1. (10)

(i) Let a, c, m be integers with $m \geq 1$. Explain how to find out the number of solutions, modulo m, of the congruence $ax \equiv c \pmod{m}$.

(ii) Find all solutions (if any) to the congruence $4x \equiv 8 \pmod{12}$.

2. (20)

(i) State Fermat's little theorem.

(ii) Find the number a with $1 \leq a \leq 7$ such that $11^{864} \equiv a \pmod{7}$. (Hint: you do not need to use successive squaring. First calculate $11^{7-1} \pmod{7}$.)

(iii) Find the number b with $1 \leq b \leq 13$ such that $11^{864} \equiv b \pmod{13}$.

(iv) Find the number c with $1 \leq c \leq 19$ such that $11^{864} \equiv c \pmod{19}$.

(v) Using the Chinese remainder theorem and your answers above, or otherwise, find the number n with $1 \leq n \leq 1729$ such that $11^{864} \equiv n \pmod{1729}$. (Hints: (a) $1729 = 7 \times 13 \times 19$; (b) you should be able to answer this part of the question with no further calculations.)

3. (10) Prove that there are infinitely many primes.

4. (20)

(i) Find $\phi(93)$.

(ii) Find $\phi(5555)$.

(iii) Find $\sigma(8128)$, and comment on any significant features of your answer.

(iv) Show that for p prime and $k > 0$, $\phi(p^k)\sigma(p^k) = p^{2k} - p^{k-1}$. What happens if $k = 0$?

5. (10)

(i) What does it mean to say that a is a primitive root modulo 257?

(ii) How many primitive roots are there modulo 257?

(iii) Show that 2 is not a primitive root modulo 257.

6. (10)

(i) Make a table of indices modulo 13 for the base 2 (which you may assume is a primitive root modulo 13).

(ii) Find all solutions to the congruence $x^4 \equiv 9 \pmod{13}$.

7. (20)

(i) Use quadratic reciprocity to compute the Jacobi symbol

$$\left(\frac{11}{1729}\right).$$

(ii) State Euler's criterion, which gives a formula for the Legendre symbol.

(iii) (Pretend you don't already know that 1729 is composite.) Using Euler's criterion and the Jacobi symbol calculated above, state what the value of $11^{864} \pmod{1729}$ would be if 1729 were prime. Does this contradict your earlier computed value of $11^{864} \pmod{1729}$?

Name: _____

University of Colorado

Mathematics 3110: Final Exam

May 4, 2004

Problem	Points	Score
1	10	
2	20	
3	10	
4	20	
5	10	
6	10	
7	20	
Total	100	