MATH 115
FINAL EXAM

1 (4 pts)
Solve the simultaneous congruences:

$$2x \equiv 5 \mod 7$$
$$7x \equiv -1 \mod 11$$

2 (3 pts) Let p be a prime, with $p \equiv 2 \mod 3$. Show that, for an integer a with $(a,p) = 1$, the congruence

$$x^3 \equiv a \mod p$$

always has **a unique** solution.

3. (8 pts)
Let p be a prime, and a be an integer with $(a,p) = 1$.

a) (3 pts) Show that $\{a, 2a, \cdots, (p-1)a\}$ is a reduced residue system for the modulus p.

b) (2 pts) Let $N_k = 1^k + 2^k + \cdots + (p-1)^k$. Use the results of part a) to show that

$$a^k N_k \equiv N_k \mod p$$

for any a with $(a,p) = 1$.

Note that the result of part b) can be written as

$$(a^k - 1)N_k \equiv 0 \mod p$$

for any $(a,p) = 1$.

c) (3 pt) Use the result of part b) to show that

$$N_k \equiv 0 \mod p$$

whenever k is not divisible by $p - 1$.

4. (6 pts) Let $a \geq 2, k \geq 1$ be positive integers. Put

$$n = a^k - 1$$

It's clear that $\gcd(a,n) = 1$.

a) (4 pts) Prove that the order of $a \mod n$ is equal to k, i.e. k is the smallest positive integer m, such that

$$a^m \equiv 1 \mod n$$

(Hint: $a^m - 1 < a^k - 1$ for $m < k$.)

b) (2 pts) Hence show that for k divides $\phi(a^k - 1)$, where ϕ is Euler's function.

5. (4 pts) Determine whether

$$x^2 \equiv 13 \mod 3019$$

is solvable, given that 3019 is a prime.

6. (6 pts) List all the positive definite reduced forms of discriminant -55.

7. (6 pts) Compute the quadratic irrationality represented by the periodic continued fraction

$$\overline{\langle 2, 5 \rangle} \text{ and } \overline{\langle 3, 4 \rangle}$$

8. (6 pts) Compute the continued fraction expansion of $\sqrt{11}$ and $\sqrt{30}$.

9. (7 pts) Given the continued fraction expansion of $\sqrt{19}$ is $\langle 4, \overline{2, 1, 3, 1, 2, 8} \rangle$. Find the smallest positive solution to the equation:

$$x^2 - 19y^2 = 1$$