Print name

Math 453, Hour Exam # 3

December 4, 2013

No calculators or other e-devices and no books or notes allowed.
Solve Problems 1,2,3,4. Show complete work to qualify for full credit.
Extra-credit will be given for substantial work on Problem 5.

[1] (i) (5 pts.) Find all values of an odd prime p for which the congruence

$$x^2 + 1 \equiv 0 \pmod{p}$$

has at least one solution $x \in \mathbb{Z}$.

(ii) (5 pts.) Let p and q be odd primes with $p = q + 4a$ for some $a \in \mathbb{Z}$. Prove that

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

[2] (i) (5 pts.) State the Primitive Root Theorem.
(ii) (4 pts.) Find a primitive root modulo 11 and a primitive root modulo 11^3.
(iii) (4 pts.) How many primitive roots modulo 11 are there? Find them all.
(iv) (2 pts.) Let $a \in \mathbb{Z}$ with $11 \nmid a$. What are the the allowable values for $\mathrm{ord}_{11}(a)$?

[3] (7 pts.) Let p be an odd prime and r be a primitive root modulo p. Prove that

$$\mathrm{ind}_r(p-1) = \frac{p-1}{2}.$$

[4] (8 pts.) Let $\alpha = [a_0; a_1, a_2, \ldots, a_n]$ be a finite continued fraction with $a_0 > 0$ and let $C_i = p_i/q_i$ be the i^{th} convergent of α. If $i \geq 1$, prove that

$$\frac{p_i}{p_{i-1}} = [a_i; a_{i-1}, a_{i-2}, \ldots, a_0].$$

[5] (EC: 5 pts.) Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Prove that

$$\sum_{k=1}^{p-1} \left(\frac{ka}{p}\right) = 0.$$

Print name

Math 453, Hour Exam # 3

December 4, 2013

No calculators or other e-devices and no books or notes allowed. Solve Problems 1,2,3,4. Show complete work to qualify for full credit. Extra-credit will be given for substantial work on Problem 5.

[1] (i) (5 pts.) Find all values of an odd prime p for which the congruence

$$x^2 - 2 \equiv 0 \pmod{p}$$

has at least one solution $x \in \mathbb{Z}$.

(ii) (5 pts.) Let p and q be odd primes with $p = q + 4a$ for some $a \in \mathbb{Z}$. Prove that

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

[2] (i) (5 pts.) State the Primitive Root Theorem.
(ii) (4 pts.) Find a primitive root modulo 13 and a primitive root modulo 13^3.
(iii) (4 pts.) How many primitive roots modulo 13 are there? Find them all.
(iv) (2 pts.) Let $a \in \mathbb{Z}$ with $13 \nmid a$. What are the the allowable values for $\mathrm{ord}_{13}(a)$?

[3] (7 pts.) Let p be an odd prime and r be a primitive root modulo p. Prove that

$$\mathrm{ind}_r(p-1) = \frac{p-1}{2}.$$

[4] (8 pts.) Let $\alpha = [a_0; a_1, a_2, \ldots, a_n]$ be a finite continued fraction with $a_0 > 0$ and let $C_i = p_i/q_i$ be the i^{th} convergent of α. If $i \geq 1$, prove that

$$\frac{q_i}{q_{i-1}} = [a_i; a_{i-1}, a_{i-2}, \ldots, a_1].$$

[5] (EC: 5 pts.) Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Prove that

$$\sum_{k=1}^{p-1} \left(\frac{ka}{p}\right) = 0.$$