lambda's handy dandy IB number theory cheat sheet

 This Cheat sheet is mainly modeled after the discrete mathematics section in Pearson's IB Mathematics HL textbook.

Fundamental concepts

Well-ordering principle. Each non-empty subset of $\mathbb{Z}^+$ has a least element.

Mathematical induction. Let $P(n)$ be a proposition on $n \in \mathbb{Z}^+$. If $P(1)$ and $P(k) \implies P(k+1)$ then $P(n)$ holds for all $n \geq 1$.

Strong mathematical induction. Let $P(n)$ be a proposition on $n \in \mathbb{Z}^+$. If $P(1)$ and $P(s)$ for all $1 \leq s \leq k \implies P(k+1)$, then $P(n)$ holds for all $n \geq 1$.

Pigeonhole principle. If the union of n sets contains more than n elements, then at least one of those sets contains more than one element.

Basic divisibility definitions and results

Let $a, b \in \mathbb{Z}$.

- $a|b \iff na = b$ for some $n \in \mathbb{Z}$. We write $a|b$ when a is a factor of b and say that a *divides* b.
- $\gcd(a,b) = g \iff g$ is the greatest integer that divides both a and b, and we say that g is the *greatest common divisor* of a and b. Integers a and b are coprime if and only if $\gcd(a,b) = 1$.
- $\text{lcm}(a,b) = l \iff l$ is the smallest integer such that $a|l$ and $b|l$, and we say that l is the *least common multiple* of a and b.

Theorem 1. $\gcd(a,b) \cdot \text{lcm}(a,b) = ab$.
Theorem 2. $a|b$ and $b|c \implies a|c$.
Theorem 3. $a|b$ and $a|c \implies a|(b \pm c)$.
Theorem 4. If $a, b \in \mathbb{Z}$ with $b > 0$, then there are unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < b$. We call r the *remainder* of a divided by b, and q the *quotient*.
Theorem 5. If $a, b \neq 0$, then $gcd(a,b)$ is the smallest positive integer such that $\gcd(a,b) = ax + by$ for $x, y \in \mathbb{Z}$.
Theorem 6. If $a = bq + r$ for $b > 0$ and $0 \leq r < b$, then $\gcd(a,b) = \gcd(b,r)$.
Theorem 7. For $a, b \neq 0$, $\gcd(a,b) = 1$ if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.
Theorem 8 (Fundamental thm. of arithmetic)**.** Every $n > 1$ in $\mathbb{Z}$ can be expressed as $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ for distinct primes $p_1, \dots, p_k$ and $a_1, \dots, a_k \in \mathbb{Z}^+$.

Euclidean algorithm

Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. We can find $\gcd(a,b)$ using the *Euclidean algorithm*. Write a as

$$a = bq_1 + r_1 \quad \text{for} \quad 0 \leq r_1 < b.$$

If $r_1 = 0$ then $b|a$ and $\gcd(a,b) = b$. Otherwise if $r_1 > 0$, write b as

$$b = r_1 q_2 + r_2 for 0 \leq r_2 < r_1.$$

If $r_2 = 0$ then $\gcd(a,b) = r_1$. If $r_2 > 00$, we repeat the process as follows.

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < b \\ b &= r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} + 0 \end{aligned}$$

Then, $\gcd(a,b) = r_n$ (the last non-zero remainder).

Modular arithmetic

For $a, b \in \mathbb{Z}$, we write

$$a \equiv b \pmod{m} \iff m|(a-b),$$

and we say that a and b are *congruent modulo* m.
Theorem 9. Congruence modulo m is an equivalence relation. Also, if $a \equiv b \pmod{m}$ with $a, b, c, d, m \in \mathbb{Z}$ and $d, m > 0$, we have

$$\begin{aligned} a + c &\equiv b + c \pmod{m}, \\ a - c &\equiv b - c \pmod{m}, \\ ac &\equiv bc \pmod{m}, \\ a^d &\equiv b^d \pmod{m}. \end{aligned}$$

Theorem 10. For $a, b, c, m \in \mathbb{Z}$ with $m > 0$ and $g = \gcd(a,b)$,

$$ac \equiv bc \pmod{m} \implies a \equiv b \left(\text{mod } \frac{m}{g}\right).$$

Linear congruences

Theorem 11. If $\gcd(a,b)|b$, then the number of solutions for the congruence $ax \equiv b \pmod{m}$ which are incongruent to eachother mod m is equal to $\gcd(a,b)$.

To solve a system of multivariate linear congruences such as

$$\begin{aligned} ax + by &\equiv e \pmod{m}, \\ cx + dy &\equiv f \pmod{m}, \end{aligned}$$

you can use row-reduction to isolate variables and obtain single-variable linear congruences.

Diophantine equations

A linear homogeneous Diophantine equation in two variables $x, y \in \mathbb{Z}$ is an equation of the form $ax + by = c$ where $a, b, c \in \mathbb{Z}$.
Theorem 12. For $a, b, c \in \mathbb{Z}$, $a, b \neq 0$, the Diophantine equation $ax + by = c$ has a solution in integers (x, y) if and only if $\gcd(a,b)|c$.
Theorem 13. Let $g = \gcd(a,b)$. If $x = x_0$ and $y = y_0$ is a particular solution to $ax + by = c$ then all other solutions are of the form

$$x = x_0 + \frac{b}{g}\lambda \quad \text{and} \quad y = y_0 - \frac{a}{g}\lambda$$

where λ is an arbitrary integer.

Strategies for finding particular solutions for Diophantine equations

To find a particular integer solution to $ax + by = c$, one might use these methods.

- Trial and error (not recommended).
- Via calculator (isolate x or y on one side of the equation and enter as a function into your calculator. Many calculators have a 'table' function that plots integer values for the independent variable. Look for solutions where the dependent variable is also an integer.)
- With linear congruences (write $ax + by = c$ as $ax \equiv c \pmod{b}$ and solve).
- Use the extended (reverse) Euclidean algorithm to obtain a particular solution (x', y') for $ax' + by' = g$ where $g = \gcd(a,b)$. Then, multiply both sides of the equation by $\frac{c}{g}$ to obtain

  $$a(x'\frac{c}{g}) + b(y'\frac{c}{g}) = c,$$

  and hence obtain the particular solution $x = x'\frac{c}{g}$ and $y = y'\frac{c}{g}$ for $ax + by = c$.

Extended Euclidean algorithm (a.k.a. reverse Euclidean algorithm)

This algorithm can be used to solve the Diophantine equation $ax + by = \gcd(a, b)$. In other words, it is an algorithm to express $\gcd(a, b)$ as a linear combination of a and b. Firstly, one would apply the regular Euclidean algorithm on a and b to determine $\gcd(a, b)$, storing all the quotients and remainders, then 'reversing' the algorithm. As an example, we will find a particular solution (x, y) for $64x + 27y = \gcd(64, 27)$. Applying the Euclidean algorithm, we have

$$\begin{aligned} 64 &= 27 \cdot 2 + 10 \\ 27 &= 10 \cdot 2 + 7 \\ 10 &= 7 \cdot 1 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 + 0. \end{aligned}$$

Since 1 is the last non-zero remainder, $1 = \gcd(64, 27)$. Now, we solve for this remainder in terms of 64 and 27. We see that $1 = 7 - 3 \cdot 2$. Since 3 was one of the previous remainders, we can replace 3 with $10 - 7 \cdot 1$ to obtain

$$\begin{aligned} 1 &= 7 - (10 - 7 \cdot 1) \cdot 2 \\ &= 7 \cdot 3 - 10 \cdot 2. \end{aligned}$$

Since 7 was also a previous remainder, we can express it in terms of its previous remainders and repeat the process until we arrive at a final answer in terms of 64 and 27:

$$\begin{aligned} 1 &= 7 - (10 - 7 \cdot 1) \cdot 2 \\ &= 7 \cdot 3 - 10 \cdot 2 \\ &= (27 - 10 \cdot 2) \cdot 3 - 10 \cdot 2 \\ &= 27 \cdot 3 - 10 \cdot 8 \\ &= 27 \cdot 3 - (64 - 27 \cdot 2) \cdot 8 \\ &= 27 \cdot 19 - 64 \cdot 8 \end{aligned}$$

Hence, we have a solution $x = -8$ and $y = 19$.

Fermat's little theorem

Theorem 14. If p is prime, then for any $a \in \mathbb{Z}$, we have

$$a^p \equiv a \pmod{p}.$$

If a and p are coprime, then we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Applying the Chinese remainder thm.

Let $m_1, m_2, \ldots, m_r \in \mathbb{Z}^+$ be pairwise coprime. To find a solution modulo $M = m_1 m_2 \ldots m_r$ to the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

we first let $M_k = \frac{M}{m_k} = m_1 m_2 \ldots m_{k-1} m_{k+1} \ldots m_r$. For each $1 \le k \le r$ we can solve the congruence

$$M_k x_k \equiv 1 \pmod{m_k}.$$

to obtain x_k for $1 \le k \le r$. Then the unique solution modulo M to the original system of equations is

$$x \equiv a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_r M_r x_r \pmod{M}.$$

Integer representations & operations

Theorem 15. For any base $b \in \mathbb{Z}^+$, every $n \in \mathbb{Z}^+$ can be written in the form

$$n = a_k \cdot b^k + \cdots + a_1 \cdot b^1 + a_0 \cdot b^0 = \sum_{i=0}^{k} a_i b^i$$

for $k \in \mathbb{Z}$, $k \ge 0$, and each $a_i \in Z^+$ with $a_i \le b - 1$, and $a_k \ne 0$.
Numbers expressed in a base b other than 10 are often denoted $(a_k a_{k-1} \ldots a_2 a_1)_b$ where each a_i denotes a digit in base b.
To convert a number n from base 10 to arbitrary base b, simply divide repeatedly by b, storing the remainders. Then, reverse the list of remainders and concatenate them. The result is the base b representation of n.
To add/multiply numbers in base b, create an addition or multiplication table for all the digits in base b and proceed to use the standard long addition/multiplication algorithms.

Recurrence relations

A linear homogeneous recurrence relation (LHRR) of degree k with constant coefficients is a recurrence relation of the form

$$a_n = c_k a_{n-k} + c_{k+1} a_{n-k-1} + \ldots c_n a_1 = \sum_{i=1}^{k} c_i a_{n-i}.$$

which which defines the sequence $a_1, a_2, a_3 \ldots$.

A LHRR can be solved using its characteristic polynomial by letting $a_n = x^n$ and dividing by the highest power of x that appears in the resulting equation. For $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, we have

$$x^n - c_1 x^{n-1} - c_2 x^{n-2} = 0.$$

Dividing by x^{n-2}, the characteristic polynomial equation becomes

$$x^2 - c_1 x - c_2 = 0.$$

The roots of this equation determine the solution to the LHRR If the characteristic polynomial has two distinct real roots r_1 and r_2, then

$$a_n = b r_1^n + d r_2^n,$$

If it has one real root r, then

$$a_n = b r^n + d n r^n,$$

and if it has two conjugate complex zeroes $z_1 = (d, \theta)$ and $z_2 = (d, -\theta)$ where d is the modulus and θ is the argument, then

$$a_n = d^n (b \cos(n\theta) + d \sin(n\theta)).$$

In each case, b and d are real constants determined by the initial conditions of the LHRR.
Theorem 16. If v_n and w_n are two solutions to the LHRR a_n, then any linear combination of v_n and w_n will also be a solution (i.e., $b_n = \lambda v_n + \mu w_n$ is a solution, $\lambda, \mu \in \mathbb{R}$).

Non-homogeneous relations

A linear non-homogeneous recurrence relation (LNHRR) of degree k with constant coefficients is a recurrence relation of the form

$$a_n = \left(\sum_{i=1}^{k} c_i a_{n-i} \right) + f(n)$$

Theorem 17. If p_n is a particular solution for the LNHRR $a_n = (\sum_{i=1}^{k} c_i a_{n-i}) + f(n)$ and h_n is a solution of the associated LHRR $a_n = \sum_{i=1}^{k} c_i a_{n-i}$, then every solution for the non-homogeneous relation is of the form $p_n + h_n$.