

Arithmetic progressions and introduction to Congruences

Learning Objectives. By the end of class, students will be able to:

- State and prove facts about prime factorizations using the Fundamental Theorem of Arithmetic
- Prove there are infinitely many primes of the form $4n + 3$.

Prime factorizations

Note on $m^4 - n^4 = (m^2 - n^2)(m^2 + n^2)$: In order to show this is not prime, must prove that the factors cannot be 1 and the number itself. Hint: show that if one of the factors is 1 the other is 1 or 0 (or -1).

Corollary (Corollary 1.20). *Let $a, b \in \mathbb{Z}$ with $a, b > 0$. Then $[a, b] = ab$ if and only if $(a, b) = 1$.*

A note on “if and only if” proofs:

- You can do two directions:
 - If $[a, b] = ab$, then $(a, b) = 1$.
 - If $(a, b) = 1$, then $[a, b] = ab$.
- Sometimes you can string together a series of “if and only if statements.” Definitions are always “if and only if,” even though rarely stated that way. For example, an integer n is even if and only if there exist an integer m such that $n = 2m$:
 - An integer n is even if and only if $2 \mid n$ (definition of even)
 - if and only if there exist an integer m such that $n = 2m$ (definition of $2 \mid n$).

Theorem (Dirichlet’s Theorem). *Let $a, b \in \mathbb{Z}$ with $a, b > 0$ and $(a, b) = 1$. Then the arithmetic progression*

$$a, a + b, a + 2b, \dots, a + nb, \dots$$

contains infinitely many primes.

Surprisingly, this proof involves complex analysis. The statement that there are infinitely many prime numbers is the case $a = b = 1$.

Warning 1. *You may not use this result to prove special cases, ie, specific values of a and b .*

Lemma (Lemma 1.23). *If $a, b \in \mathbb{Z}$ such that $a = 4m + 1$ and $b = 4n + 1$ for some integers m and n , then ab can also be written in that form.*

We will not go over the proof in class.

Proof Let $a = 4m + 1$ and $b = 4n + 1$ for some integers m and n . Then

$$\begin{aligned} ab &= (4m + 1)(4n + 1) \\ &= 16mn + 4m + 4n + 1 \\ &= 4(4mn + m + n) + 1. \end{aligned}$$

■

Proposition (Proposition 1.22). *There are infinitely many prime numbers expressible in the form $4n + 3$ where n is a nonnegative integer.*

Proof (Similar to the proof that there are infinitely many prime numbers). Assume, by way of contradiction, that there are only finitely many prime numbers of the form $4n + 3$, say $p_0 = 3, p_1, p_2, \dots, p_r$, where the p_i are distinct. Let $N = 4p_1p_2 \cdots p_r + 3$. If every prime factor of N has the form $4n + 1$, then so does N , by repeated applications of Lemma 1.23. Thus, one of the prime factors of N , say p , have the for $4n + 3$. We consider two cases:

Case 1, $p = 3$: If $p = 3$, then $p \mid N - 3$ by linear combinations. Then $p \mid 4p_1p_2 \cdots p_r$. Then by ??, either $3 \mid 4$ or $3 \mid p_1p_2 \cdots p_r$. This implies that $p \mid p_i$ for some $i = 1, 2, \dots, r$. However, p_1, p_2, \dots, p_r are distinct primes not equal to 3, so this is not possible. Therefore, $p \neq 3$.

Case 2, $p = p_i$ for some $i = 1, 2, \dots, r$: If $p = p_i$, then $p \mid N - 4p_1p_2 \cdots p_r$ by linear combinations. Then $p \mid 3$. However, p_1, p_2, \dots, p_r are distinct primes not equal to 3, so this is not possible. Therefore, $p \neq p_i$ for $i = 1, 2, \dots, r$.

Therefore, N has a prime divisor of the form $4n + 3$ which is not on the list p_0, p_1, \dots, p_r , which contradicts the assumption that p_0, p_1, \dots, p_r are all primes of this form. Thus, there are infinitely many primes of the form $4n + 3$. ■