18.781 Problem Set 2

Due Wednesday, September 21 in class.

1(a). Use the Euclidean algorithm to find $\gcd(9797, 1649)$.

1(b). Find integers m and n so that

$$\gcd(9797, 1649) = m \cdot 9797 + n \cdot 1649.$$

1(c). Write the continued fraction for $9797/1649$ (see page 26 of the text).

2. Let R be the collection of complex numbers $m+n\sqrt{-3}$, with m and n integers. I'll write assumptions like this as

$$R = \{m + n\sqrt{-3} \mid m, n \in \mathbb{Z}\}.$$

2(a). Explain why R is closed under addition and multiplication.

2(b). Define a "norm" on R by

$$\|m + m\sqrt{-3}\| = m^2 + 3n^2.$$

Prove that $\|r\|$ is a non-negative integer (for all $r \in R$), and that

$$\|r \cdot s\| = \|r\| \cdot \|s\| \qquad (r, s \in R).$$

2(c). Show that the only elements of R having a multiplicative inverse are ± 1.

2(d). Call an element r of R *prime* if it has exactly four divisors (namely ± 1 and $\pm r$). Prove that 2, $1 + \sqrt{-3}$, and $1 - \sqrt{-3}$ are all prime in R.

2(e). Prove that any element of R other than 0 and ± 1 is a product of primes in R: so prime factorization is possible in R.

2(f). What remark would you make about the equations

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})?$$

3. Suppose that $a > b > 1$ are relatively prime natural numbers. According to the Euclidean algorithm, it is possible to find integers x and y so that

$$ax + by = 1.$$

Prove that we can actually arrange

$$0 < x < b, \qquad -a < y < 0.$$

(Hint: page 34 of the text might help.)

4. Problems 2.5.6 and 2.5.7 on page 33 of the text.