

## Frequently Asked Number Theory Properties

### Prime Factorization:

Every positive integer has a unique prime factorization. Suppose  $N$  factors as follows:  $N = p_1^{q_1} \cdot p_2^{q_2} \cdots p_n^{q_n}$  where each  $p$  is a prime number and each  $q$  is the power of that prime. Since each prime can be used anywhere from 0 to  $q_n$  times, the total number of different factors of  $N$  is  $(q_1 + 1)(q_2 + 1) \cdots (q_n + 1)$ . For example, the total number of factors of 360 is 24 since  $360 = 2^3 \cdot 3^2 \cdot 5^1$ , making  $(3+1)(2+1)(1+1) = 4 \cdot 3 \cdot 2 = 24$ .

### Number of Subsets:

The number of subsets of a given set is equal to  $2^N$ , where  $N$  is the number of elements in the set. This includes the entire set and the null or empty set. A set with only 5 elements therefore has  $2^5 = 32$  distinct subsets. This is easy to understand since each element is either used or not.

You might Related to #2 is the number of subsets containing a certain number of elements. This is just a combination problem. Note that the combination of  $N$  object taken  $R$  at a time is  ${}_N C_R = \binom{N}{R} = \frac{N!}{R!(N-R)!}$ . So the different number of

different sets of 5 elements taken from a set of 8 elements is

$${}_8 C_5 = \binom{8}{5} = \frac{8!}{5!3!} = \frac{8 \cdot 7 \cdot 6}{3 \cdot 2} = 56. \text{ Thus the number of subsets of any size, 0}$$

through  $N$  (of a set of  $N$  elements) is

$${}_N C_0 + {}_N C_1 + {}_N C_2 + \cdots + {}_N C_{N-2} + {}_N C_{N-1} + {}_N C_N \text{ but this is just } 2^N.$$

### Factorial:

Factorial notation is simply  $n! = n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1$ .  $0!$  is defined to be 1.

A favorite question on contests is to give the number of zeros at the end of  $N!$ .

An example will illustrate the method used to compute this. Let's work with  $27!$ .

$$27! = 27 \cdot 26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$$

Each factor of 10 will add a zero to the end of the number, and of course, factors of 10 result from factors of 5 and factors of 2. There are fewer factors of 5, so those are the ones we need to count. Each factor of 5 results in 1 zero, but each factor of 25 or  $5^2$  results in two zeros. Likewise any factor of  $125 = 5^3$  would result in 3 zeros. So, in 27 there are 5 factors of 5, one of which is also a factor of 25, so we have 5 zeros for the factors of 5 and one additional zero for the factor of 25. So there are 6 zeros at the end of  $27!$ . If we wanted to know how many factors of 6 there were in  $27!$ , we would look for powers of 3.

**Binomial Coefficients:**

The combination formula in # 3 gives us the coefficients in Pascal’s Triangle. Here is a part.

1	$1 = 2^0$
1    1	$2 = 2^1$
1    2    1	$4 = 2^2$
1    3    3    1	The sum of each row is $8 = 2^3$
1    4    6    4    1	$16 = 2^4$
${}_5C_0$ ${}_5C_1$ ${}_5C_2$ ${}_5C_3$ ${}_5C_4$ ${}_5C_5$	
1    5    10    10    5    1	$32 = 2^5$

**Floor and Ceiling:**

In number theory where you work primarily with integers,  $27 / 5 = 5$  with no remainder. One symbol that we sometimes use to denote that we are going to drop the remainder is the floor or greatest integer symbol or function. This looks like this:  $\lfloor n \rfloor =$  greatest integer less than or equal to  $n$ . So

$$\lfloor 2.7 \rfloor = 2, \quad \left\lfloor \frac{27}{5} \right\rfloor = 5, \quad \lfloor -3.6 \rfloor = -4.$$

Using this notation, we can find the

$$\text{number of zeros at the end of } 2003! \text{ As } \left\lfloor \frac{2003}{5} \right\rfloor + \left\lfloor \frac{2003}{25} \right\rfloor + \left\lfloor \frac{2003}{125} \right\rfloor + \left\lfloor \frac{2003}{625} \right\rfloor = 400 + 80 + 16 + 3 = 499$$

**Modular Arithmetic**

The remainders when dividing one integer by another always range from zero to one less than the divisor. A convenient way of denoting these remainders is with the *mod notation*. We write  $12 \equiv 2 \pmod{5}$  because the remainder when 12 is divided by 5 is 2. The integers can be divided into congruence classes mod  $m$ , sets of numbers which have the same remainder upon division by  $m$ . The congruence classes everyone is familiar with is the odd/even division of the integers. The odd numbers are congruent to  $1 \pmod{2}$ , while the evens are congruent to  $0 \pmod{2}$ .

**Problems using these facts.**

1. What is the highest power of 6 to divide  $40!$ ?
2. What is the smallest factorial to end in exactly 200 zeros? The largest?
3. What is the smallest positive integer that has exactly 30 factors?
4. Find the largest integer value of  $n$  so that  $3^n$  divides  $(25! + 26!)$ .
5. How many different positive integer factors of  $42^5$  are there?
6. If we write  $30!$  as  $2^n k$  where  $k$  is odd, find  $n$ .
7. How many distinct factors of 2004 are there? Be sure to do this with the current year as well.
8. If a factor of 4200 is chosen at random from all of its distinct factors, what is the probability that it will be odd?
9. The number of divisors of 360 is?
10. Find the highest power of 12 that divides  $100!$