Number Theory - Supplementary

COMP9020 Tutorial

JIAPENG WANG

24T3 Week2, H18B & F15A

1 Tutorial Outline

1.1 Definition

Ask yourself these questions below to test your understanding.

- What is the definition of the Floor Function and Ceiling Function?
  - What is the relationship between them?
- What is the definition of divisibility?
- What is `gcd` and how is it calculated?
  - What is `lcm`?
  - What is the relationship between `gcd` and `lcm`?
- What is the operation `div` and `%`?
  - What is the relationship between them?

1.2 Brainstorming

The following questions are open and have no standard answers.

- What properties do integers have?
- Why are prime numbers important in division?
- What are the applications of number theory in computer science?
- ......

2 Explanation for Some Exercises

This section is intended to supplement the parts I didn't explain clearly or didn't have time to cover in class. If there are any proofs you provided that are more concise than mine, I will include them as well.

Exercise 4: Find all integer x such that the following equation is true:

$$\left\lfloor \frac{x}{2} \right\rfloor + \left\lceil \frac{x}{3} \right\rceil = 5.$$

Analysis[1]**:**

The range we are searching for the solution to this equation encompasses all integers, which is vast and infinite. Therefore, a natural approach is to **narrow down the possible solutions** to a finite and manageable range through interval analysis, and then **verify each potential solution** one by one.

Proof:

It is obvious that $x > 0$. Therefore, we have $\frac{x}{2} > \frac{x}{3}$.

(Upper Bound) By the property of floor and ceil function, we have:

$$\left\lfloor \frac{x}{2} \right\rfloor \geq \left\lfloor \frac{x}{3} \right\rfloor \geq \left\lceil \frac{x}{3} \right\rceil - 1. \tag{1}$$

Therefore, the original equation satisfies:

$$5 = \left\lfloor \frac{x}{2} \right\rfloor + \left\lceil \frac{x}{3} \right\rceil \geq (\left\lceil \frac{x}{3} \right\rceil - 1) + \left\lceil \frac{x}{3} \right\rceil = 2\left\lceil \frac{x}{3} \right\rceil - 1.$$

By manipulation and the property of Ceiling Function, we have:

$$\frac{x}{3} \leq \left\lceil \frac{x}{3} \right\rceil \leq 3.$$

By solving this inequality, we have $x \leq 9$.

(Lower Bound) Similarly, from (1) we also have

$$\left\lceil \frac{x}{3} \right\rceil \leq \left\lfloor \frac{x}{2} \right\rfloor + 1.$$

Therefore,

$$5 = \left\lfloor \frac{x}{2} \right\rfloor + \left\lceil \frac{x}{3} \right\rceil \leq \left\lfloor \frac{x}{2} \right\rfloor + (\left\lfloor \frac{x}{2} \right\rfloor + 1) = 2\left\lfloor \frac{x}{2} \right\rfloor + 1.$$

By manipulation and the property of Floor Function, we have:

$$\frac{x}{2} \geq \left\lfloor \frac{x}{2} \right\rfloor \geq 2.$$

By solving this inequality, we have $x \geq 4$.

(Verify) Thus, $4 \leq x \leq 9$. Check one by one, we find that $x = 6$ is the only solution for this question. $\square$

[1] Another approach is to guess that $x = 6$ is the only solution, and then prove that other cases are not solutions. However, this method requires a more sensitive understanding of the relationships between the numbers. Choose the method that suits you best:)

Exercise 9: Find the last two digits of 7^{7^7}.

Analysis:

To find the last two digits, we need to determine the remainder when divided by 100.

First, we need to note that exponentiation has a very useful property in modular arithmetic:

Lemma 1:

If $a^b \% d = r$, then $a^{b+c} \% d = (a^c \cdot r) \% d$.

Proof:

Given that $a^b \% d = r$, there exists some integer k such that:

$$a^b = r + kd.$$

Now, consider $a^{b+c} = a^c \cdot a^b$, substitute a^b from the given condition:

$$a^{b+1} = a^c \cdot (r + kd) = a^c \cdot r + a^c \cdot kd.$$

Since $a^c \cdot kd$ is divisible by d, we have $a^{b+c} \% d = (a^c \cdot r) \% d$. $\square$

For problems like this, pay special attention to cases where **the remainder is 1 or (d - 1)**, as these cases have a particularly useful property:

Lemma 2:

If $a^b \% d = 1$, then $(a^b)^c \% d = 1$.

Proof:

Given that $a^b \% d = 1$, there exists some integer k such that:

$$a^b = 1 + kd.$$

Using the given relation $a^b = 1 + kd$, substitute into $(a^b)^c$ and apply the Binomial Theorem[a]:

$$\begin{aligned}(a^b)^c &= (1 + kd)^c \\ &= 1^c + c \cdot 1^{c-1} \cdot (kd) + \binom{c}{2} \cdot 1^{c-2} \cdot (kd)^2 + \cdots \\ &= 1 + d \cdot \left(ck + \binom{c}{2} k^2 d + \binom{c}{3} k^3 d^2 + \cdots \right)\end{aligned}$$

Thus, modulo d, we are left with:

$$(1 + kd)^c \% d = 1,$$

that is, $(a^b)^c \% d = 1$. $\square$

[a] We will discuss the proof of this theorem when we cover combination numbers.

Similarly through this way in *Lemma 2*, we can also prove[2]:

Lemma 3:
If $a^b \ \% \ d = d - 1$, then for any integer exponent c:
- When c is odd, $(a^b)^c \ \% \ d = d - 1$,
- When c is even, $(a^b)^c \ \% \ d = 1$.

From *Lemma 1* and *Lemma 2*, we can conclude that:

Extension:
If $a^b \ \% \ d = 1$, then $a^c \ \% \ d = a^{c\%b} \ \% \ d$.

Proof:
Suppose $c = kb + r, \ 0 \leq r < b$.
From *Lemma 1*, we have

$$a^c \ \% \ d = a^{kb+r} \ \% \ d = ((a^{kb} \ \% \ d) \cdot a^r) \ \% \ d.$$

From *Lemma 2*, since $a^b \ \% \ d = 1$, we have

$$a^{kb} \ \% \ d = 1.$$

Therefore, $a^c \ \% \ d = (1 \cdot a^r) \ \% \ d = a^r \ \% \ d$.

Notice that $r = c\%b$, we have that $a^c \ \% \ d = a^{c\%b} \ \% \ d$. $\square$

We will primarily use this *Extension* to address these types of issues.

Proof:
Note that $7^4 \ \% \ 100 = 1$ and $7^2 \ \% \ 4 = 1$, therefore by *Extension*,

$$\begin{aligned} 7^{7^7} \ \% \ 100 &= 7^{7^7 \% 4} \ \% \ 100 \\ &= 7^{7^{7\%2} \% 4} \ \% \ 100 \\ &= 7^{7^1 \% 4} \ \% \ 100 \\ &= 7^3 \ \% \ 100 \\ &= 343 \ \% \ 100 = 43. \end{aligned}$$

Thus, $7^{7^7} \ \% \ 100 = 43$. $\square$

[2]Notice that $(-1) =_{(d)} (d - 1)$.

Exercise 13: Are there integers x and y such that $4 = 615x + 220y$?

Analysis:

If it exists, it is sufficient to find such x, y; if not, a specific proof must be provided. For integer equation problems, we typically use number theory methods (like **divisibility, parity analysis**, ...) to prove them.

Proof:

No, there aren't. Suppose not, i.e., there exists integers x and y such that

$$4 = 615x + 220y.$$

Note that $0 < 4 < 5$, substitute the equation above, we have

$$0 < 615x + 220y = 5 \cdot (123x + 44y) < 5.$$

Therefore, by manipulate the equation, we have

$$0 < (123x + 44y) < 1.$$

Since x and y are integers, it implies that $123x + 44y$ is also an integer.
But there is no integers between 0 and 1. Contradiction!

Thus, there is no such integers x and y satisfying $4 = 615x + 220y$. $\square$