Mu Alpha Theta Number Theory Review

1 Introduction

Number theory is an enormous topic, and even the Mu Alpha Theta tests cover a ton of material despite having only 40 questions. The result of this is that if you want to win either (1) you have had a lot of experience in number theory, or (2) you learn everything really quickly and try to dump your knowledge on the test. This review is offering the latter.

2 Definitions

2.1 Sets of Numbers

- The set of integers, denoted by $\mathbb{Z}$, is the set $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- The set of natural numbers, denoted by $\mathbb{N}$, is the set $\{1, 2, 3, \ldots\}$.
- The set of rational numbers, denoted by $\mathbb{Q}$, is the set of all numbers $\frac{p}{q}$, where p and q are integers with $q \neq 0$.

2.2 Types of Natural Numbers

- A natural number is said to be prime if its only natural number divisors are 1 and itself.
- If a natural number is not 1 and is not prime, it is composite.
- 1 is neither prime nor composite.

2.3 GCD and LCM

- The greatest common divisor of two natural numbers m and n is the largest natural number that is a divisor of both m and n.
- The least common multiple of two natural numbers m and n is the smallest natural number that is divisible by both m and n.

2.4 Relatively Prime Numbers

Two natural numbers m and n are relatively prime if $\gcd(m, n) = 1$, i.e. they share no divisors except 1.

2.5 Modular Congruences

We say that $a \equiv b \pmod{c}$ (a is congruent to b modulo c) if $a - b$ is divisible by c, or, equivalently, a and b leave the same remainder when divided by c. For example $7 \equiv 3 \pmod{4}$ and $20 \equiv 0 \pmod{10}$, but $13 \not\equiv 5 \pmod{6}$.

3 Basic Number Theory

This will cover the stuff that you should be familiar with, but may need review on, as well as hopefully improve your speed in some areas.

3.1 Prime Factorization

The prime factorization of a natural number n is writing it in the form $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, where $p_1, p_2, \ldots, p_k$ are primes and $e_1, e_2, \ldots, e_k$ are positive integers. We can find the prime factorization through the use of a factor tree. This is very important and will be essential for much of what is to come.

3.2 Divisors

3.2.1 Number of Divisors

If $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ is factored into primes, the number of divisors of n is given by the formula

$$\prod_{i=1}^{k}(e_i + 1) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1).$$

For example, since $52 = 2^2 \cdot 13^1$, it has $(2 + 1)(1 + 1) = 6$ divisors. A good way to test your understanding of this concept is to see if you can find a formula for the number of divisors of n that are perfect squares, cubes, etc.

3.2.2 Sum of Divisors

If $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ is factored into primes, the sum of the divisors of n is given by the formula

$$\prod_{i=1}^{k}\left(\sum_{j=0}^{e_i} p_i^j\right) = (1 + p_1 + p_1^2 + \cdots + p_1^{e_1})(1 + p_2 + p_2^2 + \cdots + p_2^{e_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{e_k}).$$

With 52 again, the sum of the divisors is $(1 + 2 + 2^2)(1 + 13) = 7 \cdot 14 = 98$.

3.3 Finding the GCD of Two Numbers

3.3.1 Standard Way

You should know the standard way to find the GCD of two numbers: prime factorize each of them and find which of the prime factors and how many powers of each one are shared by both.

3.3.2 Euclidean Algorithm

This is a very useful way to find the GCD of two large numbers quickly. It relies on the fact that, if $a \equiv b \pmod{c}$, we have $\gcd(a, c) = \gcd(b, c)$ (assuming none of them is zero). For example, $700 \equiv 7 \pmod{21}$, so $\gcd(700, 21) = \gcd(7, 21) = 7$. Using this idea, we can algorithmically determine the GCD of two numbers. An example with 2310 and 429 is shown here:

$$\gcd(2310, 429) = \gcd(165, 429) = \gcd(165, 99) = \gcd(66, 99) = 33,$$

where in each step we simply took the bigger number modulo the smaller number.

3.4 Finding the LCM of Two Numbers

Once you have found the GCD using one of the methods described above, just use the following identity to find the LCM.

$$\gcd(m,n) \cdot \text{lcm}(m,n) = m \cdot n.$$

3.5 Working With Mods

A congruence is like an equation, but you must be careful with division. While addition, subtraction, and multiplication are more or less the same, if we have

$$a \equiv b \pmod{c}$$

and we want to divide both sides by d, we must also divide c by $\gcd(c,d)$. For example, if

$$15x \equiv 25 \pmod{35}$$

and we divide both sides by 5 we end up with

$$3x \equiv 5 \pmod{7}.$$

3.6 Bases

Sometimes, we will need to work in a base other than base-10, like base-2 or base-8. First of all, note that the largest digit in base-n is $n-1$. So we can never have a digit 3 in base-2 or 9 in base-8. A number in base-b, something like 1234_b (assume $b > 4$), just means that instead of each place value being ten times the previous one, it is b times the previous one. So where $1234 = 4 \cdot 10^0 + 3 \cdot 10^1 + 2 \cdot 10^2 + 1 \cdot 10^3$, we now have $1234_b = 4 \cdot b^0 + 3 \cdot b^1 + 2 \cdot b^2 + 4 \cdot b^3$, i.e. $1234_8 = 4+3(8)+2(8)^2+1(8)^3 = 668$. Just remember the conversion back to base-10 and you should be able to do most of the problems.

3.7 Factorial Divisibility

A lot of the time you will be asked a question like this: what is the greatest power of m that divides $n!$? Sometimes, they ask the number of zeros at the end of the factorial, which is the same as $m = 10$. Here, we will only deal with prime values of m but this is easily extended to composite ones. All this requires is counting the powers of m that show up in $n!$. You should figure out why this is equal to

$$\left\lfloor \frac{n}{m} \right\rfloor + \left\lfloor \frac{n}{m^2} \right\rfloor + \left\lfloor \frac{n}{m^3} \right\rfloor + \cdots,$$

where $\lfloor x \rfloor$ is the greatest integer less than or equal to x. The formula essentially counts multiples of m, m^2, m^3, and so on until the power is bigger than n. In the case of $m = 10$ (which is not prime, so the formula does not apply), we only need to use $m = 5$ because we know that there will be enough 2's to match up with the powers of 5 and make powers of 10. So 800! ends in

$$\left\lfloor \frac{800}{5} \right\rfloor + \left\lfloor \frac{800}{5^2} \right\rfloor + \left\lfloor \frac{800}{5^3} \right\rfloor + \left\lfloor \frac{800}{5^4} \right\rfloor = 160 + 32 + 6 + 1 = 199$$

zeros. Remember this well!

3.8 Chicken McNugget Theorem

This states that if you can buy boxes of n chicken nuggets or m chicken nuggets, the largest number of chicken nuggets you can never buy is $mn - m - n$. It is basically only useful when you see a problem in that exact form.

4 Advanced Number Theory

This will probably be new stuff, but once learned will definitely help you do better at Mu Alpha Theta. Make sure you learn them well, though, as the applications will not be too straightforward. If you understand everything in this section completely, there is little doubt that you will place. That said, if you do not understand the basic concepts above, I would spend more time on those because they make up a majority of the test.

4.1 Chinese Remainder Theorem

The Chinese Remainder Theorem states that if we have two congruences $n \equiv a \pmod{b}$ and $n \equiv c \pmod{d}$ with $\gcd(b, d) = 1$, we can find exactly one $0 \leq e < bd$ such that $n \equiv e \pmod{bd}$. Sounds complicated, but it is just saying that there is only one solution to those two congruences. For example, if we know $n \equiv 3 \pmod{10}$ and $n \equiv 1 \pmod{3}$, it must be the case that $n \equiv 13 \pmod{30}$, which satisfies both of the original congruences. The Chinese Remainder Theorem can be extended to multiple congruences as well.

4.2 Solving Modular Congruences

Solving quadratic and cubic congruences is similar to solving equations, but there are usually an infinite number of solutions, so we generally find the solutions modulo whatever we are working in. In some cases, you can just plug the answer choices in to find the solution. But when you have the find the number of solutions, a little more work is required. Here are some examples:

- Let's solve $x^2 \equiv 1 \pmod{101}$. Well, we can rearrange and factor to get $(x + 1)(x - 1) \equiv 0 \pmod{101}$. Since 101 is prime, we know either $x + 1 \equiv 0 \pmod{101}$ or $x - 1 \equiv 0 \pmod{101}$, giving us our only solutions $1, 100 \pmod{101}$.
- Now suppose we had something trickier, like $x^3 - 9x^3 + 23x + 126 \equiv 0 \pmod{141}$. The left side is not immediately factorable, but we can make it. By subtracting 141, which is equivalently 0, from both sides, we now have

$$x^3 - 9x^3 + 23x - 15 = (x - 1)(x - 3)(x - 5) \equiv 0 \pmod{141}.$$

  That's much better. Since $141 = 3 \cdot 47$, we just check logical values of x - 1, 3, 5, 48, 50, 52 all work for example. In this case, we notice that if we make it divisible by 47 it will always be divisible by 3. Make sure you understand why this is true.

4.3 The Euler ϕ (Phi) Function

If n is a natural number, then $\phi(n)$ is the number of natural numbers less than n that are relatively prime to n. For example $\phi(4) = 2$, because $\gcd(1,4) = 1$, $\gcd(2,4) \neq 1$, and $\gcd(3,4) = 1$. Also, $\phi(7) = 6$ and $\phi(10) = 4$. In particular, for primes p, $\phi(p) = p - 1$. Furthermore, if a and b are relatively prime, it is true that $\phi(a)\phi(b) = \phi(ab)$.

4.3.1 Calculating $\phi(n)$

If $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ is factored into primes, we have the formula

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

For example, since $100 = 2^2 \cdot 5^2$, we know $\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$.

4.4 Euler's Totient Theorem

This states that, given natural numbers a and m such that $\gcd(a,m) = 1$, we have

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

In general, this is used when you want to find the last digit of a power of some number $\pmod{10}$ or just the remainder when a power of some number is divided by another number. When m is prime, this is known as Fermat's Little Theorem. This is one of the more advanced concepts, so here are several examples.

- If we wanted to find the units digit of 2^{321}, we could (sort of) use Euler's Totient Theorem. While $\gcd(2,10) \neq 1$, we can still usually reduce the power without caring too much about this. Since $\phi(10) = 4$, the theorem allows us to say that $321 \equiv 1 \pmod{4}$ so $2^{321} \equiv 2^1 \equiv 2 \pmod{10}$, which gives us the units digit.
- Suppose we wanted to now find the tens digit of 3^{320}. We can in this case directly use the Totient Theorem to say that, since $\phi(100) = 40$, then $320 \equiv 0 \pmod{40}$ gives $3^{320} \equiv 3^0 \equiv 1 \pmod{100}$. Then the last two digits are 01, so the tens digit is 0.
- Lastly, we have the problem of finding the remainder when 5^{234} is divided by 13. Since 13 is prime, $\phi(13) = 12$. Therefore, $5^{234} \equiv 5^6 = 25^3 \equiv (-1)^3 = -1 \equiv 12 \pmod{13}$.

4.5 Wilson's Theorem

For some reason, this likes to show up on the Mu Alpha Theta test, so here it is. Wilson's Theorem says that if p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

4.6 Prime Number Theorem

The Prime Number Theorem states that, as n gets very, very big the number of primes less than n is approximately $\frac{n}{\ln n}$. Just remember this.

5 Random Numbers

5.1 Perfect Numbers

A perfect number is a natural number n such that the sum of all the positive divisors of n is $2n$. For example, 6 is a perfect number because $1 + 2 + 3 + 6 = 12$. The perfect numbers that are worth memorizing are $6, 28, 496, 8128$. Also note that no odd perfect number has ever been discovered.

5.2 Triangular Numbers

A triangular number is a natural number that can be written as $\frac{n(n+1)}{2}$ for some natural number n. The first few triangular numbers are 1, 3, 6, 10, 15, 21, etc.

5.3 Mersenne Primes

Any prime p that can be written in the form $2^k - 1$ is called a Mersenne prime. The first four are $3, 7, 31, 127$. Note that all known perfect numbers can be written as $2^{k-1}(2^k - 1)$, where $2^k - 1$ is a Mersenne prime.