PMATH 145 Assignment 2

Patrick Ingram

due October 13th by 12:30PM

Problem 1. Show that $n^4 + n^2 + 1$ is not prime for *any* value of $n \geq 2$.

Problem 2. Find an integer x such that $917x \equiv 231 \pmod{1001}$.

Problem 3. Prove let m and n be natural numbers with $\gcd(n, m) = 1$, and suppose that $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$. Show directly that $x \equiv y \pmod{mn}$. (Do not use the Chinese Remainder Theorem.)

Problem 4.

i. Compute $\gcd(20136, 17328)$, and then find $x, y \in \mathbb{Z}$ such that $20136x + 17328y = \gcd(20136, 17328)$. (Just one solution will do, but show all of your work.)

ii. Since $\gcd(3, 7) = 1$, it follows that any integer can be written in the form $3x + 7y$, with $x, y \in \mathbb{Z}$. Show that every integer $n \geq 12$ can actually be written in the form $3x + 7y$, where x and y are *non-negative* integers.

Problem 5.

i. Let $a, b, c \in \mathbb{Z}$ all be non-zero. We define $\gcd(a, b, c)$ to be the greatest integer which divides all three of a, b, and c. Show that the equation $ax + by + cz = d$ has a solution $x, y, z \in \mathbb{Z}$ if and only if $\gcd(a, b, c) \mid d$.

ii. Let $a_1, ..., a_n \in \mathbb{Z}$ all be non-zero, and define $\gcd(a_1, ..., a_n)$ to be the greatest integer which divides all of the integers a_i. Show that $\sum a_i x_i = b$ has a solution $x_1, ..., x_n \in \mathbb{Z}$ if and only if $\gcd(a_1, ..., a_n) \mid b$.

Problem 6. Write $\begin{pmatrix} n \\ m \end{pmatrix}$ for the binomial coefficient $\frac{n!}{m!(n-m)!}$.

i. Show that if p is prime, then $p \mid \begin{pmatrix} p \\ m \end{pmatrix}$ for any $1 \leq m \leq p - 1$.

ii. Show that for any $x, y \in \mathbb{Z}$, we have $(x + y)^p \equiv x^p + y^p \pmod{p}$. (Show this directly. Do not use Fermat's Little Theorem.)

Problem 7. The Mersenne sequence is the sequence of integers $M_n = 2^n - 1$.

i. Show that $k \mid n$ implies $M_k \mid M_n$.

ii. Show that $\gcd(M_k, M_n) = M_{\gcd(k,n)}$.

(Note: the second claim implies the first, but you might need the first to prove the second. The division algorithm is useful for the second proof.)