学院_____ 专业_____ 班级_____ 学号_____ 姓名_____ 任课教师_____

装 订 线

扬 州 大 学 试 题 纸

(2021 －2022 学年第 二 学期)

数学科学 学院 数学 21 级、信科 21 级 班(年)级课程

初等数论 自测题四

考试形式：开卷（ ）闭卷（ √ ）

题目	一	二	三	四	五	六	总分
得分							

一、名词解释（3+3+4=10 分）

1. Let *a,b* be coprime integers, write out the calculation formula of $g(a,b)$, i.e. the Frobenius number of *a,b*. Proof is not required.

2. Write out the definition of primitive root modulo m, where *m* is a positive integer(In fact, $m=2,4,p^l,2p^l$, p is an odd prime, l is a positive integer).

3. Let $n=p_1^{a_1}p_2^{a_2}\cdots p_l^{a_l}$ be a positive integer, $\phi(n)$ be Euler's phi-function, write out the formula of $\phi(n)$ (Proof is not required).

二、应用题（15+15=30 分），注意写清楚计算步骤。

4. Solve the following problem modified from a problem originally posed by Ch'in Chiu-Shao(秦九韶).

Three farmers equally divide a quantity of rice with a weight that is an integral number of pounds. The farmers each sell their rice, selling as much as possible, at three different markets where the markets use weights of 110 pounds, 120 pounds, and 135 pounds, and only buy rice in multiples of these weights. What is the least amount of rice the farmers could have divided if the farmers return home with 68 pounds, 38 pounds, and 8 pounds, respectively?

5. The most commonly used public key cryptosystem is the RSA cryptosystem (named after Ronald Rivest, Adi Shamir, and Leonard Adleman). The following is the principle:

Assume n is the product of two large primes p, q, e is a positive integer coprime to $\phi(n)$. Alice first translate the letters of her message into their numerical equivalents(00= blank, 01="A",02="B",03="C"...,26="Z".) and then form a block P. She then calculate $P^e(modn)$ to get a ciphertext block C and sends C to Bob. Now Bob has to decrypt the ciphertext block C to the block P and then get Alice's original message.

Let's try a naive example to illustrate how the RSA cryptosystem works:

Let $n = 2537 = 43 \times 59$ be the product of two primes, $e = 13$, and Bob receives the ciphertext block $C = 0130$. Please find Alice's original message.

三、计算题（10+15=25 分），注意写清楚计算步骤。

6. Solve the congruence equation $100x \equiv 690(mod\,2022)$.

7. Calculate $2022^{2021^{2020}}(mod\,666)$.

四、证明题（10+10+15=35 分），注意写清楚证明细节。

8. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ be a positive integer, where $p_1, p_2, \cdots, p_l$ are distinct primes, $a_1, a_2, \cdots, a_l$ are positive integers.

a)Prove that n is a square if and only if for all $i\,(1 \le i \le l)$, a_i is even.

b)Let $\tau(n)$ be the number of positive divisors of n, prove that $\tau(n)$ is odd if and only if n is a square.

9. a)Prove: the remainder of every square divided by 4 is either 0 or 1.
b)Prove that the sum of squares of four consecutive integers(i.e. $n^2 + (n+1)^2 + (n+2)^2 + (n+3)^2$) can't be a square.

装 订 线

10. Let a, b be two positive integers, q_k, r_k be the quotients and remainders occurred in the repeated division algorithms to find $g.c.d.(a,b)$, i.e.

$$a = bq_1 + r_1,\ 0 < r_1 < b$$

$$b = r_1q_2 + r_2,\ 0 < r_2 < r_1$$

$$\cdots$$

$$r_i = r_{i+1}q_{i+2} + r_{i+2},\ 0 < r_{i+2} < r_{i+1}$$

$$\cdots$$

P_k, Q_k are the numbers in the Extended Euclidean Algorithm, i.e.

$$P_0 = 1,\ P_1 = q_1,\ P_k = q_kP_{k-1} + P_{k-2}\ \ (k \geq 2)$$

$$Q_0 = 0,\ Q_1 = 1,\ Q_k = q_kQ_{k-1} + Q_{k-2}\ \ (k \geq 2)$$

Use induction to prove: for all positive integers k, $Q_ka - P_kb = (-1)^{k+1}r_k$