Number Theory
Fall 2023

Assignment 3.2
Due September 13

Exercise 1. Let $n \in \mathbb{N}$, $n \geq 2$. Suppose n has the property that whenever $n|ab$ for some $a, b \in \mathbb{N}$, then $n|a$ or $n|b$. Prove that n is prime. [*Suggestion.* If $n = ab$, then $n|ab$.]

Exercise 2. Use the Fundamental Theorem of Arithmetic to prove that if p is prime, then $\sqrt{p}$ is irrational.

Exercise 3. Show that every odd prime is of the form $4k \pm 1$.

Exercise 4. Prove that there are infinitely many primes of the form $4k - 1$ as follows.

a. Show that if $n_1, n_2, \ldots, n_r \in \mathbb{Z}$ all have the form $4k + 1$, then so does $n_1 n_2 \cdots n_r$. [*Suggestion.* Use induction.]

b. Suppose that $n \in \mathbb{N}$ has the form $4k - 1$. Prove that n must have a prime factor also of the form $4k - 1$.

c. Suppose $p_1, p_2, \ldots, p_r$ are primes of the form $4k - 1$ and let $N = 4p_1 p_2 \cdots p_r - 1$. Prove that N has a prime factor of the form $4k - 1$ that is different from $p_1, p_2, \ldots, p_r$.

d. Conclude that there are infinitely many primes of the form $4k - 1$.

Remarks.

1. The label "prime" for those $n \geq 2$ with the property that $n = ab$ implies $n = a$ or $n = b$ is entirely standard and completely mysterious to me. More meaningful terms might be "irreducible" or "atomic," since these more naturally suggest that the prime numbers cannot be factored nontrivially. Indeed, this is the terminology preferred in ring theory.
2. Exercise 1 shows that an integer n is prime *if and only if* n has the property that for any $a, b \in \mathbb{Z}$, $n|ab$ implies $n|a$ or $n|b$. In more general rings the latter property is what one calls "prime." While it is still true that every prime is irreducible in an arbitrary ring, the converse need not hold. The simplest example is the ring
$$\mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Z}\right\},$$
although the proof is nontrivial.
3. One can modify the argument in Exercise 4 to prove that there are also infinitely many primes of the form $4k + 1$, but this requires the theory of quadratic residues.