18.781 Problem Set 2

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

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

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

$$\begin{aligned} 9769/1649 &= 5 \quad R\ 1552 \\ & 1552 = 9769 - 5 \cdot 1649 \\ 1649/1552 &= 1 \quad R\ 97 \\ & 97 = 1649 - 1552 = 1649 - (9769 - 5 \cdot 1649) = -9769 + 6 \cdot 1649 \\ 1552/97 &= 16 \quad R\ 0. \end{aligned}$$

So $\gcd(9769, 1649) = 97 = -9769 + 6 \cdot 1649$.

2. Suppose that a and b are integers, not both zero. Prove that a and b are relatively prime if and only if $\begin{pmatrix} a \\ b \end{pmatrix}$ is the first column of a 2×2 integer matrix having an integer inverse. (The same statement is true for n relatively prime integers and $n \times n$ matrices, but it isn't quite so easy to prove.)

Write

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}, \qquad X = \begin{pmatrix} x & y \\ u & v \end{pmatrix}.$$

Suppose a and b are relatively prime. Our job is to find integers c, d, x, y, u, v so that $XA = I$:

$$ax + by = 1, \quad au + bv = 0, \quad cx + dy = 0, \quad cu + dv = 1.$$

Number theory provides x and y making the first equation true. To get the second, you might (from 18.02 experience) guess the solution $u = -b,\ v = a$. That makes the fourth equation

$$-cb + da = 1,$$

for which you have at hand the solution $c = -y, d = x$. By magic, this solution makes the third equation true as well.

Summarizing, if x and y satisfy $ax + by = 1$, then

$$\begin{pmatrix} x & y \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a & -y \\ b & x \end{pmatrix} = I$$

Conversely, if the desired matrices A and X exist, then the first row of X provides the equation proving that a and b are relatively prime.

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

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

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

Addition happens "coordinate by coordinate," so closure is obvious. For multiplication,

$$(m + n\sqrt{-3})(m' + n'\sqrt{-3}) = (mm' - 3nn') + (mn' + nm')\sqrt{-3}.$$

Here $mm' - 3nn'$ and $mn' + nm'$ are both integers, so the product is in R.

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

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

(This is the square of the absolute value of the complex number.) Prove that $\|r\|$ is a non-negative integer (for all $r \in R$), and that

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

Easy proof is that norms of complex numbers multiply.

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

Because of (b), the norm of the multiplicative inverse must be the multiplicative inverse of the norm. Norms are nonnegative integers, and the only one of those with a multiplicative inverse is 1. So the elements having an inverse must have norm 1. The only integer solutions of $1 = m^2 + 3n^2$ are $(\pm 1, 0)$, so ± 1 are the only elements that *might* have multiplicative inverses. In fact each is its own inverse.

3(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.

The norms of the factors of an element must factor the norm; so (since these elements have norm 4) a factorization must be either (norm 1) times (norm 4), (which is $(\pm 1)(\mp r)$) or a product of two norm two elements. But the equation $m^2 + 3n^2 = 2$ has no integer solutions; so these elements can have no nontrivial factorization.

3(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.

A formal statement is that any element r of norm greater than 1 has a factorization

$$r = p_1 \cdot p_2 \cdots p_k, \qquad p_i \text{ prime}.$$

We'll prove this by induction on $\|r\|$. In case of norm two the statement is empty (there are no elements of R of norm two); so suppose $\|r\| \geq 3$ and the assertion is known for all elements of smaller norm. If r is prime, then the equation $r = r$ is a desired factorization. If r is not prime, then

$$r = r_1 r_2, \qquad \|r_i\| > 1.$$

By the multiplicativity of norm,

$$\|r_i\| = \|r\|/\|r_{2-i}\| < \|r\|,$$

so by inductive hypothesis each r_i has a prime factorization. Multiplying them together, we get a prime factorization of r.

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

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

These are two prime factorizations of 4, so there is no *uniqueness* theorem for the prime factorization in R. The point of this exercise is to point out that the Fundamental Theorem of Arithmetic is not just formal nonsense: it's proving something that can fail in a very similar setting.

4. 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

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

(You can use an idea from 18.03: if you have one solution (x, y) then you can add to it any solution of the "homogeneous equation" $ax' + by' = 0$.)

Start with *any* solution $ax' + by' = 1$. Applying division with remainder to x' and b, we find q and r so that

$$x' = bq + r, \qquad 0 \leq r < b.$$

Adding to our solution (x', y') the homogeneous solution $(-bq, aq)$, we get a solution

$$(x, y) = (x' - bq, y' + aq) = (r, y).$$

The condition $0 \leq x < b$ is immediate; since a and b are relatively prime, $x = 0$ is impossible. Once we know that $0 < x < b$, we get

$$by = 1 - ax, \qquad 1 > by > 1 - ab, \qquad 0 \geq by > -ab,$$

and therefore

$$-a < y \leq 0.$$

The possibility $y = 0$ is ruled out by a and b being relatively prime, so we get the desired bounds.

One point of *this* exercise is to make this condition for relatively prime *computable*. If you ask your computer, "are there integers x and y so that $ax + by = 1$?" it may look forever and you won't know whether an answer is just over the next hill. But if you ask your computer, "are there integers $0 < x < b$ and $-a < y < 0$ so that $ax + by = 1$?", you face a predictable wait until you have a definite answer.