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 $p \mid ab$, then $p|a$ or $p|b$.

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

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

   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*

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

   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.

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!).

Thu Jan 27 01:03:17 EST 2005

Theorem 3.1 : If prime p divides ab, then p divides a or p divides b.

Proof: By contradiction: assume p divides neither a nor b.

$p \nmid a$, so $\gcd(p, a) = 1$

$p \nmid b$, so $\gcd(p, b) = 1$

Then $\gcd(p, ab) = 1$ because of the one thing we already proved.

$\gcd(p,a) = 1 \Rightarrow \exists (x,y) \;/\; px + ay = 1$

$\gcd(p,b) = 1 \Rightarrow \exists (u,v) \;/\; pu + bv = 1$

$1 = (px+ay)(pu+bv) = pxpu + pbxv + puay + abyv$

$= p[\quad] + ab[\quad]$ $\therefore \gcd(p, ab) = 1$

But p (a prime > 1) divides ab!

Contradiction.

Pythagoras: $\sqrt{2}$ is irrational.

By contradiction: suppose not. Then

$\sqrt{2} = \frac{a}{b}$ $\quad \gcd(a, b) = 1$

Thus

$$2 = \frac{a^2}{b^2} \Rightarrow \quad 2b^2 = a^2 \quad \Rightarrow$$

$$2 \mid a^2$$

$\Rightarrow 2 \mid a$ by Thm 3.1

So $\exists\, d \in \mathbb{Z}$ / $2d = a$. Hence

$$2 = \frac{(2d)^2}{b^2} = \frac{4d^2}{b^2}, \text{ so}$$

$b^2 = 2d^2$. Hence $2 \mid b$.

This contradicts $\gcd(a, b) = 1$.

Q.E.D.

#3d, p 44

$$3p+1 = n^2 \Rightarrow \quad p = 5$$

$$3p = n^2 - 1$$

$$3p = (n-1)(n+1)$$

Two possible solns:

$n-1 = 3$ and $n+1 = p$

or

$n-1 = p$ and $n+1 = 3$

$n = 4$, $\Rightarrow$ $\boxed{p = 5}$

$n = 2 \Rightarrow p = 1$ (not prime!)

#13 If $n > 1$ and not of the form $6k+3$, then $n^2 + 2^n$ is composite.

Allowed forms: $6k$, $6k+2$, $6k+4$

$6k+1$ $\quad$ $6k+5$

evens,

so n^2+2^n is even & composite

Consider the other two forms:

$$(6k+1)^2 + 2^{6k+1} = \underbrace{36k^2 + 12k + 1}_{\text{divisible by 3}} + \underbrace{2^{6k+1}}$$

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

$$= 36k^2 + 60k + 25 + 16(2^{6k+1} + 1 - 1)$$

$$= \underbrace{36k^2 + 60k + 9}_{\text{divisible by 3}} + 16\underbrace{(2^{6k+1} + 1)}$$

Question is: does $3 \mid 2^{6k+1} + 1$

By induction

$$2^{6k+1} = 2 \cdot 2^{6k} \Rightarrow 2 \cdot (2^6)^k = 2 \cdot 64^k$$

For $k \geq 0$

$k = 0$:

$$2^{6 \cdot 0 + 1} + 1 = 3 \quad \checkmark$$

Inductive step:

Consider true for k; show for $k+1$. So assume $3 \mid 2^{6k+1} + 1$.

Consider $2^{6(k+1)+1} + 1 =$

$$2^6 \cdot 2^{6k+1} + 1 =$$

$$2^6\left(2^{6k+1} + 1 - 1\right) + 1 =$$

$$2^6\left(2^{6k+1} + 1\right) - 2^6 + 1 =$$

$$2^6\underbrace{\left(2^{6k+1} + 1\right)}_{\text{divisible by 3 by assumption}} - \underbrace{63}_{3 \cdot 21}$$

Therefore $2^{6(k+1)+1} + 1$ is divisible by 3.

So both forms $6k+1$ & $6k+5$ give values divisible by 3, and not equal to three; hence they're composite.