Lecture: Mon 8/31/05

1. Pythagorean triples

   - Number theory: properties of integers $\mathbb{Z}$
     finding integer solutions to equations
   - Example: Pythagorean triples
     all 3 sides of a right triangle are whole numbers
     solve $a^2 + b^2 = c^2$ for integers $a, b, c > 0$.
   - Let $x = a/c\,,\ \ y = b/c\,$, then solve:
     $x^2 + y^2 = 1$ for rational numbers $x, y \in \mathbb{Q}$.
     find rational points (x, y) on unit circle
   - Projection of circle from $(-1, 0)$ to line $x = 1$:
     miraculously, rational points $(1, t)$ on line
     correspond one-to-one with rational points (x, y) on circle
   - E.g. $t = \frac{3}{2}$, line between $(1, t)$ and $(-1, 0)$ is $y = \frac{3}{4}(x{+}1)$
     intersect with $x^2 + y^2 = 1 \quad\Longrightarrow\quad 1 - x^2 = \frac{9}{16}(x + 1)^2$
     $\Longrightarrow \quad 1 - x = \frac{9}{16}(x + 1) \quad\Longrightarrow\quad (x, y) = (\,\frac{7}{25}\,,\ \frac{24}{25}\,)$
     $\Longrightarrow \quad (a, b, c) = (7, 24, 25)$.

2. Prime factorization of integers

   - divisibility: $a|b \quad\Longleftrightarrow\quad b = ac$ for some $c \in \mathbb{Z}$
     a is a factor of b , a divides b , b is divisible by a
   - prime p means only possible factors $d|p$ are $d = 1, p$
     convention: 1 is *not* a prime
   - Fundamental Theorem of Arithmetic (Unique Factorization):
     Any positive integer n can be factored into primes: $n = p_1 p_2 \cdots p_r$.
     This can be done in only one way (except for the order of the factors).

3. Greatest common divisor

   - $\gcd(a, b) = \max\{\, d$ such that $d|a$ and $d|b\,\}$
   - Euclidean algorithm to find $\gcd(a, b)$
     Example: $(a, b) = (36, 15)$
     repeat division with remainder until remainder is 0:

$$\begin{array}{ccc}
(36,15) & 36 = 2(15) + 6 & 3|36 \\
(15,6) & 15 = 2(6) + 3 & 3|15 \\
(6,3) & 6 = 2(3) + 0 & 3|6
\end{array}$$

- Claim: (i) $3|36$ and $3|15$ (ii) $d|36$ and $d|15 \implies d|3$
  Proof of (i): clear from above.
  Proof of (ii): $3 = 2(6) - 15$, $6 = 2(15) - 36$
  so back-substitute: $3 = 2(2(15) - 36) - 15 = -36 + 3(15)$
  Since $3 = \ell(36) + m(15)$, if $d|36$ and $d|15$, then $d|3$.

4. General Euclidean Algorithm to find $\gcd(a, b)$

   - $x_0 := a$, $x_1 = b$, repeat division with remainder:
     $x_0 = q_1x_1 + x_2$, $x_1 = q_2x_2 + x_3$, $\cdots$, $x_{n-1} = q_nx_n + 0$
   - Proposition: $x_n = \gcd(a, b)$.
   - Claim: (i) $x_n|a$ and $x_n|b$ (ii) $x_n = \ell a + mb$ for $\ell, m \in \mathbb{Z}$
   - Prove Claims just as in above example, and prove Proposition using Claims.

5. Lemma: For p a prime: $p|ab \implies p|a$ or $p|b$.

   - Proof: Let $d = \gcd(p, a)$. Since $d|p$, we have $d = p$ or $d = 1$. If $d = p$, then $p|a$, OK. If $d = 1$, then $1 = d = \ell p + ma$, so $b = \ell pa + mab$. Since $p|\ell pa$ and $p|abm$, we have $p|b$, OK.

6. Proof of Fundamental Theorem of Arithmetic

   - Obviously there is some factorization of n into primes: keep factoring until factors are prime. But why unique (except for rearrangement)?
   - Suppose $p_1 \cdots p_r = q_1 \cdots q_s$. Then $p_1|q_1(q_2 \cdots q_s)$. Use Lemma: if $p_1|q_1$, then $p_1 = q_1$. If $p_1|q_2 \cdots q_s$, repeat to get $p_1 = q_2$ or $p_1|q_3 \cdots q_s$. In the end, we find $p_1 = q_i$ for some i.
   - Removing $p_1 = q_i$ from both sides of the product, get: $p_2 \cdots p_r = q_1 \cdots q_{i-1}q_{i+1} \cdots q_s$.
     Now repeat to find $p_2 = q_j$, and remove this factor from both sides, etc.
   - This process ends when there are no more primes on right or left side, leaving 1. But this means the product of remaining primes on the other side is 1, so the other side must have no primes left either. Thus $r = s$.
   - In the end, we find the list $p_1, \ldots , p_r$ is a rearrangement of the list $q_1, \ldots , q_s$, so factorization is unique.