Math 465 - Spring 2021 April 22nd, 2021
Group Discussion 8

---

(1) Prove that there are infinitely many primes. One way to do this is by means of contradiction: assuming $p_1, p_2, \ldots, p_k$ are the only primes, consider the number $p_1 p_2 \cdots p_k + 1$.[1]

(2) Prove that there are infinitely primes $\equiv 3 \bmod 4$. (*Hint:* assuming $p_1, p_2, \ldots, p_k$ are the only primes $\equiv 3 \bmod 4$, consider the number $4p_1 p_2 \cdots p_k - 1$.) Explain why this is much easier than to prove that there are infinitely primes $\equiv 1 \bmod 4$.[2]

(3) Prove that $p \in \mathbb{Z}_{>1}$ is prime if and only if $a^{p-1} \equiv 1 \bmod p$ for all $a \not\equiv 0 \bmod p$.[3] Explain how this can be used for a test for *compositeness* of an integer without actually factoring it.

---

[1] Your proof probably uses two "obvious" but nontrivial facts, namely, (1) that every integer can be uniquely factored into primes, and (2) that two adjacent integers are relatively prime.

[2] There is a general result, known as *Dirichlet's Theorem*, which says that given $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, there are infinitely primes $\equiv a \bmod b$.

[3]