Math 126 Number Theory

Prof. D. Joyce, Clark University

3 Feb 2006

Due Monday. From page 32, exercises 5, 7, 12, 13, 15.

Due Wednesday. From page 35, exercises 1, 2.

For next time. Read through section 2.4.

Last meeting. The unique factorization theorem.

Today. Some applications of the unique factorization theorem including irrationality of surds. Some of these theorems are interesting, like the irrationality of surds, some are clarifying, like the next one, and some some might be called lemmas since their purpose won't be clear until we use them.

The first one just clarifies what the prime factorizations of powers look like.

Theorem. The exponents in the prime factorization of an n^{th} power c^n of a number c are all divisible by n. Thus, if a prime p divides c^n, then its n^{th} power also divides c^n, so p divides c.

Proof: Let the prime factorization of c be

$$c = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

Then a prime factorization of c^n is

$$c^n = p_1^{ne_1} p_2^{ne_2} \cdots p_r^{ne_r}.$$

The unique factorization theorem says that there is only one prime factorization, and in this prime factorization the exponents are all divisible by n, therefore the exponents in the prime factorization of c^n are all divisible by n. Q.E.D.

The next theorem is interesting. It's a general theorem that shows that surds like $\sqrt{2}$ are irrational numbers. A *surd* is the n^{th} root of a number that is not a perfect n^{th} power.

Theorem. Suppose that a is not a perfect n^{th} power, that is, that there is no b such that $b^n = a$. Then the n^{th} root of a is not a rational number.

Proof: We'll prove the contrapositive instead which says that if $\sqrt[n]{a}$ is a rational number, then a is a perfect n^{th} power.

Suppose that $\sqrt[n]{a}$ is a rational number, that is, $\sqrt[n]{a} = r/s$ where r and s are integers. We may assume that r and s are relatively prime since otherwise we could divide them both by their greatest common divisor (r, s). Then $a = r^n/s^n$, and so

$$as^n = r^n.$$

We'll show that $s = 1$.

Suppose that $s > 1$. Then some prime p divides s. Since $p|as^n$, therefore $p|r^n$. Therefore, by the previous theorem, $p|r$. But p can't divide both r and s since they're relatively prime, a contradiction. Therefore $s = 1$.

Since $s = 1$, therefore $a = r^n$. Q.E.D.

The following theorem isn't particularly interesting, but it will be useful later when we solve Diophantine equations.

Lemma. If an n^{th} power is the product of two relatively prime numbers, then each of those number are also n^{th} powers. That is, if $c^n = ab$ where $(a, b) = 1$, then there exist numbers d and e such that $d^n = a$, $e^n = b$, and $c = de$.

Proof: Since a and b are relatively prime, the primes that appear in their prime factorizations are distinct. So if

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \quad \text{and} \quad b = p_{r+1}^{e_{r+1}} \cdots p_{r+s}^{e_{r+s}}$$

are the prime factorizations of a and b where the p_i's are distinct. Then $c^n = ab$ has the prime factorization

$$c^n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}} \cdots p_{r+s}^{e_{r+s}}.$$

Now, since c^n is a perfect n^{th} power, all the exponents e_i in this prime factorization are divisible by n. That means all the exponents in the prime factorizations of a and b are divisible by n. Hence, a and b are n^{th} powers. Q.E.D.