Math Notes

Sidharth Baskaran

March 12, 2022

Table of Contents

Preface

These notes are meant to be a resource for discrete and fundamental mathematics essential for competitive programming and general-purpose problem-solving. The resources used are chiefly EECS70: Discrete Mathematics and Probability and the AoPS Volume 1 book. An emphasis is placed on proof techniques as well.

1 Integer Mathematics

1.1 Last Digit Property

To find the last digit of the sum of product of two integers, we simply apply the operation to the last digit of each contributing integer.

Example 1. To find the last digit of $7^{42} + 42^7$, we break the answer down to the sum of the last digit of each number.

$$\begin{aligned} 7^{42} &= 7^2 \cdot (7^4)^{10} \\ &\implies 9 \cdot 1^{10} \\ &\implies 9 \end{aligned} \qquad\qquad 42^7 \implies 2^7 = 128 \implies 8$$

1.2 Modular arithmetic

A modulo equation $R = a \bmod b$ can be expressed as $a = kb + R$. Typically, $a \geq 0$ but if we consider $a < 0$, then it must be that $R > 0$ and $k < 0$ because R must be in the set of *residues*, which we have as positive.

A complete set of residues $\{a_0, a_1, \ldots, a_{m-1}\}$ (aka a covering system) exist if

$$a_i \equiv i \bmod m$$

To denote equivalence of a number a in mod b, we say

$$a \equiv c \bmod b$$

Example 2. The last digit problem is simplified, for one can apply the mod operation prior to performing the main operation.

$$\begin{aligned} 7^{42} &\equiv 7^2 \bmod 10 \\ &\equiv 9 \bmod 10 \end{aligned} \qquad\qquad \begin{aligned} 42^7 &\equiv 2^7 \bmod 10 \\ &\equiv 8 \bmod 10 \end{aligned}$$

There are useful properties of modular congruences. Let $a \equiv b \bmod m$ and $p \equiv q \bmod m$. Then, $\forall c \in \mathbb{Z}_+$:

$$a + c \equiv b + c \bmod m \tag{1}$$
$$a - c \equiv b - c \bmod m \tag{2}$$
$$ac \equiv bc \bmod m \tag{3}$$
$$a^c \equiv b^c \bmod m \tag{4}$$
$$(a + p) \equiv (b + q) \bmod m \tag{5}$$
$$ap \equiv bq \bmod m \tag{6}$$

1.3 Divisibility Rules

1.3.1 Divisibility by 2, 4, 8

To test divisibility by 4 and 8, the last 2 and 3 digits respectively must be divisible by 4 and 8 respectively. This is because 4 divides a multiple of 100 and 8 a multiple of 1000. This is proven by breaking the number into its base 10 composition.

Checking a number n for 8, we use the fact that $1000^k \equiv 0 \bmod 8$.

$$n \equiv 100a + 10b + c \bmod 8$$

So check if the hundreds, tens and unit places are divisible by 8. Similar argument for 4.

1.3.2 Divisibility by 3

Note that $100 \equiv 10 \cdot 10 \bmod 3 \equiv 1 \cdot 1 \bmod 3$. In general we can say that $10^n \equiv 1 \bmod 3$. If we take for example the 4-digit number $abcd$:

$$\begin{aligned} abcd &\equiv 10^3 \cdot a + 10^2 \cdot b + 10c + d \bmod 3 \\ &\equiv a + b + c + d \bmod 3 \end{aligned}$$

Thus, if $a + b + c + d \equiv 0 \bmod 3$, $abcd$ is divisible by 3.

1.3.3 Divisibility by 5

The number must end in either 0 or 5.

1.3.4 Divisibility by 6

The number must be both divisible by 2 and 3.

1.3.5 Divisibility by 7

If we desire to test some n, note that we can write $n = 10a + b$. Multiplying by 2 does not change the divisibility by 7, so $2n = 20a + 2b \implies n = \frac{20a+2b}{2} = \frac{21a-(a-2b)}{2}$. Then, it follows that

$$\begin{aligned} n &\equiv \frac{21a - (a - 2b)}{2} \bmod 7 \\ &\equiv 2b - a \bmod 7 \end{aligned}$$

1.3.6 Divisibility by 9

Similar to 3, $10^n \equiv 1 \bmod 9$. Using the same methods as for divisibiity by 3, we conclude that the sum of digits in a number must be divisible by 9.

1.3.7 Divisibility by 11

We can break a number N into

$$N = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + a_0$$

For 10^k, if k is odd, then, $10^k \equiv -1 \bmod 11$ else if even $10^k \equiv 1 \bmod 11$. Let us assume n is even, then

$$\begin{aligned} N &\equiv a_n - a_{n-1} + a_{n-2} - a_{n-3} + \ldots + a_0 \bmod 11 \\ &\equiv (a_n + a_{n-2} + \ldots + a_0) - (a_{n-1} + a_{n-3} + \ldots + a_1) \bmod 11 \end{aligned}$$

So $N \equiv 0 \bmod 11$ if the difference of even and odd-indexed digit sums is divisble by 11.

1.4 Prime Numbers

A number can be broken into the product of its prime factors. Note that the largest factor of a number N must be less than or equal to $\sqrt{N}$. There are also infinite prime numbers.

Proof. Suppose there exist a finite number of primes $p_1, p_2, \ldots, p_n$. We know that a prime number is only divisible by unity and itself. Then, suppose we have $P = \prod_{i=1}^{n} p_i + 1$. P is not divisible by any of the primes, only itself or 1. But since $P \geq 1$ it must have a prime factorization, so the list we initially provided does not cover all of the primes. $\square$

1.5 Factors

Greatest common factor (GCF) is the greatest common factor between two numbers. Can find by taking product of all prime numbers common to both. Expressed as $(a, b) = c$ where $c = \text{gcf}(a, b)$. When $(a, b) = 1$, they are relatively prime.

Least common multiple is smallest number that divides both numbers evenly. Expressed as $[a, b] = c$ where $c = \text{lcm}(a, b)$. Easily found by observing prime factorization and creating a set which contains the factors of either number, and the largest exponent if the bases are the same. Identical to finding the least common denominator.

There is a general identity which can be proved, of which the dual is also true.

$$[a_1, a_2, a_3, a_4, \ldots, a_n]\left(\text{permlist}\binom{n}{2}\right) = \prod_{i=1}^{n} a_i$$

Proof. Let p be a prime common to all $a_1, \ldots, a_n$ where $a_1 = p^{c_1}, a_2 = p^{c_2}, \ldots, a_n = p^{c_n}$. WLOG, we state that $c_1 \leq c_2 \cdots \leq c_n$. Then the LCM of all a_i is p^{c_n} and the GCD of all possible two-product permutations is $p^{\sum_{i=1}^{n-1} c_i}$ because the summation power is minimized given those bounds, of which the product is $p^{\sum_{i=1}^{n} c_i}$. We have found that the product of the GCD and LCM shares a prime factorization term with the product of all the numbers a. Each number a_i cannot contain a larger power of p than c_i, so the factor p to the power the sum of all c_i must only belong to the product of all a_i. $\square$

2 Sequences & Series

2.1 Arithmetic and Geometric Series

Arithmetic series of form $a, a+d, a+2d, a+3d, \ldots$ has common difference d. A general term can be described as $a+(n-1)d$ where there are n terms in the sequence. To find the sum, we rewrite the terms in reverse order.

$$\begin{aligned}
S &= a + (a+d) + \ldots + (a+(n-1)d) \\
&= (a+(n-1)d) + (a+(n-2)d) + \ldots + a \\
2S &= n(2a+(n-1)d) \\
S &= \frac{n(2a+(n-1)d)}{2} \\
&= \frac{n(a_1+a_n)}{2}
\end{aligned}$$

Geometric series have a common ratio r, closed-form summation can be derived similarly to above.

$$\begin{aligned}
S &= a + \ldots + ar^{n-1} \\
Sr &= ar + \ldots + ar^n \\
S(1-r) &= a(1-r^n) \\
S &= \frac{a(1-r^n)}{1-r}
\end{aligned}$$

2.2 Infinite Series

Infinite series converges if the sums tend to a fixed value. Terms must tend to zero–this means that the partial sums of the first n terms approach a fixed value. However, terms can tend to zero but the series can itself diverge–if the sums do not tend to a fixed value. Arithmetic series can never converge except for a special case.

Proof. (Arithmetic series never converge except for $a = 0, d = 0$.)
The formula for the sum of an arithmetic series is

$$\begin{aligned} S &= \frac{n(2a+(n-1)d)}{2} \\ &= \frac{2an+dn^2-dn}{2} \\ &= an + \frac{d}{2}n^2 - \frac{d}{2}n \\ &= \frac{d}{2}n^2 + \left(a - \frac{d}{2}\right)n \end{aligned}$$

Then, taking the limit of $S(n)$,

$$\lim_{n\to\infty} \frac{d}{2}n^2 + \left(a - \frac{d}{2}\right)n = \pm\infty$$

This remains true unless $a = 0, d = 0$. □

Geometric series converge given a special condition.

Proof. (Convergence of geometric series)
The geometric series sum of the first n terms is given by

$$S = \frac{a(1-r^n)}{1-r}$$

Then,

$$S_c = \lim_{n\to\infty} \frac{a(1-r^n)}{1-r} = \pm\infty$$

where the sum is negative infinity if $n = 2k+1 | k \in \mathbb{Z}$ and $r < -1$, else if $r > 1$ the sum is positive infinity. Taking the special case of $|r| < 1$, the limit becomes

$$S_c = \frac{a}{1-r}$$

which is the infinite geometric sum under the convergence case. □