William Strimling

Homework 4

Question 5

Let p be a prime integer greater than 3

Considering the formula $p = r \pmod 6$, we know r can only possibley be 0, 1, 2, 3, 4 or 5 for any number r as defined by the Division Theorem where $p = 6q + r$ and $0 \le r < d$.

If we take r to be 0, it follows that $p = 6q + 0$ by the division theorem and that $p = 6q$. Because there exists some integer k ($k = 6$) where $p = kq$, and int $p \neq 0$ (its > 3), we can conclude $q \mid p$ by the definition of divides. In the case where $p \neq 6$, it follows that p is not prime by the definition primality – there is some integer q, that divides it other than 1 and itself. Therefore it follows that $p \equiv 0 \mod 6$ is false. Similarly in case where $p = 6$, it would appear that p is prime however $2 \mid 6$ and $3 \mid 6$ and thus 6 is not prime by the definition of prime and we can finally conclude that $p \equiv 0 \mod 6$ is disproven.

If we take r to be 2, it follows that $p = 6q + 2$ by the division theorem and therefore that $p = 2(3q + 1)$ by using algebra. Based on the division theorem, we know $(3q + 1)$ is an integer because in $p = 6q + 2$, $p \in \mathbb{Z}$ and $q \in \mathbb{Z}$ by the division theorem and integers are closed under addition and multiplication. Because we know $(3q + 1)$ is a integer, we know $2 \mid p$ by the definition of divides, and therefore that p is not prime in the case of $r = 2$ because it is shown to be divisible by something other than 1 and itself.

If we take r to be 3, it follows that $p = 6q + 3$ by the division theorem, and by Algebra that $p = 3(2q + 1)$. We know $q \in \mathbb{Z}$ and therefore that $6q + 3$ is an integer because integers are closed under additions and multiplication. We also know $p = 3(2q + 1)$ is an integer for the same reason. Therefore and by the definition of divides, $3 \mid p$ and it follows that in the case $r = 3$, p is not prime as it is divided by something other than 1 and itself.

If we take r to be 4, it follows that $p = 6q + 4$ by the division theorem. We also know $p, q \in \mathbb{Z}$ and therefore that $(6q + 4)$ is $\in \mathbb{Z}$ because integers are closed under addition and similarly that $2(3q + 2)$ is an integer. Therefore, by the definition of divides $2 \mid p$ and thus p is not prime in the case of $r = 4$ because it can be devided by a number other than 0 and itself by the divides theorem and definition of prime.

Because r cannot be 0, 2, 3, or 4 as proven above in $p = r \pmod 6$, it follows that r must be either 1 or 5 and thus proves the original claim that for any integer prime that is > 3, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.