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

装 订 线

扬 州 大 学 试 题 纸

(2020 －2021 学年第 二 学期)

数学科学 学院 数学 20 级、信科 20 级 班(年)级课程

初等数论 (A)卷

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. Write out the definition of prime number.

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. Write out the content of Chinese Remainder Theorem(proof is not required).

二、应用题（20 分），注意写清楚计算步骤。

4. 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 $P^e(mod n)$ 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 $n = 2759 = 31 \times 89$ be the product of two primes, $e = 227$, and Bob receives the ciphertext block $C = 1207$. Please find Alice's original message.

线 订 装

三、计算题（10+10+10+10=40 分），注意写清楚计算步骤。

5. a) Is 1 a prime or a composite?

b) Is 137 a prime or a composite? Give your reason. If 137 is a composite, factorize it into prime powers.

c) Is 2021 a prime or a composite? Give your reason. If 2021 is a composite, factorize it into prime powers.

6. a) Calculate $gcd(7525, 2881)$.

b) Calculate $gcd(55^{55}, 555!)$.

7. a) Convert $(2227)_8$ to base-11 representation.

b) Convert $(5316)_8$ to hexadecimal representation.

8. Solve the following system of congruence equations :

$$\begin{cases} x \equiv 11(mod16) \\ x \equiv 15(mod18) \\ x \equiv 19(mod20) \end{cases}$$

四、证明题（**20+10=30** 分），注意写清楚证明细节。

9. a) Let $x_0=\frac{p}{q}(p,q$ are coprime integers) be a rational root of an integral coefficients polynomial $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ ($a_0,a_1,\cdots,a_n$ are integers), prove that: $q\,|\,a_n$ and $p\,|\,a_0$.

b) Let x_0 be a rational root of a monic integral coefficients polynomial $x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ ($a_0,a_1,\cdots,a_{n-1}$ are integers), prove that x_0 is an integer.

c) Let m be a positive integer, m is not a square, prove that $\sqrt{m}$ is an irrational number.

d) Prove that $\sqrt{1000009}$ is an irrational number.

10. a) Prove that all prime factors of $2^{2^5}+1$ are $64k+1$ type integers.

b) Prove that $641\mid(2^{2^5}+1)$.