Number Theory Section Summary: 3.2

The Sieve of Eratosthenes

1. **Summary**

There are an infinite number of primes! You knew that, but now you should be able to prove it.

A composite number a can be written as bc, where, WLOG, $b \leq c$. If b is prime, then, since $b^2 \leq bc = a$, then a possesses a prime less than $\sqrt{a}$; if not, then b contains a prime factor p, which must be less than $\sqrt{a}$ - and this factor must also be a prime factor of a, since $p|b$, and $b|a$. It suffices then, to look for prime factors of a among the primes $\leq \sqrt{a}$.

Example: Determine whether 3731 is prime, or find its prime factorization.

The sieve of Eratosthenes is an interesting historical artifact: an early method for determining primes.

Example (homework): #2, p. 50.

2. **Theorems**

Theorem 3.4 (Euclid): The primes are infinite in number.

Theorem 3.5: If p_n is the n^{th} prime, then $p_n \leq 2^{2^{n-1}}$.

Corollary: For $n \geq 1$, there are at least $n+1$ primes less than 2^{2^n}.

3. **Properties/Tricks/Hints/Etc.**

Between $n \geq 2$ and $2n$ there is at least one prime, from which one can show that for $n \geq 2$,

$$p_n < 2^{2^n}$$

$\sqrt{3731} \approx 61+$

change

$3731 = 7 \cdot 533$

$\sqrt{533} = 23$

+

change

$3731 = 7 \cdot 13 \cdot 41$

Tue Feb 1 16:00:08 EST 2005

Theorem 3.4: The primes are infinite in number.

By contradiction: suppose not. Then there is a finite set of primes $\{p_1, \ldots, p_n\}$.

Consider

$$P = p_1 \cdots p_n + 1 > p_i \quad \forall i,\ i = 1, \ldots, n$$

(so P is not a prime).

But

$$P - p_1 \cdots p_n = 1,$$

so $\gcd(P, p_i) = 1 \quad \forall i \quad i = 1, \ldots, n.$

Hence P is prime (no prime factors!).

Contradiction.

#5 p 50

$n = \_\_\_$, composite

Show that it has a prime factor ≤ 31.

Largest: 999

$\sqrt{999} = 31 + \text{change}$