Lecture: Wed 9/7/05

1. Fundamental Theorem of Arithmetic (Unique Factorization)

   - Any positive integer n can be expressed *in only one way* as:
     $$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$
     for some primes $p_1, \ldots, p_r$ and integers $k_1, \ldots, k_n \geq 0$. That is, n can be uniquely identified by how many powers of each prime divide it.
   - Proof: Division algorithm $\Longrightarrow$ Euclidean algorithm for gcd $\Longrightarrow$ Key property of primes (if $p|ab$ then $p|a$ or $p|b$) $\Longrightarrow$ Fundamental Theorem
   - Proposition: If $m/n \in \mathbb{Q}$ is in lowest terms, and $\sqrt{m/n} \in \mathbb{Q}$, then $\sqrt{m}, \sqrt{n} \in \mathbb{Z}$.
     Proof: Suppose a/b in lowest terms with $\sqrt{m/n} = a/b$. Let $p_1, \ldots, p_r$ be all the primes which divide any one of a, b, m, n, and write: $a = p_1^{a_1} \cdots p_r^{a_r}$, $b = p_1^{b_1} \cdots p_r^{b_r}$, etc. Now write out $a^2\, n = b^2\, m$ in terms of prime products, and show that $m = a^2$ and $n = b^2$.

2. Sieve of Eratosthenes to list primes

   - Make list of numbers 1,2, ... ,n. Cross out 1 (not a prime). Circle first uncrossed number 2, cross out all multiples of 2. Again circle first uncrossed number 3, cross out all multiples of 3. Repeat until all numbers are circled or crossed out: circled ones are the primes.
   - In fact, after you circle a given prime p, the first new number you cross out will be p^2. Thus, you can stop crossing out when $p^2 > n$, and just circle all remaining numbers. (Thanks to Benjamin Osborn & Alan Kish for the explanation.)

3. The sequence of primes

   - p = 2, 3, 5, 7,, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...
   - Theorem: There exist infinitely many primes.
     Proof (Euclid): Consider any list of primes: $p_1, p_2, \ldots, p_r$, and let $n := p_1 p_2 \cdots p_r + 1$. Now if $p_i | n$, then $p_i | (n - p_1 \cdots p_r) = 1$, but no prime divides 1, so this is impossible. Thus the prime factors of n are different from $p_1, \ldots, p_r$, and we can extend our list with new primes. Repeating, we can extend the list indefinitely.

- Example: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$, so the new primes are 59 and 509. We skip over many primes this way, but we do get an infinite list.
- Fermat's formula: $F(n) = 2^{2^n} + 1$ takes values: $F(0) = 3$, $F(1) = 5$, $F(2) = 17$, $F(3) = 257$, which are all prime. Fermat conjectured $F(n)$ is always prime, but this is false. Primes $p = F(n)$ are called Fermat primes, but only 5 such p are known! (What are they?)
- Is there any formula $f(n)$ giving only primes? None is known.

4. Prime Number Theorem

- Let p_n = the n^{th}-largest prime; and $\pi(n) :=$ the number of primes $\leq n$.
- For two sequences $f(n), g(n)$, we write $f(n) \approx g(n)$ to mean that the percentage difference between the two sides approaches zero for large n:
$$\lim_{n \to \infty} \frac{f(n)}{g(n)} = 1 \,.$$
- Theorem:
$$p_n \approx n \log(n) \qquad \text{and} \qquad \pi(n) \approx \frac{n}{\log(n)} \,,$$
where log means natural logarithm (base e).
- Proof uses sophisticated complex analysis, encoding the sequence of primes in terms of the Riemann zeta function
$$\zeta(s) := \prod_{p \text{ prime}} \frac{1}{1 - p^s} \,.$$

5. Twin Primes

- Pairs of primes (p, q) with $q = p + 2$. E.g. (11,13) and $(71, 73)$.
- Conjecture: There are infinitely many pairs of twin primes. If you prove it, you'll be famous!