MAT 311 Final exam

Number theory

May 15th, 2017

1. Let a be an integer number and p be a prime. Determine whether each of the following statements is true. If so, give a proof. If not give a counterexample.
   (a) If $(a, p) = p$ then $(a^2, p^2) = p^2$.
   (b) If $(a, p^2) = p$ then $(a + p, p^2) = p$.
   (c) If $(a^2, p) = p$ then $(a, p) = p$.
2. Show that if $n > 1$ and n divides $(n-1)! + 1$ then n is prime.
3. Show that if p is prime and $p > 3$ then $p^2 + 2$ is not prime. (HInt: Study the divisibility of $p^2 + 2$ by small primes)
4. Find the greatest common divisor of 1066 and 1492 by the Euclidean algorithm.
5. Find the reminder of 5^{10} divided by 19.
6. Prove that $(n + 1)^5$ is congruent mod 5 to $n^5 + 1$
7. Find all the solutions of the following congruences.
   (a) $12x \equiv 9 \pmod{15}$
   (b) $3x \equiv 1 \pmod{7}$
   (c) $12x \equiv 9 \pmod{12}$
8. Determine the integers n such that the reminder of dividing n by 11 is 10 and the reminder of dividing n by 3 is 1.
9. Find the primes p and q such that $n = p.q = 493$ and $\phi(n) = 448$.
10. Using RSA encryption with $n = 33$
    (a) If $e = 7$, encrypt the message 10, if possible. If not, explain why.
    (b) If $e = 3$, encrypt the message 10, if possible. If not, explain why.
    (c) A message encoded message with $n = 33$ and $e = 5$ is 6. Find the plaintext (decoded) message.
11. Let s be a primitive root of the prime p, Show that if $p \equiv 1 \pmod{4}$ then $-s$ is a also a primitive root.
12. Evaluate the following continued fractions
    (a) $\langle 4, 2, 4, 2, \ldots \rangle$
    (b) $\langle 3, 2, 5 \rangle$
13. Determine the continued fraction expansion of $\sqrt{17}$
14. Evaluate the following Legendre symbols
    (a) $\left(\frac{4}{229}\right)$

(b) $\left(\frac{2}{43}\right)$

(c) $\left(\frac{6}{53}\right)$

15. Show that $\phi(n) = \sum_{d|n} d\mu(\frac{n}{d}) = n \sum_{d|n} \mu(d)/d$

16. Recall that $\sigma(n)$ is the sum of positive divisors of a positive integer n. Find all n such that $\sigma(n) = 31$.