南开大学本科生2021 - 2022学年第二学期《数论》期末考试试卷(A卷)

草 稿 区

任课教师: 专业: 年级: 学号: 姓名: 成绩:

Pick and solve 9 of the first 10 questions. Show all work to receive full credits. Write your solutions in either Chinese or English. 合分时会去掉前10道题中的一个最低分. 解答写得要详细. 中英文作答均可.

得 分

一、(10分) Let N be a large integer, let $P=(\log N)^B$ for some positive constant B, and let $Q=N/P$. For integers a and q such that $1\le q\le P$, $1\le a\le q$, and $(a,q)=1$, let $\mathfrak{M}(q,a)$ denote the interval $|\alpha-a/q|\le 1/Q$. Here we are considering the real numbers modulo 1. Prove that $\mathfrak{M}(q,a)$ and $\mathfrak{M}(q',a')$ are disjoint if $a/q\ne a'/q'$.

令N是一个大的正整数, 对给定的正常数B令$P=(\log N)^B$以及$Q=N/P$. 对满足$1\le q\le P$, $1\le a\le q$, $(a,q)=1$的正整数a和q, 定义$\mathfrak{M}(q,a)$为由不等式$|\alpha-a/q|\le 1/Q$给出的模1的意义下的区间. 证明当$a/q\ne a'/q'$时两个区间$\mathfrak{M}(q,a)$和$\mathfrak{M}(q',a')$不相交.

得 分

二、(10分) Does the Diophantine equation $a^3+b^4=c^5$ have infinitely many solutions (a,b,c) such that $a,b,c\in\mathbb{Z}_{\geq 1}$? Hint: consider the equation modulo primes.
丢番图方程$a^3+b^4=c^5$有无穷多组正整数解吗? 提示: 考虑该方程模素数p.

草 稿 区

得 分

三、(10分) Apply the Chinese Remainder Theorem to solve the linear Diophantine system

$$\begin{cases} x \equiv 5 \pmod{3}, \\ x \equiv 18 \pmod{5}, \\ x \equiv 2022 \pmod{7}. \end{cases}$$

使用中国剩余定理解丢番图方程组

$$\begin{cases} x \equiv 5 \pmod{3}, \\ x \equiv 18 \pmod{5}, \\ x \equiv 2022 \pmod{7}. \end{cases}$$

草 稿 区

得 分

四、(10分) Let p be an odd prime. Let ζ be a given generator of the cyclic group $\mathbb{F}_p^\star$. Let $G=\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^i$, where $\left(\frac{i}{p}\right)$ is the Legendre symbol. Prove $G^2=\left(\frac{-1}{p}\right)p$.

令p为一个奇素数. 令ζ为乘法循环群$\mathbb{F}_p^\star$的一个给定的生成元. 令$G=\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^i$, 其中$\left(\frac{i}{p}\right)$是勒让德符号. 证明$G^2=\left(\frac{-1}{p}\right)p$.

草 稿 区

得 分

五、(10分) Alice publishes her public key $(15,7)$. (1) Compute Alice's private key. (2) Suppose that Bob wants to send the number 2 to Alice. Compute the ciphertext c he will send in the open channel. (3) After receiving the ciphertext c, check that Alice is able to recover the original message using her private key.
Alice的公钥是$(15,7)$. (1)计算Alice的私钥. (2)Bob想把数字2发给Alice, 他应该如何加密? (3) Alice在收到Bob发来的数字之后如何使用她的私钥进行解密?

草 稿 区

得 分

六、(10分) Prove that for $c > 0$ we have

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{1}{s}\mathrm{d}s=\frac{1}{2}.$$

证明对$c > 0$我们有

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{1}{s}\mathrm{d}s=\frac{1}{2}.$$

草 稿 区

得 分

七、(10分) Apply the prime number theorem to estimate $\sum\limits_{p\le n}\frac{1}{p}$, find the main term in the asymptotic formula.
使用素数定理估计和式$\sum\limits_{p\le n}\frac{1}{p}$, 给出渐进公式中的主项.

草 稿 区

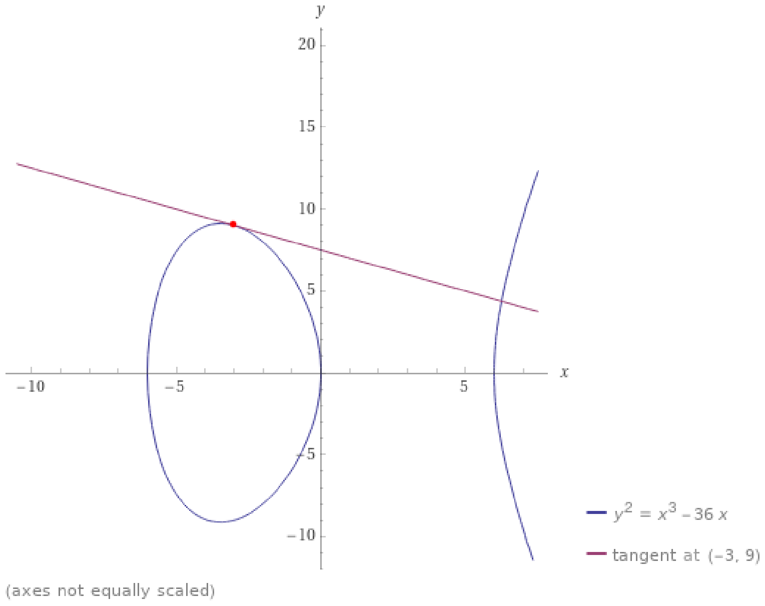
得 分

八、(10分) Which elements are in the ring of integers of the field $\mathbb{Q}(\sqrt{-13})$?
域$\mathbb{Q}(\sqrt{-13})$的代数整数环包含哪些元素?

草 稿 区

得 分

九、(10分) Let $E: y^2 = x^3 - 36x$ be an elliptic curve over $\mathbb{Q}$. What is $(-3,9)+(-3,9)$ on E?
对$\mathbb{Q}$上的椭圆曲线$E: y^2 = x^3 - 36x$, 在E上计算$(-3,9)+(-3,9)$.



草 稿 区

得 分

十、(10分) Right or Wrong. 判断题.

The number 1 is a prime.
数字1是一个素数.

The number -2 is a prime.
数字-2是一个素数.

The curve $E : y^2 = x^3$ is an elliptic curve over $\mathbb{Q}$.
曲线$E : y^2 = x^3$是一个$\mathbb{Q}$上的椭圆曲线.

For any given Dirichlet character χ, the corresponding L-function $L(s, \chi)$ has trivial zeros at -2, -4, -6, $\ldots$.
狄利克雷特征函数χ对应的L-函数$L(s, \chi)$的平凡零点在负偶数上.

For any given Dirichlet character χ, the non-trivial zeros of the corresponding L-function $L(s, \chi)$ are symmetric with respect to the x axis.
狄利克雷特征函数χ对应的L-函数$L(s, \chi)$的非平凡零点关于x轴对称.

得 分

十一、(10分) Feel free to make any suggestions and comments. 随便写点啥.