The Equation List

Combinatorics

General

1. $\sum_{0\le k\le n} \binom{n-k}{k} = Fib_{n+1}$
2. $\binom{n}{k} = \binom{n}{n-k}$
3. $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$
4. $k\binom{n}{k} = n\binom{n-1}{k-1}$
5. $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$
6. $\sum_{i=0}^{n} \binom{n}{i} = 2^n$
7. $\sum_{i\ge 0} \binom{n}{2i} = 2^{n-1}$
8. $\sum_{i\ge 0} \binom{n}{2i+1} = 2^{n-1}$
9. $\sum_{i=0}^{k} (-1)^i \binom{n}{i} = (-1)^k \binom{n-1}{k}$
10. $\sum_{i=0}^{k} \binom{n+i}{i} = \sum_{i=0}^{k} \binom{n+i}{n} = \binom{n+k+1}{k}$
11. $1\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \ldots + n\binom{n}{n} = n2^{n-1}$
12. $1^2\binom{n}{1} + 2^2\binom{n}{2} + 3^2\binom{n}{3} + \ldots + n^2\binom{n}{n} = (n+n^2)2^{n-2}$
13. **Vandermonde's Identify:** $\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}$
14. **Hockey-Stick Identify:** $n, r \in N, n > r, \sum_{i=r}^{n} \binom{i}{r} = \binom{n+1}{r+1}$
15. $\sum_{i=0}^{k} \binom{k}{i}^2 = \binom{2k}{k}$
16. $\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}$
17. $\sum_{k=q}^{n} \binom{n}{k}\binom{k}{q} = 2^{n-q}\binom{n}{q}$
18. $\sum_{i=0}^{n} k^i \binom{n}{i} = (k+1)^n$
19. $\sum_{i=0}^{n} \binom{2n}{i} = 2^{2n-1} + \frac{1}{2}\binom{2n}{n}$
20. $\sum_{i=1}^{n} \binom{n}{i}\binom{n-1}{i-1} = \binom{2n-1}{n-1}$
21. $\sum_{i=0}^{n} \binom{2n}{i}^2 = \frac{1}{2}\left(\binom{4n}{2n} + \binom{2n}{n}^2\right)$
22. **Highest Power of 2 that divides $^{2n}C_n$:** Let x be the number of 1s in the binary representation. Then the number of odd terms will be 2^x.Let it form a sequence. The n-th value in the sequence (starting from n = 0) gives the highest power of 2 that divides $^{2n}C_n$.
23. **Pascal Triangle**
    - In a row p where p is a prime number, all the terms in that row except the 1s are multiples of p.
    - Parity: To count odd terms in row n, convert n to binary. Let x be the number of 1s in the binary representation. Then the number of odd terms will be 2^x.
    - Every entry in row $2^n - 1, n \ge 0$, is odd.
24. An integer $n \ge 2$ is prime if and only if all the intermediate binomial coefficients $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ are divisible by n.
25. **Kummer's Theorem:** For given integers $n \ge m \ge 0$ and a prime number p, the largest power of p dividing $\binom{n}{m}$ is equal to the number of carries when m is added to n-m in base p. For implementation take inspiration from lucas theorem.
26. Number of different binary sequences of length n such that no two 0's are adjacent=Fib_{n+1}
27. **Combination with repetition:** Let's say we choose k elements from an n-element set, the order doesn't matter and each element can be chosen more than once. In that case, the number of different combinations is: $\binom{n+k-1}{k}$
28. Number of ways to divide n persons in $\frac{n}{k}$ equal groups i.e. each having size k is

$$\frac{n!}{k!^{\frac{n}{k}}\left(\frac{n}{k}\right)!} = \prod_{n\ge k}^{n-=k} \binom{n-1}{k-1}$$

29. The number non-negative solution of the equation: $x_1 + x_2 + x_3 + \ldots + x_k = n$ is $\binom{n+k-1}{n}$
30. Number of ways to choose n ids from 1 to b such that every id has distance at least k $= \left(\frac{b-(n-1)(k-1)}{n}\right)$
31. $\sum_{i=1,3,5,\ldots}^{i\le n} \binom{n}{i} a^{n-i} b^i = \frac{1}{2}((a+b)^n - (a-b)^n)$
32. $\sum_{i=0}^{n} \frac{\binom{k}{i}}{\binom{n}{i}} = \frac{\binom{n+1}{n-k+1}}{\binom{n}{k}}$
33. **Derangement:** a permutation of the elements of a set, such that no element appears in its original position. Let $d(n)$ be the number of derangements of the identity permutation fo size n.

$$d(n) = (n-1)\cdot(d(n-1)+d(n-2)) \text{ where } d(0)=1, d(1)=0$$

34. **Involutions:** permutations such that $p^2 =$ identity permutation. $a_0 = a_1 = 1$ and $a_n = a_{n-1} + (n-1)a_{n-2}$ for $n > 1$.
35. Let $T(n,k)$ be the number of permutations of size n for which all cycles have length $\le k$.

$$T(n,k) = \begin{cases} n! & ; n \le k \\ n\cdot T(n-1,k) - F(n-1,k)\cdot T(n-k-1,k) & ; n > k \end{cases}$$

Here $F(n,k) = n\cdot(n-1)\cdot\ldots\cdot(n-k+1)$

36. **Lucas Theorem**
    - If p is prime, then $\binom{p^a}{k} \equiv 0 (\mod p)$
    - For non-negative integers m and n and a prime p, the following congruence relation holds:

$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i}$ $(mod\ p)$, where,

$m = m_k p^k + m_{k-1} p^{k-1} + \ldots + m_1 p + m_0$,

and

$n = n_k p^k + n_{k-1} p^{k-1} + \ldots + n_1 p + n_0$

are the base p expansions of m and n respectively. This uses the convention that $\binom{m}{n} = 0$,when $m < n$.

37. $\sum_{i=0}^{n} \binom{n}{i} \cdot i^k$

$= \sum_{i=0}^{n} \binom{n}{i} \cdot \sum_{j=0}^{k} \left\{ {k \atop j} \right\} \cdot i^{\underline{j}}$

$= \sum_{i=0}^{n} \binom{n}{i} \cdot \sum_{j=0}^{k} \left\{ {k \atop j} \right\} \cdot j! \binom{n}{i}$

$= \sum_{i=0}^{n} \frac{n!}{(n-i)!} \cdot \sum_{j=0}^{k} \left\{ {k \atop j} \right\} \cdot \frac{1}{(i-j)!}$

$= \sum_{i=0}^{n} \sum_{j=0}^{k} \frac{n!}{(n-i)!} \cdot \left\{ {k \atop j} \right\} \cdot \frac{1}{(i-j)!}$

$= n! \sum_{i=0}^{n} \sum_{j=0}^{k} \left\{ {k \atop j} \right\} \cdot \frac{1}{(n-i)!} \cdot \frac{1}{(i-j)!}$

$= n! \sum_{i=0}^{n} \sum_{j=0}^{k} \left\{ {k \atop j} \right\} \cdot \binom{n-j}{n-i} \cdot \frac{1}{(n-j)!}$

$= n! \sum_{j=0}^{k} \left\{ {k \atop j} \right\} \cdot \frac{1}{(n-j)!} \sum_{i=0}^{n} \cdot \binom{n-j}{n-i}$

$= \sum_{j=0}^{k} \left\{ {k \atop j} \right\} \cdot n^{\underline{j}} \cdot 2^{n-j}$

Here $n^{\underline{j}} = P(n,j) = \frac{n!}{(n-j)!}$ and $\left\{ {k \atop j} \right\}$ is stirling number of the second kind.

So, instead of $O(n)$, now you can calculate the original equation in $O(k^2)$ or even in $O(k \log^2 n)$ using NTT.

38. $\sum_{i=0}^{n-1} \binom{i}{j} x^i = x^j (1-x)^{-j-1} \left(1 - x^n \sum_{i=0}^{j} \binom{n}{i} x^{j-i} (1-x)^i \right)$

39. $x_0, x_1, x_2, x_3, \ldots, x_n$

$x_0 + x_1, x_1 + x_2, x_2 + x_3, \ldots x_n$

...

If we continuously do this n times then the polynomial of the first column of the n-th row will be

$$p(n) = \sum_{k=0}^{n} \binom{n}{k} \cdot x(k)$$

40. If $P(n) = \sum_{k=0}^{n} \binom{n}{k} \cdot Q(k)$, then,

$$Q(n) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \cdot P(k)$$

41. If $P(n) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \cdot Q(k)$, then,

$$Q(n) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \cdot P(k)$$

Catalan Numbers

42. $C_n = \frac{1}{n+1} \binom{2n}{n}$
43. $C_0 = 1, C_1 = 1$ and $C_n = \sum_{k=0}^{n-1} C_k C_{n-1-k}$
44. Number of correct bracket sequence consisting of n opening and n closing brackets.
45. The number of ways to completely parenthesize n+1 factors.
46. The number of triangulations of a convex polygon with n+2 sides (i.e. the number of partitions of polygon into disjoint triangles by using the diagonals).
47. The number of ways to connect the $2n$ points on a circle to form n disjoint i.e. non-intersecting chords.
48. The number of monotonic lattice paths from point $(0, 0)$ to point (n, n) in a square lattice of size $n \times n$, which do not pass above the main diagonal (i.e. connecting $(0, 0)$ to (n, n)).
49. The number of rooted full binary trees with n+1 leaves (vertices are not numbered). A rooted binary tree is full if every vertex has either two children or no children.
50. Number of permutations of $1, \ldots, n$ that avoid the pattern 123 (or any of the other patterns of length 3); that is, the number of permutations with no three-term increasing sub-sequence. For $n = 3$, these permutations are $132,\ 213,\ 231,\ 312$ and 321.\displaystyle For $n = 4$, they are $1432,\ 2143,\ 2413,\ 2431,\ 3142,\ 3214,\ 3241,\ 3412,\ 3421,\ 4132,\ 4213,\ 4231,\ 4312$ and 4321.
51. **Balanced Parentheses count with prefix:** The count of balanced parentheses sequences consisting of $n + k$ pairs of parentheses where the first k symbols are open brackets. Let the number be $C_n^{(k)}$, then

$$C_n^{(k)} = \frac{k+1}{n+k+1} \binom{2n+k}{n}$$

Narayana numbers

52. $N(n,k) = \frac{1}{n} \binom{n}{k} \binom{n}{k-1}$
53. The number of expressions containing n pairs of parentheses, which are correctly matched and which contain k distinct nestings. For instance, $N(4, 2) = 6$ as with four pairs of parentheses six sequences can be created which each contain two times the sub-pattern '()'.

Stirling numbers of the first kind

54. The Stirling numbers of the first kind count permutations according to their number of cycles (counting fixed points as cycles of length one).
55. $S(n, k)$ counts the number of permutations of n elements with k disjoint cycles.
56. $S(n,k) = (n-1) \cdot S(n-1,k) + S(n-1,k-1),\ where,\ \ S(0,0) = 1, S(n,0) = S(0,n) = 0$
57. $\sum_{k=0}^{n} S(n,k) = n!$
58. The unsigned Stirling numbers may also be defined algebraically, as the coefficient of the rising factorial:

$$x^{\bar{n}} = x(x+1)\ldots(x+n-1) = \sum_{k=0}^{n} S(n,k) x^k$$

59. Lets $[n, k]$ be the stirling number of the first kind, then

$$\left[{n \atop n-k}\right] = \sum_{0 \le i_1 < i_2 < i_k < n} i_1 i_2 \ldots . i_k.$$

Stirling numbers of the second kind

60. Stirling number of the second kind is the number of ways to partition a set of n objects into k non-empty subsets.
61. $S(n, k) = k \cdot S(n-1, k) + S(n-1, k-1), where\ S(0,0) = 1, S(n, 0) = S(0, n) = 0$
62. $S(n, 2) = 2^{n-1} - 1$
63. $S(n, k) \cdot k!$ = number of ways to color n nodes using colors from 1 to k such that each color is used at least once.
64. An r-associated Stirling number of the second kind is the number of ways to partition a set of n objects into k subsets, with each subset containing at least r elements. It is denoted by $S_r(n, k)$ and obeys the recurrence relation. $S_r(n+1, k) = kS_r(n, k) + \binom{n}{r-1} S_r(n-r+1, k-1)$
65. Denote the n objects to partition by the integers $1, 2, \ldots, n$. Define the reduced Stirling numbers of the second kind, denoted $S^d(n, k)$, to be the number of ways to partition the integers $1, 2, \ldots, n$ into k nonempty subsets such that all elements in each subset have pairwise distance at least d. That is, for any integers i and j in a given subset, it is required that $|i - j| \ge d$. It has been shown that these numbers satisfy, $S^d(n, k) = S(n-d+1, k-d+1), n \ge k \ge d$

Bell number

66. Counts the number of partitions of a set.
67. $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} \cdot B_k$
68. $B_n = \sum_{k=0}^{n} S(n, k)$,where $S(n, k)$ is stirling number of second kind.

Math

General

69. $ab \mod ac = a(b \mod c)$
70. $\sum_{i=0}^{n} i \cdot i! = (n+1)! - 1.$
71. $a^k - b^k = (a-b) \cdot (a^{k-1}b^0 + a^{k-2}b^1 + \ldots + a^0 b^{k-1})$
72. $\min(a+b, c) = a + \min(b, c-a)$
73. $|a-b| + |b-c| + |c-a| = 2(\max(a, b, c) - \min(a, b, c))$
74. $a \cdot b \le c \to a \le \left\lfloor \frac{c}{b} \right\rfloor$ is correct
75. $a \cdot b < c \to a < \left\lfloor \frac{c}{b} \right\rfloor$ is incorrect
76. $a \cdot b \ge c \to a \ge \left\lfloor \frac{c}{b} \right\rfloor$ is correct
77. $a \cdot b > c \to a > \left\lfloor \frac{c}{b} \right\rfloor$ is correct
78. For positive integer n, and arbitrary real numbers m, x,

$$\left\lfloor \frac{\lfloor x/m \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{mn} \right\rfloor$$

$$\left\lceil \frac{\lceil x/m \rceil}{n} \right\rceil = \left\lceil \frac{x}{mn} \right\rceil$$

79. Lagrange's identity:

$$\left(\sum_{k=1}^{n} a_k^2\right)\left(\sum_{k=1}^{n} b_k^2\right) - \left(\sum_{k=1}^{n} a_k b_k\right)^2 = \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} (a_i b_j - a_j b_i)^2$$
$$= \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1, j\ne i}^{n} (a_i b_j - a_j b_i)^2$$

80. $\sum_{i=1}^{n} ia^i = \frac{a(na^{n+1} - (n+1)a^n + 1)}{(a-1)^2}$
81. **Vieta's formulas:**
   Any general polynomial of degree n

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

(with the coefficients being real or complex numbers and $a_n \ne 0$) is known by the fundamental theorem of algebra to have n (not necessarily distinct) complex roots $r_1, r_2, \ldots, r_n$.

$$\begin{cases} r_1 + r_2 + \ldots + r_{n-1} + r_n = -\frac{a_{n-1}}{a_n} \\ (r_1 r_2 + r_1 r_3 + \ldots + r_1 r_n) + (r_2 r_3 + r_2 r_4 + \ldots + r_2 r_n) + \ldots + r_{n-1} r_n = \frac{a_{n-2}}{a_n} \\ \vdots \\ r_1 r_2 \ldots r_n = (-1)^n \frac{a_0}{a_n}. \end{cases}$$

Vieta's formulas can equivalently be written as

$$\sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} \left(\prod_{j=1}^{k} r_{i_j}\right) = (-1)^k \frac{a_{n-k}}{a_n},$$

82. We are given n numbers $a_1, a_2, \ldots, a_n$ and our task is to find a value x that minimizes the sum,

$$|a_1 - x| + |a_2 - x| + \ldots + |a_n - x|$$

optimal x = median of the array.
if n is even $x = [\text{left median,right median}]$ i.e. every number in this range will work.

For minimizing

$$(a_1 - x)^2 + (a_2 - x)^2 + \ldots + (a_n - x)^2$$

optimal $x = \frac{(a_1 + a_2 + \ldots + a_n)}{n}$

83. Given an array a of n non-negative integers. The task is to find the sum of the product of elements of all the possible subsets. It is equal to the product of $(a_i + 1)$ for all a_i
84. **Pentagonal number theorem:** In mathematics, the pentagonal number theorem states that

$$\prod_{n=1}^{\infty}(1 - x^n) = \prod_{k=-\infty}^{\infty} (-1)^k x^{\frac{k(3k-1)}{2}} = 1 + \prod_{k=1}^{\infty} (-1)^k \left(x^{\frac{k(3k+1)}{2}} + x^{\frac{k(3k-1)}{2}}\right).$$

In other words,

$$(1-x)(1-x^2)(1-x^3)\cdots = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \cdots.$$

The exponents $1, 2, 5, 7, 12, \cdots$ on the right hand side are given by the formula $g_k = \frac{k(3k-1)}{2}$ for $k = 1, -1, 2, -2, 3, \cdots$ and are called (generalized) pentagonal numbers.

It is useful to find the partition number in $O(n\sqrt{n})$

Fibonacci Number

85. $F_0 = 0, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$
86. $F_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-k-1}{k}$
87. $F_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n$
88. $\sum_{i=1}^{n} F_i = F_{n+2} - 1$
89. $\sum_{i=0}^{n-1} F_{2i+1} = F_{2n}$
90. $\sum_{i=1}^{n} F_{2i} = F_{2n+1} - 1$
91. $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$
92. $F_m F_{n+1} - F_{m-1} F_n = (-1)^n F_{m-n}$
    $F_{2n} = F_{n+1}^2 - F_{n-1}^2 = F_n(F_{n+1} + F_{n-1})$
93. $F_m F_n + F_{m-1} F_{n-1} = F_{m+n-1}$
    $F_m F_{n+1} + F_{m-1} F_n = F_{m+n}$
94. A number is Fibonacci if and only if one or both of $(5 \cdot n^2 + 4)$ or $(5 \cdot n^2 - 4)$ is a perfect square
95. Every third number of the sequence is even and more generally, every k^{th} number of the sequence is a multiple of F_k
96. $gcd(F_m, F_n) = F_{gcd(m,n)}$
97. Any three consecutive Fibonacci numbers are pairwise coprime, which means that, for every n,
    $gcd(F_n, F_{n+1}) = gcd(F_n, F_{n+2}), gcd(F_{n+1}, F_{n+2}) = 1$
98. If the members of the Fibonacci sequence are taken $mod\ n$, the resulting sequence is periodic with period at most $6n$.

Pythagorean Triples

99. A Pythagorean triple consists of three positive integers a, b, and C, such that $a^2 + b^2 = c^2$. Such a triple is commonly written (a, b, c)
100. Euclid's formula is a fundamental formula for generating Pythagorean triples given an arbitrary pair of integers m and n with $m > n > 0$. The formula states that the integers

$$a = m^2 - n^2, b = 2mn, c = m^2 + n^2$$

form a Pythagorean triple. The triple generated by Euclid's formula is primitive if and only if m and n are coprime and not both odd. When both m and n are odd, then a, b, and c will be even, and the triple will not be primitive; however, dividing a, b, and c by 2 will yield a primitive triple when m and n are coprime and both odd.

101. The following will generate all Pythagorean triples uniquely:

$$a = k \cdot (m^2 - n^2), b = k \cdot (2mn), c = k \cdot (m^2 + n^2)$$

where m, n, and k are positive integers with $m > n$, and with m and n coprime and not both odd.

102. **Theorem:** The number of Pythagorean triples {a,b,n} with $maxa, b, n = n$ is given by

$$\frac{1}{2}\left(\prod_{p^\alpha || n} (2\alpha + 1) - 1\right)$$

where the product is over all prime divisors p of the form $4k + 1$.
The notation $p^\alpha || n$ stands for the highest exponent α for which p^α divides n
Example: For $n = 2 \cdot 3^2 \cdot 5^3 \cdot 7^4 \cdot 11^5 \cdot 13^6$, the number of Pythagorean triples with hypotenuse n is $\frac{1}{2}(7.13 - 1) = 45$.
To obtain a formula for the number of Pythagorean triples with hypotenuse less than a specific positive integer N, we may add the numbers corresponding to each $n < N$ given by the Theorem. There is no simple way to compute this as a function of N.

Sum of Squares Function

103. The function is defined as
     $r_k(n) = |(a_1, a_2, \ldots, a_k) \in \mathbf{Z^k} : n = a_1^2 + a_2^2 + \ldots + a_k^2|$
104. The number of ways to write a natural number as sum of two squares is given by $r_2(n)$. It is given explicitly by $r_2(n) = 4(d_1(n) - d_3(n))$ where d1(n) is the number of divisors of n which are congruent with 1 modulo 4 and d3(n) is the number of divisors of n which are congruent with 3 modulo 4.

     The prime factorization $n = 2^g p_1^{f_1} p_2^{f_2} \ldots q_1^{h_1} q_2^{h_2} \ldots$, where p_i are the prime factors of the form $p_i \equiv 1 \pmod 4$, and q_i are the prime factors of the form $q_i \equiv 3 \pmod 4$ gives another formula $r_2(n) = 4(f_1 + 1)(f_2 + 1) \ldots$, if all exponents h_1,h_2,... are even. If one or more h_i are odd, then $r_2(n) = 0$.
105. The number of ways to represent n as the sum of four squares is eight times the sum of all its divisors which are not divisible by 4, i.e.
     $r_{4}\left(n \right) = 8 \displaystyle\sum {d| n;4 \nmid d}dr{8}\left(n\right) = 16 \displaystyle\sum _{d|n} \left(-1\right)^{n+d}d^{3}$

Number Theory

General

106. for $i > j$, $\gcd(i, j) = \gcd(i - j, j) \le (i - j)$
107. $\sum_{x=1}^{n} [d|x^k] = \left\lfloor \frac{n}{\prod_{i=0} p_i^{\left\lceil \frac{e_i}{k} \right\rceil}} \right\rfloor$,

     where $d = \prod_{i=0} p_i^{e_i}$. Here, $[a|b]$ means if a divides b then it is 1, otherwise it is 0.

108. The number of lattice points on segment (x_1, y_1) to (x_2, y_2) is $\gcd(abs(x_1 - x_2), abs(y_1 - y_2)) + 1$
109. $(n-1)! \mod n = n - 1$ if n is prime, 2 if $n = 4$, 0 otherwise.
110. A number has odd number of divisors if it is perfect square
111. The sum of all divisors of a natural number n is odd if and only if $n = 2^r \cdot k^2$ where r is non-negative and k is positive integer.
112. Let a and b be coprime positive integers, and find integers $a\prime$ and $b\prime$ such that $aa\prime \equiv 1 \mod b$ and $bb\prime \equiv 1 \mod a$. Then the number of representations of a positive integers (n) as a non negative linear combination of a and b is

$$\frac{n}{ab} - \left\{\frac{b\prime n}{a}\right\} - \left\{\frac{a\prime n}{b}\right\} + 1$$

Here, x denotes the fractional part of x.

113. $\sum_{i=1}^{a}\sum_{j=1}^{b}\sum_{k=1}^{c} d(i\cdot j\cdot k) = \sum_{\gcd(i,j)=\gcd(j,k)=\gcd(k,i)=1} \left\lfloor \frac{a}{i} \right\rfloor \left\lfloor \frac{b}{j} \right\rfloor \left\lfloor \frac{c}{k} \right\rfloor$ Here, $d(x) =$ number of divisors of x.

114. **Gauss's generalization of Wilson's theorem:**,
Gauss proved that,

$$\prod_{\substack{k=1 \\ \gcd(k,m)=1}}^{m} k \equiv \begin{cases} -1 \pmod{m} & \text{if } m = 4,\ p^\alpha,\ 2p^\alpha \\ 1 \pmod{m} & \text{otherwise} \end{cases}$$

where p represents an odd prime and α a positive integer. The values of m for which the product is -1 are precisely the ones where there is a primitive root modulo m.

Divisor Function

115. $\sigma_x(n) = \sum_{d|n} d^x$

116. It is multiplicative i.e if $\gcd(a,b) = 1 \to \sigma_x(ab) = \sigma_x(a)\sigma_x(b)$.

117.
$$\sigma_x(n) = \prod_{i=1}^{r} \frac{p_i^{(a_i+1)x} - 1}{p_i^x - 1}$$

118. **Divisor Summatory Function**
    - Let $\sigma_0(k)$ be the number of divisors of k.
    - $D(x) = \sum_{n\le x} \sigma_0(n)$
    - $D(x) = \sum_{k=1}^{x} \lfloor \frac{x}{k} \rfloor = 2\sum_{k=1}^{u} \lfloor \frac{x}{k} \rfloor - u^2$, where $u = \sqrt{x}$
    - $D(n) =$Number of increasing arithmetic progressions where $n+1$ is the second or later term. (i.e. The last term, starting term can be any positive integer $\le n$. For example, $D(3) = 5$ and there are 5 such arithmetic progressions: $(1,2,3,4); (2,3,4); (1,4); (2,4); (3,4)$.

119. Let $\sigma_1(k)$ be the sum of divisors of k. Then, $\sum_{k=1}^{n} \sigma_1(k) = \sum_{k=1}^{n} k \left\lfloor \frac{n}{k} \right\rfloor$

120. $\prod_{d|n} d = n^{\frac{\sigma_0}{2}}$ if n is not a perfect square, and $= \sqrt{n}\cdot n^{\frac{\sigma_0-1}{2}}$ if n is a perfect square.

Euler's Totient function

121. The function is multiplicative.
This means that if $\gcd(m,n) = 1, \phi(m\cdot n) = \phi(m)\cdot\phi(n)$.

122. $\phi(n) = n\prod_{p|n}(1 - \frac{1}{p})$

123. If p is prime and (k \geq 1), then, $\phi(p^k) = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$

124. $J_k(n)$, the Jordan totient function, is the number of k-tuples of positive integers all less than or equal to n that form a coprime $(k+1)$-tuple together with n. It is a generalization of Euler's totient, $\phi(n) = J_1(n)$.
$J_k(n) = n^k \prod_{p|n}(1 - \frac{1}{p^k})$

125. $\sum_{d|n} J_k(d) = n^k$

126. $\sum_{d|n} \phi(d) = n$

127. $\phi(n) = \sum_{d|n} \mu(d)\cdot\frac{n}{d} = n\sum_{d|n}\frac{\mu(d)}{d}$

128. $\phi(n) = \sum_{d|n} d\cdot\mu(\frac{n}{d})$

129. $a|b \to \varphi(a)|\varphi(b)$

130. $n|\varphi(a^n - 1)$ for $a, n > 1$

131. $\varphi(mn) = \varphi(m)\varphi(n)\cdot\frac{d}{\varphi(d)}$ where $d = gcd(m,n)$
Note the special cases

$$\varphi(2m) = \begin{cases} 2\varphi(m) & ;if\, m\, is\, even \\ \varphi(m) & ;if\, m\, is\, odd \end{cases}$$

$$\varphi(n^m) = n^{m-1}\varphi(n)$$

132. $\varphi(lcm(m,n))\cdot\varphi(gcd(m,n)) = \varphi(m)\cdot\varphi(n)$
Compare this to the formula $lcm(m,n)\cdot gcd(m,n) = m\cdot n$

133. $\varphi(n)$ is even for $n \ge 3$. Moreover, if if n has r distinct odd prime factors, $2^r|\varphi(n)$

134. $\sum_{d|n}\frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}$

135. $\sum_{1\le k\le n, \gcd(k,n)=1} k = \frac{1}{2}n\varphi(n)$ for $n > 1$

136. $\frac{\varphi(n)}{n} = \frac{\varphi(rad(n))}{rad(n)}$ where $rad(n) = \prod_{p|n, p\, prime} p$

137. $\phi(m) \ge \log_2 m$

138. $\phi(\phi(m)) \le \frac{m}{2}$

139. When $x \ge \log_2 m$, then

$$n^x \mod m = n^{\phi(m)+x \mod \phi(m)} \mod m$$

140. $\sum_{1\le k\le n, \gcd(k,n)=1} \gcd(k-1,n) = \varphi(n)d(n)$ where $d(n)$ is number of divisors. Same equation for $\gcd(a\cdot k - 1, n)$ where a and n are coprime.

141. For every n there is at least one other integer $m \ne n$ such that $\varphi(m) = \varphi(n)$.

142. $\sum_{i=1}^{n}\varphi(i)\cdot\lfloor\frac{n}{i}\rfloor = \frac{n*(n+1)}{2}$

143. $\sum_{i=1, i\%2\ne0}^{n}\varphi(i)\cdot\lfloor\frac{n}{i}\rfloor = \sum_{k\ge1}[\frac{n}{2^k}]^2$. Note that $[\,]$ is used here to denote round operator not floor or ceil

144.
$$\sum_{i=1}^{n}\sum_{j=1}^{n} ij[\gcd(i,j) = 1] = \sum_{i=1}^{n}\varphi(i)i^2$$

145. Average of coprimes of n which are less than n is $\frac{n}{2}$.

Mobius Function and Inversion

146. For any positive integer n, define $\mu(n)$ as the sum of the primitive n^{th} roots of unity. It has values in $-1, 0, 1$ depending on the factorization of n into prime factors:
    - $\mu(n) = 1$ if n is a square-free positive integer with an even number of prime factors.
    - $\mu(n) = -1$ if n is a square-free positive integer with an odd number of prime factors.
    - $\mu(n) = 0$ if n has a squared prime factor.

147. It is a multiplicative function.

148. $$\sum_{d|n}\mu(d)=\begin{cases}1 & ;n=1\\ 0 & ;n>0\end{cases}$$

149. $\sum_{n=1}^{N}\mu^2(n)=\sum_{n=1}^{\sqrt{N}}\mu(k)\cdot\left\lfloor\frac{N}{k^2}\right\rfloor$ This is also the number of square-free numbers $\leq n$

150. **Mobius inversion theorem:** The classic version states that if g and f are arithmetic functions satisfying $g(n)=\sum_{d|n}f(d)$ for every integer $n\geq 1$ then $g(n)=\sum_{d|n}\mu(d)g\left(\frac{n}{d}\right)$ for every integer $n\geq 1$

151. If $F(n)=\prod_{d|n}f(d)$, then $F(n)=\prod_{d|n}F\left(\frac{n}{d}\right)^{\mu(d)}$

152. $\sum_{d|n}\mu(d)\phi(d)=\prod_{j=1}^{K}(2-P_j)$ where p_j is the primes factorization of d

153. If $F(n)$ is multiplicative, $F\not\equiv 0$, then $\sum_{d|n}\mu(d)f(d)=\prod_{i=1}(1-f(P_i))\cdot$ where p_i are primes of n.

GCD and LCM

154. $\gcd(a,0)=a$
155. $\gcd(a,b)=\gcd(b,a \mod b)$
156. Every common divisor of a and b is a divisor of $\gcd(a,b)$.
157. if m is any integer, then $\gcd(a+m\cdot b,b)=\gcd(a,b)$
158. The gcd is a multiplicative function in the following sense: if a_1 and a_2 are relatively prime, then $\gcd(a_1\cdot a_2,b)=\gcd(a_1,b)\cdot\gcd(a_2,b)$.
159. $\gcd(a,b)\cdot\operatorname{lcm}(a,b)=|a\cdot b|$
160. $\gcd(a,\operatorname{lcm}(b,c))=\operatorname{lcm}(\gcd(a,b),\gcd(a,c))$.
161. $\operatorname{lcm}(a,\gcd(b,c))=\gcd(\operatorname{lcm}(a,b),\operatorname{lcm}(a,c))$.
162. For non-negative integers a and b, where a and b are not both zero, $\gcd(n^a-1,n^b-1)=n^{\gcd(a,b)}-1$
163. $\gcd(a,b)=\sum_{k|a \text{ and } k|b}\phi(k)$
164. $\sum_{i=1}^{n}[\gcd(i,n)=k]=\phi\left(\frac{n}{k}\right)$
165. $\sum_{k=1}^{n}\gcd(k,n)=\sum_{d|n}d\cdot\phi\left(\frac{n}{d}\right)$
166. $\sum_{k=1}^{n}x^{\gcd(k,n)}=\sum_{d|n}x^d\cdot\phi\left(\frac{n}{d}\right)$
167. $\sum_{k=1}^{n}\frac{1}{\gcd(k,n)}=\sum_{d|n}\frac{1}{d}\cdot\phi\left(\frac{n}{d}\right)=\frac{1}{n}\sum_{d|n}d\cdot\phi(d)$
168. $\sum_{k=1}^{n}\frac{k}{\gcd(k,n)}=\frac{n}{2}\cdot\sum_{d|n}\frac{1}{d}\cdot\phi\left(\frac{n}{d}\right)=\frac{n}{2}\cdot\frac{1}{n}\cdot\sum_{d|n}d\cdot\phi(d)$
169. $\sum_{k=1}^{n}\frac{n}{\gcd(k,n)}=2*\sum_{k=1}^{n}\frac{k}{\gcd(k,n)}-1$, for $n>1$
170. $\sum_{i=1}^{n}\sum_{j=1}^{n}[\gcd(i,j)=1]=\sum_{d=1}^{n}\mu(d)\lfloor\frac{n}{d}\rfloor^2$
171. $\sum_{i=1}^{n}\sum_{j=1}^{n}\gcd(i,j)=\sum_{d=1}^{n}\phi(d)\lfloor\frac{n}{d}\rfloor^2$
172. $\sum_{i=1}^{n}\sum_{j=1}^{n}i\cdot j[\gcd(i,j)=1]=\sum_{i=1}^{n}\phi(i)i^2$
173. $F(n)=\sum_{i=1}^{n}\sum_{j=1}^{n}\operatorname{lcm}(i,j)=\sum_{l=1}^{n}\left(\frac{\left(1+\lfloor\frac{n}{l}\rfloor\right)\left(\lfloor\frac{n}{l}\rfloor\right)}{2}\right)^2\sum_{d|l}\mu(d)ld$
174. $\gcd(\operatorname{lcm}(a,b),\operatorname{lcm}(b,c),\operatorname{lcm}(a,c))=\operatorname{lcm}(\gcd(a,b),\gcd(b,c),\gcd(a,c))$
175. $\gcd(A_L,A_{L+1},\ldots,A_R)=\gcd(A_L,A_{L+1}-A_L,\ldots,A_R-A_{R-1})$.'
176. Given n, If $SUM=LCM(1,n)+LCM(2,n)+\ldots+LCM(n,n)$ then SUM = $\frac{n}{2}(\sum_{d|n}(\phi(d)\times d)+1$

Legendre Symbol

177. Let p be an odd prime number. An integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic nonresidue modulo p otherwise. The Legendre symbol is a function of a and p defined as

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a\not\equiv 0 \pmod{p},\\ -1 & \text{if } a \text{ is a non-quadaratic residue modulo } p,\\ 0 & \text{if } a\equiv 0 \pmod{p}\end{cases}$$

178. Legenres's original definition was by means of explicit formula $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod{p}$ *and* $\left(\frac{a}{p}\right)\in -1,0,1.$

179. The Legendre symbol is periodic in its first (or top) argument: if\ $a\equiv b \pmod{p}$, then $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

180. The Legendre symbol is a completely multiplicative function of its top argument: $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

181. The Fibonacci numbers $1,1,2,3,5,8,13,21,34,55,\ldots$ are defined by the recurrence $F_1=F_2=1, F_{n+1}=F_n+F_{n-1}$. If p is a prime number then
$F_{p-\left(\frac{p}{5}\right)}\equiv 0 \pmod{p},\quad F_p\equiv\left(\frac{p}{5}\right) \pmod{p}.$

For example,

$\left(\frac{2}{5}\right)=-1,\quad F_3=2,\quad F_2=1,$

$\left(\frac{3}{5}\right)=-1,\quad F_4=3,\quad F_3=2,$

$\left(\frac{5}{5}\right)=\ 0,\quad F_5=5,$

$\left(\frac{7}{5}\right)=-1,\quad F_8=21,\quad F_7=13,$

$\left(\frac{11}{5}\right)=\ 1,\quad F_{10}=55,\quad F_{11}=89,$

182. Continuing from previous point, $\left(\frac{p}{5}\right)=$ infinite concatenation of the sequence $(1,-1,-1,1,0)$ from $p\geq 1$.

183. If $n=k^2$ is perfect square then $\left(\frac{n}{p}\right)=1$ for every odd prime except $\left(\frac{n}{k}\right)=0$ if k is an odd prime.

Miscellaneous

184. $a + b = a \oplus b + 2(a\&b)$.
185. $a + b = a \mid b + a\&b$
186. $a \oplus b = a \mid b - a\&b$
187. k_{th} bit is set in x iff $x \mod 2^{k-1} \geq 2^k$. It comes handy when you need to look at the bits of the numbers which are pair sums or subset sums etc.
188. k_{th} bit is set in x iff $x \mod 2^{k-1} - x \mod 2^k \neq 0$ ($= 2^k$ to be exact). It comes handy when you need to look at the bits of the numbers which are pair sums or subset sums etc.
189. $n \mod 2^i = n\&(2^i - 1)$
190. $1 \oplus 2 \oplus 3 \oplus \cdots \oplus (4k - 1) = 0$ for any $k \geq 0$
191. **Erdos Gallai Theorem:** The degree sequence of an undirected graph is the non-increasing sequence of its vertex degrees A sequence of non-negative integers $d_1 \geq d_2 \geq \cdots \geq d_n$ can be represented as the degree sequence of finite simple graph on n vertices if and only if $d_1 + d_2 + \cdots + d_n$ is even and

$$\sum_{i=1}^{k} d_i \leq k(k-1) + \sum_{i=k+1}^{n} \min(d_i, k)$$

holds for every k in $1 \leq k \leq n$.