初等数论自测题四 参考答案与评分标准

一、名词解释

1. $g(a,b)=ab-a-b$. ……………………………………3 分

2. Let m be a positive integer(In fact, $m=2,4,p^l,2p^l$, p is an odd prime, l is a positive integer.), a is an integer coprime to m, if $o_m(a)=\phi(m)$ ($o_m(a)$ is the order of a modulo m, ϕ is the Euler function), then a is called a primitive root modulo m.

…………………………………3 分

3. $\phi(n)=(p_1^{a_1}-p_1^{a_1-1})(p_2^{a_2}-p_2^{a_2-1})\cdots(p_l^{a_l}-p_l^{a_l-1})$ …………………………………4 分

二、应用题

4.

Sol:

Assume each farmer have x pounds of rice, then it requires to find the minimum positive integral solution of the following system of congruence equations:

$$\begin{cases} x\equiv 68(mod\ \ 110) \\ x\equiv 38(mod\ \ 120) \\ x\equiv 8(mod\ \ 135) \end{cases}$$

……………………………………………3 分

Since 110, 120, 135 are not pairwise coprime, rearrange the system of congruence equations, we get…………参考课堂例题写出求解过程

…………将以上同余方程组转换成模的数两两互素的同余方程组 4 分、求解新的同余方程组的过程 5 分、答案 2 分

Each farmer have 5678 pounds of rice at least. ………………………1 分

5.

Sol:

参考课上例题写出求解过程，答案是“TV”

…………………………………前三个过程每个 4 分、最后的转码过程 1 分、答案 2 分（需作答）

三、计算题

6.

Sol:

参考课上例题写出求解过程

$x \equiv 108(mod\, 2022)$， $x \equiv 1119(mod\, 2022)$.

…………………解方程的过程 6 分、答案 4 分（每个解 2 分）

7.

Sol:

$666 = 2 \times 9 \times 37$ ……………………………………………………………1 分

Let $x = 2022^{2021^{2020}}(mod\, 666)$, by Chinese Remainder Theorem, x is the minimum nonnegative integral solution of the following system of congruence equations.

$$\begin{cases} x \equiv 2022^{2021^{2020}}(mod\ \ 2) \\ x \equiv 2022^{2021^{2020}}(mod\ \ 9) \\ x \equiv 2022^{2021^{2020}}(mod\ \ 37) \end{cases}$$

…………………………………………2 分

Use properties of congruence, we have:

$$\begin{cases} x \equiv 0^{2021^{2020}} \equiv 0(mod\ \ 2) \\ x \equiv 6^{2021^{2020}} \equiv 0(mod\ \ 9) \\ x \equiv 24^{2021^{2020}}(mod\ \ 37) \end{cases}$$

Since 24 is coprime to 37, by Fermat's Little Theorem, $24^{36} \equiv 1(mod\, 37)$. We need to calculate $2021^{2020}(mod\, 36)$.

Note that $2021^{2020} \equiv 1^{2020} \equiv 1(mod\, 4)$,

$2021^{2020} \equiv 5^{2020}(mod\, 9)$, Since 5 is coprime to 9 and $\phi(9) = 6$, by Euler's Theorem, $5^6 \equiv 1(mod\, 9)$, so $2021^{2020} \equiv 5^{2020} \equiv 4(mod\, 9)$.

Thus $2021^{2020} \equiv 13(mod\, 36)$.

Hence $24^{2021^{2020}} \equiv 24^{13} \equiv 18(mod\ \ 37)$ (Here we use the repeated squaring Method)

The system of congruence equations converts to

$$\begin{cases} x \equiv 0^{2021^{2020}} \equiv 0(mod\ \ 2) \\ x \equiv 6^{2021^{2020}} \equiv 0(mod\ \ 9) \\ x \equiv 18(mod\ \ 37) \end{cases}$$

…………………………整个转换过程 8 分

Use Chinese Remainder Theorem, we find $x \equiv 18(mod\ \ 666)$.

……………………………………3 分

So $2022^{2021^{2020}} (mod\, 666) = 18$. ……………………………………1 分

四、证明题

8.

Proof：

a)和自测题二 10a)类似。 …………………4 分

b) $\tau(n) = (a_1 + 1)(a_2 + 1)\cdots(a_l + 1)$. …………………2 分

So $\tau(n)$ is odd if and only if for all $i\,(1 \le i \le l)$, $a_i + 1$ is odd, which equivalents to for all $i\,(1 \le i \le l)$, a_i is even, which by part a), is equivalent to n is a square. ………4 分

9.

Proof：

a) Let x be an integer,

if $x = 2k$ is even(where k is an integer), then

$x^2 \equiv (2k)^2 \equiv 4k^2 \equiv 0(mod\, 4)$. ……………………………………2 分

if $x = 2k + 1$ is odd(where k is an integer), then

$x^2 \equiv (2k+1)^2 \equiv 4k^2 + 4k + 1 \equiv 1(mod\, 4)$. ……………………………………2 分

b)Note that $n, n+1, n+2, n+3$ is a complete residue system modulo 4. ……………2 分

Thus $n^2 + (n+1)^2 + (n+2)^2 + (n+3)^2 \equiv 0^2 + 1^2 + 2^2 + 3^2 \equiv 2(mod\ \ 4)$. ……………3 分

But by part a), the remainder of every square divided by 4 is either 0 or 1.

Thus $n^2 + (n+1)^2 + (n+2)^2 + (n+3)^2$ can't be a square. ……………1 分

10.

Proof:

Use induction on k.

If $k=1$, then $Q_k a - P_k b = a - q_1 b = r_1 = (-1)^{1+1} r_k$, the statement holds. ……………3 分

If $k=2$, then $Q_k a - P_k b = q_2 a - (1+q_1q_2)b = -r_2 = (-1)^{2+1} r_k$, the statement also holds.

………………………………………3 分

（注意归纳初始要验证两个情形）

Assume when $k \le l$ ($l \ge 2$)，the statement holds. ………………………………3 分

（注意是第二数学归纳法）

When $k = l+1$, we have:

$$(-1)^{l+2} r_{l+1} = (-1)^l (r_{l-1} - q_{l+1} r_l)$$ ………………………………2 分

By induction hypothesis,

$$(-1)^l (r_{l-1} - q_{l+1} r_l) = (Q_{l-1}a - P_{l-1}b) + q_{l+1}(Q_l a - P_l b) = (q_{l+1}Q_l + Q_{l-1})a - (q_{l+1}P_l + P_{l-1})b = Q_{l+1}a - P_{l+1}b$$

………………………………4 分

By induction, we get the consequence.