

Final Exam

Math 258
(Fall 06)

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 $\leq \sqrt{n}$. (25 pts)

(b) Use the above to examine whether 101 is prime.

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

(e) If p_1, p_2, \dots, 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. Appropriate formula for $\mathbf{lcm}(a,b)$ gives that the $\mathbf{lcm}(5 \cdot 7 \cdot 11^2, 2 \cdot 3^2 \cdot 7^3)$ is: (5 pts)

A. $3^2 \cdot 5 \cdot 7^2 \cdot 11$

B. $2 \cdot 3^2 \cdot 5 \cdot 7^3 \cdot 11^2$

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 \mathbf{Z}_m (20 pts)

(b) Use the *extended Euclidean algorithm* to write the $\mathbf{gcd}(35, 78)$ as a linear combination of 35 and 78. Use that relation to find the inverse of 35 in Z_{78} .

4. (a) Show that if a, b, k and m are integers such that $a \equiv b \pmod{m}$ and $k \geq 1, m \geq 2$, then $a^k \equiv b^k \pmod{m}$. (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 $3x \equiv 4 \pmod{7}$ is:

- A. $x \equiv 12 \pmod{7}$ B. $x \equiv 5 \pmod{7}$ C. $x \equiv 6 \pmod{7}$ D. $x \equiv 4 \pmod{7}$

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

6. 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? (5 pts)

7. (a) Determine whether the following relation on the set of all functions from \mathbf{Z} to \mathbf{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 $f(x) = x^2$?

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

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

- (b) Are the elements 2 and 5 equivalent?