Math 541
Problem Set 10

7.6.5. (a) Let $\varphi : \mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ be the natural map. Solving the simultaneous congruences $x \equiv a_i \mod n_i$ is the same as finding an $x \in \mathbb{Z}$ such that $\varphi(x) = (a_1, a_2, \ldots, a_n)$. Since the n_i are pairwise relatively prime, the ideals $n_i\mathbb{Z}$ are pairwise comaximal, so by the Chinese Remaidner Theorem, φ is surjective, so there is such an x. Suppose that y is another solution. Then $\varphi(y) = \varphi(x)$, so $\varphi(x-y) = 0$, so $x - y \in \ker\varphi$. But the Chinese Remainder Theorem tells us that $\ker\varphi = n_1 n_2 \cdots n_k\mathbb{Z}$, so $x \equiv y \mod n_1 n_2 \cdots n_k$.

(b) By construction, $t_i n_i' \equiv 1 \mod n_i$. If $j \neq i$ then n_i divides n_j', so $t_j n_j' \equiv 0 \mod n_i$. Thus

$$a_1 t_1 n_1' + \cdots + a_i t_i n_i' + \cdots + a_k t_k n_k' \equiv a_1 \cdot 0 + \cdots + a_i \cdot 1 + \cdots + a_k \cdot 0 \mod n_i$$

as required.

(c) Take $n_1 = 8$, $n_2 = 25$, and $n_3 = 81$. Then $n_1' = 25 \cdot 81 \equiv 1 \cdot 1 \mod 8$, $n_2' = 8 \cdot 81 \equiv 8 \cdot 6 = 48 \equiv -2 \mod 25$, and $n_3' = 8 \cdot 25 \equiv 38 \mod 81$. Thus $t_1 = 1$, $t_2 = -13$, and $t_3 = 32$, so

$$x \equiv 1 \cdot 1 \cdot 81 \cdot 25 - 2 \cdot 13 \cdot 81 \cdot 8 + 3 \cdot 32 \cdot 8 \cdot 25 = 4377 \mod 16200.$$

8.1.4. (a) Since $(a, b) = 1$, there are $x, y \in R$ such that $ax + by = 1$, so $acx + bcy = c$. Now a divides acx and bcy, so a divides c.

More generally, there are $x, y \in R$ such that $ax + by = (a, b)$, so $acx + bcy = (a, b)c$. Now a divides acx and bcy, so a divides $(a, b)c$, so $a/(a, b)$ divides c.

(b) We showed in Exercise 0.2.4 that these are solutions; now we show that these are the only solutions. If $ax + by = N$ then $ax + by = ax_0 + by_0$, so

$$a(x - x_0) = b(y_0 - y). \tag{1}$$

Thus a divides $b(y_0 - y)$, so $a/(a, b)$ divides $y_0 - y$, so there is an $m \in \mathbb{Z}$ such that

$$y_0 - y = m\frac{a}{(a, b)}, \tag{2}$$

so $y = y_0 - ma/(a, b)$. Substituting (2) into (1), we have

$$a(x - x_0) = bm\frac{a}{(a, b)}$$
$$x - x_0 = m\frac{b}{(a, b)}$$

so $x = x_0 + mb/(a, b)$.

8.2.5. (a) That I_3 is not principal is proved in example 2 on page 273. For I_3', the proof is almost identical. It remains to show that $I_2 = (2, 1+\sqrt{-5})$ is not principal. Let N be the field norm $N(a+b\sqrt{-5}) = a^2 + 5b^2$. Observe that for all $r \in R$, $N(r) \geq 0$, $N(r) = 1$ if and only if $r = \pm 1$, and $N(r) \neq 2$.

Suppose that I_2 is generated by one element $r \in R$. Then r divides 2 and $1 + \sqrt{-5}$, so $N(r)$ divides $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$, hence is either 1 or 2. $N(r) \neq 2$, so $N(r) = 1$, so $r = \pm 1$, so $I_2 = (1)$. Thus there are $x, y \in R$ such that $2x + (1 + \sqrt{-5})y = 1$. If we multiply through by $1 - \sqrt{-5}$ we get $2(1 - \sqrt{-5})x - 4y = 1 - \sqrt{-5}$, but this is impossible since $1 - \sqrt{-5}$ is not a multiple of 2.

8.3.5. Let N be the field norm $N(a+b\sqrt{-n}) = a^2+nb^2$. Again observe that for all $r \in R$, $N(r) \geq 0$, $N(r) = 1$ if and only if $r = \pm 1$, and $N(r) \neq 2$ since $n \geq 3$.

(a) First we show that 2 is irreducible. Suppose that $2 = rs$ with $r, s \in R$. Taking norms, we have $4 = N(r)N(s)$, so $N(r)$ is 1, 2, or 4. If $N(r) = 1$ then r is a unit. $N(r) = 2$ is impossible. If $N(r) = 4$ then $N(s) = 1$, so s is a unit.

Next we show that $\sqrt{-n}$ is irreducible. Suppose that $\sqrt{-n} = (a+b\sqrt{-n})(c+d\sqrt{-n})$. Taking norms,

$$n = (a^2+nb^2)(c^2+nd^2).$$

Thus $b = 0$ or $d = 0$, for otherwise $(a^2+nb^2)(c^2+nd^2) \geq n^2$. If $b = 0$ then $a^2 = 1$ since n is squarefree, so $a+b\sqrt{-n} = \pm 1$ is a unit. Similarly, if $d = 0$ then $c+d\sqrt{-n}$ is a unit.

Last we show that $1+\sqrt{-n}$ is irreducible. Suppose that $1+\sqrt{-n} = (a+b\sqrt{-n})(c+d\sqrt{-n})$. Since $N(1+\sqrt{-n}) = 1+n < n^2$, we have $b = 0$ or $d = 0$ as before. If $b = 0$ then $1+\sqrt{-n} = ac+ad\sqrt{-n}$, so $ad = 1$, so $a = \pm 1$, so $a+b\sqrt{-n}$ is a unit. Similarly, if $d = 0$ then $c+d\sqrt{-n}$ is a unit.

(b) If n is odd then $(1+\sqrt{-n})(1-\sqrt{-n}) = 1+n$ is a multiple of 2, but neither factor is a multiple of 2, so 2 is not prime.

If n even then there is an $m > 1$ with $n = 2m$ since $n \geq 3$. Then $(\sqrt{-n})^2 = -2m$, but $\sqrt{-n}$ does not divide either factor, as follows. If $\sqrt{-n}$ divides m then there are $a, b \in \mathbb{Z}$ with $m = (a+b\sqrt{-n})(\sqrt{-n}) = -bn + a\sqrt{-n}$, so $-bn = m$, but this is impossible since $m < n$. Similarly, $\sqrt{-n}$ does not divide 2. Thus $\sqrt{-n}$ is not prime.

In either case R contains an irreducible that is not prime, hence is not a U.F.D.

(c) If n is odd then $I = (2, 1+\sqrt{-n})$ is not principal, as follows. Suppose on the contrary that $I = (r)$. Then there is an $s \in R$ with $2 = rs$, so one of r and s is a unit as we saw above. If s is a unit then $r = 2s^{-1}$, but $1+\sqrt{-n}$ is a multiple of r and not of 2, so this is impossible. If r is a unit then $I = (1)$, so there are $x, y \in R$ such that $2x+(1+\sqrt{-n})y = 1$. If we multiplying through by $1-\sqrt{-n}$ we get $2(1-\sqrt{-n})x + (1+n)y = 1-\sqrt{-n}$, but this is impossible since $1-\sqrt{-n}$ is not a multiple of 2.

If n is even then $I = (2, \sqrt{-n})$ is not principal, as follows. Suppose on the contrary that $I = (r)$. Then $N(r)$ divides $N(2) = 4$ and $N(\sqrt{-n}) = n$, which is squarefree, so $N(r)$ is 1 or 2, so $r = \pm 1$. Thus $I = (1)$, so there are $x, y \in R$ such that $2x + \sqrt{-n}y = 1$. If we Multiply through by $\sqrt{-n}$ we get $2\sqrt{-n}x - ny = \sqrt{-n}$, but this is impossible since $\sqrt{-n}$ is not a multiple of 2.

9.1.4. Define a map $\mathbb{Q}[x,y] \to \mathbb{Q}[y]$ by $x \mapsto 0$ and $y \mapsto y$; that is,

$$\sum_{i,j} a_{ij}x^iy^j \mapsto \sum_j a_{0j}y^j.$$

This map is surjective onto the integral domain $\mathbb{Q}[y]$, so its kernel (x) is prime.

Define another map $\mathbb{Q}[x,y] \to \mathbb{Q}$ by $x \mapsto 0$ and $y \mapsto 0$; that is,

$$\sum_{i,j} a_{ij}x^iy^j \mapsto a_{00}.$$

This map is surjective onto the field $\mathbb{Q}$, so its kernel (x,y) is maximal (and hence prime).

Since $(x) \subseteq (x,y)$, (x) is not maximal.