Number Theory Cheat Sheet

1. If $(a, b) = 1$, $a \mid n$, and $b \mid n$, then $ab \mid n$. Note that (a, b) is the notation for the greatest common divisor of a and b.
2. If $d|m$ and $d|n$, then d divides any linear combination of m and n, i.e., $d|(am + bn)$.
3. **Euclid's Lemma**: If p is prime and p divides ab (for integers $a,\ b$), then p divides a or p divides b.
4. **Fermat's Little Theorem** If p is a prime number, then for any integer a:
$$a^p \equiv a(mod\ p)$$
5. **Fermat's Little Theorem (variation)** If p is a prime number and $(a, p) = 1$, then for any integer a:
$$a^{p-1} \equiv 1(mod\ p)$$
6. **LCM Property**: If a number n is divisible by integers a and b, then n must be divisible by the least common multiple of a and b, i.e.,
$$(a \mid n) \wedge\ (b \mid n) \Longrightarrow \operatorname{lcm}(a, b) \mid n$$
7. **Euler's theorem** is a generalization of Fermat's little theorem: For any modulus *n* and any integer a coprime to n, one has $a^{\varphi(n)} \equiv 1(mod\ n)$, where $\varphi(n)$ denotes Euler's totient function (which counts the integers from 1 to n that are coprime to n). Fermat's little theorem is indeed a special case, because if *n* is a prime number, then $\varphi(n) = n - 1$.
8. **Bézout's identity** Let a and b be integers with greatest common divisor d. Then there exist integers x and y such that $ax + by = d$. Moreover, the integers of the form $az + bt$ are exactly the multiples of d.
9. An equation of the form $Ax \equiv B(\mathrm{mod}\ M)$ has a solution if and only if (A, M) divides B, where A, B and $M > 1$ are integers.
10. The **identity associated with Euclid's algorithm**: For any integers x, y, and k, we have that $(x, y) = (x, y - kx)$.
11. If $(a, b) = 1$, then a has a multiplicative inverse modulo b.
12. The **Rational Root Theorem** provides a method for identifying all possible rational roots (solutions that can be written as fractions) of a polynomial equation with integer coefficients. Let $P(x)$ be a polynomial with integer coefficients defined as:
$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$
$a_n, a_{n-1}, \ldots, a_0$ are integers such that $a_n \neq 0$ and $a_0 \neq 0$.

    If the polynomial has a rational root $x = \frac{p}{q}$ (where p and q are coprime integers), then p is a factor of the constant term a_0 and q is a factor of the leading coefficient a_n.

13. Let $n_1, \ \dots, \ n_k$ (which are often called moduli or divisors) be integers greater than 1, and let $N = n_1 \times \dots \times n_k$. The **Chinese Remainder Theorem** (CRT) asserts that if the n_i are pairwise coprime, and if $r_1, \dots, r_k$ are integers such that $0 \leq r_i < n_i$, then the system

$$x \equiv r_1 (mod\, n_1)$$

$$x \equiv r_2 (mod\, n_2)$$

$$\dots$$

$$x \equiv r_k (mod\, n_k)$$

has a solution x, and any two solutions, x_1 and x_2, are congruent modulo N, i.e.,

$$x_1 \equiv x_2 (mod\, N)$$

14. **The Chinese Remainder Theorem (Counting Form)**

Premise Let $n_1, \ \dots, \ n_k$ be pairwise coprime integers (meaning $(n_i, n_j) = 1$ for all $i \neq j$), and let $N = n_1 \times \dots \times n_k$.

The Bijection Principle (Generalization) There exists a **one-to-one correspondence (bijection)** between the integer x in the range $0 \leq x < N$ and the unique tuple of residues $(r_1, r_2, \dots, r_k)$ defined by:

$$r_1 \equiv x (mod\, n_1)$$

$$r_2 \equiv x (mod\, n_2)$$

$$\dots$$

$$r_k \equiv x (mod\, n_k)$$

This means every possible combination of residues maps to exactly one integer x in the range.

The Counting Consequence Consider a problem where a valid solution x must satisfy independent conditions modulo each n_i. Let c_i be the number of valid solutions for congruence i.

Because every valid tuple of residues corresponds to exactly one valid solution x, the **total number of solutions** x in the range $0 \leq x < N$ is the product of the individual counts:

$$\text{Total Solutions} = c_1 \times c_2 \times \dots \times c_k$$

15. There are an infinite number of prime numbers.

16. **Wilson's Theorem**: A positive integer $p > 1$ is prime if and only if

$$(p-1)! \equiv -1 (mod\, p)$$

17. **Fundamental Theorem of Arithmetic**: Every integer greater than 1 either is a prime number itself or can be represented as the product of prime numbers and that, moreover, this representation is unique, up to the order of the factors.

18. A natural number n is divisible by 3 if and only if 3 divides the sum of the digits in n.
19. A natural number n is divisible by 11 if and only if the difference between the sum of the digits in the odd positions (1^{st}, 3^{rd}, 5^{th} ...) and the sum of the digits in the even positions (2^{nd}, 4^{th}, 6^{th} ...) is divisible by 11.
20. If $a \equiv b (mod\ c)$ prove that $a^k \equiv b^k\ (mod\ c)$ for positive integer k.
21. **Fundamental Theorem of Cyclic Groups:** In a cyclic group $G = \langle g \rangle$ of order k, the number of elements x in G such that $x^m = 1$ is (m, k).
22. The linear **Diophantine equation** $ax + by = c$ has an integer solution if and only if $(a, b) \mid c$.
23. If $(a, b) = g$, then $(\frac{a}{g}, \frac{b}{g}) = 1$.
24. If x_0, y_0 is a solution of the **Diophantine equation** $ax + by = c$ where $g = (a, b)$ then all other solutions are given by

$$x = x_0 + bgt,\ y = y_0 - agt,\ t \in \mathbb{Z}$$

25. Let $f(x)$ be a polynomial with integer coefficients. For any distinct integers a and b: $(a - b)$ divides $f(a) - f(b)$.