期中考试题

1. 对于任意整数 m, 求最大公因数 $(21m+4, 14m+3)$. (10 分)

2.

1) 求最大公因数 $(252, 198)$, 并把它表为 252 和 198 的整系数线性组合. (5 分)

2) 求最小公倍数 $[252, 198]$. (5 分)

3. 求 20! 的标准素因子分解式. (10 分)

4. 求 $5x+7y=41$ 的全部正整数解. (10 分)

5. 证明多项式

$$x^6+x^5+\cdots+x+1$$

不能分解为两个低于 6 次的有理系数多项式的乘积. (10 分)

6. 令 $\sigma(n)$ 为 n 的所有正因数之和. 求 $\sigma(117)$. (10 分)

7. 令 $\varphi(m)$ 为 Euler 函数. 求 $\varphi(7\cdot 9\cdot 11)$. (10 分)

8. 解同余方程 $7x\equiv 1 \pmod{31}$. (10 分)

9. 解同余方程组

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

(10 分)

10. 问同余方程

$$x^2\equiv 14 \pmod{55}$$

是否有解？ (10 分)

解题概要

1. 用 Fermat 定理 $(p|\, n^p - n)$, 对任意整数 n, 证明

$$2730|\, n^{13} - n.$$

(10 分)

因为 $2730 = 2 \times 3 \times 5 \times 7 \times 13$, 所以只要这些素数能整除 $n^{13} - n$ 即可. 例如,

$$n^{13} - n = (n^3)^4 n - n \equiv n^5 - n \equiv n^3 - n \equiv 0 \pmod 3.$$

2. 解同余方程组

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 4 \pmod 7. \end{cases}$$

(10 分)

按照第二章中的标准解法.

3. 由 Wilson 定理

$$(p-1)! \equiv -1 \pmod p$$

推出：当 p 为奇素数时，有

$$2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{1}{2}(p+1)} \pmod p.$$

(5 分)

因为

$$\begin{aligned} 2 \cdot 4 \cdots (p-1) &\equiv (-1)(p-2) \cdot (-1)(p-4) \cdots (-1)1 \\ &\equiv (-1)^{\frac{p-1}{2}} 1 \cdot 3 \cdots (p-2) \pmod p, \end{aligned}$$

所以,

$$
\begin{aligned}
2^2\cdot 4^2\cdots(p-1)^2 &\equiv (-1)^{\frac{p-1}{2}}1\cdot 3\cdots(p-2)\cdot 2\cdot 4\cdots(p-1)\\
&\equiv (-1)^{\frac{p-1}{2}}(p-1)!\equiv (-1)^{\frac{p+1}{2}}\pmod p.
\end{aligned}
$$

4. 求以 3 为二次剩余的素数 $p(>3)$. (10 分)

见第 41 页上的例 1.

5. 问同余方程

$$x^2\equiv 23\pmod{91}$$

是否可解？如果可解的话，有几个 $\bmod 91$ 的解？ (10 分)

因为 $91=7\times 13$, 所以由第 31 页上的定理 1 知，同余方程

$$x^2\equiv 23\pmod{91} \tag{1}$$

的解数为两方程

$$x^2\equiv 23\pmod{7} \tag{2}$$

$$x^2\equiv 23\pmod{13} \tag{3}$$

的解数之积.

由 Legendre 符号的计算知,

$$(\frac{23}{7})=1,\qquad (\frac{23}{13})=1.$$

因此，方程 (2), (3) 各有两个解，从而方程 (1) 有四个解. 这里不必给出具体的解.

6. 令

$$f(x)=x^4+\bar{4}x^3+x^2+\bar{2}x+\bar{4},\qquad g(x)=x^3+\bar{3}x^2+\bar{5}$$

为 $\mathbb{F}_7[x]$ 上的多项式. 求 $f(x)$ 和 $g(x)$ 的最大公因式 $d(x)$(首项系数为 1), 并将 $d(x)$ 写成

$$d(x)=r(x)f(x)+s(x)g(x),$$

这里 $r(x)$, $s(x)$ 均属于 $\mathbb{F}_7[x]$. (10 分)

由多项式的辗转相除法，可得

$$d(x) = x + \bar{1} = (\bar{3}x + \bar{1})f(x) + (\bar{4}x^2 + \bar{3}x + \bar{5})g(x).$$

7. 设 $s > 1$. 令 $\mu(n)$ 为 Möbius 函数,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

证明

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \frac{\zeta(s)}{\zeta(2s)}.$$

(10 分)

因为级数的项是积性函数，而且级数是绝对收敛的，所以由 Euler 乘积公式可得

$$\zeta(s) = \prod_p \Big(1 - \frac{1}{p^s}\Big)^{-1},$$

$$\zeta(2s) = \prod_p \Big(1 - \frac{1}{p^{2s}}\Big)^{-1},$$

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \prod_p \Big(1 + \frac{1}{p^s}\Big).$$

因此,

$$\frac{\zeta(s)}{\zeta(2s)} = \prod_p \frac{(1 - \frac{1}{p^{2s}})}{(1 - \frac{1}{p^s})} = \prod_p (1 + \frac{1}{p^s}) = \sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s}.$$

8. 令 $d(r)$ 为除数函数．证明

$$\sum_{r\,|\,n} d^3(r) = \Big(\sum_{r\,|\,n} d(r)\Big)^2.$$

(10 分)

因为两边都是积性函数，所以只需对于素数幂验证即可. 由

$$\sum_{r\mid p^a} d^3(r) = \sum_{l=0}^{a} d^3(p^l) = \sum_{l=0}^{a}(l+1)^3,$$
$$\Big(\sum_{r\mid p^a} d(r)\Big)^2 = \Big(\sum_{l=0}^{a} d(p^l)\Big)^2 = \Big(\sum_{l=0}^{a}(l+1)\Big)^2,$$

以及恒等式 (用归纳法证明)

$$1^3+2^3+\cdots+m^3 = (1+2+\cdots+m)^2,$$

可得结论.

9. 令 $\varphi(n)$ 为 Euler 函数， $\mu(n)$ 为 Möbius 函数. 对于 $x \geq 1$, 证明

$$\sum_{n\leq x}\frac{\varphi(n)}{n} = \sum_{n\leq x}\frac{\mu(n)}{n}\Big[\frac{x}{n}\Big].$$

(10 分)

因为 $\varphi(n)$ 是 n 的 Möbius 反变换，所以

$$\varphi(n) = n\sum_{d\mid n}\frac{\mu(d)}{d},$$

见第 110 页定理 2. 也可以

$$\varphi(n) = n\prod_{p\mid n}\Big(1-\frac{1}{p}\Big) = n\sum_{d\mid n}\frac{\mu(d)}{d}.$$

因此,

$$\sum_{n\leq x}\frac{\varphi(n)}{n} = \sum_{n\leq x}\sum_{d\mid n}\frac{\mu(d)}{d} = \sum_{d\leq x}\frac{\mu(d)}{d}\sum_{\substack{n\leq x\\ d\mid n}}1 = \sum_{d\leq x}\frac{\mu(d)}{d}\Big[\frac{x}{d}\Big].$$

也可以从右边推出左边.

$$\sum_{n\leq x}\frac{\mu(n)}{n}\Big[\frac{x}{n}\Big] = \sum_{n\leq x}\frac{\mu(n)}{n}\sum_{l\leq\frac{x}{n}}1 = \sum_{m\leq x}\sum_{ln=m}\frac{\mu(n)}{n}$$
$$= \sum_{m\leq x}\sum_{n\mid m}\frac{\mu(n)}{n} = \sum_{m\leq x}\frac{\varphi(m)}{m}.$$

10. 对于 $x \geq 2$, 利用渐近公式

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1),$$

证明

$$\sum_{p \leq x} \frac{\log^3 p}{p} = \frac{1}{3} \log^3 x + O(\log^2 x),$$

这里 p 表示素数. (10 分)

这是 Abel 求和的一个直接应用，与第 94 页定理 2 相似，令

$$S(n) = \sum_{p \leq n} \frac{\log p}{p} = \log n + r(n), \qquad r(n) = O(1),$$

可化为

$$-\sum_{2 \leq n \leq x} \log^2 n \log(1 - \frac{1}{n}).$$

11. 令 $\varphi(n)$ 为 Euler 函数. 对于 $x \geq 2$, 证明

$$\sum_{n \leq x} \frac{1}{\varphi(n)} = O(\log x).$$

(5 分)

我们有

$$\begin{aligned}\varphi(n) &= n \prod_{p \mid n} \Big(1 - \frac{1}{p}\Big) = n \prod_{p \mid n} \Big(1 - \frac{1}{p^2}\Big) \prod_{p \mid n} \Big(1 + \frac{1}{p}\Big)^{-1} \\ &\geq n \prod_{p} \Big(1 - \frac{1}{p^2}\Big) \prod_{p \mid n} \Big(1 + \frac{1}{p}\Big)^{-1},\end{aligned}$$

因此,

$$\frac{1}{\varphi(n)} \ll \frac{1}{n} \prod_{p \mid n} \Big(1 + \frac{1}{p}\Big) \ll \frac{1}{n} \sum_{d \mid n} \frac{1}{d}.$$

于是,

$$\begin{aligned}\sum_{n \leq x} \frac{1}{\varphi(n)} &\ll \sum_{n \leq x} \frac{1}{n} \sum_{d \mid n} \frac{1}{d} = \sum_{d \leq x} \frac{1}{d} \sum_{\substack{n \leq x \\ d \mid n}} \frac{1}{n} \\ &= \sum_{d \leq x} \frac{1}{d^2} \sum_{l \leq \frac{x}{d}} \frac{1}{l} \ll \sum_{d \leq x} \frac{1}{d^2} \log x \ll \log x.\end{aligned}$$

由考试的结果看出，对于数学分析的基本训练还有不足，例如数列的变换，无穷乘积， Abel 求和等. 有时间适当找一些数学分析的题来做.

对于学过的数论内容掌握还不够牢固，讲过的内容还要反复看，和学过的代数和数学分析的内容产生一些联系.

多动手写写学习心得，在草稿纸上自己推导学过的内容.