Math 435 Number Theory I

Midterm 1–Solutions

1) (10pt) State the Fundamental Theorem of Arithmetic.

If $n > 1$, then there are prime numbers $p_1, \ldots, p_m$ and $e_1, \ldots, e_m \in \mathbb{N}$ such that $N = p_1^{e_1} \cdots p_m^{e_m}$. Moreover this factorizaiton is unique up to permutation of the p_i. In other words, if $p_1 < \ldots < p_m$, $q_1 < \ldots < q_s$ are primes, $f_1, \ldots, f_s \in \mathbb{N}$ and $N = q_1^{f_1} \cdots q_s^{f_s}$, then $m = s$, and $q_i = p_i$, $e_i = f_i$ for all $i = 1, \ldots, m$.

2) (30 pt) Decide if the following statements are TRUE or FALSE. If FALSE, explain why it is FALSE or give a counterexample

a) If $a|c$ and $b|c$, then $\operatorname{lcm}(a, b)|c$.

TRUE

b) There is unique congruence class mod 81 solving the congruence $6x \equiv 15 (\text{mod } 81)$.

FALSE. Since $\gcd(6, 15, 81) = 3$, there will be 3 incongruent solutions mod 81.

c) There is a unique congruence class mod 810 solving the system of congruences

$$x \equiv 7(\text{mod } 10), x \equiv 12(\text{mod } 15) \text{ and } x \equiv 22(\text{mod } 81).$$

FALSE. If $x \equiv 12(\text{mod } 15)$, then $x \equiv 0(\text{mod } 3)$. But if $x \equiv 22(\text{mod } 81)$, then $x \equiv 1(\text{mod } 3)$, so there are no solutions.

d) If $a|n$ and $b|n$, then $ab|n$.

FALSE. $6|24$ and $3|24$ but $18 \not| 24$.

3)(15pt) Use the Euclidean algorithm to find $\gcd(195, 165)$ and to find integers x, y such that $195x + 165y = \gcd(195, 165)$.

$$\begin{aligned} 195 &= 165 + 30 \\ 165 &= 5(30) + 15 \\ 30 &= 2 * 15 \end{aligned}$$

Thus $\gcd(195, 165) = 15$

$$\begin{aligned} 15 &= 165 - 5(30) \\ &= 165 - 5(195 - 165) \\ &= 6(165) - 5(195) \end{aligned}$$

4) (15pt) Find all congruence classes solving the system of equations

$$3x \equiv 2 (\text{mod } 5) \text{ and } x \equiv 2 (\text{mod } 7).$$

First note that $3x \equiv 2 \text{mod } 5$ if and only if $x \equiv 4 (\text{mod } 5)$. So we must solve the system

$$x \equiv 4 (\text{mod } 5) \text{ and } x \equiv 2 (\text{mod } 7).$$

We need to find u, v such that $7u \equiv 1 (\text{mod } 5)$ and $5v \equiv 1 (\text{mod } 7)$. We can take $u = 3$ and $v = 3$.

Thus we can take

$$x = 4(7)(3) + 2(5)(3) = 114 \equiv 9 (\text{mod } 35)$$

and $[9]$ is the unique congruence class mod 35.

5) (10pt) Prove that $n \in \mathbb{N}$ is prime if and only if $\gcd(n, (n-1)!) = 1$.

6) (10pt) Suppose the decimal representation of N is $a_m a_{m-1} \ldots a_0$ (i.e., $N = \sum_{i=0}^{m} a_i 10^i$). Prove that

$$N \equiv a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^m a_m (\text{mod } 11).$$

In particular n is divisible by 11 if and only if $a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^m a_m$ is.

7) Suppose a, b, c are integers and $\gcd(a, b) = 1$. Prove there is $n \in \mathbb{Z}$ such that $\gcd(an + b, c) = 1$.