Number Theory Section Summary: 3.1

The Fundamental Theorem of Arithmetic

1. Definitions

prime, composite: An integer $p > 1$ is called a **prime number**, or simply a **prime**, if its only positive divisors are 1 and p; otherwise it is called **composite**.

2. Theorems

Theorem 3.1: If p is prime and $p|ab$, then $p|a$ or $p|b$.

Proof: Given p prime and $p|ab$.

Assume $p \nmid a$. Therefore $\gcd(p,a)=1$, and $p|b$ by Euclid's lemma.

Symmetrically, if $p \nmid b$ then $p|a$. (Possibly p divides both!). But certainly $p|a$ or $p|b$.

Corollary 1: If p is prime and $p|a_1a_2\ldots a_n$, then $p|a_k$ for some k, $1 \le k \le n$.

Proof: Assume p prime, and $p \mid a_1 \cdots a_n$.

By induction:

Anchor: $p \mid a_1 a_2$, then $p \mid a_1$ or $p \mid a_2$ by the theorem.

$P(k) \Rightarrow P(k+1)$

$\Rightarrow$: Assume true for $n=k$; prove true for $n=k+1$.

Demonstrate $P(k+1)$: $p \mid a_1 \cdots a_{k+1} \Rightarrow p \mid a_j$ for some j, $1 \le j \le k+1$.

$a_1 \cdots a_{k+1} = (a_1 \cdots a_k)\, a_{k+1}$

$p \mid (a_1 \cdots a_k)\, a_{k+1}$, so by the theorem $p \mid a_1 \cdots a_k$ or $p \mid a_{k+1}$. So either $p \mid a_j$ for $1 \le j \le k$ (by assumption) or $p \mid a_{k+1}$

So $p \mid a_j$ for $1 \le j \le k+1$.

$\therefore P(k+1)$

QED.

Corollary 2: If $p, q_1, q_2, \ldots, q_n$ are all prime and $p|q_1q_2\ldots q_n$, then $p = q_k$ for some k, $1 \le k \le n$.

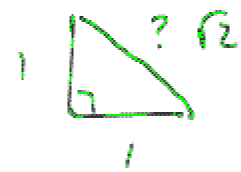
Theorem 3.2 (Fundamental Theorem of Arithmetic): Every positive integer $n > 1$ can be expressed as a product of primes uniquely (up to the order of the primes in the product).

Corollary: Any positive integer $n > 1$ can be written uniquely in a *canonical form*

$$\boxed{n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}$$

where, for $i = 1, 2, \ldots, r$ each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 \cdots < p_r$.

Theorem 3.3 (Pythagoras): $\sqrt{2}$ is irrational.



Let's look at the alternative proof that our author suggests:

Assume $\boxed{\sqrt{2} = \frac{a}{b}}$ $a, b \in \mathbb{Z}$ in reduced form: $\gcd(a,b) = 1$

Bad assumption!

$\exists\, x, y \in \mathbb{Z}$ / $\boxed{ax + by = 1}$

$\sqrt{2}(ax + by) = \sqrt{2}$ $a = \sqrt{2}\, b$

$\sqrt{2}ax + \sqrt{2}by = \sqrt{2}$ $\sqrt{2}a = 2b$

$\sqrt{2}\,a x + a y = \sqrt{2}$

$\underbrace{2b x + a y}_{\text{integer}} = \sqrt{2} \in \mathbb{Z}$! Contradiction!

3. Properties/Tricks/Hints/Etc.

Pythagoras's theorem above is the one that purportedly caused one of his disciples his life: the hapless fellow disclosed the fact that there were these irrational numbers that couldn't be written as the ratio of integers, and other members of the school sent him to swim with the fishes... at least that's the story!;)

4. Summary

Hopefully you're well aware of these results: it's just now that we're seeing how they're deduced from simple principles, such as the well-ordering principle (there it is again!).

#4 If $p \geq 5$ then $p^2 + 2$ is composite.

p 44

p takes form $6k+1$ or $6k+5$

Suppose $p = 6k+1$

$$(6k+1)^2 + 2 = \underbrace{36k^2 + 12k + 3}_{3 \mid \text{this} \Rightarrow \text{composite}}$$

Suppose $p = 6k+5$

$$(6k+5)^2 + 2 = 36k^2 + 60k + 25 + 2$$

$$= \underbrace{36k^2 + 60k + 27}_{3 \mid \text{this} \Rightarrow \text{composite}}$$

Q.E.D.

#6 a) $n^4 + 4$, $n > 1$, is composite.

$$(n^2 + an + 2)(n^2 - bn + 2)$$

$$= n^4 + [\, a - b \,] n^3 + [\, 4 - ab \,] n^2 + [\, 2a - 2b \,] n + 4$$

$\boxed{a = b = 2}$

$$n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$$

make sure neither factor is 1

$\Rightarrow$ $n^4 + 2$ is composite

---

c) $8^n + 1$, $n \geq 1$ is composite

$$2^n + 1 \mid 2^{3n} + 1$$

$$8^n + 1 = (2^3)^n + 1 = 2^{3n} + 1$$

$$2^n + 1 \mid 8^n + 1$$

So we've found a factor, $\neq 8^n + 1$, $+ \neq 1$. Hence $8^n + 1$ is composite.

d) $n > 11$ can be written as the sum of two composite numbers.

Suppose n even, $n = 2k$.

Consider

$$n - 6 = 2k - 6 = 2(k-3)$$

$$n = 6 + 2(k-3)$$

two composites

$n > 11$ & even $\Rightarrow$ $k \geq 5$

Suppose n odd, $n = 2k+1$.

Consider

$$n - 9 = (2k+1) - 9 = 2(k-4)$$

$$n = 9 + 2(k-4)$$

Two composite numbers, provided $k \geq 6$