Elementary Number Theory
Spring 2022　Problem Set III

2022 年 5 月 11 日

一、名词解释

Write out the definitions(resp. contents) of following concepts(resp. theorems):

1. congruent(modulo m), where m is a positive integer.
2. residue class(modulo m), where m is a positive integer.
3. complete residue system(modulo m), where m is a positive integer.
4. reduced residue system(modulo m), where m is a positive integer.
5. Euler's Theorem
6. Fermat's Little Theorem
7. Wilson's Theorem
8. Chinese Remainder Theorem
9. the order of a modulo m, where m is a positive integer,a is an integer coprime to m.
10. primitive root modulo m, where $m = 2, 4, p^l, 2p^l$,p is an odd prime,l is a positive integer.
11. Carmichael Number

二、计算题

1. (1 point)

   a) Which of the following sets are complete residue systems modulo 3? Give your reason.

   $$\{221, 324, -235\}, \quad \{-205, 887, 0\}, \quad \{2020, 10086, -10000\}$$

   b) Which of the following sets are reduced residue systems modulo 12? Give your reason.

   $$\{0, 1, 2, \cdots, 11\}, \quad \{-11, 125, -77, 35\}, \quad \{11, 13, -19, 55\}$$

2. (2 points)

a) Is 2022 a prime or a composite? Give your reason.

b) Calculate $2021!(mod 2022)$.

c) Is 1999 a prime or a composite? Give your reason.

d) Calculate $1998!(mod 1999)$.

3. (3 points)

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ be a positive integer,

a) Write out the computation formula(proof is not required) of Euler's ϕ-function $\phi(n)$.

b) Calculate $\phi(2022)$, $\phi(2023)$, $\phi(2024)$.

c) Find the number of positive integers less than 2022 that are coprime to 2022.

d) Find the number of positive integers between 1111 and 9199 that are coprime to 2022.

e) Find the number of positive integers less than 2022 that are coprime to 10000.

4. (3 points)

a) Calculate the last digit of the hexadecimal representation of 2022^{2021}.

b) Calculate the last digit of the hexadecimal representation of 2021^{2022}.

c) Calculate the last digit of the duodecimal representation of 2021^{2022}.

d) Find the last three digits of the decimal representation of 2022^{2021}.

e) Find the last two digits of the decimal representation of the number $1^{1000} + 2^{1000} + \cdots + 2021^{1000} + 2022^{1000}$.

5. (3 points)

Solve the following Diophantine equations:

a) $x^8 + 2x^7 + 3x^6 + 4x^5 + 5x^4 + 6x^3 + 7x^2 + 8x + 9 = 0$

b) $3x^2 + 2 = y^2$

c) $x^2 + y^2 = 3z^2$

d) $x^2 + y^2 = 48z^2$

e) $7x^3 = y^3 + 2$

6. (2 points)

Find the number of solutions of following congruence equations:

a) $1234x \equiv 555(mod 2022)$

b) $777x \equiv 888(mod 2022)$

c) $x^3 + 19x + 35 \equiv 0(mod 105)$

7. (3 points)

Solve the following congruence equations:

a) $1234x \equiv 555(mod 2022)$

b) $777x \equiv 888(mod 2022)$

c) $x^3 + 19x + 35 \equiv 0(mod 105)$

8. (3 points)

Solve the following system of congruence equations :

a)

$$x \equiv 2(mod 4)$$

$$x \equiv 3(mod 9)$$

$$x \equiv 5(mod 25)$$

b)

$$x \equiv 22(mod 25)$$

$$x \equiv 12(mod 30)$$

$$x \equiv 2(mod 35)$$

c)

$$x \equiv 42(mod 55)$$

$$x \equiv 42(mod 66)$$

$$x \equiv 20(mod 77)$$

$$x \equiv 86(mod 88)$$

9. (3 points)

   a) Calculate $10^{100}(mod2022)$.

   b) Calculate $2023^{1022}(mod2048)$.

   c) Calculate $2021^{2022}(mod105)$.

   d) Calculate $2022^{2021^{2020}}(mod105)$.

10. (3 points)

    a) For what kind of positive integer n, there exists a primitive root modulo n?

    b) In $2018, 2019, 2020, 2021, 2022$, which number(or numbers) has a primitive root?

    c) Is 999 a primitive root modulo 2018? If your answer is yes, give your reason. If your answer is no, then calculate the order of 999 modulo 2018.

    d) Is 999 a primitive root modulo 2200? If your answer is yes, give your reason. If your answer is no, then calculate the order of 999 modulo 2200.

    e) Use d) to calculate $999^{1001}(mod2200)$.

    f) Use Chinese Remainder Theorem, calculate $999^{1001}(mod2200)$.

11. (2 points)

    a) Check if 2022 is a primitive root modulo 49.

    b) Check if 3 is a primitive root modulo 7^{2022}.

12. (3 points)

    a) Find all positive integers n such that the last four digits of the decimal representation of 2022 times n are ”1234”.

    b) Find all positive integers n such that the last three digits of the hexadecimal representation of 2021 times n are ”AAA”.

    c) Find the least positive integer n such that n is twice a square, three times a cubic, and five times a fifth power.

三、应用题

1. (3 points)

   Find the day of the week of the following dates:

   a) October 1, 1949 (The Founding day of the people's Republic of China)

   b) July 20, 1969 (First man on the moon)

   c) $10^{10^{10}}$ days after today(May 10, 2022 Tuesday)

   d) 10^{10} days before today(May 10, 2022 Tuesday)

2. (3 points)

   Alice is using her computer to calculate

   $$12345678909876543 21^{20172018201920 20}(mod 31415926535897932626)$$

   If the computer use 1 second to calculate the product of two 20-digits number, and 1 second to calculate the remainder of a 40-digits number divided by a 20-digits number, then is it possible to get the result in 5 minutes? Give your reason.

3. (3 points)

   The most commonly used public key cryptosystem is the RSA cryptosystem(named after Ronald Rivest, Adi Shamir, and Leonard Adleman). The following is the principle:

   Assume n is the product of two large primes p, q, e is a positive integer coprime to $\phi(n)$. Alice first translate the letters of her message into their numerical equivalents(00= blank, 01="A", 02="B", 03="C"...etc.) and then form a block P. She then calculate $P^e(modn)$ to get a ciphertext block C and sends C to Bob. Now Bob has to decrypt the ciphertext block C to the block P and then get Alice's original message.

   Let's try a naive example to illustrate how the RSA cryptosystem works: Let $n = 2759 = 31 \times 89$ be the product of two primes, $e = 679$, and Bob receives the ciphertext block $C = 1872$. Please find Alice's original message.

4. (3 points)

   A Band of 17 pirates have stolen some gold coins. When the pirates divided the coins into equal piles, 3 coins were left over. When they fought over who should get the extra coins, one of the pirates was slain. When the remaining pirates divided the coins into equal piles, 10 coins were left over. When they fought again over who should get the extra coins, another pirate was slain. When they divided the coins in equal piles again, no coins were left over. How many gold coins at least?

5. (3 points)

   A sunny afternoon, Sherlock Holmes and Doctor Watson are chatting while drinking black tea.

   Holmes: *Watson, Let's play a game.*

   Watson: *...Okay.*

   Holmes: *Just think a 3-digits integer, keep it in your mind. Then you divide this integer by 7,11,13 respectively, and just tell me the remainders. I can tell you the integer in your mind.*

   Watson: *Em, the remainders are 1,6 and 3.*

   a) Find the integer.

   Watson: *Unbelievable! ...I guess there must be something concerned with "7,11 and 13", right?*

   Holmes just smiles,

   Watson: Seems that I found the blind spot, ha-ha. I will think a 3-digits integer, and tell you the remainder of dividing this integer by 25,30,35 respectively, Can you tell me the integer in my mind this time, Sherlock?

   Holmes smiles: I'll try.

   Watson: *Em, this time, the remainders are 13,18 and 13.*

   b) Find the integer.

   Watson:*" Wonderful! What a magic! Sherlock, Is this the power of deduction?"*

   Holmes laughs:*" No, Watson, It is the power of Chinese Remainder Theorem."*

6. (3 points)

   Overcoming all kinds of obstacles, Edmond Dant è s finally came to Monte Cristo and found the treasure buried in the island...

   With the help of the crossbow, Dant è s opened the treasure chest, and countless gems reflected in his eyes. The gems shine like stars in the sky, making him dizzy. He then counted the gems and found that:

   a) If he picked 5(and 7, 11) gems each time, and there was always 1 gem left, How many gems at least?

   b) If he picked 6(and 8,10) gems each time, then in the last pick there need exactly 1 gem more to fulfill the pick, How many gems at least?

   c) If he picked 6(and 8, 10) gems each time, and there is always 1 gem left, but if he picked 11 gems each time, then there were no gems left. How many gems at least?

   d) If he picked 9 gems each time, then there were 6 gems left; If he picked 10 gems each time, then there were 8 gems left; If he picked 11 gems each time, then there were 8 gems left; How many gems are there at least?

   e) If he picked 8 gems each time, then there were 1 gems left; If he picked 9 gems each time, then there were 2 gems left; If he picked 10 gems each time, then there were 9 gems left; How many gems are there at least?

7. (3 points)

   Solve the following problem originally posed by Ch'in Chiu-Shao(秦九韶).

   Three farmers equally divide a quantity of rice with a weight that is an integral number of pounds. The farmers each sell their rice, selling as much as possible, at three different markets where the markets use weights of 83 pounds, 110 pounds, and 135 pounds, and only buy rice in multiples of these weights. What is the least amount of rice the farmers could have divided if the farmers return home with 32 pounds, 70 pounds, and 30 pounds, respectively?

8. (2 points)

   An astronomer knows that a satellite orbits the Earth in a period that is an exact multiple of 1 hour that is less than 1 day. If the astronomer notes that the satellite completes 11 orbits in an interval that starts when a 24-hour clock reads 0 hours and ends when the clock reads 17 hours, how long is the orbital period of the satellite?

9. “国士无双”的韩信是我国古代著名军事家，他留下了很多脍炙人口的故事，以下“韩信点兵”就是其中之一：

   传说韩信的算术水平极其高超，他在点兵时，为保守机密，先让士兵从*1*至*3*报数，记下最后一个士兵报的数字，再让士兵从*1*至*5*报数，再次记下最后一个士兵报的数字，最后让士兵从*1*至*7* 报数，再次记下最后一个士兵报的数字。结合方队，他就能算出小队士兵的总数（一个具体的实例见上题）。

   明朝数学家程大卫对此编出了四句“孙子歌诀”（《算法统宗》卷五*:* ⋯⋯物不知总，孙子歌曰（又云韩信点兵也））：

   三人同行七十稀，五树梅花廿一枝，七子团圆正半月，除百零五便得知。

   a)说明如何应用“孙子歌诀”来求解“韩信点兵”。

   b)解释“韩信点兵”和“孙子歌诀”的原理。

   c)选取适当的模数（比如韩信用的是三、五、七），仿照“孙子歌诀”，编一个求解歌诀（不限绝句，可以是五言、长诗、近代诗甚至rap），并举例应用歌诀。

四、证明题

1. (3 points)

   a) Prove that $2021x^{999} + 999x^{666} + 2021$ has no integral roots.

   b) Prove that $x^2+y^2-3z^2$ has no integral roots except $(x, y, z) = (0, 0, 0)$.

2. (3 points)

   a) Prove: a $4k + 3$ type positive integer always has a $4k + 3$ type prime factor.

   b) Prove: there are infinitely many $4k + 3$ type primes.

c) Prove: a $6k+5$ type positive integer always has a $6k+5$ type prime factor.

d) Prove: there are infinitely many $6k+5$ type primes.

3. (3 points)

a) Prove that a $3k+2$ type integer can't be a square.

b) Prove that the sum of squares of three consecutive integers(i.e. $n^2+(n+1)^2+(n+2)^2$) can't be a square.

c) Prove that integers of $4k+2$ type or $4k+3$ type can't be a square.

d) Prove that the sum of squares of four consecutive integers(i.e. $n^2+(n+1)^2+(n+2)^2+(n+3)^2$) can't be a square.

e) Prove that the sum of squares of five consecutive integers(i.e. $n^2+(n+1)^2+(n+2)^2+(n+3)^2+(n+4)^2$) can't be a square.

f) Prove that the sum of squares of 100 consecutive integers(i.e. $n^2+(n+1)^2+(n+2)^2+\cdots+(n+99)^2$) can't be a square.

4. (3 points)

a) Let m be a positive integer, a, b be two integers and $gcd.(a, m) = 1$. Let x runs through a complete residue system modulo m.

Prove: $ax+b$ runs through a complete residue system modulo m.

b) Let $m_1, m_2, \cdots, m_k$ be pairwise coprime positive integers. Let $x_1, x_2, \cdots, x_k$ run through a complete residue system modulo $m_1, m_2, \cdots, m_k$ respectively.

Prove:

$$M_1x_1 + M_2x_2 + \cdots + M_kx_k$$

runs through a complete residue system modulo $m = m_1m_2\cdots m_k$, where $M_i = \frac{m}{m_i}$.

c) Let $m_1, m_2, \cdots, m_k$ be positive integers. Let $x_1, x_2, \cdots, x_k$ run through a complete residue system modulo $m_1, m_2, \cdots, m_k$ respectively.

Prove:

$$x_1 + m_1x_2 + m_1m_2x_3 + \cdots + m_1m_2\cdots m_{k-1}x_k$$

runs through a complete residue system modulo $m = m_1m_2\cdots m_k$.

5. (3 points)

   Let m be an even positive integer, $\{a_1, a_2, \cdots, a_m\}$ and $\{b_1, b_2, \cdots, b_m\}$ are two complete residue systems modulo m.

   Prove: $\{a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m\}$ is not a complete residue systems modulo m.

6. (2 points)

   Prove: for each positive integer n,

   a) $(2^{5n+1} + 5^{n+2})$ is a multiple of 27.

   b) $2^n + (-1)^n$ is not a multiple of 3.

7. (3 points)

   Let $a_n = 2^{3^n} + 1$, $n = 1, 2, 3, \cdots$. Use induction to prove: for each positive integer n, $3^{n+1} || a_n$.

8. (3 points)

   $A = (a_{ij})_{n \times n}$,$B = (b_{ij})_{n \times n}$ are two $n \times n$ matrices with integral entries.

   a) Prove: If $a_{ij} \equiv b_{ij} (modm)$ for all $1 \le i, j \le n$, then

   $$det(A) \equiv det(B)(modm)$$

   b) Show that

   $$det \begin{bmatrix} 1118 & 2448 & 2526 & 4830 & 1155 \\ 5211 & 2535 & 4824 & 3025 & 9009 \\ 2418 & 2430 & 3011 & 1926 & 2508 \\ 1824 & 4826 & 3048 & 3324 & 3048 \\ 8424 & 2664 & 8826 & 5535 & 3019 \end{bmatrix} \neq 0$$

9. (3 points)

   A composite number n is called a pseudo prime if $2^n \equiv 2(mod \;\; n)$.

   a)Prove: 341 is a pseudo prime.

   b)Prove: If m is a pseudo prime, then $2^m - 1$ is also a pseudo prime.

   c)Prove: There are infinitely many pseudo primes.

10. (3 points)

a) Is 173 a prime or a composite? Give your reason. If 173 is a composite, factorize it into prime powers.

b) Prove: for any integer a coprime to 173,

$$a^{172} \equiv 1 (mod 173)$$

c) Is 1729 a prime or a composite? Give your reason. If 1729 is a composite, factorize it into prime powers.

d) Prove: for any integer a coprime to 1729,

$$a^{1728} \equiv 1 (mod 1729)$$

11. (3 points)

a) Prove that all primes factors of $2^{37} - 1$ are $74k + 1$ type integers.

b) Prove that $223 | (2^{37} - 1)$

(Thus the Mersenne number $2^{37} - 1$ *is not a Mersenne prime number.)*

c) Prove that all primes factors of $2^{2^5} + 1$ are $64k + 1$ type integers.

d) Prove that $641 | (2^{2^5} + 1)$

(Thus the Fermat number $2^{2^5} + 1$ *is not a prime number.)*

注意事项

1. 以上是本课程第三部分（同余理论）讲解结束后的习题课内容，也是要求大家第三部分要掌握的内容的底限。我们不会直接提供习题答案给大家，大家需要根据上课笔记内容独力或和同学们合作讨论完成这些题目。

2. 这些题目不用交（作业题目是根据这些题目稍作变化后的题目），但是习题课上会让大家上台讲解这些题目。上台讲解会有讲解分，题号旁边的数字上台讲解习题正确的讲解分。

3. 平时成绩＝签到考勤分（10分）+上课纪律分（30分）+作业分数（20分）+讲题分+期中考试成绩×40%，大于100按100计算。

4. 拒绝上台讲题或是上台后一言不发一字不写的会得到D的评分，第一次评分为D不扣平时分，从第二次评分为D开始，每次评分D扣5分平时分。

5. 总评成绩$=$平时成绩$\times 40\%+$期末考试卷面成绩$\times 60\%$。

6. **新：疫情原因，我们没有举行期中考试，平时成绩和总评成绩计算公式将变更，具体等学校出台相关规定后更新。**