2015-09-07 Problems

Introduction to Number Theory

1. Let $n \in \mathbb{N}$. Show that if $2^n - 1$ is prime, then n is prime.

2. Show that (the validity of) the Goldbach conjecture implies the ternary Goldbach conjecture.

3. Show that there exist infinitely many primes p of the form $p = 4n + 3\,(n \in \mathbb{N})$.

4. Another proof that there exist infinitely many primes.
4.1. Show that (ignoring the problem of convergence)

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p:prime} \left(1 - \frac{1}{p}\right)^{-1}.$$

4.2. Show that $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges (i.e., tends to infinity). Hint: The following diverges

$$1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \cdots$$

4.3. Conclude that there are infinitely many prime numbers.

5.1. Prove that $n \in \mathbb{N}$ is prime if and only if n is not divisible by any prime $p < n$.
5.2. Prove that $n \in \mathbb{N}$ is prime if and only if n is not divisible by any prime $p \leq \sqrt{n}$.
5.3. List all prime numbers < 100.
5.4. Show that 8627 is prime. (may use calculator)

6. (Unique factorization theorem) Any natural number > 1 can be expressed uniquely in the form

$$p_1^{a_1} \cdots p_m^{a_m}$$

where p_i are distinct prime numbers and $a_i \in \mathbb{N}$ for each $1 \leq i \leq m$ for some $m \in \mathbb{N}$.
6.1. Show that any natural number can be expressed (not necessarily uniquely) as a product of prime numbers.
6.2. Show that the expression above is unique, that is, if

$$p_1^{a_1} \cdots p_m^{a_m} \text{ and } q_1^{b_1} \cdots q_n^{b_n}$$

are two expressions of the same number (q_i are primes), then $n = m$, $a_i = b_i$, and $q_i = p_i$ for each i (here we set $p_1 < \cdots < p_m$ and $q_1 < \cdots < q_n$). Hint: Show 9.2.1 below first.

6.2.1. Show that if $p^a = q^b$ with p, q primes and $a, b \in \mathbb{N}$, then $p = q$ and $a = b$.

7. Let $a, b \in \mathbb{N}$.
7.1. Show that any common divisor of a and b divides the greatest common divisor $gcd(a, b)$.
7.2.1. Show that if $gcd(a, b) = 1$, then there exist $c, d \in \mathbb{N}$ such that $ac + bd = 1$.
7.2.2. Show that if $gcd(a, b) = e$, then there exist $c, d \in \mathbb{N}$ such that $ac + bd = e$.
7.3.1. Let $J \subset \mathbb{Z}$ be a subset such that "if $e, f \in J$, then $e - f \in J$". Show that there exists $n \in \mathbb{Z}$ such that $J = n\mathbb{Z}$
7.3.2. Set $D(a, b) = \{ax + by \,|\, x, y \in \mathbb{Z}\}$. Show that if $e, f \in D(a, b)$, then $e - f \in D(a, b)$.
7.3.3. From 7.3.1 and 7.3.2, we know that $D(a, b) = m\mathbb{Z}$ for some $m \in \mathbb{N}$. Show $m = gcd(a, b)$.
7.4. Show $gcd(a, b) = gcd(b, a - qb)$.

8. Let $a > b$ be natural numbers. Recall Euclid's algorithm:

$$\begin{array}{rcll} a & = & bm_1 + r_1 & (0 \leq r_1 < b) \\ b & = & r_1 m_2 + r_2 & (0 \leq r_2 < r_1) \\ r_1 & = & r_2 m_3 + r_3 & (0 \leq r_3 < r_2) \\ & \vdots & & \\ r_{s-1} & = & r_s m_{s+1} + r_{s+1} & (0 \leq r_{s+1} < r_s) \end{array}$$

where $m_i \in \mathbb{N}$ with $r_{s+1} = 0$ and $r_s \neq 0$
8.1. Given natural numbers $x > y$, show that there exist a unique pair (w, z) of nonnegative integers such that $x = yz + w$ with $0 \leq w < y$.
8.2. Prove that r_s divides both a and b.
8.3. Prove that any common divisor of a and b divides r_s. Conclude that r_s equals the greatest common divisor $gcd(a, b)$. (May use 7.1 above)

9.1. What is the smallest integer > 100 such that when divided by 3,4, or 5, the remainder is 2?
9.2. What is the smallest positive integer such that when divided by 11,12,13 respectively the remainder is 3,4,5 respectively?

10.1. Find all pairs of integers (x, y) such that $11x + 7y = 1$.
10.2. Find all triples of integers (x, y, z) such that $11x + 7y + 3z = 1$.

11. Let p_n denote the n-th prime. For example, $p_1 = 2, p_2 = 3, \ldots$. Show that $p_n \leq 2^{2^{n-1}}$.