MATH 347   Homework #3.   Sketch of solutions.

Note Title

#1 Let $a, b \in \mathbb{Z}$. Suppose $ua + vb = c$ for some $u, v \in \mathbb{Z}$. Prove that $\gcd(a,b) \mid c$.

By definition $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$. Therefore $\gcd(a,b)$ divides any linear combination of a and b. In particular it divides $c = ua + vb$.

#2 Suppose next: $ua + vb = 1$ for some $x, y \in \mathbb{Z}$. Prove that $\gcd(a,b) = 1$.

By #1 $\gcd(a,b) \mid 1$. The only positive integer that divides 1 is 1. Hence $\gcd(a,b) = 1$.

#3 a) Show that for any $n \in \mathbb{N}$, $\gcd(n+1, n) = 1$.

$1 \cdot (n+1) + (-1) n = 1$. #2 $\Rightarrow$ $\gcd(n+1, n) = 1$.

b) Show that for any $n \in \mathbb{N}$ and any $q \in \mathbb{Z}$

$$\gcd(qn+1, n) = 1.$$

$1 \cdot (qn+1) + (-q) n = 1$

#4 Let $p_1, p_2, \ldots p_n$ be prime numbers. Show that $p_i \nmid (p_1 p_2 \cdots p_n + 1)$ for any i, $1 \le i \le n$.

Let $q_i := (p_1 p_2 \ldots p_n)/p_i$. It's an integer and $p_1 \ldots p_n + 1 = q_i p_i + 1$. By (4b), $\gcd(q_i p_i + 1, p_i) = 1$

Now, if $p_i \mid q_i p_i + 1$, then $p_i \mid \gcd(q_i p_i + 1, p_i) = 1$

Contradiction.

Therefore $p_i \nmid p_1 \ldots p_n + 1$

#5. Show that there are infinitely many prime numbers.

Proof by contradiction. Suppose there are only finitely many prime numbers. Call them $p_1, p_2, \ldots p_n$. Consider $q = p_1 p_2 \cdots p_n + 1$. Since $q > p_i$ for each i, $q \neq p_i$ for any i. $\Rightarrow$ q is not a prime. Since $p_i \nmid q$ by #4, $\gcd(q, p_i) = 1$ [recall: for any number $x \in \mathbb{Z}$ and any prime p, $\gcd(x, p)$ is either p or 1]. $\Rightarrow$ q is not a product of primes. This contradicts:

Theorem: Every integer q, $q > 1$, is a prime or a product of primes.