxed{a = bq + r}$.

To see that $r < b$, suppose $r \geq b \Rightarrow r = b + m$ for some $0 \leq m < r$, then $m = a - (q+1)b \in A$, contradicting the minimality of r.

(2) Uniqueness: Suppose

$$a = q_1 b + r_1 = q_2 b + r_2$$

with $0 \leq r_1 < b$ and $0 \leq r_2 < b$

and assume without loss of gen. that $r_2 \geq r_1$.

So $r_2 - r_1 = (q_1 - q_2)b \Rightarrow b \mid r_2 - r_1$

so either $r_2 - r_1 \geq b$ or $r_2 - r_1 = 0$

but $r_2 - r_1 < b$ (why?) so $r_1 = r_2$

$\Rightarrow q_1 = q_2$ (why?). ∎

Example application:

Proposition: $\boxed{(3 \mid a^2) \Leftrightarrow (3 \mid a)}$

Proof: "$\Leftarrow$": If $3 \mid a$ then $a = 3b$ for some integer b and $a^2 = (3b)^2 = 3(3b^2)$ so $3 \mid a^2$.

"$\Rightarrow$": By the division theorem

$a = 3q + r$ where $r = 0, 1, \text{or } 2$.

We want to show that $3 \mid a^2 \Rightarrow r = 0$.

Suppose, to the contrary that $a = 3q + 1$ or $a = 3q + 2$.

If $a = 3q + 1$ then $a^2 = (3q+1)^2 = 9q^2 + 6q + 1$

$= 3(3q^2 + 2q) + 1$

So 3 doesn't divide a^2, by the division theorem, which is a contradiction.

If $a = 3q + 2$ then $a^2 = (3q+2)^2 = 9q^2 + 12q + 4$

$= 3(3q^2 + 4q + 1) + 1$

So 3 doesn't divide a^2, by the division theorem, which is a contradiction. ∎

Another application:

- Theorem: There are infinitely many primes

Proof: We will use the fact that every integer (≥ 0) can be written as a product of primes ($n \geq 2$) (we'll prove this after).

Our proof will be by contradiction. Suppose there are only n primes $p_1, p_2, \ldots p_n$.

Let $a = \prod_{i=1}^{n} p_i + 1$ and note that by the fact above, a is a product of primes, so there is an $i \in \{1, \ldots, n\}$ such that $p_i \mid a$, but that would imply that $a = p_i q$ (for some $q \in \mathbb{Z}$) while $a = p_i \left(\prod_{\substack{j=1 \\ i \neq j}}^{n} p_j \right) + 1$

which is a contradiction (it violates the uniqueness of the division theorem).

So, there are infinitely many primes

Theorem: Every integer n, $n \geq 2$, is a product of primes.

Comment: If n is prime, we will consider it a product of primes (itself).

Proof: We will prove this by strong induction.

Base case: ($n = 2$) 2 is prime so the prop. is true in this case.

Inductive step: Want to show that

(any integer m, $2 \leq m \leq k$ can be written as a product of primes)

$\Rightarrow$

(any integer m, $2 \leq m \leq k+1$ can be written as a product of primes).

This is obviously true for $2 \leq m \leq k$ by the inductive hypothesis.

Remains to show that $k+1$ can be written as a product of primes.

Two cases: (I) $k+1$ is prime.

In this case we're done.

(II) $k+1$ is not prime.

In this case $k+1$ has a divisor b, $1 < b < k+1$. Thus $k+1 = bq$ where $1 < b, q < k+1$.

So $k+1 = bq$

↳↳ less than $k+1$ & greater than 1

By our ind. hyp. b & q can each be written as a prod. of primes so $k+1$ is now a prod. of primes