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.

$7 | 3731 : \quad 7 \cdot 533 = 7 \cdot 13 \cdot 41$

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 $\boxed{p_n \leq 2^{2^{n-1}}.}$

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 $n \geq 2$,

$$\boxed{p_n < 2^n.}$$

Thm 3.4: The primes are infinite.
By contradiction, suppose not: there are only n primes, $\{p_1, \ldots, p_n\} = S$.
Consider $\boxed{P = p_1 \cdots p_n + 1.}$ $P > p_i$ for all

$i = 1, \ldots, n$. If it's prime we're done (that's a contradiction) because $P \neq p_i$ for any i, so the set S didn't include all primes ($P \notin S$).

So assume P is composite - which means it has a prime factorization. In particular it has a prime factor q. But $q \notin S$ either, because if $q = p_i$ for some i, then $q \mid P$ and

$$q \mid p_1 \cdots p_n,$$

so

$$q \mid P - p_1 \cdots p_n = 1.$$

That can't be, so the prime of P, q, wasn't in S. But that's a contradiction! S was supposed to contain all the primes!

$\therefore$ The primes are infinite in number.

Alternate choice for P:

$$p_n! + 1, \quad \text{where } p_n \text{ is the "biggest" prime.}$$

Theorem 3.5: If p_n is the n^{th} prime, then

$$p_n \leq 2^{2^{n-1}}$$

By induction (2^{nd} principle):

Base case: $n=1 \Rightarrow \boxed{p_1 = 2}$
(first prime, $n=1$)

$$2 \leq 2^{2^0} = 2 \checkmark$$

$\Rightarrow$: Assume true through $n=k$, & consider

$$p_{k+1} \le \underline{p_1 \cdots p_k + 1}$$

$\leftarrow$ P from the previous proof — either prime itself or it has a factor q / $p_k < q < P$

$$\le 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{k-1}} + 1$$

$$= 2^{\underbrace{1+2+2^2+\cdots+2^{k-1}}} + 1$$

$\uparrow$ geometric series

$$1+2+\cdots+2^{k-1} = \frac{2^k - 1}{2-1}$$

$$= 2^{2^k - 1} + 1$$

$$\le 2^{2^k-1} + 2^{2^k-1}$$

$$= 2 \cdot 2^{2^k-1} = 2^{2^k}$$

$$= 2^{2^{(k+1)-1}}$$

$$p_{k+1} \le 2^{2^{(k+1)-1}}$$

$\therefore$ True by induction.

#3 Given that $p \nmid n$ for all primes $p \le \sqrt[3]{n}$, show that n is either a prime or the product of two primes.

By contradiction, assume 3 factors,

$\sqrt[3]{n} < p_1 \le p_2 \le p_3$.

$$n = p_1 p_2 p_3 \ge p_1^3 > (\sqrt[3]{n})^3 = n$$

Contradiction. Hence n can have at most 2 prime factors (either it's prime or has two prime factors). ✓

#5 Three digit composites must have a prime factor ≤ 31.

By contradiction; assume not. Then

$n = p \cdot q \cdot m \qquad p \leq q, \; m \geq 1$ composite.

$n = pqm \geq 37 \cdot 37 \cdot m \geq 37^2 > 1000$;

so n was not a 3-digit number. Contradiction.