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 $n = 1, 2, \ldots, 13$, list the numbers $4n-1$, and underline those that are prime.

SOLUTION:

$$\underline{3}, \underline{7}, \underline{11}, 15, \underline{19}, \underline{23}, 27, \underline{31}, 35, 39, \underline{43}, \underline{47}, 51.$$

(b) Say $p_i = 4n_i - 1$ is prime for some integers n_i and $i = 1, \ldots, k$. 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 $p_1, \ldots, p_k$. First prove that N is not divisible by any of $p_1, \ldots, p_k$.

SOLUTION: Let $M := 4p_1p_2\cdots p_k = N+1$. For each i, since p_i divides M, if it also divides N, then it divides $M - N = 1$, which is impossible.

(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?

SOLUTION: By the division algorithm, every integer k can be written as

$$k = 4q + r$$

for a unique integer q and unique $r \in \{0, 1, 2, 3\}$. Now, k can be written as $k = 4q+3$ if and only if it can be written as $4q'-1$ (letting $q' = q+1$). So every integer can be uniquely written in one of the forms

$$4n-1, \quad 4n, \quad 4n+1, \quad 4n+2.$$

Now note that $4n$ and $4n+2$ are even, and $4n-1$ and $4n+1$ are odd.

(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.

SOLUTION: Say $N = q_1^{e_1}\ldots q_\ell^{e_\ell}$ is the prime factorization of N and $q_i = 4m_i + 1$ for all i. Now completely expand

$$N = (4m_1+1)^{e_1}(4m_2+1)^{e_2}\cdots(4m_\ell+1)^{e_\ell}$$

as a polynomial in the m_i. Each term that involves any m_i is divisible by 4, and the only term not involving an m_i is 1.

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

SOLUTION: What we have shown is that given primes $p_1, \ldots, p_k$ of the form $4n-1$, we can find a prime p_{k+1} of the from $4n-1$, distinct from those already in the list. We can then apply our argument to the list $p_1, \ldots, p_{k+1}$, to find another prime p_{k+2} of the form $4n-1$. Etc.

(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 $p_1, \ldots, p_6$ 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., $83 = 21\cdot 4-1$.

SOLUTION: We have $p_1 = 3$, $p_2 = 7$, and we have seen that $4\cdot 3\cdot 7-1 = 83$ where $83 = 4\cdot 21-1$. So $p_3 = 83$. We then have the prime factorization

$$4\cdot 3\cdot 7\cdot 83-1 = 6971,$$

and $6971 = 1743-1$ is prime. So $p_4 = 6971$. The next prime factorization to consider is

$$4\cdot 3\cdot 7\cdot 83\cdot 6971-1 = 61\cdot 796751,$$

with $61 = 4\cdot 15+1$ and $796751 = 4 * 199188-1$. So $p_5 = 796751$. Next,

$$4\cdot 3\cdot 7\cdot 83\cdot 6971 * 796751-1 = 5591\cdot 6926049421,$$

with $5591 = 4\cdot 1398-1$ and $6926049421 = 4\cdot 1731512355+1$. So $p_6 = 5591$.

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 $b, a+b, 2a+b, 3a+b, \ldots$ 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 $4n-1$.