

Binomial coefficient

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}, \quad k \geq 0 \text{ int, } n \in \mathbb{R}.$$

n integer

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \# \text{ of subsets with } k \text{ elts of a set with } n \text{ elts.}$$

Cor: if n integer, $\binom{n}{k}$ integer

Cor: The product of k consecutive integers is divisible by k!

Proof: $n(n-1)\cdots(n-k+1)$ is the form of any k consecutive integers

$$= \begin{cases} \binom{n}{k} k! & n \geq k \\ 0 & 0 \leq n < k \\ (-1) \binom{-n+k-1}{k} k! & n < 0 \end{cases}$$

Binomial Thrm: For every $n \geq 1$ and $x, y \in \mathbb{R}$,

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

Proof: By induction on n:

$$n=1. \quad x+y = \binom{1}{0}y + \binom{1}{1}x = y+x.$$

Assume true for $n-1$, prove for n.

$$\begin{aligned} (x+y)^n &= (x+y)(x+y)^{n-1} = (x+y) \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-1-k} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^{k+1} y^{n-1-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\ &= \sum_{k=1}^n \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} = x^n + \sum_{k=1}^{n-1} \left[\binom{n-1}{k-1} + \binom{n-1}{k} \right] x^k y^{n-k} + y^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \end{aligned}$$

$$\text{Lemma: } \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$$

$$\text{Proof: } \frac{(n-1)(n-2)\cdots(n-k+1)}{(k-1)!} + \frac{(n-1)(n-2)\cdots(n-k)}{k!} =$$

$$\frac{(n-k+k)[(n-1)(n-2)\cdots(n-k+1)]}{k!} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \binom{n}{k}$$

Congruences:Def: $m \neq 0$ integer, $a, b \in \mathbb{Z}$. a is congruent to b mod m if $m | a-b$.Notation: $a \equiv b \pmod{m}$.Lemma: $a \equiv b \pmod{m} \Leftrightarrow \{a+mx \mid x \in \mathbb{Z}\}$ and $\{b+my \mid y \in \mathbb{Z}\}$ are equalPr. If $m | (a-b)$, then $a-b = mx_0$. $\{a+mx\} = \{b+m(x_0+x)\} = \{b+my\}$.conversely, if $\{a+mx\} = \{b+my\}$, then $a = b+my_0 \Rightarrow a-b = my_0 \Rightarrow m | a-b$.

Thm $a, b, c, d \in \mathbb{Z}$, then

(1) $a \equiv b \pmod{m}$ iff $b \equiv a \pmod{m}$ iff $b-a \equiv 0 \pmod{m}$

(2) if $a \equiv b \pmod{m}$ and $b \equiv c$, then $a \equiv c \pmod{m}$

(3) & (4) if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $\begin{cases} a+c \equiv b+d \pmod{m} \\ ac \equiv bd \pmod{m} \end{cases}$

(5) if $a \equiv b \pmod{m}$ and $d|m, d \neq 0$, then $a \equiv b \pmod{d}$

(6) $a \equiv b \pmod{m}$ and $c \neq 0$, then $ac \equiv bc \pmod{mc}$.

Proof of (4):

$$\begin{aligned} a &= b + mx_0 & c &= d + my_0 & ac &= (b + mx_0)(d + my_0) = bd + mby_0 + mdx_0 + m^2x_0y_0 \\ & & & & &= bd + m(by_0 + dx_0 + mx_0y_0) \Rightarrow m|ac - bd. \end{aligned}$$

ex: $m=10$.

Every integer is congruent to exactly one elt. of $\{0, 1, \dots, 9\}$

by division with remainder $n = 10q + r, 0 \leq r < 10. \Rightarrow n \equiv r \pmod{10}$

$$7+5=12=10+2 \equiv 2 \pmod{10}$$

$$6 \cdot 3 = 18 \equiv 8 \pmod{10}$$

Warning! $ax \equiv ay \pmod{m}$ does not imply $x \equiv y \pmod{m}$.

ex: $2 \cdot 5 \equiv 2 \cdot 0 \pmod{10}$, but $5 \not\equiv 0$.

Thm: $ax \equiv ay \pmod{m}$ iff $x \equiv y \pmod{\frac{m}{(a,m)}}$

Proof: (1) \Rightarrow (2). $ax - ay = m\mathbb{Z} \Rightarrow \frac{a}{(a,m)}(x-y) = \frac{m}{(a,m)}\mathbb{Z}$

Now $\frac{a}{(a,m)} \mid \frac{m}{(a,m)}\mathbb{Z}$ and $(\frac{a}{(a,m)}, \frac{m}{(a,m)}) = 1$.

Thus, $\frac{a}{(a,m)} \mid \mathbb{Z} \Rightarrow x-y = \frac{m}{(a,m)}(\mathbb{Z}/\frac{a}{(a,m)}) \leftarrow \text{integer}$.