Number Theory Notes

Ernesto Diaz

September 16, 18 2019

DATE September 16, 2019

Consider our binomial Coefficient $\binom{n}{k}$ if 0$\leq k \leq$n we define

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

for k > n we define $\binom{n}{k}$ =0.

Fix a value of n, let $a_k = \binom{n}{k}$

Example n=3, $a_0 = \binom{3}{0} = 1$, $a_1 = \binom{3}{0} = 3$, $a_2 = \binom{3}{0} = 3$, $a_3 = \binom{3}{0} = 1$, $a_4 = 0 = a_5, a_6, \ldots$

Can we find a generating function for this sequence?

f(x)=$\sum_{i=1}^{\infty} \binom{n}{k} x^i$

Binomial Theorem: $(x+y)^n = \sum_{i=1}^{\infty} \binom{n}{i} x^i y^{n-i}$

set y=1 in this expression to get

$(x+1)^n = \sum_{i=1}^{\infty} \binom{n}{i} x^i$

Generalized Binomial coefficient if c$\in \mathbb{R}$ and k$\geq$0 is an integer we can define $\binom{c}{k} = \frac{c(c-1)...(c-k)}{k!}$

Note: that if c is a positive integer then this definition agrees with the old definition.

Using this definition we get generalized binomial theorem for c $\in \mathbb{R}$

$(x+1)^n = \sum_{i=1}^{\infty} \binom{c}{i} x^i$}Infinite if c$\notin \mathbb{N}$

Can we find a generating function for this sequence?

f(x)=$\sum_{i=1}^{\infty} \binom{n}{k} x^i$

Suppose we have a sum of n terms $x_1 + x_2 + \cdots + x_n$ we care about order in which we do the addition.

we want to insert parenthesis to make it unambiguous the order in which the additions are preformed

Example: n=4

$x_1 + x_2 + x_3 + x_4$

$((x_1 + x_2) + x_3) + x_4$

$x_1 + (x_2 + (x_3 + x_4))$

$(x_1 + (x_2 + x_3)) + x_4$

$(x_1 + x_2) + (x_3 + x_4)$

These are all the ways (5 ways to do it)

What if we had n terms?

Let c$_n$ count the number of ways to do addition of n terms

c$_1$=1, c$_2$ = 1, c$_3$ = 2, c$_4$ = 5,...

if we have n terms, there has to be 1 addition that happens last. Pick which

addition happens last
there are Size: k + (n-k)
$c_n = \sum_{i=1}^{n-1} c_i c_{n-i}$
c_{n-i}¡- ways to sum the last (n-i) terms
c_i¡- ways to sum the first i terms
Use generating functions:
Define c(x) = $\sum_{i=0}^{\infty} c_i x^i$
lest square this!
$c(x)^2 = (\sum_{i=0}^{\infty} c_i x^i)^2 =$
$c(x)^2 = \sum_{j=0}^{\infty}(\sum_{i=0}^{\infty} c_i c_{j-1})x^j$
$\sum_{i=0}^{\infty} c_i c_{j-1}$ ¡- foil out squares
Counting the ways to insert parenthesis to make $a_1 + a_2 + \cdots + a_n$ unambiguous (if order of doing addition mattered) count this by $c_n$some operation occurs last
$(a_1 + \cdots + a_i) + (a_{i+1} + \cdots + a_n)$
$c_i = a_1 + \cdots + a_i$
$c_{n-i} = a_{i+1} + \cdots + a_n$
Use generating Functions
$c(x) = \sum_{i=1}^{n-1} c_i c_{n-i}$
$c(x)^2 = (\sum_{i=0}^{\infty} c_i x^i)^2 =$
$c(x)^2 = \sum_{j=0}^{\infty}(\sum_{i=0}^{\infty} c_i c_{j-1})x^j$

$$\begin{aligned}
c(x)(x(c(x))) &= (c_0 + c_1x + c_2x^2 + \dots)(c_0 + c_1x + c_2x^2 + \dots) \\
&= 0x^0 + c_0^2x + (c_0c_1 + c_1c_0)x^2 + (c_0c_2 + c_1c_1 + c_2c_0)x^3 + \dots \\
c(x) &= c_0 + c_1x + c_2x^2 + \cdots + c_jx^j \text{ sum operation occurs} \\
c_0 &= 1 \\
c_jx &= (\sum_{i=0}^{j-1} c_jc_{j-i-1})x^i \\
c(x) &= 1 + xc(x)^2 \\
c_n &= \sum_{i=0}^{n-1} c_ic_{n-i-1}\text{Valid for } n \geq 1 \\
c(x) &= c_0 + c_1x + c_2x^2 + \dots \\
1 + xc(x)^2 &= 1 + x * ((c_0c_0) + (c_1c_0 + c_0c_1)x + \dots)\text{Remember } c_0 = 1 \\
c(x) &= 1 + xc(x)^2 \\
0 &= 1 - c(x) + x(c(x))^2\text{let y =c(x)} \\
0 &= 1 - (1)y + xy^2\text{By Quadratic Formula} \\
\text{y} &= \frac{1 \pm \sqrt{1-4x}}{2x} \\
c(x) &= \frac{1 \pm \sqrt{1-4x}}{2x}\text{We don't want an } x^{-1}\text{term in the generating function} \\
&= \text{ if we choose "t" we would get a (1/x) term, therefore} \\
c(x) &= \frac{1 \pm \sqrt{1-4x}}{2x} = \sum_{n=0}^{\infty} c_nx^n \\
&= \frac{1}{2x}(1-4x)^{1/2}\text{Us generalized binomial theorem!} \\
&= \frac{1}{2x}(1 - \sum_{i=1}^{\infty}(-4x)^i\binom{1/2}{i}) \\
&= \frac{-1}{2}(-1)^{n+1}(4)^{n+1}(\frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)\dots(\frac{1}{2}-n)}{(n+1)!}) \\
&= \frac{1}{2}(-1)^n(4)^{n+1}(\frac{\frac{1}{2}(\frac{-1}{2})(\frac{-3}{2})\dots(\frac{1-2n}{2})}{(n+1)!}) \\
&= \frac{1}{2}(4)^{n+1}((\frac{(\frac{1}{2})(\frac{3}{2})\dots(\frac{2n-1}{2})}{(n+1)!})
\end{aligned}$$

$$
\begin{aligned}
&= (4)^n\left(\frac{(\frac{1}{2})^n(1)(3)\dots(2n-1)}{(n+1)!}\right) \\
&= (4)^n\left(\frac{(\frac{1}{2})^n(1)(3)\dots(2n-1)}{(n+1)!}\right)\left(\frac{(n!)(1/2)^n(2^n)}{n!}\right) \\
&= \frac{4^n(1/2)^n(1/2)^n(2n!)}{(n+1)!(n!)} \\
&= \frac{2n!}{(n+1)!n!} \\
&= \frac{1}{n+1}\frac{2n!}{n!n!} \\
&= \frac{1}{n+1}\binom{2n}{n} \\
c_n &= \frac{1}{n+1}\binom{2n}{n} < -\text{This is the Catalan Numbers}
\end{aligned}
$$

Corollary: $\binom{2n}{n}$ is divisible by (n+1)
Modular arithmetic:
Definition: a$\equiv$ b(mod c) "a is congruent to b modulo c" if c|(a-b)
Example: 12 $\equiv$ 2(mod 5) because 5|(12-2)
Theorem: $\equiv$ is an equivalence relation
Recall an equivalence relation ˜satisfies 3 things:

- Reflexive: a ˜a
- Symmetric: a ˜b, b ˜a
- Transitive: if a ˜b, b ˜c, then a ˜c

Proof. Reflexive and Symmetric properties are trivial to show.
Transitive: Suppose a $\equiv$ b(mod n)) and b $\equiv$ c(mod n))
This means n|(a-b) and n|(b-c)
(a-b)+(b-c)=(a-c)
since n divides the 1st two it divides the third as well so a$\equiv$c(mod n) □

Theorem if a $\equiv$ a' (mod n) and b $\equiv$ b' (mod n) then a $\pm$ b $\equiv$ a'$\pm$ b' (mod n) and ab $\equiv$ a'b' (mod n)

Proof. Addition/subtraction is trivial to show so we will proceed to prove multiplication. we know n|(a-a') and n|(b-b'), we want to show that n|(ab-a' b') write

$$ab - a'b' = ab + (ab' - ab') - a'b' \qquad = a(b - b') + (a - a')b'$$

and we know that n divides (b-b') and (a-a')
So n|(ab-a' b') □

DefinitionWe call equivalence class of numbers equivalent to a(mod n) the residue class a(mod n) or sometimes a residue.

DATE September 18, 2019
We start the class by proposing a question:
When can we "divide" modulo n?
We introduce a law of modulo

Cancellation Law: if bc $\equiv$ bd (mod n) and gcd(b,n) = 1 then c $\equiv$ d (mod n)

Proof. : Suppose gcd(b,n)=1 and bc $\equiv$ bd (mod n) then n—(bc-db) since gcd(b,n)=1 this tells us that n—(c-d) so c $\equiv$ d (mod n) $\square$

This is false in general when gcd(b,n) $\neq$ 1
Example: 3(4) $\equiv$ 3(8) (mod 12) but 4 $\not\equiv$ 8 (mod 12).

Define: A complete reside System (mod n) is a set $\{r_1, r_2, \ldots, r_k\}$ of integers such that

1. $r_i \not\equiv r_j$ (mod n) if i $\neq$ j
2. if m is any integer where exists an r_j with m $\equiv r_j$ (mod n)

Example: If n=3 {0,1,2} forms a complete residue system (mod 3), {-1,0,1} is also a complete residue system, so does {5,9,22}

Theorem: Any Complete Residue System (mod n) $\{r_1, r_2, \ldots, r_k\}$ has exactly n elements.

Proof. Take $t_1 = 0, t_2 = 1, \ldots, t_n =$ n - 1.
The set $\{t_1, t_2, \ldots, t_n\}$ forms a complete residue system since:

1. If i $\neq$ j then 1+i-t, where 1<n. so $t_i \neq t_j$ (mod n)
2. If m is any integer we can do division with remainder m = q*n + s, $0 \leq s < n$ so m $\equiv$ s (mod n) and s $\in \{t_1, t_2, \ldots, t_n\}$

Note that $\{t_1, t_2, \ldots, t_n\}$ has size n. Now if $\{r_1, r_2, \ldots, r_n\}$ is also a complete residue system. Then each $r_i \equiv t_j$ for some j. we can't have $r_j \equiv t_j$ and $r_l \equiv t_j$ (mod n) if i $\neq$ l since the r_j are all distinct so k $\leq$ n. likewise we can match an r_j to each t_j since the r's also form a complete system so k $\geq$ n. So any complete residue system has size n. $\square$

Definition: Say that $\{r_1, r_2, \ldots, r_k\}$ is a reduced residue system (mod n) if

1. $r_i \not\equiv r_j$ for any i $\neq$ j

2. gcd(r_i,n)=1 for all i

3. if gcd(m,n)=1 then there exists an i with m $\equiv r_i$ (mod n)

Example: n=12 {1,5,7,11} or {13,17,19,23} or {-5,-1,1,5}
Definition: for any positive integer n we define φ(n) to be the count of numbers i $\in \{1, 2, \ldots, n-1\}$ which have gcd(i,n)=1
Example: φ(12)=4 Note
Observation: if n is prime the φ(p) = p-1
Example: p=5 reduced residue system {1,2,3,4}
Theorem: Any reduced residue system (mod n) contains exactly φ elements

Proof. It is nearly identical to the one for complete residue systems. □

Note: if we take any two elements of a reduced system and multiply them we get another integer which has gcd of 1 with n and thus is equivalent to a different reduced residue (mod n).
The collection of reduced residue form a group under multiplication
Denoted by $(\mathbb{Z}/n\mathbb{Z})^x$ - for a group
Euler's Theorem: if n is any positive integer and gcd(a,n) = 1 then $a^{\varphi(n)}$ $\equiv$ 1 (mod n)

Proof. Let $\{r_1, r_2, \ldots, r_k\}$ be a reduced residue system (mod n)
Note: it has size φ(n) multiply these residue together R = $r_1, r_2, \ldots, r_{\varphi(n)}$(mod n)
Now let s_i = ar_i(mod n) Then the s_i are all distinct mod n since if $s_i \equiv s_j$ (mod n) then $a * r_i \equiv a * r_j$ (mod n) by the cancellation property we have $r_i \equiv r_j$ (mod n). Therefore $\{s_1, s_2, \ldots, s_\varphi\}$ is also a reduced residue system.
Multiply the s_i together to get
$s_1, s_2, \ldots, s_{\varphi(n)} \equiv r_1, r_2, \ldots, r_{\varphi(n)} \equiv$ R (mod n) (possibly in a different order)
Also $s_1, s_2, \ldots, s_{\varphi(n)} = (ar_1), (ar_2), \ldots, (ar_{\varphi(n)}) \equiv a^{\varphi(n)} r_1 r_2 \ldots r_{\varphi(n} \equiv a^{\varphi(n)}$R (mod n)
so R$\equiv$ $a^{\varphi(n)}$ R(mod n) Since gcd(R,n)=1
use the cancellation property to get $1 \equiv a^{\varphi(n)}$ (mod n) □

Corollary: (Fermat's Little Theorem) If P is a prime $\varphi(p)$ =p-1 so $a^{\varphi(p)} \equiv a^{p-1} \equiv 1$(mod n).