Math 113 Group Problems for Wednesday, Week 11

PROBLEM 1. This problem will show there are infinitely many primes of the form $4n-1$.

(a) For $n = 1, 2, \dots, 13$, list the numbers $4n-1$, and underline those that are prime.

(b) Say $p_i = 4n_i - 1$ is prime for some integers n_i and $i = 1, \dots, k$. Define

$$N = 4p_1p_2 \cdots p_k - 1.$$

Our goal is to show N is divisible by some prime of the form $4n-1$ that is not among $p_1, \dots, p_k$. First prove that N is not divisible by any of $p_1, \dots, p_k$.

(c) Why is it the case that for every odd number k there exists a unique integer n such that either $4n-1$ or $4n+1$, but not both?

(d) We have just seen that every odd integer is either of the form $4n-1$ or $4n+1$. By the definition of N, we see N is of the former type. Since N is odd, every prime dividing N is odd, and thus has the form $4n-1$ or $4n+1$ for some n. By considering the prime factorization of N show that if every prime dividing N were of type $4n+1$, then N would be of type $4n+1$, too.

(e) How do the above results constitute a proof that there are infinitely many primes of the form $4k-1$?

(f) Let's put our proof method to work in order to generate primes of the form $4n-1$. The first two primes of the form $4n-1$ are $p_1 = 3 = 4 \cdot 1 - 1$ and $p_2 = 7 = 2 \cdot 4 - 1$. Find a prime factor p_3 of $N = 4p_1p_2 - 1$ of the form $4n-1$. Repeat, letting $N = p_1p_2p_3 - 1$ to find p_4 of the form $4n-1$ dividing this new N. Continue in this way finding primes $p_1, \dots, p_6$ of the form $4n-1$. You will want to use a computer. For example, at the website https://sagecell.sagemath.org/, if I type `factor(4*3*7-1)`, and hit the `Evaluate` button, I get 83, which indicates that $4 \cdot 3 \cdot 7 - 1$ is already prime. Then typing `83//4` and hitting `Evaluate`, I see that the quotient of 83 upon division by 4 is 20. Then typing `83 - 20*4`, I see the remainder is 3, and thus `83 - 21*4` is -1, i.e., $83 = 21 \cdot 4 - 1$.

In 1837 Dirichlet proved that if a and b are integers sharing no prime factors, then there are infinitely many primes of the form $an+b$. (We just proved the special case where $a = 4$ and $b = -1$.) The sequence $b, a+b, 2a+b, 3a+b, \dots$ is called an *arithmetic progression*. In 2004, Green and Tao proved that given any positive integer k, there exists a sequence of k prime numbers that are consecutive elements of an arithmetic progression. For instance, $3, 7$ and 11 are consecutive primes of the form $4n-1$.