信息安全数学基础（1）模拟考试20200614

一、判断题（20 分）

(i) 设d 是正整数n 的大于1 的正因数. 则d 是素数. （ ）

(ii) 设a, b, c 是正整数. 若$c|a \cdot b$, 则有$c|a$ 或$c|b$. （ ）

(iii) 设$p = 151$ 是奇素数. 则p 可表示为2 个整数的平方和$p = x^2 + y^2$. （ ）

(iv) 设$p = 151$ 是奇素数. 则14 是模p 平方剩余. （ ）

(v) 设$m = 17^2 \cdot 2011$. 则模m 原根存在. （ ）

二、单选题（20分）

(i) 同余式组 $\begin{cases} x \equiv b_1 \pmod 3 \\ x \equiv 0 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases}$ 的解是（ ）

(A) $70b_1$ (B) $21b_1$ (C) $15b_1$ (D) $105b_1$.

(ii) 设m 是正整数. 设$(a, m) = 1$. 则序列

$u(a) = \{a_k = a^k \mod m\}_{k\geq 1}$ 的周期是（ ）

(A) m (B) $m - 1$ (C) $m + 1$ (D) 欧拉函数$\varphi(m)$.

三、多选题（20分）

(i) 设p, q 都是不同的奇素数, $m = p^2 \cdot q^2$. 则存在整数a, 使得

(A) $\mathrm{ord}_m(a) = p \cdot q \cdot (p - 1) \cdot (q - 1)$.

(B) $\mathrm{ord}_m(a) = p \cdot q \cdot [p - 1, q - 1]$.

(C) $\mathrm{ord}_m(a) = p(p - 1)$.

(D) $\mathrm{ord}_m(a) = q(q - 1)$.

(ii) 圆周率π 的最佳有理逼近是(　　)

(A) $\dfrac{22}{7}$　　(B) $\dfrac{339}{108}$　　(C) $\dfrac{333}{106}$　　(D) $\dfrac{355}{113}$.

四、简答题（40分）

(i) 简述如何产生大素数

(ii) 设$a = 20200614,\ b = 151.$ 有理分数$\dfrac{a}{b}$ 的简单连分数及渐近分数，并求s, t 使得

$$s \cdot a + t \cdot b = (a, b)$$