Mon Nov 12

HW 5 due Friday

Today: The Binomial Theorem

Problem: What are the coefficients of $(1+x)^n$?

$(1+x)^0 = 1$

$(1+x)^1 = 1 + x$

$(1+x)^2 = 1 + 2x + x^2$

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

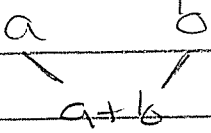
$(1+x)^4 = 1 + 4x + 6x^2 + 4x^3 + x^4$

Is there a pattern?

"Pascal's Triangle":

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5  10  10   5   1
```

Pascal's Recurrence:



Can we prove it?

Notation:

Define $\binom{n}{k} := $ coeff. of x^k in $(1+x)^n$,

i.e. $(1+x)^n = \sum_k \binom{n}{k} x^k$

Say:
$$\binom{n}{k} = 0 \text{ if } k > n \text{ or } k < 0.$$

Goal: Study these "binomial coefficients"

☆ Theorem: For all $n, k \in \mathbb{Z}$ with $n \geq 1$ we have

$$\boxed{\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}}$$

"$\binom{n-1}{k-1}$ $\binom{n-1}{k}$" → $\binom{n}{k}$

Pascal's Recurrence.

"Proof by example": We have

$$(1+x)^5 = (1+x)(1+x)^4 = (1+x)^4 + x(1+x)^4$$

$$= \begin{array}{r} 1 + 4x + 6x^2 + 4x^3 + x^4 \\ + \quad 1x + 4x^2 + 6x^3 + 4x^4 + x^5 \\ \hline 1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5 \end{array}$$

∎

Formal Proof: We have

$$(1+x)^n = (1+x)(1+x)^{n-1} = (1+x)^{n-1} + x(1+x)^{n-1}$$

$$= \left[\binom{n-1}{0} + \binom{n-1}{1}x + \cdots + \binom{n-1}{k}x^k + \cdots + \binom{n-1}{n-1}x^{n-1}\right] + \left[\binom{n-1}{0}x + \cdots + \binom{n-1}{k-1}x^k + \cdots + \binom{n-1}{n-2}x^{n-1} + \binom{n-1}{n-1}x^n\right]$$

$$= \binom{n-1}{0} + \cdots + \left[\binom{n-1}{k} + \binom{n-1}{k-1}\right]x^k + \cdots + \binom{n-1}{n-1}x^n.$$

Hence,

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \text{coeff of } x^k \text{ in } (1+x)^n$$

$$= \binom{n}{k} \quad \text{by definition}$$

Q: Initial conditions? $\binom{0}{k} = \begin{cases} 1 & \text{if } k=0 \\ 0 & \text{if } k \neq 0 \end{cases}$.

0 0 0 0 0 1 0 0 0 0 0

0 0 0 0 1 1 0 0 0 0

0 0 0 1 2 1 0 0 0

0 0 1 3 3 1 0 0

0 1 4 6 4 1 0

1 5 10 10 5 1 etc.

We can compute $\binom{n}{k}$ recursively, but is there a "formula"?

DEF: Given $n \in \mathbb{Z}$ with $n \geq 1$ define

$$n! := n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$$

"factorial"

Also define $0! := 1$ (you'll see why)

Theorem: For $n \geq 0$ and $0 \leq k \leq n$, we have

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

Proof: For $n \geq 0$, define $f(n,k) := n!/(k!(n-k)!)$

and let $P(n) =$ "$\binom{n}{k} = f(n,k)\ \forall\ 0 \leq k \leq n$"

We will prove by induction on n that

$$P(n) = T \quad \forall\ n \geq 0.$$

(k is just along for the ride)

(i) Base case:

Note that $P(0) = T$ since $\binom{0}{0} = 1 = \frac{0!}{0!0!}$ ✓

(ii) Induction step:

Now fix $N \geq 0$ and [suppose $P(N) = T$,

i.e. $\binom{N}{k} = \frac{N!}{k!(N-k)!} \quad \forall\, 0 \leq k \leq N$.

We want to show $P(N+1) = T$. Easy for $k = 0$ or $N+1$, so let $1 \leq k \leq N$. Then

$$\binom{N+1}{k} = \binom{N}{k} + \binom{N}{k-1} \qquad \text{by Theorem } \bigstar$$

$$= \frac{N!}{k!(N-k)!} + \frac{N!}{(k-1)!(N-k+1)!} \qquad \text{by assumption}$$

$$= \frac{(N-k+1)\,N!}{(N-k+1)\,k!(N-k)!} + \frac{k\,N!}{k\,(k-1)!(N-k+1)!}$$

$$= \frac{(N-k+1)N! + kN!}{k!(N-k+1)!}$$

$$= \frac{(N+1)N!}{k!(N-k+1)!} = \frac{(N+1)!}{k!((N+1)-k)!}$$]

By PI, we're done. ▨

eg. Coefficient of x^7 in $(1+x)^{10}$ is

$$\binom{10}{7} = \frac{10!}{7!\,3!} = \frac{10 \cdot 9^{3} \cdot 8^{4} \cdot 7!}{8 \cdot 2 \cdot 1 \cdot 7!}$$

$$= 120.$$

$$(1+x)^{10} = 1 + \cdots + 120x^7 + \cdots + x^{10}$$

That's nice but the proof is not enlightening :(

Where did I get the formula

$$\frac{n!}{k!\,(n-k)!}$$??

Wed Nov 14

HW 5 due Fri

Today: Binomial Coefficients $\binom{n}{k}$.

Recall our definition:

$\binom{n}{k}$:= the coeff of x^k in $(1+x)^n$

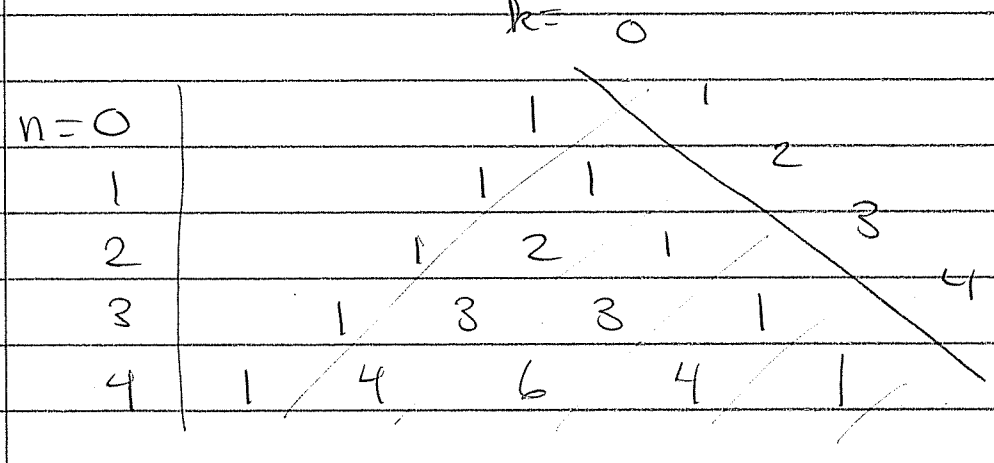
i.e. $(1+x)^n = \sum_k \binom{n}{k} x^k$

We used the simple idea

$$(1+x)^n = (1+x)(1+x)^{n-1}$$
$$= (1+x)^{n-1} + x(1+x)^{n-1}$$

To prove Pascal's Recurrence:

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



Example.

$$(1+x)^4 = (1+x)^3 + x(1+x)^3$$

$$= \left(1 + 3x + 3x^2 + 1x^3\right) + \left(1x + 3x^2 + 3x^3 + 1x^4\right)$$

$$1 + 4x + 6x^2 + 4x^3 + 1x^4 \quad \checkmark$$

Then we used Pascal's Recurrence to prove by induction that

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

But this proof was not enlightening. Where does the formula

$$\frac{n!}{k!(n-k)!}$$

come from?

Here's a better idea: First note that

$$(a+b)^n = \sum \binom{n}{k} a^{n-k} b^k$$

since

$$(*) \quad (1+\tfrac{b}{a})^n = \sum \binom{n}{k} (\tfrac{b}{a})^k \qquad \text{by definition}$$

Multiply both sides of $(*)$ by a^n to get

$$a^n(1+\tfrac{b}{a})^n = \sum \binom{n}{k} (\tfrac{b}{a})^k a^n$$

$$(a(1+\tfrac{b}{a}))^n = \sum \binom{n}{k} b^k \frac{a^n}{a^k}$$

$$(a+b)^n = \sum \binom{n}{k} a^{n-k} b^k \qquad \checkmark$$

Now temporarily pretend that $ab \neq ba$:

$$(a+b)^0 = 1$$

$$(a+b)^1 = a+b$$

$$(a+b)^2 = a^2 + (ab+ba) + b^2$$

$$(a+b)^3 = a^3 + \{aab + aba + baa\} + \{abb + bab + bba\} + b^3$$

put $a=1$, $b=x$

$$1 + 3x + 3x^2 + 1x^3$$

Conclusion:

$\binom{n}{k}$ = # words of length n using $n-k$ "a"s and k "b"s.

eg $\binom{4}{2} = \frac{4!}{2!2!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1 \cdot 2 \cdot 1} = 6$

counts the words aabb, abab, abba, baab, baba, bbaa.

Corollary: $\binom{n}{k} = \binom{n}{n-k}$ (symmetry of Pascal's Δ)

Proof: Just switch $a \leftrightarrow b$.

$\binom{n}{k}$ = # words length n with $n-k$ "a"s and k "b"s

= # words length n with $n-k$ "b"s and k "a"s

= $\binom{n}{n-k}$

This leads to a new, better proof of

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

But first we need a Lemma.

Lemma:

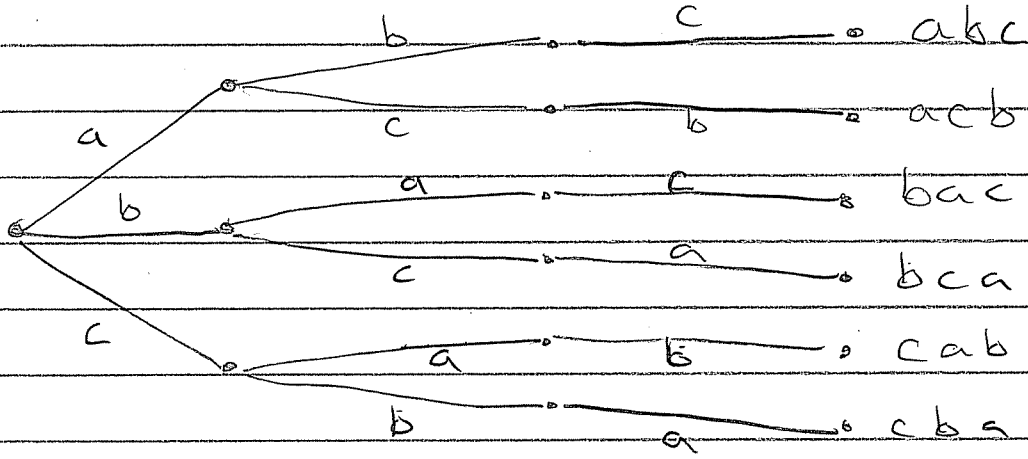
$n!$ = # words with n distinct letters.

eg. $n=3$, letters a, b, c.

Words: abc, acb, bac, bca, cab, cba

words $= 3! = 3 \cdot 2 \cdot 1 = 6$ ✓

Proof: Decision tree.



3 choices × 2 choices × 1 choice $= 3!$

Proof of $\binom{n}{k} = \frac{n!}{k!(n-k)!}$:

There are $n!$ words with (distinct) letters

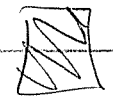
$$a_1, a_2, \cdots, a_{n-k}, b_1, b_2, \cdots, b_k$$

On the other hand, we could count them a different way.

$$n! = \#\text{words} = \binom{n}{k} \cdot (n-k)! \cdot k!$$

- $\binom{n}{k}$: choose word with $n-k$ unlabeled "a"s, k unlabeled "b"s
- $(n-k)!$: label the "a"s in $(n-k)!$ ways
- $k!$: label the "b"s in $k!$ ways.

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



Summary (Binomial Theorem 4.34) :

$$(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} b^k a^{n-k}$$

Fri Nov 16.

HW 5 due now.

HW 6 (TBA) due Wed Nov 28

Exam 3 Fri Nov 30.

THE END.

Summary: We know that

$$\binom{n}{k} = \text{coefficient of } x^k \text{ in } (1+x)^n$$

$$= \#\text{ words with } n-k \text{ "a"s and } k \text{ "b"s.}$$

$$= \frac{n!}{k!(n-k)!}$$

But why do we say $\binom{n}{k}$ = "n choose k"?

Let A be any set, say

$$A = \{a_1, a_2, \dots, a_n\}$$

We can encode any subset $S \subseteq A$ as a binary vector $(v_1, v_2, \ldots, v_n) \in \{0,1\}^n$ as follows:

$$v_i = \begin{cases} 1 & \text{if } a_i \in S \\ 0 & \text{if } a_i \notin S \end{cases}$$

Example: $A = \{a, b, c\}$

subsets		binary vectors	
$\emptyset$		0 0 0	
$\{a\}$		1 0 0	
$\{b\}$		0 1 0	How
$\{c\}$	$\longleftrightarrow$	0 0 1	Many?
$\{a,b\}$	bijection	1 1 0	
$\{a,c\}$		1 0 1	
$\{b,c\}$		0 1 1	
$\{a,b,c\}$		1 1 1	

Theorem: If $|A| = n$, then

A has exactly 2^n different subsets.

Proof: There are 2^n binary vectors length n:

$$\underbrace{2 \times 2 \times 2 \times \ldots \times 2}_{\text{1st 2nd 3rd} \quad \text{nth choices}} = 2^n$$

Cute notation:

Let $2^A := \{\text{subsets of } A\}$

- a set of sets
- called the "power set" of A

Q: Why is it cute?

A: Because $|2^A| = 2^{|A|}$.

Q: How many subsets of size k?

Let $|A| = n$. Then

Subsets $S \subseteq A$ with $|S| = k$ $\longleftrightarrow$ binary vectors with k "1"s and $n-k$ "0"s

Recall: Let $X = \{$ binary vectors with k "1"s and $n-k$ "0"s $\}$

Count orderings of symbols

$1_1, 1_2, \ldots, 1_k, 0_1, 0_2, \ldots, 0_{n-k}$

in two different ways:

$$n! = |X| \cdot k! \cdot (n-k)!$$

$$\Rightarrow |X| = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Thus we have proved

Theorem: If A is a set with $|A| = n$ then

$\binom{n}{k}$ = # subsets $S \subseteq A$ with $|S| = k$.

= # ways to "choose" k things from n things.

Example: I have 10 books on my shelf and I want to give you 3.

There are

$$\binom{10}{3} = \text{"10 choose 3"}$$

$$= \frac{10!}{3!\,7!} = \frac{10 \cdot \cancel{9}^{3} \cdot \cancel{8}^{4} \cdot \cancel{7!}}{\cancel{3} \cdot \cancel{2} \cdot 1 \cdot \cancel{7!}}$$

$$= 120$$

ways to do this.

Corollary:

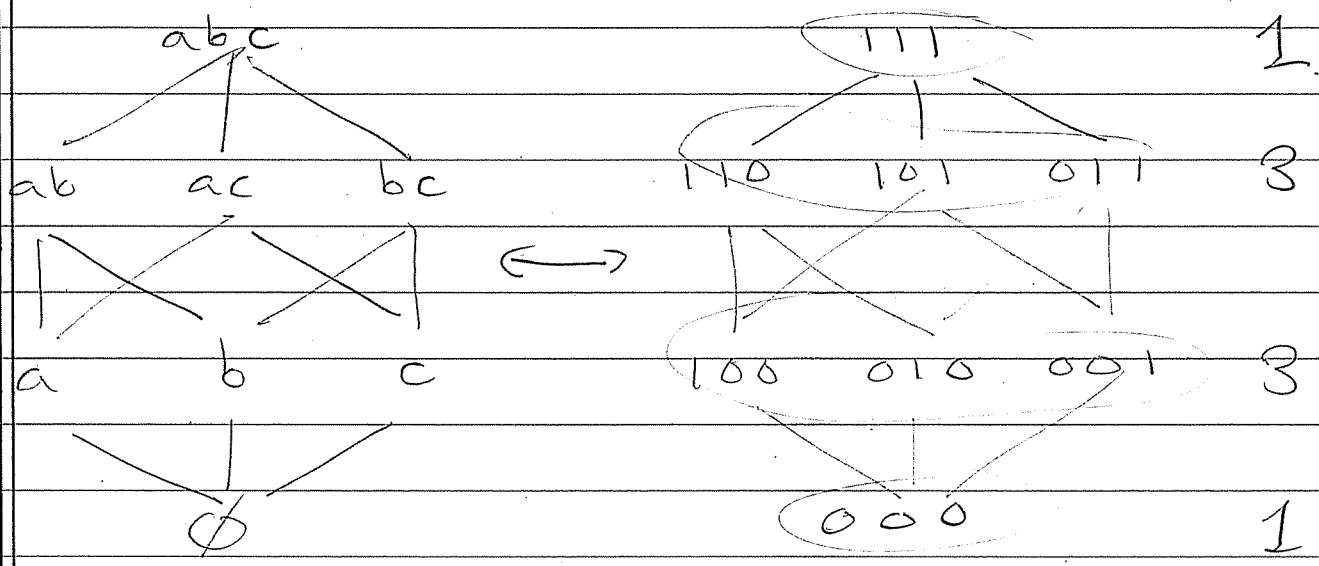
$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$$

Proof: Both sides count the subsets of a set $|A| = n$. ∎

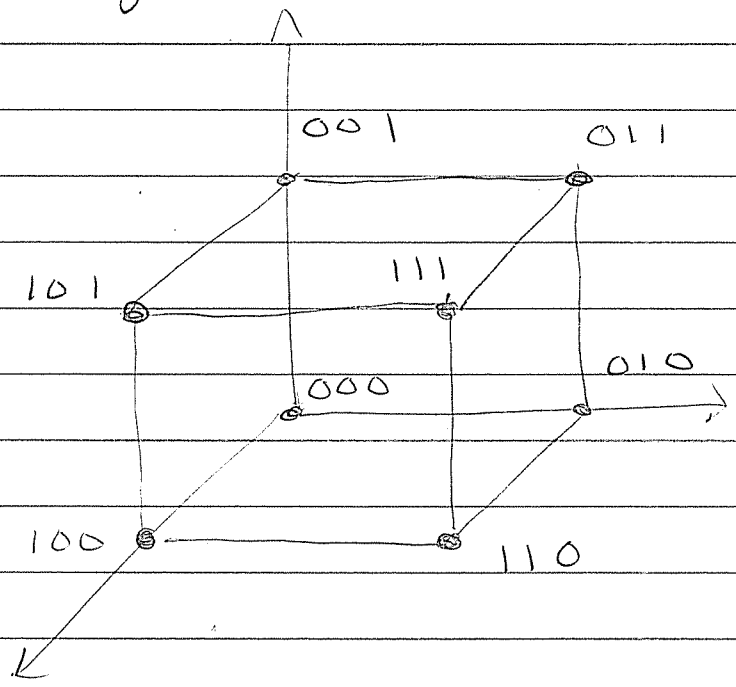
See:

1	$1 : 2^0$
1 1	$2 = 2^1$
1 2 1	$4 = 2^2$
1 3 3 1	$8 = 2^3$
1 4 6 4 1	$16 = 2^4$

Picture: Subsets of $\{a, b, c\}$

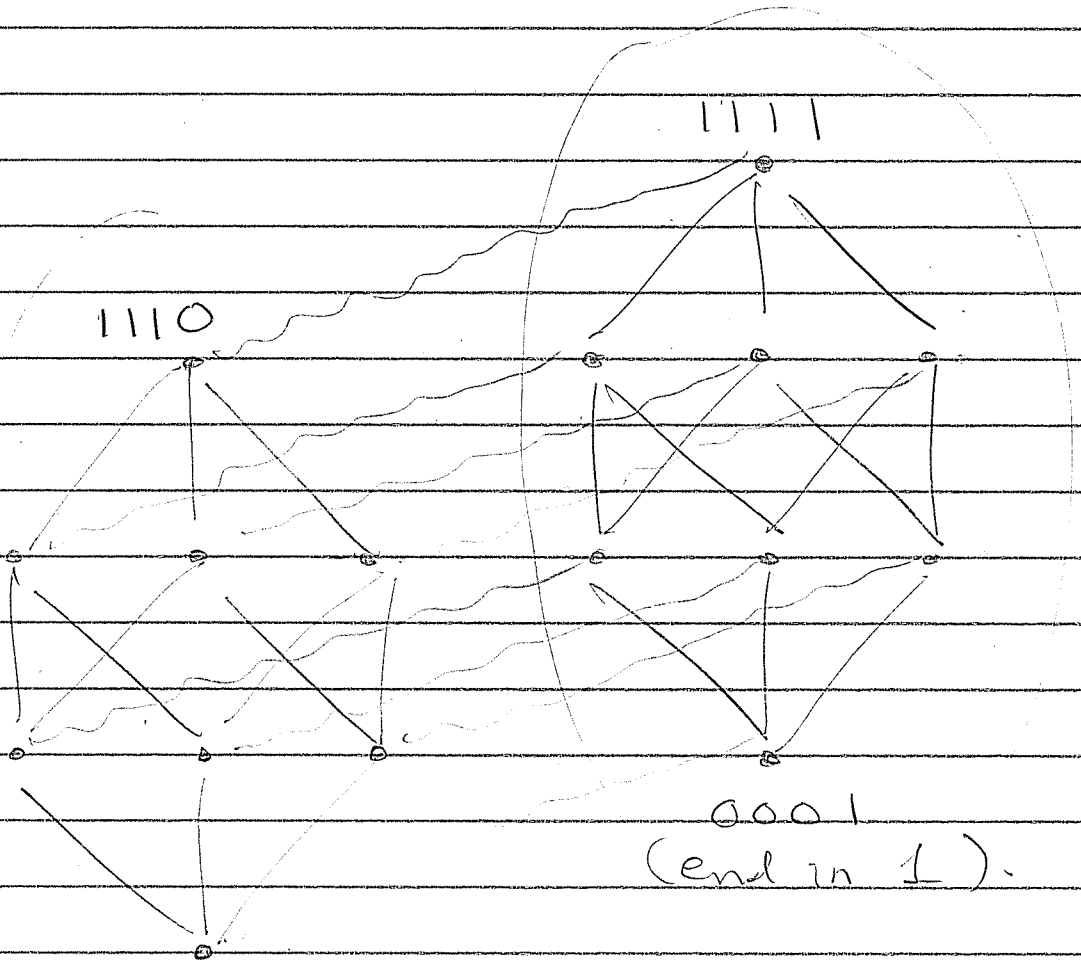


Geometry?



A cube!

Next: n=4 is a "hypercube".



$$2^3 + 2^3 = 2^4$$

Recursive Structure!

Mon Nov 19

HW 6 due Wed Nov 28

Exam 3 Fri Nov 30.

This week: Cryptography.

The math behind modern cryptography begins with

Fermat's little Theorem (1640):

Given $a, p \in \mathbb{Z}$ with p prime and $p \nmid a$, then

$$a^{p-1} = 1 \mod p.$$

(i.e. $p \mid a^{p-1} - 1$)

We can rephrase this. Multiply both sides by a to get

$$\boxed{a^p = a \mod p}$$

This holds for all $a, p \in \mathbb{Z}$ with p prime.

As usual, Fermat left behind no proof of FLT. ☹

First published proof by Euler (1736) uses Binomial Theorem and Induction.

Lemma ("Freshman's Dream"):

Given $a, b, p \in \mathbb{Z}$ with p prime we have

$$(a+b)^p = a^p + b^p \mod p.$$

Examples:

$$(a+b)^2 = a^2 + \cancel{2}^{0}ab + b^2 \mod 2$$

$$(a+b)^3 = a^3 + \cancel{3}^{0}a^2b + \cancel{3}^{0}ab^2 + b^3 \mod 3$$

$$(a+b)^4 = a^4 + \cancel{4}^{0}a^3b + \cancel{6}^{2}a^2b^2 + \cancel{4}^{0}ab^3 + b^4 \mod 4$$

$$= a^4 + 2a^2b^2 + b^4 \mod 4$$

(4 is not prime!)

$$(a+b)^5 = a^5 + \cancel{5}^{0}a^4b + \cancel{10}^{0}a^3b^2 + \cancel{10}^{0}a^2b^3 + \cancel{5}^{0}ab^4 + b^5$$

$$= a^5 + b^5 \mod 5 \quad \checkmark$$

Proof: By Binomial Theorem we have

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$$

hope this is zero mod p.
i.e. divisible by p.

Indeed, we will show that $p \mid \binom{p}{k}$ for $1 \leq k \leq p-1$.

Note $\binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{Z}$

Consider prime factorization of numerator and denominator. We have $p \mid p!$.

But $p \nmid k!(p-k)!$ since otherwise Euclid's Lemma $\Rightarrow$ p divides some number $< p$, contradiction.

Hence $p \mid \frac{p!}{k!(p-k)!}$ for $1 \leq k \leq p-1$.

So how did Euler prove FLT? Induction!

Fix prime $p \in \mathbb{Z}$ and let

$$P(n) = \text{“ } n^p = n \bmod p \text{ ”}$$

claim: $P(n) = T \quad \forall\, n \geq 0$.

Informally,

$0^p = 0 \bmod p$ ✓

$1^p = 1 \bmod p$ ✓

$2^p = (1+1)^p = 1^p + 1^p = 1 + 1 = 2 \bmod p$ ✓

$3^p = (1+2)^p = 1^p + 2^p = 1 + 2 = 3 \bmod p$ ✓

etc. ▨

Summary: for all $a, p \in \mathbb{Z}$ with p prime

we have $a^p = a \bmod p$.

$(p \mid a^p - a = a(a^{p-1} - 1))$

↓

By Euclid this means $p \mid a$ OR $p \mid a^{p-1} - 1$.

If $p \nmid a$ we have

$$\boxed{a^{p-1} = 1 \bmod p}$$

Q: Does FLT have a converse?

i.e. If $a^n = a \bmod n$ for all $a \geq 0$, does it follow that n is prime??

A: NO. We have

$$a^{561} = a \bmod 561 \quad \forall\, a \geq 0$$

But $561 = 3 \cdot 11 \cdot 17$ NOT prime.

Say 561 is a "Carmichal number"

Theorem (1994)

$\exists$ ∞ many Carmichal numbers ☹

Luckily, they are quite rare ☺

Problem: Factoring numbers is HARD.

But computing $a^b \bmod c$ is computationally easy (logarithmic)

Idea: Given $n \in \mathbb{Z}$, compute $a^n \bmod n$ for some small a.

If $a^n = a \bmod n$,

say n is a "pseudoprime base a"

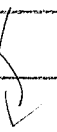
Hope: If n is a pseudoprime, then n is probably prime.

This works very well. In fact if

$$2^n = 2 \bmod n$$

(i.e. n is a pseudoprime base 2)

Then n is very likely prime.



If $2^n = 2 \bmod n$ and n is NOT prime we call n a "Poulet number".

First few Poulet numbers are

341, 561, 645, 1105, 1387, ...

There are only 21853 Poulet #'s $< 25 \times 10^9$
But there are $\approx$ 1 billion primes in this range.!

Therefore, if we choose a random number $n \leq 25 \times 10^9$, we have

$$P(n \text{ is prime, given that } 2^n = 2 \bmod n)$$

$$\approx 1 - \frac{21853}{10^9}$$

$$\approx 0.999998$$

That's pretty good!

Wed Nov 21

HW 6 due Wed Nov 28

Exam 3 Fri Nov 30

Today: Cryptography

Recall Fermat's little Theorem (1640):

Given $a, p \in \mathbb{Z}$ with p prime and $\gcd(a,p) = 1$, we have

$$a^{p-1} = 1 \mod p$$

"$p \mid (a^{p-1} - 1)$"

On HW 6.2 you will prove a slight generalization:

Given $a, p, q \in \mathbb{Z}$ with p and q prime and $\gcd(a, pq) = 1$, we have

$$a^{(p-1)(q-1)} = 1 \mod pq.$$

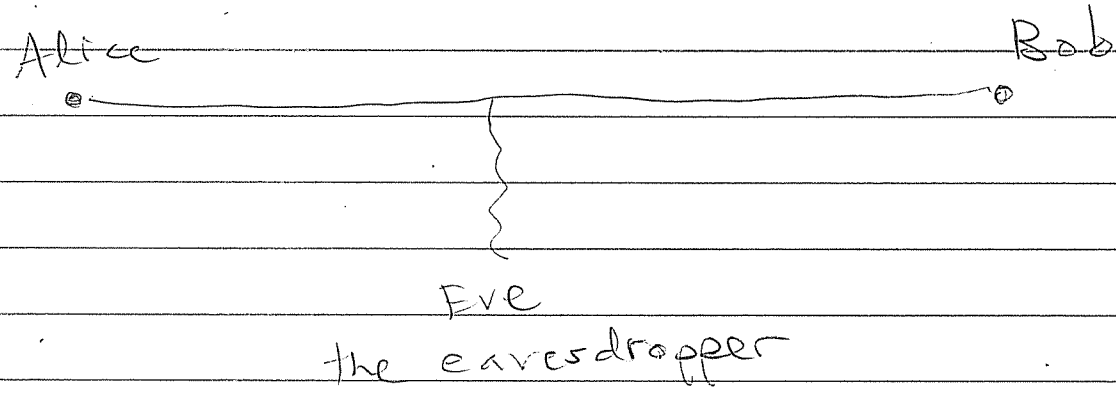
"$pq \mid (a^{(p-1)(q-1)} - 1)$"

Why do we care? ☺

Cryptography:

Alice and Bob want to send secrets to each other.
In olden days they would meet in secret to establish a tricky code. Then they could use the code to send secrets from a distance.

Problem: But what if they can't meet?
(chicken and egg)



Old Idea:
The problem is impossible

Then a revolution (1976):
"Diffie-Hellman-Merkle key exchange"

The idea:

Alice in secret	in Public	Bob in secret
	Choose large prime p and base $\gcd(g, p) = 1$.	
Choose secret $a \in \mathbb{Z}$ and compute $A = g^a \bmod p$	$\longrightarrow$ send A.	Choose secret $b \in \mathbb{Z}$ and compute $B = g^b \bmod p$
	send B $\longleftarrow$	
Compute $s = B^a \bmod p$		Compute $s = A^b \bmod p$.

Note. $s = A^b = (g^a)^b = g^{ab} = g^{ba}$

$= (g^b)^a = B^a \bmod p$

Now Alice and Bob share the "secret" s. (They can use it to set up a cipher.)

Eve knows: g, p, A, B

She wants: a, b, s.

She must compute

$$a = \log_g(A) \mod p$$
$$b = \log_g(B) \mod p$$

But this is computationally HARD.

The system is <u>secure</u> if we have

Compute	compute
$g^a \mod p$	$\log_g(A) \mod p$
$\longleftarrow$	$\longrightarrow$
EASY	HARD

OK, but this is still inconvenient

(Alice and Bob have to send 2 messages — what if Bob is asleep?)

Improvement: The RSA crypto system
(Rivest-Adleman-Shamir, 1977)

Alice wants to receive secret messages, so
- she chooses 2 large primes p, q.
- chooses random e with $\gcd(e, (p-1)(q-1)) = 1$

She Publishes and Keeps Secret

$\underbrace{e \;\&\; n := pq}$ $\qquad$ $\underbrace{p, q, (p-1)(q-1)}$

public key $\qquad$ private key.

To send Alice a message:
- convert message to a number $1 \le m \le n$
- compute $c := e^m \bmod n$
- send c to Alice
(the "ciphertext").

Alice decodes the message:
- she computes $d := e^{-1} \bmod (p-1)(q-1)$
(Euclidean Alg.)
- Then, Claim:

$$m = c^d \bmod n$$ ☺

Why? Working mod n we have

$$c^d \equiv (m^e)^d$$
$$\equiv m^{ed} \qquad ed = 1 \bmod (p-1)(q-1).$$
$$\equiv m^{1+k(p-1)(q-1)}$$
$$\equiv m\left(m^{(p-1)(q-1)}\right)^k$$
$$\equiv m(1)^k \qquad \text{FLT \& HW6.2.}$$
$$\equiv m \pmod n$$

✓

Eve Know : e and $n = pq$.

wants : $(p-1)(q-1)$ and hence

$d = e^{-1} \bmod (p-1)(q-1)$

Idea:

Getting $(p-1)(q-1)$ from pq is HARD!

"Factoring" is HARD!

Strange: DHM and RSA were independently (earlier) discovered by British Intelligence GCHQ and declassified in 1997.

See "The Code Book", by Simon Singh

Mon Nov 26

HW 6 due Wed
Exam 3 Fri + Math Club Wed
Today: "Review"
Wed: Review

Q: What are the coefficients of $(a+b+c)^n$?

Pretend a, b, c don't commute
i.e. $ab \neq ba$, $ac \neq ca$, $bc \neq cb$

$(a+b+c)^0 = 1$

$(a+b+c)^1 = a+b+c$

$(a+b+c)^2 = (a+b+c)(a+b+c)$

$= aa + ab + ac + ba + bb + bc + ca + cb + cc$

$= aa + \{ab + ba\} + bb$

$+ \{ac + ca\} + \{bc + cb\}$

$+ cc$

1 2 1
2 2
1

{ commute

$= a^2 + b^2 + c^2 + 2ab + 2ac + 2bc.$

27 terms

$$(a+b+c)^3 = (a+b+c)(a+b+c)(a+b+c)$$

$$= aaa + \{aab + aba + baa\} + \{abb + bab + bba\} + bbb$$

$$\{aac + aca + caa\} + \{abc + acb + bac + bca + cab + cba\} + \{bbc + bcb + cbb\}$$

$$+ \{acc + cac + cca\} + \{bcc + cbc + ccb\}$$

$$+ ccc$$

(commute)

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

$$+ 3a^2c + 6abc + 3b^2c$$

$$+ 3ac^2 + 3bc^2$$

$$+ c^2$$

Formula?

		1		
	1		1	
1		2		1
	3		3	
3		6		3
	3		3	
3		3		
	1			

For general n, each term of $(a+b+c)^n$ looks like

$$f(i,j,k)\, a^i b^j c^k$$

for some $i, j, k \geq 0$ with $i+j+k=n$

Observe: Coefficient $f(i,j,k)$ = # words with i "a"s, j "b"s and k "c"s.

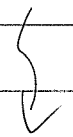
Can we count these words? Yes!

Theorem: Given $i,j,k \geq 0$ with $i+j+k=n$ we have

$$f(i,j,k) = \frac{n!}{i!\, j!\, k!}$$

Proof: Let $f(i,j,k)$ = # words with i "a"s, j "b"s and k "c"s.

Instead of counting these directly,



let's count the words that use the labeled symbols

$$\underbrace{a_1, a_2, \dots, a_i, b_1, b_2, \dots, b_j, c_1, c_2, \dots, c_k}_{n \text{ distinct symbols.}}$$

$\Longrightarrow$ (easy) there are $n!$ such words.

On the other hand, we could first place the unlabeled a's, b's, c's, and then label them

$$n! = f(i,j,k) \cdot i! \cdot j! \cdot k!$$

$f(i,j,k)$: # unlabeled words

$i! \cdot j! \cdot k!$: # ways to label them

Divide by $i! \, j! \, k!$ to get

$$f(i,j,k) = \frac{n!}{i! \, j! \, k!}$$

Corollary (Trinomial Theorem):

$$(a+b+c)^n = \sum_{\substack{i,j,k \geq 0 \\ i+j+k=n}} \frac{n!}{i!\,j!\,k!}\, a^i b^j c^k$$

Suggestive Notation: For $i+j+k=n$

$$\binom{n}{i,j,k} := \frac{n!}{i!\,j!\,k!}$$

a "trinomial coefficient"

Compare Binomial Theorem:

$$(a+b)^n = \sum_{\substack{i,j \geq 0 \\ i+j=n}} \frac{n!}{i!\,j!}\, a^i b^j$$

$j = n-i$ if you want

$$\binom{n}{i,j} = \frac{n!}{i!\,j!}$$

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

OR

$(n-k)$: redundant

∃ Pascal's Recurrence? Yes!

Theorem: $\forall\ i+j+k=n,\ i,j,k \geq 0$, have

$$\boxed{\binom{n}{i,j,k} = \binom{n-1}{i-1,j,k} + \binom{n-1}{i,j-1,k} + \binom{n-1}{i,j,k-1}}$$

"Pascal's Pyramid"

Proof: $\binom{n-1}{i-1,j,k} + \binom{n-1}{i,j-1,k} + \binom{n-1}{i,j,k-1}$

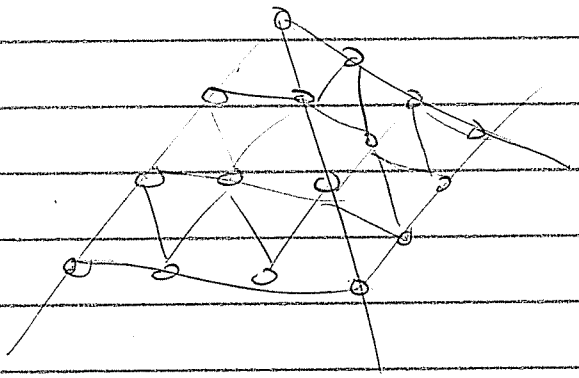
$$= \frac{i\,(n-1)!}{i\,(i-1)!\,j!\,k!} + \frac{j\,(n-1)!}{j\,i!\,(j-1)!\,k!} + \frac{k\,(n-1)!}{k\,i!\,j!\,(k-1)!}$$

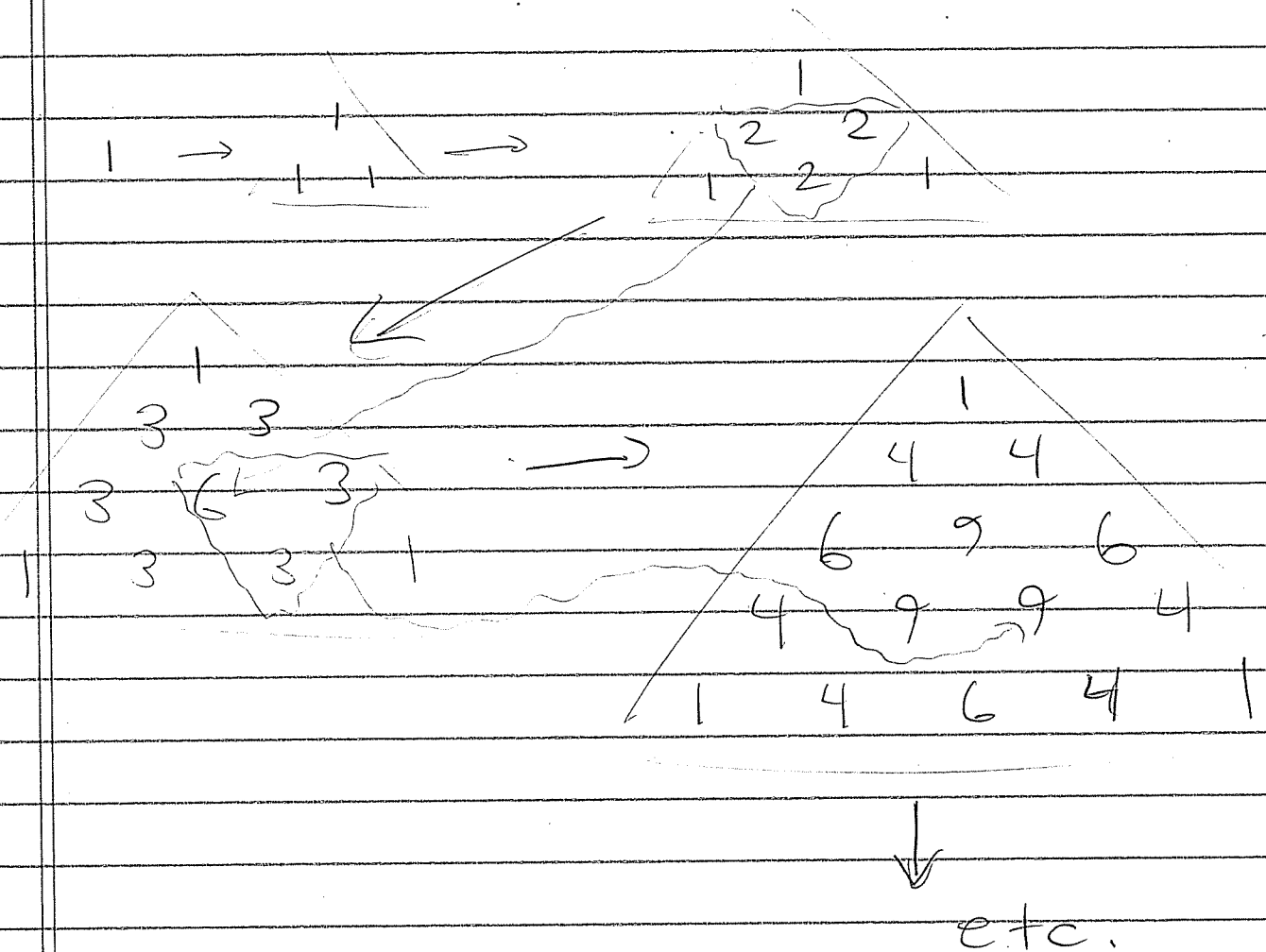
$$= \frac{i\,(n-1)! + j\,(n-1)! + k\,(n-1)!}{i!\,j!\,k!}$$

$$= \frac{(i+j+k)(n-1)!}{i!\,j!\,k!} = \frac{n\,(n-1)!}{i!\,j!\,k!}$$

$$= \frac{n!}{i!\,j!\,k!} = \binom{n}{i,j,k}$$

Pascal's Pyramid: Every entry is the sum of the 3 above.





Application: How many different "words" can you make from the letters

m, i, s, s, i, s, s, i, p, p, i ?

11 letters total

1 m
4 i
4 s
2 p

It's the coefficient of $m^1 i^4 s^4 p^2$ in the expansion of $(m+i+s+p)^{11}$

i.e.

$$\binom{11}{1,4,4,2} = \frac{11!}{1!\,4!\,4!\,2!}$$

$$= \frac{11 \cdot 10 \cdot 9 \cdot \cancel{8} \cdot 7 \cdot \cancel{6} \cdot 5 \cdot \cancel{4!}}{\cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot 1 \cdot \cancel{2} \cdot 1 \cdot \cancel{4!}}$$

$$= 11 \cdot 10 \cdot 9 \cdot 7 \cdot 5$$

$$= 34650.$$

However, most of them are unpronouncable

Wed Nov 28

HW 6 due NOW.
Exam 3 Friday.
Today: Review

Topics for Exam 3:

(1) Induction
✓ (2) Binomial (Trinomial, etc.) Theorem

Induction is built-into the integers.
It's an axiom.

Peano's Axioms for $\mathbb{N}$ (1889):

$\mathbb{N}$ is a set with a function $S: \mathbb{N} \to \mathbb{N}$ satisfying 4 axioms. (Think $S(n) =$ "$n+1$")

(P1) $1 \in \mathbb{N}$
(P2) $\forall n \in \mathbb{N}$, $S(n) \neq 1$.
(P3) $\forall m, n \in \mathbb{N}$, $m \neq n \Rightarrow S(n) \neq S(m)$
(P4) $\forall K \subseteq \mathbb{N}$, $K \neq \emptyset$, we have.

If • $1 \in K$
and • $\forall n \in \mathbb{N}$, $n \in K \Rightarrow S(n) \in K$.
then $K = \mathbb{N}$.

Variety : ∃ at least 3 ways to express (p4)

WO : Every nonempty $K \subseteq \mathbb{N}$ has a least element. i.e.

$$\forall K \in 2^{\mathbb{N}} \setminus \{\emptyset\}, \exists x \in K, \forall y \in K, x \leq y.$$

PI : Let $P : \mathbb{N} \to \{T, F\}$.

If • $P(b) = T$ for some $b \in \mathbb{N}$.
and • $\forall k \geq b$, $P(k) \Rightarrow P(k+1)$

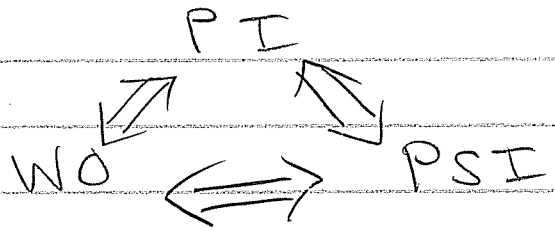
then $P(n) = T \quad \forall n \in \mathbb{N}, n \geq b$.

PSI : Let $P : \mathbb{N} \to \{T, F\}$

If • $P(b) = T$ for some $b \in \mathbb{N}$
and • $\forall k \geq b$, we have
$(P(b) = P(b+1) = \cdots = P(k) = T) \Rightarrow (P(k+1) = T$

then $P(n) = T \quad \forall n \in \mathbb{N}, n \geq b$.

Fact:



Examples:

(1) PI: Prove that $6 \mid (2n^3 + 3n^2 + n) \quad \forall\, n \geq 1$.

Proof: Let $P(n) =$ "$6 \mid (2n^3 + 3n^2 + n)$".

Note that $P(1) =$ "$6 \mid 6$" $= T$.

Now fix some $k \geq 1$ and assume that $P(k) = T$, i.e. $\exists\, l \in \mathbb{Z}$ such that $6l = 2k^3 + 3k^2 + k$. We want to show $P(k+1) = T$. Indeed,

$$2(k+1)^3 + 3(k+1)^2 + (k+1)$$

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

$$= (2k^3 + 3k^2 + k) + 6k^2 + 6k + 2 + 6k + 3 + 1$$

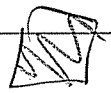
$\Big\}$

$$= 6\ell + 6k^2 + 12k + 6.$$

$$= 6(\ell + k^2 + 6k + 1).$$

Hence $6 \mid [2(k+1)^3 + 3(k+1)^2 + (k+1)]$

as desired.]

By PI we have $P(n) = T \ \forall \ n \geq 1$ 

(2) WO: $\sqrt{2}$ is irrational.

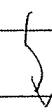
Proof: Assume $\sqrt{2}$ is rational.
Then the set

$$K = \{x \in \mathbb{N} : \exists\, y \in \mathbb{N} \text{ with } \sqrt{2} = \frac{x}{y}\} \subseteq \mathbb{N}$$

is not $\emptyset$. By WO $\exists$ smallest $a \in K$,
say $\sqrt{2} = a/b$. Square to get

$a^2 = 2b^2 \Rightarrow a^2$ even $\Rightarrow a$ even

Say $a = 2\ell$ for some $\ell \in \mathbb{N}$.



But then:

$$2b^2 = a^2 = 4\ell^2 \implies b^2 = 2\ell^2$$

$$\implies 2 = b^2/\ell^2 \implies \sqrt{2} = b/\ell.$$

$$\implies b \in K.$$

But $\sqrt{2} > 1 \implies b\sqrt{2} > b \implies a > b$.
This contradicts the fact that $a \in K$ is smallest.

(3) PSI: Every $n \geq 2$ has a prime factor

Proof: Let $P(n)$ = "$\exists$ prime p with $p \mid n$"

Note that $P(2) = T$ since 2 is prime and $2 \mid 2$.

Now fix $k \geq 2$ and [assume

that $P(2) = P(3) = \cdots = P(k) = T$.
We want to show that $P(k+1) = T$.

If $k+1$ is prime we're done since $(k+1) \mid (k+1)$.
Otherwise $\exists\ 1 < a, b < k+1$ with.

$$k+1 = ab.$$

Since $P(a) = T$ $\exists$ prime p with $p \mid a$.
But then $p \mid (k+1)$. Hence $P(k+1) = T$. ∎

By PSI we have $P(n) = T\ \forall\ n \geq 2$