# MO Cheat Sheet

## Algebra

1. Inequalities

   - Always guess equality case
   - (Homogenisation) $a_1 a_2 \cdots a_n = 1 \iff a_1 = \frac{b_1}{b_2}, a_2 = \frac{b_2}{b_3}, \cdots a_n = \frac{b_n}{b_1}$
     $xyz = x + y + z + 2 \iff x = \frac{b+c}{a}, y = \frac{c+a}{b}, z = \frac{a+b}{c}$
     $x^2 + y^2 + z^2 - xyz = 4 \iff x = a + \frac{1}{a}, y = b + \frac{1}{b}, z = c + \frac{1}{c}$
     $x^2 + y^2 + z^2 + xyz = 4 \iff x = 2\cos A, y = 2\cos B, z = 2\cos C$
   - (Cauchy) For $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \in \mathbb{R}$, $(\sum a_i^2)(\sum b_i^2) \geq (\sum a_i b_i)^2$, eq when $\frac{a_i}{b_i} = k$.
     (Titu) For $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \in \mathbb{R}^+$, $\sum \frac{a_i^2}{b_i} \geq \frac{(\sum a_i)^2}{\sum b_i}$. Force square in numerator.

     Try to make numerator as strong as possible, denominators degree roughly equal
   - (Holder) If $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n, \ldots, z_1, z_2, \ldots, z_n$ are nonnegative real numbers and $\lambda_a, \lambda_b, \ldots, \lambda_z$ are nonnegative reals with sum of 1, then

$$a_1^{\lambda_a} b_1^{\lambda_b} \cdots z_1^{\lambda_z} + \cdots + a_n^{\lambda_a} b_n^{\lambda_b} \cdots z_n^{\lambda_z} \leq (a_1 + \cdots + a_n)^{\lambda_a} (b_1 + \cdots + b_n)^{\lambda_b} \cdots (z_1 + \cdots + z_n)^{\lambda_z}.$$

   - (Chebyshev) If $a_1 \geq \cdots \geq a_n$ and $b_1 \geq \cdots \geq b_n$, then $n(\sum a_i b_i) \geq (\sum a_i)(\sum b_i)$.
   - (Weighted AMGM) Let $a_1, a_2, \cdots, a_n$ and $w_1, w_2, \cdots w_n$ be positive reals with $\sum w_i = 1$. For any $r \neq 0 \in \mathbb{R}$, define $\mathcal{P}(r) = (w_1 a_1^r + w_2 a_2^r + \cdots + w_n a_n^r)^{1/r}$, and $\mathcal{P}(0) = \sum a_i^{w_i}$. Then if $r > s$, $\mathcal{P}(r) \geq \mathcal{P}(s)$ with equality iff $a_1 = a_2 = \cdots a_n$.

     (Note: $w_i = \frac{1}{n}$ and $r$ =2/1/0/-1 gives $QM \geq AM \geq GM \geq HM$.)
   - (Schurhead) If $a_1, a_2, \cdots a_n$ are positive reals and $(x_1, x_2, \cdots x_n) \succ (y_1, y_2, \cdots, y_n)$, then $[x_1, x_2, \cdots x_n] \geq [y_1, y_2, ..., y_n]$. For any $r \in \mathbb{N}$, $[r+2, 0, 0] + [r, 1, 1] \geq 2[r+1, 1, 0]$.
   - (Jensen) If $f$ is convex ($f''(x) \geq 0$), then $\sum f(a_i) \geq nf(\frac{\sum a_i}{n})$. The reverse is true when $f$ is concave.
   - (Karamata) If $f$ is convex ($f''(x) \geq 0$) and $(x_1, x_2, \cdots x_n) \succ (y_1, y_2, \cdots, y_n)$, then $\sum f(x_i) \geq \sum f(y_i)$. The reverse is true when $f$ is concave.

2. FEs

- Guess solutions, check if additive/can scale or shift
- For $\mathbb{R}$ to $\mathbb{R}$, swap variables, find zeros, make things disappear, show odd/even and sub $x \to -x$. $x \to f(x)$. Solve simul equations
- Show injectivity/surjectivity (possibly at a point/over a range)
- If pseudo-linear/pseudo-multiplicative i.e. $f(x+c) = f(x) + d$, $f(cx) = df(x)$ then compare $P(x, y)$ with $P(x+c, y)$ or $P(cx, y)$.
- $f(x+y) = f(x) + f(y)$ implies linear if
  - over $\mathbb{Q}$, $\mathbb{R}^+$
  - $f$ is bounded (above or below) on any non-trivial interval
  - continuous anywhere/monotonic over some interval
  - $f$ satisfies any non-trivial polynomial relation, e.g. $f(x)^n = xf(x^{n-1})$ or $f(x^3) = x^2 f(x)$. Shift $f(x) = x + k$ for integer $k$ and view as polynomial in $k$, compare coeffs
  - $f(\frac{1}{x})f(x) = 1$. Consider $f(\frac{1}{x^2+x}) = f(\frac{1}{x}) - f(\frac{1}{x+1})$
- For $\mathbb{R}^+$ to $\mathbb{R}^+$, 1234 bash, 3 variable method. If can show monotonic suffices to find over rationals. Do the $\frac{f(x)}{x}$ flip.
- For iterative FEs, especially $f(n) = n + 1$, the following may be useful: unbounded, injective, surjective after a point, no cycles, nothing goes to $1$, consider values that LHS,RHS hit.

3. Sequences

- For real sequences, try telescope/finding something constant. Try to show it is monotonic/bounded/can take finitely many values/periodic.
- For integer/rational sequences, try to find monovariant/something that is unbounded, for example mod $p$, numerator/denominator, $v_p$.
- **A non-increasing sequence of positive integer is eventually constant.
- Any two-term linear recurrence with integer coeffs and $f_0 = 0, f_1 = 1$ satisfies $\text{gcd}(f_m, f_n) = f_{\text{gcd}(m,n)}$.

4. Polynomials

- Consider roots, coefficients, degree. $Q(x) = x^n P(\frac{1}{x})$.
- (FTOA) A real polynomial of degree $n$ has at most $n$ roots.
- If $a$ is a complex root then so is $\overline{a}$, with the same multiplicity. **We can write any real polynomial as a product of linear and quadratic factors.
- (Lagrange) If $x_1 < x_2 < \cdots x_n$ are complex numbers, and $a_1, a_2, \cdots a_n$ are complex, then there is a unique poly of degree at most $n-1$ such that $f(x_i) = a_i$.
- For Poly FEs, foolproof way is to guess the solution $p$ and consider $g(x) = f(x) - p$, contradiction by degree.

## Combinatorics

1. INDUCT (especially f there is optimal substructure).
2. Invariants/Monovariants
   - If process feels like its "spreading things out" consider sum of squares.
   - If some things are more important, consider weighted sums.
   - For swapping problems, consider number of inversions.
   - Discrete continuity/IVT, if only change by +/- 1, will hit every number in between.
3. Double counting
   - Count pairs/tuples/triples of things
   - Keep eq cases in mind, when need to deal with $\binom{n}{k}$ use jensen.
   - For planar graphs, consider double counting angles, faces, edges, vertices.
4. Graph Theory
   - May be useful to double count edges/triangles/triples of vertices/angles (for planar graphs). (Strong) induction on number of edges/vertices. For partition problems, find a monovariant, e.g. number of edges across groups.
   - (Turan) A $K_{r+1}$ free graph with $n$ vertices has at most $(1-\frac{1}{r})\frac{n^2}{2}$ edges.
   - (Brook) For any graph with maximum degree $d$, the chromatic number is $\leq d+1$.
   - (Hall's Marraige Theorem) For a bipartite graph $G(A,B)$, having an $A$ perfect matching $\iff$ for all vertex subsets $W$ of $A$, $|N(W)| \geq |W|$.
   - (Euler) For a planar graph $G$ with $V$ vertices, $E$ edges and $R$ regions (including the infinite one), $V+R=E+2$. $\therefore E \leq 3V-6$.
   - (Redei) Every tournament has a hamiltonian path.
   - (Camion-Moon) In a tournament, if can reach any vertex from any other vertex, graph has a hamiltonian cycle.
   - (Ramsey) For any positive integers $r, s$, there exists $n$ such that for any $r$ colouring of $K_n$, there is a monochromatic $K_r$.
   - **Graphs with degree exactly 2 for each vertex can be partitioned into disjoint cycles.
5. Residues
   - For questions asking to show some residues exists, may be easier to induct to show all residues exist, if residues are the same after adding an element then global sum/product.
   - (Cauchy Davenport) For any prime $p$ and sets $A, B \pmod{p}$, $|A+B| \geq \min\{p,\ |A|+|B|-1\}$
6. Probabilistic method
   - (Linearity of expectations) Given any not necessarily independent variables $X_1, X_2, \cdots X_n$, $\mathbb{E}[X_1 + X_2 + \cdots X_n] = \mathbb{E}[X_1] + \cdots \mathbb{E}[X_n]$.
   - (Direct existence proofs) To show there is some construction with value $k$ (integer), suffices to show average value (of some subset of all possible constructions) $> \lfloor k \rfloor$. Pick variables randomly (with equal probability).

7. Combigeom

   - Consider maximal length segment, maximal area triangle, and other extremal stuff. **Convex hull.
   - (Sylvester-Gallai) For every finite set of points there exists a line passing through exactly 2 of them, or passing through all.
   - (De Bruijn-Erdos). Let $P$ be a set of $n$ points not all on a line. Let $m$ be the number of lines determined by $P$. Then, $m \geq n$ and equality holds iff exactly $n-1$ of the points are collinear.

8. Asymptotic bounds

   - Consider the minimal/maximal subset which works, and find properties from there. E.g. minimal covering of a superset $\implies$ every set has a unique element.

## Geometry

1. Concyclicity
   - Angle chase, POP, find center, add 5th point
   - (Ptolemy) In cyclic quad $ABCD$, $AB \times CD + AD \times BC = AC \times BD$.
   - (Reim) parallel + cyclic $\implies$ more cyclic
   - (Spiral) **If two circles intersect and lines pass through one intersection point, consider the other intersection. Spiral comes in pairs. Can be useful to see if more points are part of the same spiral. If there are two segments of equal lengths, can consider their spiral center to get congruent triangles.
2. Power of a point
   - Radical axis/center (zero radius circle!!)
   - If random segment intersect with circle, consider extending both to force PoP.
   - (Linearity of PoP) Given 2 circles $c_1, c_2$, $Pow(P, c_1, c_2) = Pow(P, c_1) - Pow(P, c_2)$ is linear. If $P$ on $BC$, then $f(P) = \frac{PC}{BC} f(B) + \frac{PB}{BC} f(C)$.
   - (Forgotten Coaxiality lemma) Let 2 circles $c_1, c_2$ intersect at $A, B$. Then the locus of points $P$ such that $\frac{Pow(P,c_1)}{Pow(P,c_2)} = k$ is a circle passing through $A, B$.
3. Collinearity and concurrency
   - Menelaus/Ceva, Pascal, **sine rule
   - (Desaurges) For triangles $ABC$, $XYZ$, if $AB \cap XY$, $AC \cap XZ$, $BC \cap YZ$ are collinear, then $AX, BY, CZ$ are concurrent.
   - (Pappus) Given collinear triples of points $ABC$, $XYZ$, $AY \cap BX$, $AZ \cap CX$ and $BZ \cap CY$ are collinear.
4. Incenter Configs ($ABC$ vertices, $DEF$ intouch points, $I$ incenter, $M_A$ midpoint of minor arc $BC$)
   - (Chicken feet) $M_AB = M_AI = M_AC = M_AO_A$ where $O_A$ is the $A$ excenter. Note if $AB + BC = 2BC$ can ptolemy to show $I$ is midpoint of $AM_A$.
   - (Diameter of incircle) If $D'$ is the reflection of $D$ across $I$, then $AD'$ passes through the $A$ extouch.
   - (Iran Lemma) For a triangle, draw a midline, an angle bisector, and a touch-chord, each generated from different vertex, then the three lines are concurrent.
   - (Sharkydevil) Let $S = (AEIF) \cap (ABC)$. Then $S$ is a spiral center, so $SIA'$ collinear where $A'$ is the $A$ antipode. Also, $SDM_A$ collinear. If $N_A$ is midpoint of major arc $BC$, then $N_AS, EF, BC$ are concurrent.
   - (Feuerbach point) The nine-point circle is tangent to the incircle at $Fe$.
5. Mixtilinear Configs ($B_1, C_1$ are touchpoints, $T_A$ is intouch)
   - $T_AI$ passes through the midpoint of major arc $BC$.
   - $T_AB_1$ passes through $M_C$.
   - Midpoint of $B_1C_1$ is $I$.

- $AM_CT_AM_B$ is harmonic.
- $AT_A$ and $AE$ are isogonal where $E$ is the $A$-extouch.

6. Orthocenter Configs ($DEF$ feet of perp, $M$ midpoint of $BC$, $A'$ antipode)

   - Many cyclic quadrilaterals, also PoP at $H$ is often useful.
   - ($HM$ line) Reflection of $H$ about $BC$, $M$ ($A'$) lie on $(ABC)$.
   - (Nine-point circle) Midpoints, $DEF$, midpoints of $AH, BH, CH$ lie on circle.
   - (Queue/Humpty point) Define $Q_A = (AH) \cap (ABC)$, $H_A = (HA) \cap (BHC)$ (they are the same point, in different triangles). $Q_A$ is on $HM$ while $H_A$ is on $AM$. $H_A$ lies on the circle through $A$ tangent to $BC$ at $B$ and vice versa.

7. Symmedian Configs

   - The symmedian $AS$ divides the opposite side in the ratio of the square of the sides
   - Any antiparallel line to $BC$ intersects the symmedian at its midpoint.
   - Tangents to $B, C$ intersect on symmedian. Second intersection of symmedian with circumcenter form a harmonic quad.
   - (Dumpty point) The midpoint of the symmedian is $Q_A$, which lies on $(BOC)$. It lies on the circle through $C$ tangent to $AB$ at $A$ and vice versa. Dumpty and Humpty are isogonal.

8. Random configs

   - (Simson Line), given $(ABCD)$, feet of perpendiculars from $D$ to $AB, BC, CA$ are collinear.
   - (Isogonal Lemma) If $P, Q$ are isogonal conjugate wrt $ABC$, $AP \sin \angle BPC = AQ \sin \angle BQC$
   - (Ratio Lemma) Let $\omega$ be a circle through $B, C$, and let a line meet $\omega$ at $A, D$ and $BC$ at $E$. Then $\frac{BE}{CE} = \frac{BA}{CA}\frac{BD}{CD}$. Consider function $f(Z) = \pm\frac{XZ}{YZ}$. Then if $ABXY$ cyclic and $AB$ meet $XY$ at $C$, $f(A)f(B) = f(C)$. Suppose $ABXY$ cyclic and $E, F$ on $XY$. Then $ABEF$ cyclic iff $f(A)f(B) = f(E)f(F)$.

9. Proj Geom

   - (Harmonic bundles) $(A, C; B, D) = -1 \iff (ACBD)$ harmonic $\iff \frac{CA}{CB} = \frac{DA}{DB}$.
   - Let $l$ and $d$ be two lines, with $A, B, C, D$ on $l$. Take $E$ to be any other point not on the lines and the intersection of $EA, EB, EC, ED$ with $d$ are $A', B', C', D'$. Then, $(ACBD)$ harmonic $\iff (A'C'B'D')$ harmonic
   - Let $P$ be tangent to a circle at $X, Y$. Take a line through $P$ intersecting the circle at $A$ and $B$ and $AB \cap XY = Q$. $(AXBY)$ and $(ABQP)$ are harmonic.
   - Let $ABC$ be a triangle with concurrent cevians $AD, BE, CF, X = EF \cap BC$ (possibly at infinity). Then $(XDBC)$ harmonic.
   - Let $ABC$ be a triangle with incenter $I$, $A$-excenter $I_A$, $AI \cap BC = D$. $(II_AAD)$ harmonic.
   - (Midpoints) Let $M$ be the midpoint of $AB$. Then $(ACBD)$ harmonic iff $BM \times BD = BA \times BC$ or $DB \times DM = DC \times DA$ or $MA \times MC = MB \times MD$.
   - (Brocard's Theorem) Let $ABCD$ be a cyclic quad with circumcenter $O$, then $O$ is the orthocenter of the triangle formed by the pairwise intersection of sides.
   - (La Hire) For a point $P$ and a circle $C$, define its polar to be the line passing through the 2 tangency points from $P$ to $C$. Define the pole of a line $l$ as the point $P$ which has $l$ as its polar. Then $X$ lies on the polar of $Y$ iff $Y$ lies on the polar of $X$.

## Number Theory

1. Diophantine equations

   - MOD! Factorise, infinite descent, bound by ineqs.
   - (Vieta Jumping) Suppose result is not true, consider minimal sum $(a, b)$ satisfying result, write quadratic with coeffs in $b$ (WLOG $a < b$ or vice versa) with one root $a$, show the other root is $< a$.
   - (Thue's lemma) Let $n > 1$ be an integer and $a$ be an integer coprime to $n$, then there exists integers $x, y$ with $0 < |x|, |y| < \sqrt{n}$ such that $ay \equiv x \pmod{n}$.
   - (Pell's equation) The equation $x^2 - dy^2 = 1$ where $d$ is not a square has infinitely many solutions, by factorising into $x - \sqrt{(d)}y$ and $x + \sqrt{(d)}y$, with norm 1, and raising to any power. **Useful for construction as well.

2. Primes, $v_p$, order, QRs

   - Consider prime dividing LHS, especially the smallest one. With order, this forces $\gcd(p - 1, n) = 1$.
   - ($v_p$) $v_p$ is a completely additive function. $v_p(x + y) \geq \min(v_p(x), v_p(y))$. **To show $a|b$ suffices to show $v_p(a) \leq v_p(b)$.
   - (Legendre's) $v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots$
   - (Orders) $ord_p(a)$ is the smallest $n$ such that $a^n \equiv 1 \pmod{p}$. Fundamental theorem of orders: if $a^n \equiv 1 \pmod{p}$ then $n|ord_p(a)$.
   - (Burton) Primitive roots exists mod $2, 4, p^a, 2p^a$.
   - (Powers mod $p$) Let $p > 2$ be a prime. For any integer $x$, $1^x + 2^x + \cdots + (p-1)^x \equiv -1$ if $p - 1|x$ and $0$ otherwise.
   - (LTE) Let $p > 2$ be a prime and $p \nmid a, b$, $p|a - b$. Then $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$. For $p = 2$, if $n$ is even then $v_2(a^n - b^n) = v_2(a^2 - b^2) + v_2(\frac{n}{2})$
   - (Zsigmondy's) Let $a, b$ be coprime positive integers. Then for any $n > 1$, $a^n - b^n$ has a prime divisor which does not divide any $a^k - b^k$ for $n < k$, except for $2^6 - 1^6$ and ($n = 2$, $a + b$ is a power of $2$).
   - (Quadratic Residues) There are exactly $\frac{p-1}{2}$ quadratic residues.
   - (Legendre) Let $(\frac{x}{p})$ =1 if $x$ is a QR, $-1$ if $x$ is a NQR, $0$ if $p|x$. Then $(\frac{x}{p})$ is completely multiplicative. $(\frac{x}{p}) = x^{\frac{p-1}{2}} \pmod{p}$.
   - (LOQR) for $p, q > 2$, $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.
   - (Special cases of LOQR) 2 is a QR iff $p \equiv \pm 1 \pmod{8}$. 3 is a QR iff $p \equiv \pm 1 \pmod{12}$. -1 is a QR iff $p \equiv 1 \pmod{4}$.

3. Arithmetic functions

   - **Swap order of summations
   - Number of divisors $d(n)$, sum of divisors $\sigma(n)$, number of coprime integers $\varphi(n)$ and the mobius function $\mu(n) = (-1)^m$ if $n$ is squarefree and has $m$ prime divisors, and 0 otherwise, are multiplicative. **It is sufficient to determine a multiplicative function over prime powers.

- (Dirichlet Convolution) If $f$ is multiplicative, then $F(n) = \sum_{d|n} f(n)$ is multiplicative. If $f, g$ are multiplicative then so is $\sum_{d|n} f(d)g(\frac{n}{d})$.
- (Mobius inversion) If $g(n) = \sum_{d|n} f(n)$, then $f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d})$.
- (Double counting divisors) $\sum d(i) = \sum \lfloor \frac{n}{i} \rfloor$, $\sum \sigma(i) = \sum i \lfloor \frac{n}{i} \rfloor$.

4. Polynomials

- **$m - n | f(m) - f(n)$. If $P$ has a cycle, then it has a cycle of length $2$.
- (Schur's lemma) There exists infinitely many primes dividing $P(n)$ for some $n$.
- (Bezout) If two rational polynomials $P, Q$ have gcd $D$, then there are rational polynomials $R, S$ such that $PR - QS = D$.
- (Gauss' lemma) If an integer polynomial can be factored into rational polynomials, then it can be factored into integer polynomials.
- (Rational root theorem) If $\frac{p}{q}$ is a root of $P$, then $q|a_n$ and $p|a_0$.
- (Irreducibility) Eisenstein: If $p \nmid a_n, p^2 \mid a_0$ and $p|a_{n-1}, a_{n-2}, \cdots a_0$, $P$ is irreducible. Perron: If $a_n = 1, a_0 \neq 0$ and $|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_0|$, then irreducible. Consider size, if an integer polynomial has at most one root with absolute value $\geq 1$, and $P(0) \neq 0$, then irreducible.
- (Minimal polynomial) For any algebraic number $\alpha$, its minimal polynomial is the rational polynomial of minimal degree such that $P(\alpha) = 0$. Minimal polynomials are irreducible, if some other $Q(\alpha) = 0$ then $P|Q$. Adding or multiplying 2 algebraic integers gives another algebraic integer.

5. NTFEs

- Very often, find small values, force primes (Dirichlet may help), find infinite, find all.