一、(10分)

(1) 求 12423 和 4551 的最大公因子；(5分)

(2) 求二元一次方程 $12423x+4551y=392247$ 的全部整数解(3分)，并列出其中正整数解(2分)。

$\frac{37}{4\overline{)151 7}}$

1\. (1) 123

答案对5分，答案错但知道辗转相除3分

(2) $\begin{cases} x=3+37t \\ y=78-101t \end{cases}$ $(t\in\mathbb{Z})$

正整数解 (3, 78)

全体整数解和正整数解 x, y 各1分。

全体整数解形式 (+37t, −101t) 1分。

二、(10分)

(1) 设 m,n 是正整数，求 3^m-1 和 3^n-1 的最大公因子，并给出详细计算或证明过程(5分)。

(2) 求解一次同余方程 $2^{2024}x\equiv 7 \pmod{25}$.

2.(1) $3^{(m,n)}-1$

知道辗转相除得 3 分

只写答案得 3 分

全对 5 分

(2) $x\equiv 2 \pmod{25}$

知道欧拉定理 2 分

答案正确 5 分

三、（共10分）判断一次同余方程组

$$\begin{cases} x \equiv 7 \pmod{15} \\ x \equiv 19 \pmod{24} \\ x \equiv 27 \pmod{40} \end{cases}$$

是否有解？有解的话，求出全部解；无解的话，请解释原因。

3. $x \equiv 67 \pmod{120}$

拆解质因数错（如24拆为3和2），但会用中国剩余定理得5分

答案正确但过程过于不严谨（如就写了一行经观察得）得8分

全部正确10分

四、(15分) 定义在正整数集合上的函数

$$\sigma_{-2}(n) = \sum_{1 \le d | n} \frac{1}{d^2}.$$

(1) 设 $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ 为正整数 n 的标准分解，给出 $\sigma_{-2}(n)$ 的解析表达式。

(2) $\sigma_{-2}(n)$ 是正整数集合上的积性函数吗？为什么？

(2) 计算 $\sigma_{-2}(2024)$.

4.

(1) $\prod_{i=1}^{k} \sum_{n_i=0}^{\alpha_i} p_i^{-2n_i}$ （或其他一切与此等价的形式）

(2) 是．由(1)中表达式显然

(3) $\sigma_{-2}(2024) = (1+\frac{1}{4}+\frac{1}{16}+\frac{1}{64})(1+\frac{1}{121})(1+\frac{1}{529})$

$= \frac{85}{64} \times \frac{122}{121} \times \frac{530}{529}$

$= \frac{1374025}{1024144}$

(1) 答案对5分，答案错根据步骤酌情给分

(2) 判断3分，若将"积性函数"理解成"完全积性函数"，根据证明情况酌情给分，全对5分．

(3) 因式分解 2分；
知道利用积性 1分；
表达式正确 1分；
算对答案的计算高手 1分．
共5分

五、(15分) 设 $a \geq 2, m \geq 2$ 满足 $ax + my = 1$，其中 x, y 为两个整数。

(1) 一定存在正整数 $d \leq m-1$ 使得 $m|(a^d - 1)$；

(2) 设 d_0 为满足(1)的最小正整数 d, 那么 $m|(a^h - 1)$ 的充分必要条件是 $d_0|h$.

(3) 令 $\varphi(\cdot)$ 为欧拉函数，则有 $d_0|\varphi(m)$.

(1) $(a, m) = 1$，则由 Euler 定理 $a^{\varphi(m)} \equiv 1 \pmod m$ 或 $m | a^{\varphi(m)} - 1$. (2′)

$\varphi(m) \leq m-1$，因为对 $m = \prod_1^{l} p_j^{\alpha_j}$，$\varphi(m) = m \cdot \prod_1^{l} (1 - p_j^{-1}) < m$ (3′)

(2) 由带余除法，存在 $q, r \in \mathbb{Z}$ 且 $0 \leq r < d_0$ 使得 $h = d_0 q + r$.

则 $a^h \equiv (a^{q_0})^{d} \cdot a^r \equiv a^r \pmod m$.

于是 $m | a^h - 1 \Leftrightarrow a^h \equiv 1 \pmod m \Leftrightarrow a^r \equiv 1 \pmod m \Leftrightarrow r = 0 \Leftrightarrow d_0 | h$.

"$\Leftarrow$" 与 "$\Rightarrow$" 3′+2′，不分先后

(3) 在(2)中取 $h = \varphi(m)$. (5′)

六、(10分) 设 $(G,\cdot)$ 是有限群，证明：

(1) 群 G 的指数为 2 的子群 N 为正规子群。

~~(2) 给出对称群 S_3 的一个非平凡正规子群。~~ 给出 S_3 的所有子群及正规子群

(1) $\forall g\in G\setminus N$, $G = N\sqcup gN = N\sqcup Ng$, 故 $Ng=gN$. 而 N 是子群, 故 $\forall g\in N$, $gN=N=Ng$

从而 $N\trianglelefteq G$

(2) 用置换的标准记号

子群 S_3, $\{Id\}$, $\underbrace{\{(1\ 2), Id\}\quad \{(1\ 3), Id\}}_{1'}$ $\{(2\ 3), Id\}$ $\underbrace{\{(1\ 2\ 3), Id\}}_{1'}$

正规子群 $\underbrace{S_3, \{Id\}}_{1'}$, $\underbrace{\{(1\ 2\ 3), Id\}}_{2'}$

平凡的不写倒扣

没有0.5扣这

(1) 另记. 由条件, G 有分划 $G = N\sqcup aN$, 其中 $a\notin N$.

$\forall g\in G$, $\forall n\in N$.

· 若 $g\in N$, 则 $gng^{-1}\in N$.

· 若 $g\notin N$, 则 $g\in aN$, $\Rightarrow \exists n'\in N$ $g=an'$.

$$gng^{-1} = an'nn'^{-1}a^{-1} = a\tilde{n}a^{-1} \quad [\tilde{n}:=n'nn'^{-1}\in N].$$

若 $a\tilde{n}a^{-1}\notin N$, 则 $a\tilde{n}a^{-1}\in aN \Rightarrow \exists n_0\in N$: $a\tilde{n}a^{-1}=an_0$

$\Rightarrow \tilde{n}a^{-1}=n_0 \Rightarrow n_0^{-1}\tilde{n}=a\in N$, 矛盾.

所以 $gng^{-1}=a\tilde{n}a^{-1}\in N$

故 $gng^{-1}\in N$ 总成立, 即 $N\trianglelefteq G$ [N 已知是子群].