## Lecture: Fri 9/9/05

1. Prop: If $m/n \in \mathbb{Q}$ in lowest terms, and $\sqrt{m/n} \in \mathbb{Q}$, then $\sqrt{m}$, $\sqrt{n} \in \mathbb{Z}$.

   - First Proof (based on Fund Thm of Arithmetic). Assume $a/b$ in lowest terms with $(a/b)^2 = m/n$, so that $a^2 n = b^2 m$. Let $p_1, \ldots, p_r$ be all primes dividing $a, b, n, m$, and let $a = p_1^{a_1} \cdots p_r^{a_r}$, $b = p_1^{b_1} \cdots p_r^{b_r}$, etc., with integers $a_i, b_i, m_i, n_i \geq 0$. Then $a^2 = b^2 m$ is equivalent (by the Fund Thm) to $2a_i + n_i = 2b_i + m_i$.

     We have $\gcd(a,b) = \gcd(m,n) = 1$. We will show $2a_i = m_i$ and $2b_i = n_i$ for all $i$, so $a^2 = m$, $b^2 = n$.

     – Suppose $p_i | a$. We have: $p_i \not| b$. Also $p_i | a^2 n = b^2 m$, so $p_i | m$ and $p_i \not| n$. Thus: $a_i, m_i > 0$ and $b_i = n_i = 0$. Thus $2a_i + n_i = 2b_i + m_i$ means $2a_i = m_i$ and $2b_i = n_i = 0$.

     – Suppose $p_i | b$. Similarly we get $a_i = m_i = 0$ and $b_i, n_i > 0$ and $2a_i = m_i = 0$, $2b_i = n_i$.

     – Suppose $p_i \not| a, b$. If $p_i | m$ then $p_i | b^2 m$ and $p_i | b^2$ and $p_i | b$. But then $\gcd(a,b) > 1$, so this cannot happen. Similarly $p_i | n$ cannot happen. Thus $p_i \not| a, b, m, n$, so forget about $p_i$.

     First Proof is done.

   - Lemma on Uniqueness of Fractions. If $a/b = c/d$ are both positive fractions in lowest terms, then $a = c$ and $b = d$.

     Proof of Lemma: We have $\gcd(a,b) = 1$, so we can write $1 = ma + nb$, so $c = mac + nbc = mac + nad = a(mc + nd)$, so $a|c$. Also $d = mad + nbd = mbc + nbd = b(mc + nd)$ so $b|d$. Similarly use $1 = pc + qd$ to get $c|a$ and $d|b$. Conclude $a = c$ and $b = d$.

   - Second Proof of Prop (based on Uniqueness of Fractions). Suppose $a/b$ in lowest terms with $(a/b)^2 = m/n$. Then $a^2/b^2 = m/n$ with both sides in lowest terms (prove!), $a^2 = m$ and $b^2 = n$.

   - Both proofs ultitmately rest on the key lemma resulting from the Euclidean algortithm: we can always write $\gcd(a,b) = ma + nb$ for some $m, n \in \mathbb{Z}$.

2. Fermat's Little Theorem: If $p$ is prime, then $p \,|\, n^p - n$ for any $n \in \mathbb{Z}$.

   - Proof (David Krcatovic): Use induction on $n$. For $n = 1$, the statement is obvious. Now assume $p \,|\, n^p - n$. By the Binomial Theorem:

     $$\begin{aligned} (n{+}1)^p - (n{+}1) &= n^p + pn^{p-1} + \tfrac{1}{2}p(p{-}1)n^{p-2} + \cdots + pn + 1 - (n{+}1) \\ &= (n^p - n) + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!}\, n^{p-k}\,. \end{aligned}$$

     In the last expression, $p$ divides the first term by the inductive hypothesis, and $p$ divides each term in the summation because the numerator contains the prime $p$, and every term in the denominator is less than $p$. Conclusion: $p \,|\, (n{+}1)^p - (n{+}1)$, so the induction proceeds, and the Theorem is true for every positive integer $n$.