MA347 – HW2

Jonathan Lam

January 21, 2021

Page 9 #1 and Page 13 #1

1. Prove that there are infinitely many prime numbers.

   Proof. Let $\{p_i\} = 2, 3, \ldots, P$ be the set of primes up to and including P. Let $N = \prod_i p_i + 1$. By the fundamental theorem of arithmetic, any natural number $n > 2$ must be factorable into a product of primes, i.e., N must have a prime factor. It suffices to prove that any prime dividing N is greater than P; then, given any prime P, we can prove the existence of a larger prime using this method.

   Let d be a prime that divides N, and $N = qd$. Rearranging:

$$N - \prod_i p_i = 1$$

$$qd - \prod_i p_i = 1$$

$$qd - \left[\prod_{i \neq j} p_i\right] p_j = 1$$

   From this we see that 1 is in the ideal generated by d and p_j, for any prime $p_j \leq P$, and thus d is relatively prime with all primes no greater than P. Thus any prime factor of N must be larger than P. □

2. Let $n, d \in \mathbb{N}$ and assume $1 < d < n$. Show that n can be written in the form

$$n = c_0 + c_1 d + \cdots + c_k d^k$$

with integers c_i such that $0 \leq c_i < d$, and that these integers c_i are uniquely determined.

Proof. To show existence, since we have $n, d \in \mathbb{N}$, we can use the Euclidean algorithm to find c_0, n_1 such that

$$n = c_0 + n_1 d \tag{1}$$

where $0 \leq c_0 < d$. Similarly, we can use the Euclidean algorithm on the quotient n_1:

$$n_1 = c_1 + n_2 d \tag{2}$$

with a similar constraint on c_1; we can keep iterating (2) using n_i, d and the Euclidean algorithm to find c_i, n_{i+1} until the quotient n_i becomes zero. (With every step, the quotient becomes smaller, since $qd \leq n$ and $d > 1$, so the quotient must reach zero after some finite number of iterations.) After substituting and simplifying the expression, n is expressed in the form shown in the hypothesis, in which each coefficient fits the constraint $0 \leq c_i < d$; i.e., this construction leads to an expression of the form:

$$n = c_0 + (c_1 + (c_2 + (\cdots + c_k d)d)d)d = c_0 + c_1 d + c_2 d^2 + \cdots + c_k d^k$$

To show uniqueness, we use the second form of induction. The base case is that c_0 is uniquely determined by the Euclidean algorithm in (1). For the inductive step, assume that $\{c_i\}_1^r$ are uniquely determined, and show that c_{r+1} is then determined. We know that c_i, d uniquely determines n_{i+1} by the Euclidean algorithm, so $\{n_{i+1}\}_1^r$ are also uniquely determined. Thus we have $n_{r+1}, d \in \mathbb{N}$ both uniquely determined, which uniquely determine c_{r+1}. Thus every $c_i \in \{c_i\}_1^k$ is uniquely determined. □