Unit 2: Prime Time

Paul Ycay
MATH 409- Athabasca University

December 13, 2019

The following theorems are ones to be marked. There is a seperate file of handwritten notes for the rest of the theorems in this chapter

Theorem 2.3. A natural number $n > 1$ is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divide n.

Proof. We want to prove two statements:
ⓐ n is prime if and only if $p \leq \sqrt{n}$, $p \nmid n$.
ⓑ $p \leq \sqrt{n}$ and $p \nmid n$ if and only if n is prime

Proof of ⓐ: Suppose n is not prime, i.e. $\exists x, y \in \mathbb{Z}$ such that $n = xy$, where $1 < x < n$ and $1 < y < n$. Now if n is not prime, then $x \leq y$, for example. Moreover, since $x \in \mathbb{Z}$, x has a prime divisor p such that $p \leq x \leq y$. Now, assume $p > \sqrt{n}$ $\implies p^2 > n \implies p^2 > xy$. This is a contradction since we assumed p is at least smaller than x, which is at least smaller than y. Then p cannot be a divisor of x or y. Thus, $p \nmid n$ and n is prime, based on these inequalities.

Proof of ⓑ: Suppose $p|n$ and $p > \sqrt{n}$. By the Fundamental Theorem of Arithmetic, $n = {p_1}^{r_1}{p_2}^{r_2} \cdots {p_k}^{r_k}$, for some $k \in \mathbb{N}$. Since $p > \sqrt{n}$, denote $p = p_1$. Then $p_1p_1 > n \implies p_1p_1 > {p_1}^{r_1}{p_2}^{r_2} \cdots {p_k}^{r_k}$, a contradiction. Thus, n is prime. $\square$

Theorem 2.20. There do not exist natural numbers m and n such that $7m^2 = n^2$

Proof. Assume $m = {p_1}^{a_1}{p_2}^{a_2} \cdots {p_k}^{a_k}$ and $n = {q_1}^{b_1}{q_2}^{b_2} \cdots {q_s}^{b_s}$.
Then $7m^2 = 7{p_1}^{2a_1}{p_2}^{2a_2} \cdots p_j^{2a_j} \cdots {p_k}^{2a_k}$, for some $1 \leq j \leq k$. Since 7 is prime, assume $p_j = 7$. Then $7p_j^{2a_j}{=}7 \cdot 7^{2a_j+1}$, where $2a_j + 1$ is even. However, $n^2 = {q_1}^{2b_1}{q_2}^{2b_2} \cdots {q_s}^{2b_s}$, and all of its factors are even, since $2b_i$ is even for some $1 \leq i \leq s$. Thus, there are no such factors in $7m^2$ that divides any factors in n^2, and vice versa. Therefore, $7m^2 \neq n^2$. $\square$

Theorem 2.23. Show that $7^{\frac{1}{3}}$ is irrational

Proof. Assume that $\sqrt[3]{7}$ is rational, i.e., $\exists x, y \in \mathbb{Z}$ such that

$$\begin{aligned}\sqrt[3]{7} &= \frac{x}{y}\\ 7 &= \frac{x^3}{y^3}\end{aligned}$$

Then $gcd(x^3, y^3) = 1$, since $\frac{x^3}{y^3}$ still has to be rational.
Then $7y^3 = x^3 \implies 7|x^3 \implies 7|x$. In other words, $\exists a \in \mathbb{Z}$ such that $x = 7a$

$$\begin{aligned}7y^3 &= (7a)^3\\ 7y^3 &= 7\cdot 7\cdot 7\cdot a^3\\ y^3 &= 7\cdot 7\cdot a^3 && \text{(by dividing both sides by 7)}\end{aligned}$$

Then $7|y^3 \implies 7|y$. Therefore $7|x$, $7|y$, $7|x^3$, & $7|y^3$. But we claimed that $gcd(x^3.y^3) = 1$, a contradiciton. Thus $\sqrt[3]{7}$ is irrational. □

Theorem 2.27. Let p be a prime and let $a, b \in \mathbb{Z}$. If $p|a$, then $p|a$ or $p|b$.

Proof. By contrapositition.
Sps $p \nmid a$ and $p \nmid b$. In other words, $gcd(p, a) = 1 = gcd(p, b)$ Then $\exists x, y, t, s \in \mathbb{Z}$ such that

$$\begin{aligned}① \; px + ay &= 1\\ ② \; pt + bs &= 1\\ \text{Multiply ① by ②} \implies (px + ay)(pt + bs) &= 1\\ p^2tx + pbsx + payt + aybs &= 1\\ p(ptx + bsx + ayt) + ab(ys) &= 1\\ pf + abg &= 1 \quad \because (f = ptx + bsx + ay) \in \mathbb{Z}\ , (g = ys) \in \mathbb{Z}\end{aligned}$$

Thus, $gcd(ab, p) = 1$. In other words, $p \nmid ab$, which is what we want satisfied for the contrapositive of this theorem. □

Theorem 2.37. If $r_1, r_2, \ldots, r_m$ are natural numbers and each one is congruent to 1 *modulo* 4, then the product $r_1 r_2 \cdots r_m$ is also congruent to 1 *modulo* 4.

Proof. Suppose for integers $a_1, a_2, a_3 \ldots, a_m$

$$\begin{aligned} r_1 &= 1 + 4a_1 \\ r_2 &= 1 + 4a_2 \\ &\vdots \\ r_m &= 1 + 4a_m \end{aligned}$$

Then

$$\begin{aligned} &r_1 r_2 \cdots r_m \\ &= \prod_{i=1}^{m} (1 + 4a_i) \\ &= (1 + 4a_1)(1 + 4a_2) \cdots (1 + 4a_m) \\ &= 1 + [4(a_1 + a_2 + \cdots + a_m) + 4^2(a_1 a_2 + a_2 a_3 + \cdots + a_{m-1} a_m) + \\ &\quad 4^3(a_1 a_2 a_3 + a_2 a_3 a_4 + \cdots + a_{m-2} a_{m-1} a_m) + \cdots + 4^m(a_1 a_2 \cdots a_m)] \\ &= 1 + 4t \quad \text{(The above in square brackets is a multiple of 4 and can be expressed as some integer } t\text{)} \end{aligned}$$

Thus, $r_1 r_2 \cdots r_m$ has a remainder 1 when divided by 4. $\square$

Theorem 2.38. There are infinitely many prime numbers that are congruent to 3 *modulo* 4.

Proof. By contrary, suppose that there are finitely many prime numbers that are congruent to 3 *modulo* 4. Moreover, consider the set of primes denoted by $A = \{p_1, p_2, \ldots, p_m\}$, $m < \infty$. Here, we fix p_1 to be 3, since 2 is never congruent to 3 *modulo* 4. Let $d := 4n + 3$ be some integer, $n \in \mathbb{Z}$. Since n is an integer, it can be expressed as a product of primes. More precisely, assume that n is a product of all primes in A, subtracted by 1, to maintain its prime property. Then $d = 4(p_1 p_2 \cdots p_m - 1) + 3$. Now arise two cases.
Suppose d is not prime. Then $\exists x \in \mathbb{Z}$ such that x is a divisor of $d \implies x = 4k + 3$, $k \in \mathbb{Z}$.
Suppose d is prime. Then d has to be some element in set A, which is impossible. Clearly, $4(p_1 p_2 \cdots p_m - 1) + 3$ is greater than p_i for any $p_1 = 3 \leq p_i \leq p_m$ contained in A.
A contradiction, and thus no p_i can divide d. Therefore, there are infinitely many primes congruent to 3 *modulo* 4. $\square$