2024 春季学期数论初步期末考试

命题人：　　　**考试时间：**2024.6.11 20:00-22:00　**整理人：Aut**

1. (10 points) Calculate $(314, 159)$.
(10 分) 计算最大公因子 $(314, 159)$.

2. (10 points) Solve the congruence $6x \equiv 3 \pmod{15}$.
(10 分) 解同余方程 $6x \equiv 3 \pmod{15}$.

3. (8 points) Calculate the remainder of $2^{11213} - 1$ modulo 11.
(8 分) 求 $2^{11213} - 1$ 模 11 的余数.

4. (10 points) Solve the system of congruences

$$\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 4 \pmod 9 \\ x \equiv 3 \pmod 5 \end{cases}.$$

(10 分) 解同余方程组

$$\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 4 \pmod 9 \\ x \equiv 3 \pmod 5 \end{cases}.$$

5. (15 points) (a) Show that 2 is a primitive root of 19;
(b) Find all solutions to the equation $x^3 \equiv 1 \pmod{19}$.
(15 分) (a) 证明 2 是模 19 的原根;
(b) 求方程 $x^3 \equiv 1 \pmod{19}$ 的全部解.

6. (10 points) Calculate $\left(\dfrac{5}{7}\right)$.
(10 分) 求 $\left(\dfrac{5}{7}\right)$ 的值.

7. (10 points) Calculate $\displaystyle\sum_{a=1}^{p-1} g_a$.
(10 分) 求 $\displaystyle\sum_{a=1}^{p-1} g_a$ 的值.

8. (15 points) (a) Let $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$. Show that $(2\omega+1)^2 = -3$;

(b) Let p be an odd prime. Determine $\left(\frac{-3}{p}\right)$.

(15 分) (a) 设 $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$, 证明: $(2\omega+1)^2 = -3$;

(b) 设 p 是素数, 讨论 $\left(\frac{-3}{p}\right)$ 的值.

9. (12 points) (a) let μ be the number of negative least residues of the integers $a, 2a, 3a, \cdots, \frac{p-1}{2}a$. Show that

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

(b) Let p be a prime. Show that $(p-1)! \equiv -1 \pmod{p}$.

(12 分) (a) 设 μ 为 $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ 中负最小剩余的个数. 证明

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

(b) 设 p 为素数. 证明 $(p-1)! \equiv -1 \pmod{p}$.

1. (10 points)

Calculate $(187, 221)$.
计算最大公因子 $(187, 221)$.

Proof. $(187, 221) = (187, 34) = (17, 34) = 17$. $\square$

2. (10 points)

Let $a, b, c \in \mathbb{Z}$. Show that the equation $ax + by = c$ has solutions in integers iff $(a, b)|c$.
设 $a, b, c \in \mathbb{Z}$. 证明方程 $ax + by = c$ 有整数解, 当且仅当 $(a, b)|c$.

Proof. $\Rightarrow$: $(a, b)|a, (a, b)|b$, then $(a, b)|ax + by = c$.
$\Leftarrow$: $\exists u, v, q \in \mathbb{Z}$, such that $(a, b) = au + bv, c = (a, b)q$. Then $c = auq + bvq$, which means

$$x = uq, y = vq$$

as a solution of the equation. $\square$

3. (15 points)

If a is a nonzero integer, then for $n > m$ show that $(a^{2^n} + 1, a^{2^m} + 1) = 1$ or 2 depending on whether a is odd or even.
设 a 是非零整数, $n > m$. 证明 $(a^{2^n} + 1, a^{2^m} + 1) = 1$ 或 2 取决于 a 是奇数或偶数.

Proof. For $n > m$, notice that

$$a^{2^n} - 1 = (a - 1)(a + 1)(a^2 + 1)(a^{2^2} + 1) \cdots (a^{2^m} + 1) \cdots (a^{2^{n-1}} + 1),$$

so $a^{2^m} + 1 | a^{2^n} - 1$, then $(a^{2^n} + 1, a^{2^m} + 1) | (a^{2^n} + 1, a^{2^n} - 1) = 1$ or 2.
If a is odd, $a^{2^n} + 1, a^{2^m} + 1$ are both even, $2 | (a^{2^n} + 1, a^{2^m} + 1)$, then $(a^{2^n} + 1, a^{2^m} + 1) = 2$.
If a is even, $a^{2^n} + 1, a^{2^m} + 1$ are both odd, then $(a^{2^n} + 1, a^{2^m} + 1) = 1$. $\square$

4. (10 points)

Show that $\sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d) = n$ for all n.
证明等式 $\sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d) = n$ 对所有 n 成立.

Proof. Since $\sigma(n) = \sum\limits_{d|n} \mathrm{Id}(d)$, then by **Mobius Inversion Theorem**,

$$n = \mathrm{Id}(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d).$$

$\square$

5. (15 points)

Show that there are infinitely many primes congruent to $-1 \mod 6$.
证明模 6 同余 -1 的素数有无穷多.

Proof. Notice that odd numbers are one of the form $6k-1, 6k+1, 6k+3$. But $6k+3$ has a divisor 3, all odd prime numbers except 3 have the form $6k-1$ or $6k+1$. Since $(6k_1+1)(6k_2+1) = 6(k_1k_2+k_1+k_2)+1$, every integer of the form $6k-1$ must have a prime divisor of the form $6k'-1$.

Now suppose that $p_1 < p_2 < \cdots < p_m$ are all primes of the form $6k-1$. Let $N = 6p_1 \cdots p_m - 1$, which is not divisible by any p_i. Moreover, N is not divisible by any number of the form $6k+1$, hence N is a prime greater than p_m, contradiction! □

6. (10 points)

If n is not prime, show that $(n-1)! \equiv 0 \pmod n$, except when $n = 4$.
设 n 不是素数且 $n \neq 4$, 证明 $(n-1)! \equiv 0 \pmod n$.

Proof. $(4-1)! = 6 \equiv 2 \pmod 4$. When $n > 4$, then $n = a \cdot b$, where $2 \le a \le b \le n-1$.

If $b = a$, then $n > 2a$ for $n > 4$, that's $a < n-a$. Since $a(n-a) \equiv a(-a) = -n \equiv 0 \pmod n$, and $a(n-a)|(n-1)!$, then $(n-1)! \equiv 0 \pmod n$.

If $b > a$, then $a \cdot b = n \equiv 0 \pmod 4$. Since $ab|(n-1)!$, hence $(n-1)! \equiv 0 \pmod n$. □

7. (15 points)

Suppose that a is a primitive root modulo p^n, p an odd prime. Show that a is a primitive root modulo p.
设 p 是奇数, a 是模 p^n 的一个原根. 证明 a 也是模 p 的原根.

Proof. Suppose $a^r \equiv 1 \pmod p$, by **Lemma 3**,

$$a^{rp} \equiv 1 \pmod{p^2}, \quad a^{rp^2} \equiv 1 \pmod{p^3}, \ldots, a^{rp^{n-1}} \equiv 1 \pmod{p^n}.$$

Since a is a primitive root modulo p^n, then rp^{n-1} should be divisible by $\phi(p^n) = (p-1)p^{n-1}$, that's $p-1 \mid r$. Hence, the smallest r such that $a^r \equiv 1 \pmod p$ is $p-1$. □

8. (15 points)

Use the fact that 2 is a primitive root modulo 29 to find all solutions to

$$x^7 \equiv 1 \pmod{29}.$$

利用 2 是模 29 的原根, 求方程 $x^7 \equiv 1 \pmod{29}$ 的全部解.

Proof. Since 2 is a primitive root modulo 29. Let $x = 2^y$, then

$$x^7 \equiv 1 \pmod{29} \Leftrightarrow 2^{7y} \equiv 1 \pmod{29} \Leftrightarrow 7y \equiv 0 \pmod{\phi(29)},$$

so $28 = \phi(29) \mid 7y$, that's $y = 4, 8, 12, 16, 20, 24, 28$. Since $(7, \phi(29)) = 7$, and

$$2^4 \equiv 16 \pmod{29}, \quad 2^8 \equiv 24 \pmod{29}, \quad 2^{12} \equiv 7 \pmod{29},$$
$$2^{16} \equiv 25 \pmod{29}, \quad 2^{20} \equiv 23 \pmod{29}, \quad 2^{24} \equiv 20 \pmod{29}, \quad 2^{28} \equiv 1 \pmod{29},$$

the 7 solutions to $x^7 \equiv 1 \pmod{29}$ are $16, 24, 7, 25, 23, 20, 1$. □