# Big Formula Sheet 

Julian Zhang

September 2022

## 1 Introduction

this is my attempt to not lose it all

## 2 Algebra

### 2.1 Manipulations

## Theorem: Common Algebraic Manipulations:

1. $(a \pm b)^{2}=a^{2} \pm 2 a b+b^{2}$ (square of sum/difference)
2. $(a+b+c)^{2}=a^{2}+b^{2}+c^{2}+2(a b+a c+b c)$ (square of 3 sums)
3. $a^{2}-b^{2}=(a+b)(a-b)$ (difference of squares)
4. $(a \pm b)^{3}=a^{3} \pm 3 a^{2} b+3 b^{2} a \pm b^{3}$ (cube of sum/difference)
5. $a^{3} \pm b^{3}=(a \pm b)\left(a^{2} \pm a b+b^{2}\right)$ (sum/difference of cubes)
6. $a^{3}+b^{3}+c^{3}=(a+b+c)\left(a^{2}+b^{2}+c^{2}-a b-a c-b c\right)$ (cube of 3 sums)
7. $a^{n}-b^{n}=(a-b)\left(a^{n-1}+a^{n-2} b+\ldots+a b^{n-2}+b n-1\right)$ (generalized difference)
8. $a^{n}+b^{n}=(a+b)\left(a^{n-1}+a^{n-2} b+\ldots+a b^{n-2}+b n-1\right)$ (generalized sum for odd n )

### 2.2 Functions

Definition: A real function defined on $(a, b)$ is said to be convex if

$$
f\left(\frac{x}{y}\right) \leq \frac{f(x)+f(y)}{2}, x, y \in(a, b)
$$

If the opposite inequality holds, it is called concave

## Theorem: Function Properties:

1. If $f(X)$ and $g(x)$ are convex functions on $(a, b)$, then so are $h(x)=f(x)+g(x)$ and $M(x)=$ $\max f(x), g(x)$
2. If $f(X)$ and $g(x)$ are convex functions on $(a, b)$ and if $g(x)$ is nondecreasing on $(a, b)$, then it is convex on $(a, b)$
3. Given two functions $f(x), g(x)$ such that the domain of definition of $f$ contains the range of $g$. the composition of $f$ and $g$ is defined by $(f \circ g)(x):=f(g(x))$
4. If $f=g$ we write $f^{2}$ instead of $f \circ f$

### 2.3 Polynomials

Definition: Broadly speaking, a polynomial is the combination of more than one integer powers. The general form of a polynomial is:

$$
P(x)=a_{n} x^{n}+a_{n-1} x^{n-1}+\ldots a_{0}
$$

### 2.3.1 Root-finding Theorems

## Theorem: Factor Theorem:

Given a polynomial $P(x)=a_{n} x^{n}+a_{n-1}+\ldots a_{0},(x-k)$ is a factor of $P(x)$ if and only if $P(k)=0$, or if $k$ is a root of $P$

## Theorem: Remainder Theorem:

Given a polynomial $P(x)=a_{n} x^{n}+a_{n-1}+\ldots a_{0}$, the remainder of $P(x)$ divided by any $x-k$ is $P(k)$

## Theorem: Fundamental Theorem of Algebra:

Given a polynomial $P(x)$ of the $n$th degree, $P(x)$ has exactly $n$ complex roots, each of which can be expressed as $a+b i$. Given the $n$ roots $x_{1}, x_{2}, \ldots x_{n}$ of a polynomial $P(x)$, we have that

$$
P(x)=a\left(x-x_{1}\right)\left(x-x_{2}\right) \ldots\left(x-x_{n}\right)
$$

### 2.3.2 Coefficient Theorems

Theorem: Binomial Coefficient Theorem:

$$
(a+b)^{2}=\binom{n}{0} a^{n}+\binom{n}{1} a^{n-1} b+\ldots+\binom{n}{k} a^{n-k} b^{k}+\binom{n}{n-1} a b^{n-1}+\binom{n}{n} b^{n}
$$

## Theorem: Multinomial Coefficient Theorem:

$$
\left(x_{1}+x_{2}+\ldots x_{x}\right)^{n}=\sum_{i_{1}+i_{2}+\ldots i_{m}}^{n}\left(\frac{n!}{i_{1}!i_{2}!!_{m}!}\right) x_{1}^{i_{1}} x_{2}^{i_{2}} \ldots x_{m}^{i_{m}}
$$

## Theorem: Vieta's Theorems:

Given a polynomial $P(x)=a_{n} x^{n}+a_{n-1}+\ldots a_{0}$ with $n$ (not necessarily distinct) complex roots, we have that

$$
\begin{gathered}
r_{1}+r_{2}+\cdots+r_{n}=-\frac{a_{n-1}}{a_{n}} \\
r_{1} r_{2}+r_{1} r_{3}+\cdots+r_{n-1} r_{n}=\frac{a_{n-2}}{a_{n}} \\
\vdots \\
r_{1} r_{2} r_{3} \cdots r_{n}=(-1)^{n} \frac{a_{0}}{a_{n}}
\end{gathered}
$$

Compactly, this equates to

$$
\sum_{1 \leq i_{1}<i_{2}<\cdots<i_{k} \leq n}\left(\prod_{j=1}^{k} r_{i_{j}}\right)=(-1)^{k} \frac{a_{n-k}}{a_{n}}
$$

Vietas on the cubic $a x^{3}+b x^{2}+c x+d$ results in:

$$
\begin{aligned}
r_{1}+r_{2}+r_{3} & =\frac{-b}{a} \\
r_{1} r_{2}+r_{1} r_{3}+r_{2} r_{3} & =\frac{c}{a} \\
r_{1} r_{2} r_{3} & =\frac{-d}{a}
\end{aligned}
$$

### 2.3.3 Linear Function Optimization

The linear function $a x+b y=c$ has a maximized product $x y$ of: $\frac{x^{2}}{4 a b}$ when $x=\frac{c}{2 a}, y=\frac{c}{2 b}$.

$$
\begin{aligned}
y & =\frac{c-a x}{b} \\
x\left(\frac{c-a x}{b}\right) & =\frac{c x-a x^{2}}{b} \\
& =-\frac{1}{b}\left(a x^{2}-c x\right) \\
& =-\frac{1}{b}\left(a x^{2}-c x+\frac{c^{2}}{4 a^{2}}-\frac{c^{2}}{4 a^{2}}\right) \\
& =-\frac{1}{b}\left(\sqrt{a} x-\frac{c}{2 a}\right)^{2}+\frac{c^{2}}{4 a^{2} b}
\end{aligned}
$$

with a vertex at $\frac{c}{2 a}$. Plugging in x gives us a y value of $\frac{c}{2 b}$.

### 2.3.4 Partial Fraction Decomposition

Theorem: Partial Fraction Decomposition: Given a rational function

$$
f(x)=\frac{1}{L_{1}(x) L_{2}(x)+\ldots L_{n}(x) Q_{1}(x) Q_{2}(x) \ldots Q_{m}(x)}
$$

Where each $L_{i}$ is a linear factor and each $Q_{j}$ is an irreducible quadratic, there exist real numbers $A_{1}, A_{2}, \ldots A_{n}, B_{1}, B_{2}, \ldots B_{m}, \ldots C_{1}, C_{2}, \ldots C_{m}$ such that

$$
f(x)=\frac{A_{1}}{L_{1}(x)}+\frac{A_{2}}{L_{2}(x)}+\ldots \frac{A_{n}}{L_{n}(x)}+\frac{B_{1} x+c_{1}}{Q_{1}(x)}+\frac{B_{2} x+c_{2}}{Q_{2}(x)}+\ldots \frac{B_{m} x+c_{m}}{Q_{m}(x)}
$$

### 2.4 Logs

Theorem: Log Properties: $a^{b}=x \Longleftrightarrow \log _{a} x=b$. Thus, we have:

1. $\log _{b}(a)+\log _{b}(c)=\log _{b}(a \cdot c)$
2. $\log _{b}(a)-\log _{b}(c)=\log _{b}\left(\frac{a}{c}\right)$
3. $\log _{b}\left(a^{n}\right)=n \cdot \log _{b}(a)$
4. $\log _{a^{b}}(c)=\frac{1}{b} \cdot \log _{a}(c)$
5. $a^{\log _{a}(b)}=b$
6. $\log _{b}(a)=\frac{\log _{c}(a)}{\log _{c}(b)}$
7. $\log _{a}(b) \log _{b}(a)=1$

### 2.5 Trig

Definition: The three main trigonometric identities and their reciprocals:

$$
\begin{aligned}
\sin (x) & =\frac{o p p}{h y p} \\
\cos (x) & =\frac{a d j}{h y p} \\
\tan (x) & =\frac{o p p}{a d j} \\
\csc (x) & =\frac{1}{\sin (x)} \\
\sec (x) & =\frac{1}{\cos (x)} \\
\cot (x) & =\frac{1}{\tan (x)}
\end{aligned}
$$

### 2.5.1 Even-odd Identities

$$
\begin{gathered}
\sin (-x)=-\sin (x) \\
\cos (-x)=\cos (x) \\
\tan (-x)=-\tan (x)
\end{gathered}
$$

### 2.5.2 Period Identities

$$
\begin{array}{r}
\sin (x \pm 2 \pi)=\sin (x) \\
\cos (x \pm 2 \pi)=\cos (x) \\
\tan (x \pm \pi)=\tan (x) \\
\csc (x \pm 2 \pi)=\csc (x) \\
\sec (x \pm 2 \pi)=\sec (x) \\
\cot (x \pm \pi)=\cot (x)
\end{array}
$$

### 2.5.3 Conversion Identities

$$
\begin{aligned}
& \cos \left(\frac{\pi}{2}-x\right)=\sin (x) \\
& \sin \left(\frac{\pi}{2}-x\right)=\cos (x) \\
& \tan \left(\frac{\pi}{2}-x\right)=\tan (x) \\
& \cot \left(\frac{\pi}{2}-x\right)=\tan (x) \\
& \csc \left(\frac{\pi}{2}-x\right)=\sec (x) \\
& \sec \left(\frac{\pi}{2}-x\right)=\csc (x)
\end{aligned}
$$

### 2.5.4 Pythagorean Identities

$$
\begin{aligned}
& \sin ^{2} \theta+\cos ^{2} \theta=1 \\
& \tan ^{2} \theta+1=\sec ^{2} \theta \\
& \cot ^{2} \theta+1=\csc ^{2} \theta
\end{aligned}
$$

### 2.5.5 Sum and Difference Formulas

$$
\begin{gathered}
\sin (x \pm y)=\sin (x) \cos (y) \pm \cos (x) \sin (y) \\
\cos (x \pm y)=\cos (x) \cos (y) \mp \sin (x) \sin (y) \\
\tan (x \pm y)=\frac{\tan (x) \pm \tan (y)}{1 \mp \tan (x) \tan (y)}
\end{gathered}
$$

### 2.5.6 Product to Sum formulas

$$
\begin{aligned}
\sin (x) \sin (y) & =\frac{1}{2}[\cos (x-y)-\cos (x+y)] \\
\cos (x) \cos (y) & =\frac{1}{2}[\cos (x-y)+\cos (x+y)] \\
\sin (x) \cos (y) & =\frac{1}{2}[\sin (x+y)+\sin (x-y)]
\end{aligned}
$$

### 2.5.7 Sum to Product formulas

$$
\begin{aligned}
\sin x \pm \sin y & =2 \sin \frac{x \pm y}{2} \cos \frac{x \mp y}{2} \\
\cos x+\cos y & =2 \cos \frac{x+y}{2} \cos \frac{x-y}{2} \\
\cos x-\cos y & =-2 \sin \frac{x+y}{2} \sin \frac{x-y}{2}
\end{aligned}
$$

### 2.5.8 Double-angle formulas

$$
\begin{gathered}
\sin (2 \theta)=2 \sin (\theta) \cos (\theta) \\
\cos (2 \theta)=\cos ^{2}(\theta)-\sin ^{2}(\theta)=1-2 \sin ^{2}(\theta)=2 \cos ^{2}(\theta)-1 \\
\tan (2 \theta)=\frac{2 \tan (\theta)}{1-\tan ^{2}(\theta)}
\end{gathered}
$$

### 2.5.9 Half-angle formulas

$$
\begin{aligned}
\sin \left(\frac{x}{2}\right) & = \pm \sqrt{\frac{1-\cos (x)}{2}} \\
\cos \left(\frac{x}{2}\right) & = \pm \sqrt{\frac{1+\cos (x)}{2}} \\
\tan \left(\frac{x}{2}\right) & =\frac{1-\cos (x)}{\sin (x)}
\end{aligned}
$$

### 2.5.10 Function Laws

Law of Sines:

$$
\frac{a}{\sin (A)}=\frac{b}{\sin (B)}=\frac{c}{\sin (C)}
$$

Law of Cosines:

$$
a^{2}=b^{2}+c^{2}-2 b c \cos (A)
$$

Law of Tangents:

### 2.5.11 Area of Triangles

$$
\frac{\frac{1}{2} a b \sin (C)}{\sqrt{s(s-a)(s-b)(s-c)}}
$$

### 2.5.12 Misc Formulas

Amplitude Moderation: $a \sin x+b \cos x=\sqrt{a^{2}+b^{2}} \sin (x+\alpha)=\sqrt{a^{2}+b^{2}} \cos (x-\beta)$

### 2.6 Sequences and Series

### 2.6.1 Mean Quantities

## Definition:

- The arithmetic mean of $n$ numbers $a_{1}, a_{2}, \ldots, a_{n}$,

$$
A(a)=\frac{a_{1}+a_{2}+\ldots a_{n}}{n}
$$

- The geometric mean of $n$ nonnegative real numbers,

$$
G(a)=\sqrt[n]{\frac{1}{a_{1}}+\frac{1}{a_{2}}+\ldots \frac{1}{a_{n}}}
$$

- The square mean of $n$ real numbers,

$$
S(a)=\frac{\sqrt{a_{1}^{2}+a_{2}^{2}+\ldots+a_{n}^{2}}}{n}
$$

- The harmonic mean of $n$ real numbers,

$$
H(a)=\frac{1}{\frac{1}{a_{1}}+\frac{1}{a_{2}}+\ldots+\frac{1}{a_{n}}}
$$

## We then have the following relationships:

- $A(a) \geq G(a)$ for non-negative real numbers (AM-GM inequality)
- $S(a) \geq A(a)$ for real numbers
- $G(a) \geq H(a)$ for positive real numbers


### 2.6.2 Sum Quantities

Sum of Arithmetic Sequence: $a, a+d, a+2 d, \ldots$

$$
\sum_{i=1}^{n} a_{i}=a n+\frac{n(n-1)}{2} d
$$

Sum of Geometric Sequences: $a, a r, a r^{2}, \ldots$

$$
\begin{gathered}
\sum_{i=1}^{n} a_{i}=\frac{a\left(1-r^{n}\right)}{1-r} \\
\sum_{i=1}^{\infty} a_{i}=\frac{a}{1-r}
\end{gathered}
$$

### 2.6.3 Sequences Heuristics

1. For recursive sequences, try and look for patterns
2. If no recursive formula is given, try writing $a_{n+1}$ in terms of $a_{n}, a_{n-1}$, etc. in inductive fashion.
3. Try to telescope and cancel out series

### 2.7 Sigma Notation

### 2.7.1 Common Sequences

- $1+2+3+\ldots+n=\frac{n(n+1)}{2}$ (triangular numbers)
- $1+2+2^{2}+\ldots 2^{n}=2^{n+1}-1$ (sum of powers of 2$)$
- $1+3+5+\ldots+(2 n-1)=n^{2}$ (sum of odd numbers)
- $1^{2}+2^{2}+3^{2}+\ldots+\frac{n(n+1)(2 n+1)}{6}$ (sum of squares)
- $1^{3}+2^{3}+3^{3}+\ldots+\left(\frac{n(n+1)}{2}\right)^{2}$ (sum of cubes)


### 2.7.2 Sigma Properties

Definition: We use the uppercase Greek letter Sigma to denote summation in the following way:

$$
\sum_{i=1}^{n} x_{i}=x_{1}+x_{2}+\ldots x_{n}
$$

Theorem: Sigma Properties:

$$
\begin{gathered}
\sum_{k=1}^{n} c a_{k}=c \sum k=1^{n} a_{k} \\
\sum_{k=1}^{n}\left(a_{k}+b_{k}\right)=\sum k=1^{n} a_{k}+\sum k=1^{n} b_{k}
\end{gathered}
$$

### 2.7.3 Sigma Methods

1. By grouping/pairing up (derivation of Gaussian Sum)
2. By elimination (derivation of Geometric Series)

$$
\begin{aligned}
s & =a+a r+a r^{2}+\ldots \\
-r s & =a r+a r^{2}+a r^{3}+\ldots
\end{aligned}
$$

3. By telescoping
4. By recursive counting

### 2.8 Inequalities

### 2.8.1 AM-GM

## Theorem: AM-GM:

NOTE: This is a special case of Jensen's Inequality

$$
\frac{x_{1}+x_{2}+\cdots+x_{n}}{n} \geq \sqrt[n]{x_{1} x_{2} \cdots x_{n}}
$$

### 2.8.2 Cauchy-Schwartz

## Theorem: AM-GM:

NOTE: This is a special case of Holder's Inequality

$$
\left(a_{1}^{2}+a_{2}^{2}+\cdots+a_{n}^{2}\right)\left(b_{1}^{2}+b_{2}^{2}+\cdots+b_{n}^{2}\right) \geq\left(a_{1} b_{1}+a_{2} b_{2}+\cdots+a_{n} b_{n}\right)^{2}
$$

## 3 Number Theory

### 3.1 Bases

Definition: In base $n$, the largest possible value of a digit is $n-1$. A number $x$ in base $n$ is written as $x_{n}$, and the numerical value of $\overline{a_{k} a_{k-1} \cdots a_{0}}$ is

$$
a_{k} n^{k}+a_{k-1} n^{k-1}+\cdots a_{0}
$$

### 3.2 Divisibility

## Theorem: Fundamental Theorem of Arithmetic:

Every integer greater than 1 either is a prime itself or is the product of prime numbers. This product is unique up to the reordering of the factors. The general form is written as

$$
\prod_{i=1}^{n} p_{i}^{e_{i}}
$$

where $p_{i}$ are distinct primes and $e_{i}$ are nonnegative integers.

Definition: Let $a=\prod_{i=1}^{n} p_{i}^{d_{i}}$, and $b=\prod_{i=1}^{n} p_{i}^{e_{i}}$, then

$$
\begin{gathered}
\operatorname{gcd}(a, b)=\prod_{i=1}^{n} p_{i}^{\min \left(d_{i}, e_{i}\right)} \\
(a, b)=\prod_{i=1}^{n} p_{i}^{\max \left(d_{i}, e_{i}\right)}
\end{gathered}
$$

## Theorem: Divisibility over Bases

Given a number $x=\overline{a_{k} a_{k-1} \cdots a_{0}}=a_{k} n^{k}+a_{k-1} n^{k-1}+\cdots a_{0}$, in base n :

1. $n-1 \mid x$ if and only if $n-1 \mid a_{0}+a_{1}+\ldots+a_{k}$ (sum of digits)
2. $n \mid x$ if and only if $a_{0}=0$
3. $n+1 \mid x$ if and only if $n+1 \mid a_{0}-a_{1}+\ldots+(-1)^{k} a_{k}$ (alternating sum)

This can be generalized to factors of $n-1$ and $n+1$.

### 3.3 Diophantine Equations

## Theorem: Bezout's Identity

If $d=\operatorname{gcd}(a, b)$ then there always exist integers $x$ and $y$ such that

$$
a x+b y=d
$$

Moreover, the integers of the form $a z+b t$ are exactly the multiples of d. Many other number theory theorems, such as Euclid's Lemma and the Chinese Remainder Theorem are results of this identity.

Solve $55 x-169 y=1$ using the Euclidean Algorithm:

$$
\begin{aligned}
169 & =3 \times 55+4 \\
55 & =13 \times 4+3 \\
4 & =1 \times 3+1
\end{aligned}
$$

Since 4 and 3 are co-prime, we begin back-substitution:

$$
\begin{gathered}
4=1 \times 3+1 \Longrightarrow 4-1 \times 3=1 \\
4=1 \times(55-3 \times 4)=1 \Longrightarrow 14 \times 4=1 \times 55=1 \\
14 \times(169-3 \times 55)-1 \times 55=1 \Longrightarrow 14 \times 169-43 \times 55=1 \\
(x, y)=(-1806+169 k,-58+55 k), k \in \mathbb{Z}
\end{gathered}
$$

### 3.3.1 Common Factoring Motifs

Suppose $n=2^{50} \cdot 3^{27} \cdot 5^{15} \cdot 7^{7}$

- Number of positive divisors: $(50+1)(27+1)(15+1)(7+1)$
- Number of perfect square divisors: $\left(\left\lfloor\frac{50}{2}\right\rfloor+1\right)\left(\left\lfloor\frac{27}{2}\right\rfloor+1\right)\left(\left\lfloor\frac{15}{2}\right\rfloor+1\right)\left(\left\lfloor\frac{7}{2}\right\rfloor+1\right)$
- Product of positive divisors: $n^{\frac{d}{2}}$, paired
- Sum of divisors: $\left(1+2+2^{2}+\ldots 2^{50}\right)\left(1+3+\ldots 3^{28}\right)\left(1+5+\ldots 5^{15}\right)\left(1+7+\ldots 7^{7}\right)$ $=\left(2^{51}-1\right)\left(\frac{3^{28}-1}{2}\right)\left(\frac{5^{16}-1}{4}\right)\left(\frac{7^{8}-1}{6}\right)$


### 3.4 Mods

Theorem: Mod Properties: Let $a \equiv b(\bmod n)$, and c be a positive integer. Then,
(a) $a+c \equiv b+c(\bmod n)$
(b) $a-c \equiv b-c(\bmod n)$
(c) $a c \equiv b c(\bmod n)$
(d) $a^{c} \equiv b^{c}(\bmod n)$
(e) $a+b \equiv(a \bmod n)+(b \bmod n)(\bmod n)$
(f) $a b \equiv(a \bmod n)(b \bmod n)(\bmod n)$
(g) If $\operatorname{gcd}(c, n)=1$ and $d c \equiv e c(\bmod n)$, then $d \equiv e(\bmod n)$
(h) if $k|a, k| b$, and $k \mid n$, then $\frac{a}{k} \equiv \frac{b}{k}\left(\bmod \frac{n}{k}\right)$

### 3.4.1 Prime Mods

## Theorem: Fermat's Little Theorem:

Let $p$ be a prime number, and $a$ be an integer such that $\operatorname{gcd}(a, p)=1$. We have that:

$$
a^{p-1} \equiv 1 \bmod p
$$

## Theorem: Wilson's Theorem

For any prime number $p$, we have that

$$
(p-1)!\equiv 1 \bmod p
$$

## Theorem: Euler's Totient Theorem

Define $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ such that $\varphi(n)$ is the number of integers $1 \leq k \leq n$ such that $\operatorname{gcd}(k, n)=1$. Let $n>1$ be a positive integer and $a$ be an integer such that $\operatorname{gcd}(a, n)=1$, then

$$
a^{\varphi(n)} \equiv 1 \bmod n
$$

### 3.4.2 Quadratic Residues

Definition: Given $q$ and $n$ and that the equation $x^{2} \equiv q(\bmod n)$ has a solution, then $q$ is called the quadratic residue modulo $n$.
If this equation does not have a solution, then $q$ is called the quadratic non-residue modulo $n$.

- For example, $x^{2} \equiv 9 \bmod 15$ has a solution $x=12$, hence 9 is a quadratic residue $\bmod 15$.
- On the other hand, the equation $x^{2} \equiv 11 \bmod 15$ has no solution, hence 11 is a quadratic non-residue mod 15.
- In simpler terms, an integer $q$ is a quadratic residue $\bmod n$ if a square can take the form $(n k+q)$ for some positive integer $n$.

Theorem: Quadratic Congruences with Prime Mods: If $p$ is a prime, then

$$
x^{2} \equiv a \bmod (p)
$$

has a solution if and only if

$$
a^{\frac{p-1}{2}} \equiv 1 \bmod p
$$

### 3.4.3 Chinese Remainder Theorem

Theorem: Chinese Remainder Theorem: The system of linear congruences:

$$
\begin{gathered}
x \equiv a_{1} \bmod n_{1} \\
x \equiv a_{2} \bmod n_{2} \\
x \equiv a_{3} \bmod n_{3} \\
\ldots \\
x \equiv a_{k} \bmod n_{k}
\end{gathered}
$$

Has a solution if and only if

$$
\operatorname{gcd}\left(n_{i}, n_{j}\right) \mid\left(a_{i}-a_{j}\right)
$$

for every $i!=j$. In such a case, there is a unique solution $\bmod n$ when $n$ is the least common multiple of $n_{1}, n_{2}, \ldots n_{k}$

CRT applications: Solve the system of modular congruences:

$$
\begin{gathered}
x \equiv 1 \bmod 2 \\
4 x \equiv 3 \bmod 5
\end{gathered}
$$

First simplify the second equation to $x \equiv 3 \times 4 \equiv 2 \bmod 5$. Now we have

$$
\begin{aligned}
& x \equiv 1 \bmod 2 \\
& x \equiv 2 \bmod 5
\end{aligned}
$$

Then let $x=2 a+1=5 b+2$. A clear solution for $(a, b)$ is $a=3, b=1$. Then, $x=7$ is one solution to the system, so $x \equiv 7 \bmod 2 \times 5=10$ is the set of all solutions.

If $m$ and $n$ are not relatively prime, then let $\operatorname{gcd}(m, n)=g$. We split the system as follows:

$$
\begin{aligned}
x & \equiv a \bmod \frac{m}{g} \\
x & \equiv a \bmod g \\
x & \equiv b \bmod g \\
x & \equiv b \bmod \frac{n}{g}
\end{aligned}
$$

Then, we must check that $a \equiv b \bmod g$. If so, simply ignore the 3 rd congruence. Now, we have:

$$
\begin{aligned}
x & \equiv a \bmod \frac{m}{g} \\
x & \equiv a \bmod g \\
x & \equiv b \bmod \frac{n}{g}
\end{aligned}
$$

Now we have a system of 3 congruences, which we can solve for. If $\operatorname{gcd}\left(\frac{m}{g}, g\right)$ is not 1 , then repeat the decomposition. Essentially, decompose until we get a system of pairwise relatively prime congruences. Then solve.

## 4 Combinatorics

### 4.1 Permutations vs Combinations

Definition: The total number of permutations of $k$ elements taken from a set of $n$ elements (without repetition) is commonly denoted ${ }_{n} P_{k}$ :

$$
{ }_{n} P_{k}=n(n-1)(n-2) \cdots(n-k+1)=\frac{n!}{(n-k)!}
$$

where $n!=1 \times 2 \times \cdots \times n$ is the factorial of $n$.

Definition: The total number of combinations of $k$ elements taken from a set of $n$ elements (without repetition) is commonly denoted ${ }_{n} C_{k}$. In fact, combinations are so likely to come up in contests that we have a special notation for them: $\binom{n}{k}$.

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

### 4.2 Stars and Bars

## Theorem: Stars and Bars:

The number of ways to place $n$ indistinguishable balls into $k$ labelled urns is

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

The number of solutions in nonnegative integers to the equation $x_{1}+x_{2}+\cdots+x_{k}=n$ is

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

### 4.3 Expected Value

Definition: Expected Value: Let X be an event, then

$$
E(X)=\sum_{i} P\left(x_{i}\right) V\left(X_{i}\right)
$$

where $P\left(x_{i}\right)$ is the probability of the event and $V\left(X_{i}\right)$ is the value assigned to the event.
Properties:

1. (Linearity) Let $a$ be a constant and $X, Y$ be two events, then $E[a X+Y]=a E[X]+E[Y]$.
2. If $X$ and $Y$ are two independent events, then $E[X Y]=E[X] E[Y]$

### 4.4 Other Combo Tools

### 4.4.1 Pigeonhole Principle

## Theorem: Pigeonhole Principle:

It is impossible to place $n+1$ pigeons in $n$ holes without having one hole contain 2 or more pigeons.
Pigeonhole Applications:

- From any $n+1$ positive integers we can choose two so that their difference is divisible by $n$.
- If vertices of a triangle are in a rectangle (including the case they are on its sides), then the triangle's area is at most half of the rectangle's area.


### 4.4.2 Principle of Inclusion-Exclusion

Theorem: Principle of Inclusion-Exclusion (2 variables)

$$
|A \cup B|=|A|+|B|-|A \cap B|
$$

### 4.4.3 Recursive Counting

- Suppose the set of objects is $f(n)$. A common trick is to relate $f(n)$ to $f(n-1)$ and possibly other previous terms.
- State: A description of an intermediate stage of an event.
- Random Walk: Processes in which a person or thing is moving around some universe.


### 4.4.4 Generating Functions

Combinatorics problems will often ask to determine a certain sequence of numbers $a_{0}, a_{1}, a_{2}, \ldots \mathrm{~A}$ common technique to solve this type of problem is to encode this sequence as a (possibly infinite) polynomial,

$$
f(x)=\sum_{k=0}^{\infty} a_{k} x^{k}
$$

where the solution to the problem is one of the coefficients to the $n$th degree $x$ term.

## 5 Geometry

Theorems to memorize:

- Ptolemy's
- Ceva's
- Stewart's
- Shoelace

Strategies for geometry:

1. Draw a diagram with all the information labelled
2. Draw auxiliary lines
3. Plug in formulas directly
4. Use Algebra: Introduce variables, set up equations, calculate something in different ways
5. Use Coordinates or Vectors

## 6 Methods of Proof

All full-solution math contests will require you not only to know what things are true, but also to prove why they are true. Here are all the proof methods you will need for all high school math contests:

- Proof by Contradiction: Assuming that a false hypothesis is true, and proving that it causes something impossible to be true.
Example: Proof that $\sqrt{2}$ is irrational
- Proof by Induction:

1. Base Case: Proving that something is true for $x=1$
2. Induction Hypothesis: Assuming that something is true for a certain $x=n$
3. Induction Step: Using $x=n$ to prove that the same statement is true for $n+1$

Example: Proof that $1+2+\ldots+n=\frac{n(n+1)}{2}$

- Proof by Deduction: The opposite of induction, deduction takes a general formula and specializes it for a certain case.
Example: Most geometry problems
- Proof by Exhaustion: Splitting a hypothesis into all possible cases, and proving that it holds true for every case.

Example: Casework

