Lecture 3
Binomial Coefficients, Congruences

\[ n(n-1)(n-2)\ldots 1 = n! = \text{number of ways to order } n \text{ objects.} \]

\[ n(n-1)(n-2)\ldots (n-k+1) = \text{number of ways to order } k \text{ of } n \text{ objects.} \]

\[ \frac{n(n-1)(n-2)\ldots (n-k+1)}{k!} = \text{number of ways to pick } k \text{ of } n \text{ objects. This is called a} \]

(Definition) Binomial Coefficient:

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

Proposition 10. The product of any \( k \) consecutive integers is always divisible by \( k! \).

Proof. Wlog, suppose that the \( k \) consecutive integers are \( n-k+1, n-k+2 \ldots n-1, n \). If \( 0 < k \leq n \), then

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

which is an integer. If \( 0 \leq n < k \), then the sequence contains 0 and so the product is 0, which is divisible by \( k! \). If \( n < 0 \), then we have

\[ \prod_{i=1}^{k} (n-k+i) = (-1)^{k} \prod_{i=0}^{k-1} (-n + k - i) \]

which is comprised of integers covered by above cases.

We can define a more general version of binomial coefficient

(Definition) Binomial Coefficient: If \( \alpha \in \mathbb{C} \) and \( k \) is a non-negative integer,

\[ \binom{\alpha}{k} = \frac{(\alpha)(\alpha-1)\ldots(\alpha-k+1)}{k!} \in \mathbb{C} \]

Theorem 11 (Binomial Theorem). For \( n \geq 1 \) and \( x, y \in \mathbb{C} \):

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

Proof.

\[ (x+y)^n = (x+y)(x+y)\ldots (x+y) \quad \text{\( n \text{ times} \)} \]
To get coefficient of $x^k y^{n-k}$ we choose $k$ factors out of $n$ to pick $x$, which is the number of ways to choose $k$ out of $n$.

**Theorem 12** (Generalized Binomial Theorem). For $\alpha, z \in \mathbb{C}, |z| < 1$,

\[(1 + z)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} z^k\]

**Proof.** We didn’t go through the proof, but use the fact that this is a convergent series and Taylor expand around 0

\[f(z) = a_0 + a_1 z + a_2 z^2 \ldots \quad a_n = \frac{f^{(k)}(z)}{k!} \bigg|_{z=0}\]

---

**Pascal’s Triangle:** write down coefficients $\binom{n}{k}$ for $k = 0 \ldots n$

\[
\begin{array}{cccc}
n = 0: & & & 1 \\
n = 1: & & 1 & 1 \\
n = 2: & 1 & 2 & 1 \\
n = 3: & 1 & 3 & 3 & 1 \\
n = 4: & 1 & 4 & 6 & 4 & 1 \\
n = 5: & 1 & 5 & 10 & 10 & 5 & 1 \\
\end{array}
\]

* each number is the sum of the two above it

**Note:**

\[
\binom{m+1}{n+1} = \binom{m}{n} + \binom{m}{n+1}
\]

**Proof.** We want to choose $n + 1$ elements from the set $\{1, 2, \ldots m + 1\}$. Either $m + 1$ is one of the $n + 1$ chosen elements or it is not. If it is, task is to choose $n$ from $m$, which is the first term. If it isn’t, task is to choose $n + 1$ from $m$, which is the second term.

---

**Number Theoretic Properties**

- Factorials - let $p$ be a prime and $n$ be a natural number. Question is “what power of $p$ exactly divides $n!$?”

**Notation:** For real number $x$, then $\lfloor x \rfloor$ is the highest integer $\leq x$
Claim

\[ p^e \mid n!, \; e = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor \ldots \]

|| means exactly divides \(\Rightarrow p^e \mid n!, \; p^{e+1} \nmid n! \)

Proof. \(n! = n(n-1) \ldots 1\)

\[ \left\lfloor \frac{n}{p} \right\rfloor = \text{number of multiples of } p \text{ in } \{1, 2, \ldots n\} \]

\[ \left\lfloor \frac{n}{p^2} \right\rfloor = \text{number of multiples of } p^2 \text{ in } \{1, 2, \ldots n\}, \text{ etc.} \]

\[ \left\lfloor \frac{n}{p^3} \right\rfloor = \text{number of multiples of } p^3 \text{ in } \{1, 2, \ldots n\}, \text{ etc.} \]

\[ \left\lfloor \frac{n}{p^k} \right\rfloor = \text{number of multiples of } p^k \text{ in } \{1, 2, \ldots n\}, \text{ etc.} \]

Note: There is an easy bound on \(e\):

\[ e = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \]

\[ \leq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} \cdots \]

\[ \leq \frac{n}{1 - \frac{1}{p}} \]

\[ \leq \frac{n}{p - 1} \]

Proposition 13. Write \(n\) in base \(p\), so that \(n = a_0 + a_1p + a_2p^2 \ldots a_kp^k\), with \(a_i \in \{0, 1 \ldots p - 1\}\). Then

\[ e(a, p) = \frac{n - (a_0 + a_1 \cdots + a_k)}{p - 1} \]
Proof. With the above notation, we have

\[ \left\lfloor \frac{n}{p} \right\rfloor = a_1 + a_2 p \ldots a_k p^{k-1} \]

\[ \left\lfloor \frac{n}{p^2} \right\rfloor = a_2 + a_3 p \ldots a_k p^{k-1}, \text{ etc.} \]

\[ \vdots \]

\[ a_0 = n - p \left\lfloor \frac{n}{p} \right\rfloor \]

\[ a_1 = \left\lfloor \frac{n}{p} \right\rfloor - p \left\lfloor \frac{n}{p^2} \right\rfloor, \text{ etc.} \]

\[ \vdots \]

\[ \sum_{i=0}^{k} a = n - (p - 1) \left( \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor \ldots \right) \]

\[ \sum_{i=0}^{k} a = n - (p - 1)(e) \]

\[ e = \frac{n - \sum_{i=0}^{k} a}{p - 1} \]

\[ \blacksquare \]

**Corollary 14.** The power of prime \( p \) dividing \( \binom{n}{k} \) is the number of carries when you add \( k \) to \( n - k \) in base \( p \) (and also the number of carries when you subtract \( k \) from \( n \) in base \( p \)).

Some nice consequences:

- Entire \((2^k - 1)\)th row of Pascal’s Triangle consists of odd numbers
- \( 2^n \)th row of triangle is even, except for 1s at the end
- \( \binom{n}{p} \) is divisible by prime \( p \) for \( 0 < k < p \) (\( p \) divides numerator and not denominator)
- \( \binom{n^e}{k} \) is divisible by prime \( p \) for \( 0 < k < p^e \)

(Definition) **Congruence:** Let \( a, b, m \) be integers, with \( m \neq 0 \). We say \( a \) is congruent to \( b \) modulo \( m \) (\( a \equiv b \mod m \)) if \( m | (a - b) \) (i.e., \( a \) and \( b \) have the same remainder when divided by \( m \)).

Congruence compatible with usual arithmetic operations of addition and multiplication.
**ie.,** if \(a \equiv b \mod m\) and \(c \equiv d \mod m\)

\[
\begin{align*}
    a + c &\equiv b + d \pmod{m} \\
    ac &\equiv bd \pmod{m}
\end{align*}
\]

**Proof.**

\[
\begin{align*}
    a &= b + mk \\
    c &= d + ml \\
    a + c &= b + d + m(k + l) \\
    ac &= bd + bml + dmk + m^2kl \\
    &= bd + m(bl + dk + mkl)
\end{align*}
\]

\[\blacksquare\]

* This means that if \(a \equiv b \mod m\), then \(a^k \equiv b^k \mod m\), which means that if \(f(x)\) is some polynomial with integer coefficients, then \(f(a) \equiv f(b) \mod m\)

**NOT TRUE:** if \(a \equiv b \mod m\) and \(c \equiv d \mod m\), then \(a^c \equiv b^d \mod m\)

**NOT TRUE:** if \(ax \equiv bx \mod m\), then \(a \equiv b \mod m\) (essentially because \((x,m) > 1\)). But if \((x,m) = 1\), then true.

**Proof.** \(m | (ax - bx) = (a - b)x\), \(m\) coprime to \(x\) means that \(m | (a - b)\)

\[\blacksquare\]