COMP2711H Tutorial 7

Yuchen Mao

Department of Computer Science and Engineering,
Hong Kong University of Science and Technology

Exercise 1. For any integer a, is the following equation correct?

(1) $(a \mod 35) \mod 5 = a \mod 5$

(2) $(((a \cdot b) \mod 5) \cdot c) \mod 7 = (a \cdot ((b \cdot c) \mod 7)) \mod 5$

Exercise 2. What is the value of $2^{12345} \mod 15$?

Exercise 3. Prove that if $(m - p) \mid (mm' + pp')$, then $(m - p) \mid (mp' + pm')$

Exercise 4. Prove that there is no integer solution for $n^2 + (n+1)^2 = m^2 + 2$.

Exercise 5. Let k be a positive odd integer. Prove that $(1^k + 2^k + \ldots + 9^k) \mod (1 + 2 + \ldots + 9) = 0$.

Exercise 6. What is the greatest common divisor of $\binom{2n}{1}, \binom{2n}{3}, \ldots, \binom{2n}{2n-1}$?
Solution:

let d be the greatest common divisor of $\binom{2n}{1}, \binom{2n}{3}, \ldots, \binom{2n}{2n-1}$. Since for $i = 1, 3, 5, \ldots, 2n-1$, $d \mid \binom{2n}{i}$, we have that $d \mid \sum_{i=1}^{2n-1} \binom{2n}{i}$. $\sum_{i=1}^{2n-1} \binom{2n}{i} = 2^{2n-1}$, so d must be a power of 2.

We claim that d is the largest power of 2, namely 2^k, that divides $\binom{2n}{1} = 2n$. To see this, it suffices to show that $2^k \mid \binom{2n}{i}$ for all $i = 3, 5, 7, \ldots, 2n-1$. Since $2^k \mid 2n$, we have that $2n = q \cdot 2^k$ fir some integer q. For any i, we have

$$\binom{2n}{i} = \frac{2n\binom{2n-1}{i-1}}{i} = \frac{2^k q\binom{2n-1}{i-1}}{i}$$

Proving $2^k \mid \binom{2n}{i}$ is equivalent to proving $i \mid q\binom{2n-1}{i-1}$. We prove it by contradiction. Suppose that $i \nmid q\binom{2n-1}{i-1}$. Since i is an odd integer greater than 1, we also know that $i \nmid 2$ and $i \nmid 2^k$. It is easy to see that $i \nmid 2^k q\binom{2n-1}{i-1}$. On the other hand, since $\frac{2^k q\binom{2n-1}{i-1}}{i} = \binom{2n}{i}$ is an integer, we have that $i \mid 2^k q\binom{2n-1}{i-1}$. Contradiction!

References

[1] Fundamental number theory @Baidu Wenku.