**Topic:** The Great Theorem, Euclid’s Infinitude of Primes

**Notes on Topic:**

If a whole number G divides evenly into both N and M, where N>M, then G divides evenly into their distance, G|N-M

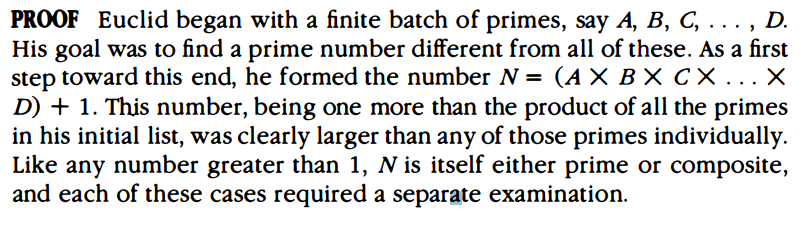
**Proof:** Since G|N and G|M, then there are integers A, B st GA=N, GB=M, then

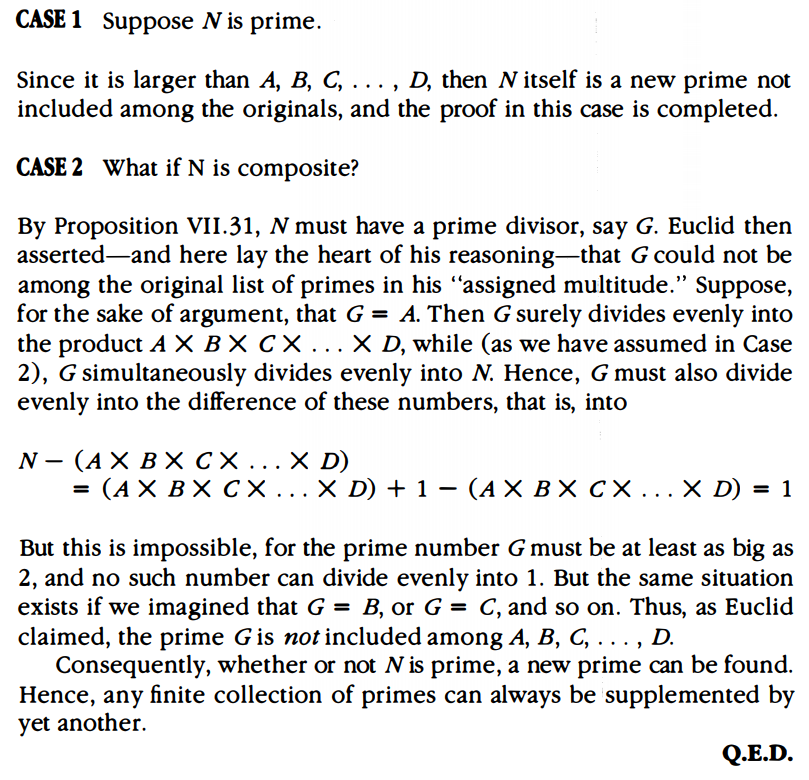
N-M= GA - GB = G (A-B)

Since A-B is an integer itself, G|N-M.

**Proposition IX.20:** Prime numbers are more than any assigned multitude of prime numbers.

Euclid means here, given any finite collection of primes numbers (any “assigned multitude”) it is possible to find a prime not in this collection. Meaning, no finite set of prime numbers could possibly exhaust all primes.



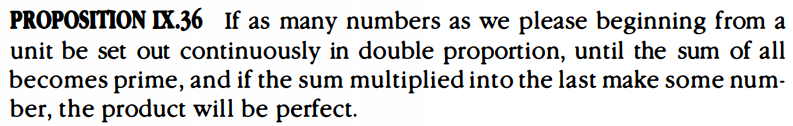


Numerical Example:

Say we are given a set of primes {2, 3, 5} if we let N = (2\*3\*5) + 1, N =31, which is prime and does not exist in the set above, thus the finite collection cannot exhaust all primes.

Say we are given {3, 5, 7} if we let N = (3\*5\*7) + 1 = 106, which is composite, but it must have a prime divisor, indeed 106 = 2 \* 53 , and both 2 and 53 are new primes not in the list.

Read proposition (to spark some interest) and suggest reading this portion of the book:



Euclid said: if where P is prime, then,

N =

N is perfect.

But this does not say that every perfect number is of this form.

Later Euler proved that any even perfect number is of this form. Where P is a Mersenne prime.

**Additional Suggested Reading**: JTG Pp. 75 on Prop IX.36

**Assignment:** Homework Problem 49, Prove Prop IX.36 (EC), 52