Zsigmondy's Theorem

Alston Yam

1 Introduction

This should serve as a list of notes summarised from this handout.

Definition 1.1 – Zsigmondy's Theorem Let a, b be coprime positive integers such that $a \geq b$, and let n be some positive integer greater than 2. Then there exists a prime divisor of $a^n - b^n$ that does not divide $a^k - b^k$ for all $1 \leq k < n$, except the cases when:

- $n = 2$ and $a + b$ is a power of 2
- $(a, b, n) = (2, 1, 6)$