Writing Assignment 3 in LaTeX

Alex Holland V00

December 2, 2020

Question 1
(a) show that q, p_1, p_2 are primes and $q|p_1p_2$, then $q = p_1$ or $q = p_2$.
(b) Suppose q, p_1, p_2, p_3 are primes and $q|p_1p_2p_3$. Prove that $q = p_1$ or $q = p_2$ or $q = p_3$.

(a)
We know that q, p_1, p_2 are primes and $q|p_1$ or $q|p_2$ as q, p_1, p_2 are primes. Because q and p_1 are primes then $q|p_1$ implies $q = p_1$. As well, q and p_2 are primes since $q|p_2$ implies $q = p_2$. Therefore, if q, p_1, p_2 are primes then $q|p_1p_2$ and so $q = p_1$. $\square$

(b)
q, p_q, p_2, p_3 are primes and $q|p_1p_2p_3$. Then $q|p_1p_2p_3$ implies $q|p_1$ or $q|p_2$ or $q|p_3$. if $q|p_1$ then $q = p_1$ since q and p_1 are primes. If $q|p_2$ the $q = p_2$ since q and p_2 are primes. If $q|p_3$ then $q = p_3$ since q and p_3 are primes. Therefore if q, p_q, p_2, p_3 are primes and $q|p_1p_2p_3$ then $q = p_1$ or $q = p_2$ or $q = p_3$. $\square$

Question 2
Let $a, b, c \in \mathbb{N}$ be such that $c|a$ and $c|b$. Prove that $c|gcd(a, b)$.

We know that a and b are natural numbers. Let's let $d = gcd(a, b)$. Then there must exist integers k_1 and k_2 such that $d = ak_1 + bk_2$. Because c divides a implies $(c|a)$ $a = ck_1$ for some $k \in \mathbb{Z}$. Also c divides b implies $(c|b)$ $b = ck_2$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned} d &= ax + by \\ &= ck_1x + ck_2y \\ &= c(k_1x + k_2y) \end{aligned}$$

Because $x, y, k_1, k_2 \in \mathbb{Z}$ then we have that $k_1x + k_2y \in \mathbb{Z}$ so $c(k_1x + k_2y)$. Therefore, $(c|d)$ which implies $c|gcd(a, b)$. $\square$

Question 3
(a) Let $c \in \mathbb{N}$ and $m \in \mathbb{N}$. The least residue of n modulo m is the the unique integer among $0, 1, ..., m - 1$ to which n is congruent modulo m. For $k \in \mathbb{N}$, explain why $k^2 \equiv 0(mod\, 4)$ or $k^2 \equiv 1(mod\, 4)$.
(b) Prove that no integer which is congruent to 4 modulo 4 can be written as a sum of two squares. That is, if $n \equiv 3(mod\, 4)$, then there are no integers x and y such that $n = x^2 + y^2$.

(a)
We are given that $n \in \mathbb{Z}$ and $m \in \mathbb{N}$ The least residue of n *modulo* m is the unique integer among $0, 1, ...m-1$ to which n is congruent to *modulo* m. We can show $k^2 \equiv 0(mod\, 4)$ or $k^2 \equiv 1(mod\, 4)$ for $k \in \mathbb{N}$

$$\begin{aligned}
(4k+0)^2 &= 16k^2 \equiv 0 \ (mod\ 4) \\
(4k+1)^2 &= 16k^2 + 8k + 1 \equiv 1 \ (mod\ 4) \\
(4k+2)^2 &= 16k^2 + 16k + 4 \equiv 0 \ (mod\ 4) \\
(4k+3)^2 &= 16k^2 + 24k + 9 \equiv 1 \ (mod\ 4) \\
(4k+4)^2 &= 16k^2 + 32k + 16 \equiv 0 \ (mod\ 4)
\end{aligned}$$

We can determine from relationship of each equation that 0 and 1 are the only residues of *modulo* 4 when we consider any integer k. Therefore for $k \in \mathbb{N}$, $k^2 \equiv 0(mod\ 4)$ or $k^2 \equiv 1(mod\ 4)$.$\square$

(b)
We need to prove that no integer which is congruent to 3 *modulo* 4 can be written as a sum of two squares that is if $n = 3\ (3\ mod\ 4)$. Then there must be no integers x and y such that $n = x^2 + y^2$. We can show the least residues of *square modulo* 3 by the set of equations

$$\begin{aligned}
(3k)^2 &= 9k^2 \\
&\equiv 0 \ (mod\ 3) \\
(3k+1)^2 &= 9k^2 + 6k + 1 \\
&\equiv 1 \ (mod\ 3) \\
(3k-1)^2 &= 9k^2 - 6k + 1 \\
&\equiv 0 \ (mod\ 3)
\end{aligned}$$

Hence, 0 and 1 are the only least residues of *modulo* 3. So $x^2 + y^2$ can take only the values 0, 1, and 2. Therefore, for any $n \in \mathbb{Z}$, $n \equiv 3\ (mod\ 4)$ such that $n = x^2 + y^2$, thus there are no integers x and y which are congruent to 3 *modulo* 4 that can be written as a sum of two squares. $\square$

Question 4
Let $b > 1$ be an integer, and $n = (d_k d_{k-1} ... d_1 d_0)_b$. Show that $(b-1)|n \Leftrightarrow d_0 + d_1 + d_2 + ... + d_k$.

Because $n = (d_k d_{k-1} ... d_1 d_0)_b$ then n is equivalent to $n = d_k \times b^k + d_{k-1} \times b^{k-1} + ... + d_1 \times b^1 + d_0 \times b^0$. From this, we can see that

$$\begin{aligned}
b &\equiv 1 \ (mod\ b-1) \\
b^k &\equiv 1 \ (mod\ b-1) \\
d_k b^k &\equiv d_k \ (mod\ b-1) \\
d_{k-1} b^{k-1} &\equiv d_{k-1} \ (mod\ b-1) \\
d_1 b^1 &\equiv d_1 \ (mod\ b-1) \\
d_0 b^0 &\equiv d_0 \ (mod\ b-1)
\end{aligned}$$

From this we can write n as $n = d_k \times b^k + d_{k-1} \times b^{k-1} + ... + d_1 \times b^1 + d_0 \times b^0 \equiv (d_k + d_{k-1} + d_1 + d_0)(mod\ b-1)$. Therefore $(b-1)|n$ is equivalent to $d_0 + d_1 + d_2 + ... + d_k$. $\square$

Question 5

In this question we will give a proof that there are infinitely many primes that's similar to Euclid's proof. We'll do it in several steps. For a positive integer n, recall that $n\ factorial$ is the integer $n(n-1)(n-2)...1$.
(a) Suppose $k \in \mathbb{N}$ is such that $2 \leq k \leq n$. Explain why the remainder when $N = n! + 1$ is divided by k equals 1.
(b) Explain why part (a) implies that N has a prime divisor greater that n.
(c) Explain why part (b) implies that there is no largest prime number.
(d) Explain why part (c) implies that there are infinitely many primes.

(a)
We can represent $N = n! + 1$ as $n! = n(n-1)(n-2)...1$. Then $n!$ can be represented in terms of n, $N - n(n-1)(n-2)...1 + 1$. So, for every $k \in \mathbb{N}$, then $k|n!$. Therefore $N \equiv 1\ (mod\ k)$ for $1 \leq k \leq n$. $\square$

(b)
Part (a) implies that, for every $k \in \mathbb{N}$, such that $1 \leq k \leq n$. No k can divide N. From this, no prime numbers from $1\ to\ n$ can divide N, so either N has a prime divisor greater than n, or N is prime number, which then can not be divisible by any k, such that $1 \leq k \leq n$. $\square$

(c)
Suppose that n is the largest prime number. By part (b), implies that $N = n! + 1$ has a prime divisor that is greater than n So, we get prime greater than n, for any $k \in \mathbb{Z}$ such that $1 \leq k \leq n$, which is a contradiction. There is no largest prime number because we always get a prime number that is greater than n. $\square$

(d)
It is determined by part (c) that there is no largest prime number, since for each prime number there exists a prime number that is larger. Therefore, this relation implies that there are infinitely many primes. $\square$