Final Exam

Math 258
(Spring 2006)

Solve the following problems. Show all your work in the space under each problem.

1. (a) Show that if $n \in \mathbf{Z}$ is a composite, then n has a prime divisor $\leq \sqrt{n}$. (18 pts)

(b) Use the above to examine whether 131 is prime.

(c) Show that there are infinitely many primes

(d) **True** or **False**: If p is prime, then $p! + 1$ is prime.

(e) If $p_1, p_2, \ldots, p_n$ are the first n consecutive primes, does it necessarily imply that $p_1 p_2 \cdots p_n + 1$ is prime?

(f) The function $f(n) = n^2 - n - 1$, $n > 2$, fails to be a prime-generating function for:

A. $n = 6$ B. $n = 10$ C. $n = 12$ D. $n = 13$

2. (a) Define the **gcd(*a*,*b*)** and **lcm(*a*,*b*)** , for $a, b \in$ **Z-{0}**. (10 pts)

(b) Appropriate formula for lcm(*a*,*b*) gives that the lcm($3^2 \cdot 5 \cdot 7^2 \cdot 11$ **,** $2 \cdot 3 \cdot 7^3$) is:

A. $3^2 \cdot 5 \cdot 7^2 \cdot 11 \cdot 2 \cdot 3 \cdot 7^3$ B. $3 \cdot 7^2$ C. $2 \cdot 3^2 \cdot 5 \cdot 7^3 \cdot 11$ D. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$

3. (a) Show that if the gcd(*a*,*m*) > 1, then *a* has **no** inverse in Z_m (12 pts)

(b) Use the *extended Euclidean algorithm* to write the gcd(87,38) as a linear combination of 87 and 38. Use that relation to find the inverse of 38 in Z_{87}.

4. (a) Show that if *a*, *b*, *k* and *m* are integers such that $a \equiv b \bmod m$ and $k \geq 1$, $m \geq 2$, then $a^k \equiv b^k \bmod m$. (15 pts)
(*Hint*: Use the identity for $a^k - b^k$).

(b) Is the converse true? Examine the case for *k* = 2.

(c) A solution to the congruency $8x \equiv 2 \bmod 13$ is:

A. $x \equiv 2 \bmod 13$ B. $x \equiv 7 \bmod 13$ C. $x \equiv 10 \bmod 13$ D. $x \equiv 13 \bmod 13$

5. Show that $\binom{2n}{2} = 2\binom{n}{2} + n^2$, where $n \in \mathbf{N} - \{\mathbf{0}\}$. (10 pts)

6. (a) What is the probability that a five-card poker hand does not contain the queen of hearts? (10 pts)

(b) What is the probability to roll a 2 in a 3-number biased die, in which 1 is three times as likely to come up as 3 and 2 is two times as likely to come up as 3?

7. A relation R on a set A is called **irreflexive** if **(** $x \in A \Rightarrow (x, x) \notin A, \forall x \in A$ **)**. In other words, no element in A relates to itself. Suppose now that a relation R is irreflexive. Is R^2 necessarily irreflexive? Explain. (5 pts)

8. (a) Determine whether the following relation on the set of all functions from **Z** to **Z** is an equivalence relation. Make sure you check all the relevant properties: (10 pts)

$$R = \{(f, g) \mid f(x) - g(x) = C \text{ , for some } C \in \mathbf{Z}, \forall x \in \mathbf{Z} \}$$

(b) What is the equivalence class of $f(x) = x^2$?

9. (a) Find the equivalence relation induced by the following partition of the set $S = \{0,1,2,3,4,5\}$: (10 pts)

$$\{0\}, \{1,2\}, \{3,4,5\} .$$

(b) Are the elements 1 and 4 equivalent?