Wed Nov 20

HW 5 due Friday.
NO CLASS NEXT WEEK.

Today: More about the Binomial Theorem.

Recall the definition of binomial coefficients:

$$(1+x)^n =: \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n$$

i.e. $\binom{n}{k}$:= coefficient of x^k in $(1+x)^n$.

We also define

$$\binom{n}{k} = 0 \quad \text{for } k<0 \text{ or } k>0.$$

☆ Theorem: For all $n, k \in \mathbb{Z}$, $n \geq 0$, we have

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

Proof Sketch: Observe that

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

Then $\binom{n}{k}$ is the coeff of x^k on the left

$\binom{n-1}{k} + \binom{n-1}{k-1}$ is the coeff of x^k on the right.

This allows us to compute $\binom{n}{k}$ recursively using Pascal's Triangle. The recurrence has initial conditions

$$\binom{0}{k} = \begin{cases} 1 & k = 0 \\ 0 & k \neq 0. \end{cases}$$

Example:

0 0 0 0 1 0 0 0 0

0 0 0 1 1 0 0 0

0 0 1 2 1 0 0

0 1 3 3 1 0

1 4 6 4 1

$\Longrightarrow$

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

But what if I just need to know $\binom{77}{18}$, without computing the whole triangle?

We want a "formula" for $\binom{n}{k}$.

Def: Given $n \geq 1$, define the factorial

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

We also define $0! = 1$ (You'll see why.).

Then we have

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

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

Proof: We will use induction on n (k is just along for the ride). So let

$$P(n) := \text{"}\binom{n}{k} = \frac{n!}{k!(n-k)!} \text{ for all } 0 \leq k \leq n\text{"}$$

We want to prove that $P(n) = T \ \forall n \geq 0$.

- Base Case: Note that $P(0) = T$ because

$$\binom{0}{0} = 1 = \frac{0!}{0!\,0!} \quad \checkmark$$

- Induction Step: Fix $N-1 \geq 1$ and assume for induction that $P(N-1) = T$. In this case we want to show that $P(N) = T$.

First note that

$$\binom{N}{0} = 1 = \frac{N!}{0!\,N!} \quad \checkmark$$

$$\therefore \binom{N}{N} = 1 = \frac{N!}{N!\,0!} \quad \checkmark$$

Now assume that $0 < k < N$.
Then we have

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

$$= \frac{(N-1)!}{k!\,(N-1-k)!} + \frac{(N-1)!}{(k-1)!\,(N-k)!} \quad \text{since } P(N-1) = T.$$

(Now we find a common denominator. Note that

$k! = k(k-1)!$ and $(N-k)! = (N-k)!(N-1-k)!$)

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

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

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

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

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

Hence $P(N) = T$. ///

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

Example: The coeff of x^7 in $(1+x)^{10}$ is

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

$$= \frac{10\cdot \overset{3}{\cancel{9}}\cdot \overset{4}{\cancel{8}}}{\cancel{3}\cdot\cancel{2}\cdot 1}$$

$$= 10\cdot 3\cdot 4 = 120.$$

That's nice but the proof is not enlightening. Where does the formula

$$\frac{n!}{k!\,(n-k)!}$$ come from ?? I.O.U.

We will use this to prove the "Freshman's Dream":

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

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Fri Nov 22

HW 5 due NOW
NO CLASS NEXT WEEK
HW 6 due Fri Dec 6
Exam 3 Mon Dec 9 in class
THE END.

Current Goal: Prove that $\forall a, p \in \mathbb{Z}$ with p prime we have

$$a^p \equiv a \pmod{p}.$$

Recall: We proved last time that

$$(1+x)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} x^k$$

for all integers $n \geq 0$.

What about a general binomial?

Example:

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)^2 \\ &= (a+b)(a^2+2ab+b^2) \\ &= (a^3+2a^2b+ab^2) + (a^2b+2ab^2+b^3) \\ &= a^3+3a^2b+3ab^2+b^3.\end{aligned}$$

☆ The Binomial Theorem: For $n \geq 0$ we have

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

Proof: If $a = 0$ we get

$$(0+b)^n = \underbrace{\binom{n}{0}0^n + \binom{n}{1}0^{n-1}b + \cdots + \binom{n}{n-1}0^1 b^{n-1}}_{\text{all zero.}} + \binom{n}{n}0^0 b^n$$

$$b^n = \binom{n}{n}0^0 b^n$$
$$= b^n \quad \checkmark$$

[Convention: we will say $0^0 = 1$.]

If $a \neq 0$ we substitute $x = \frac{b}{a}$ to get

$$\left(1 + \frac{b}{a}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \left(\frac{b}{a}\right)^k$$

$$\left(\frac{a+b}{a}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \frac{b^k}{a^k}$$

Multiply both sides by a^n to get

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

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

Now we can prove

☆ Freshman's Dream: $\forall a, b, p \in \mathbb{Z}$ with p prime we have

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

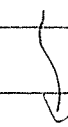
Proof: By Binomial Theorem we have

$$(a+b)^p = a^p + \underbrace{\binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1}}_{\text{Claim: This is divisible by } p} + b^p$$

We will show that for $0 < k < p$ we have $p \mid \binom{p}{k}$. Indeed, we know that

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

so the denominator divides the numerator



Note that $p \mid p! = p(p-1)(p-2)\cdots 3\cdot 2\cdot 1$.
But p does <u>not</u> divide the denominator

(Suppose $p \mid k!(p-k)!$

$p \mid k(k-1)\cdots 3\cdot 2\cdot 1\,(p-k)(p-k-1)\cdots 3\cdot 2\cdot 1$

By Euclid's Lemma, p divides some number on the right. But since $0 < k < p$, all the numbers on the right are <u>smaller</u> than p.)

We conclude that $p \mid \frac{p!}{k!(p-k)!}$.

Hence

$$(a+b)^p \equiv a^p + 0 + b^p \pmod{p}.$$

Mon Dec 2

Welcome Back!

HW 6 due Fri Dec 6

Exam 3 Mon Dec 9

NO FINAL EXAM

Where were we?

Recall the Binomial Theorem:

$\forall\, a, b, n \in \mathbb{Z}$ with $n \geq 0$ we have

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

This leads to the Freshman's Dream:

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

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

This leads to Fermat's little Theorem:

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

$$a^p \equiv a \pmod{p}$$

which can be restated as:

$\forall\, a, p \in \mathbb{Z}$ with $\gcd(a,p) = 1$ (i.e. $p \nmid a$) we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Finally, you will prove on HW 6 that

$\forall\, a, p, q \in \mathbb{Z}$ with p, q prime and $\gcd(a, pq) = 1$ (i.e. $p \nmid a$ and $q \nmid a$) we have

$$\boxed{a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.}$$

This is the foundation of modern (i.e. "public key") cryptography

☆ The RSA Cryptosystem

Alice wants to be able to receive secret messages from anyone in the world

(1) Alice selects two large primes $p \neq q$ and computes $n = pq$.

She chooses random $1 < e < (p-1)(q-1)$ with $\gcd(e, (p-1)(q-1)) = 1$.

She uses Euclidean algorithm to find $x, y \in \mathbb{Z}$ such that

$$ex + (p-1)(q-1)y = 1$$

She defines $d \equiv x \bmod (p-1)(q-1)$ so that

$$ed \equiv 1 \bmod (p-1)(q-1)$$

Proof: $ed \equiv ex$

$\equiv 1 - (p-1)(q-1)y$

$\equiv 1 \bmod (p-1)(q-1)$ //

Alice publishes (e, n), the PUBLIC ENCRYPTION KEY

and keeps secret (d, n), the PRIVATE DECRYPTION KEY.

② To send Alice a secret message:

Obtain her public key (e, n).

Convert your message to an integer $m \in \mathbb{Z}$ such that $0 \leq m < n$

Compute $c := m^e \pmod{n}$ with $0 \leq c < n$.

Send the integer c to Alice.

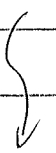
③ Alice decrypts the message as follows:

Alice receives $0 \leq c < n$.

Using her private key (d, n) she computes

$$r := c^d \pmod{n} \text{ with } 0 \leq r < n.$$

Theorem: r equals the message m



Proof: Recall that $ed \equiv 1 \bmod (p-1)(q-1)$

So we have

$$ed = 1 + k(p-1)(q-1) \text{ for some } k \in \mathbb{Z}.$$

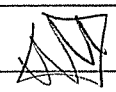
Then working mod $n = pq$ we have

$$\begin{aligned} r &\equiv c^d \\ &\equiv (m^e)^d \\ &\equiv m^{ed} \\ &\equiv m^{1+k(p-1)(q-1)} \\ &\equiv m\left(m^{(p-1)(q-1)}\right)^k \quad \bmod pq. \end{aligned}$$

Assume now that $p \nmid m$ and $q \nmid m$. Then by HW 6.4, we have

$$\begin{aligned} r &\equiv m\left(m^{(p-1)(q-1)}\right)^k \\ &\equiv m(1)^k \\ &\equiv m \quad \bmod pq. \end{aligned}$$

In the (very unlikely) case that $p \mid m$ or $q \mid m$, the proof involves the "Chinese Remainder Theorem" which we didn't discuss.



Issues:

- Why is this secure?

Eve the eavesdropper has access to

e, n and c

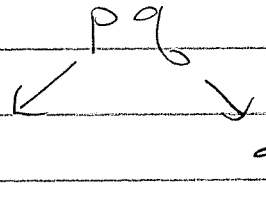
She wants to know m.

It's enough to know $(p-1)(q-1)$ since then she can compute

$$d \equiv e^{-1} \mod (p-1)(q-1)$$

and $m \equiv c^d \mod n$.

Idea: To get $(p-1)(q-1)$ from pq she must factor



But this is computationally HARD!