Foundations of Higher Mathematics
Homework 6

Problem 84

a) a = 901, b = 952

$$952 = 901(1) + 51$$
$$901 = 51(17) + 35$$
$$51 = 34(1) + 17$$
$$34 = 17(2) + 0$$

So, $\gcd(901, 952) = 17$.

$$\begin{aligned} 17 &= 51 - 34 \\ &= 51 - [901 - 51(17)] \\ &= 51(18) - 901 \\ &= (952 - 901)(18) - 901 \\ &= 952(18) - 901(19) \end{aligned}$$

b) a = 4199, b = 1748

$$4199 = 1748(2) + 703$$
$$1748 = 703(2) + 342$$
$$703 = 342(2) + 19$$
$$342 = 19(18)$$

So, gcd(4199,1748) is 19.

$$\begin{aligned} 19 &= 703 - 342(2) \\ &= 703 - [1748 - 703(2)](2) \\ &= 703 - [2(1748) - 4(703)] \\ &= (-2)1748 + 5(703) \end{aligned}$$

c) a = 377, b = 233

$$377 = 233(1) + 144$$
$$233 = 144(1) + 89$$
$$144 = 89(1) + 55$$
$$89 = 55(1) + 34$$
$$55 = 34(1) + 21$$
$$34 = 21(1) + 13$$
$$21 = 13(1) + 8$$
$$13 = 8(1) + 5$$
$$8 = 5(1) + 3$$
$$5 = 3(1) + 2$$
$$3 = 2(1) + 1$$
$$2 = 1(1) + 1$$
$$1 = 1(1) + 0$$

So, gcd(377,233) = 1.

$$1 = 377(322) + 233(-521)$$

Problem 94

Suppose a and b are non-zero integers.

1. To show that there exists a number m such that $a|m$ and $b|m$, we can define a set $\{n \in \mathbb{N}|\ a|n \text{ and } b|n\}$. We can see that ab is in our set since $a|ab$ and $b|ab$. Since our set is non-empty it has a least element m, by the least natural number principle. Thus, $a|m$ and $b|m$.

2. It follows from part 1 that $ak_0 = m$ and $bj_0 = m$. Assume that $c \in \mathbb{Z}$, such that $a|c$ and $b|c$. Thus, $ak_1 = c$ and $bj_1 = c$. We want to show that m divides c. From the division algorithm we can see that $c = mq + r$, $0 \leq r < m$. It follows that:

$$\begin{aligned} c &= mq + r \\ r &= c - mq \\ &= ak_1 - (ak_0)q \\ &= bj_1 - (bj_0)q \end{aligned}$$

So, $a|r$ and $b|r$. Since $r < m$, r must be zero because m is the least element that both a and b divide. Therefore, $m|c$.

Problem 95

Let's assume that m and m' satisfy conditions 1 and 2. Then $a|m'$ and $b|m'$ and $a|m$ and $b|m$. By condition 2 we have that $m|m'$ by replacing c by m' since it is a divisor or a and b. Similarly, $m'|m$. Therefore, $m = m'$ proving that the least common divisor is unique.

Problem 101

Let $S = \{n \in \mathbb{N}|\ \exists p : p|a_i \text{ given that } p|a_1a_2 \ldots a_n\}$. If $n = 1$, we have $p|a_1$, so clearly $p|a_i$, where $i = 1$. Assume that $n \in S$. We want to show that $n + 1 \in S$. Thus, $p|a_1a_2 \ldots a_na_{n+1}$. From the induction hypothesis there exists i such that $p|a_i$. So given that $p|a_i$ and $p|a_1a_2 \ldots a_i \ldots a_{n+1}$ we see that a_i from the induction hypothesis is still there so we are done. There is a_i such that $p|a_i$.

Problem 103

Assume $a \neq 0$, $b \neq 0$ and $d \in \mathbb{N}$ such that, $d|a$ and $d|b$.

($\Rightarrow$) Suppose that $\gcd(a, b) = d$. It follows that there exist m, n such that $ma + nb = d$. Since $d|a$ and $d|b$, we can see that $dk = a$ and $dj = b$. Thus,

$$\begin{aligned} m(dk) + n(dj) &= d \\ d(mk + nj) &= d \\ mk + nj &= 1 \end{aligned}$$

Since $k = \frac{a}{d}$ and $j = \frac{b}{d}$ (Since $d|a$ and $d|b$ it is fine to have a fraction, it will be in $\mathbb{Z}$), $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

($\Leftarrow$) Suppose $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. Then there exist m, n such that $m(\frac{a}{d}) + n(\frac{b}{d}) = 1$. It follows that

$$\begin{aligned} d[m(\frac{a}{d}) + n(\frac{b}{d}) &= 1] \\ ma + nb &= d \end{aligned}$$

Therefore, $gcd(a, b) = d$.

Problem 111

Let $p, q, r \in \mathbb{Z}$ such that 5 divides $p^2 + q^2 + r^2$. Assume not. Suppose p, q, and r do not divide 5. We can express this as $p = 5k_0 + x_0$, $q = 5k_1 + x_1$, $r = 5k_2 + x_2$ where $1 \leq x < 5$. It follows that:

$$\begin{aligned}(5k_0 + x_0)^2 + (5k_1 + x_1)^2 + (5k_2 + x_2)^2 &= \\ (25k_0^2 + 10k_0x_0 + x_0^2) + (25k_1^2 + 10k_1x_1 + x_1^2) + (25k_2^2 + 10k_2x_2 + x_2^2) &= \\ 25(k_0^2 + k_1^2 + k_2^2) + 10(k_0x_0 + k_1x_1 + k_2x_2) + (x_0^2 + x_1^2 + x_2^2)\end{aligned}$$

Since $1 \leq x_0, x_1, x_2 < 5$, we can see that 5 does not divide $p^2 + q^2 + r^2$. This is a contradiction so 5 must divide at least one of p, q, r.

Problem 112

Assume not. Suppose that $p_1, p_2, \ldots, p_i$ are the only primes of the form, $4n+3$. Let $N = p_1p_2 \ldots p_i - 1$. We can see that $4N+3$ is $4(p_1p_2 \ldots p_i - 1) + 3 = 4p_1p_2 \ldots p_i - 1$. We can see that every prime in our list of primes in the form $4n+3$ leaves a remainder of 4. Thus, $4N+3$ is prime which contradicts our statement that $p_1, p_2, \ldots, p_i$ are the only primes of the form $4n+3$. Therefore, there are infinitely many primes of the form $4n+3$.

Problem 118a) Since the gcd(17,13) = 1, there are no solutions, by theorem 3.16.

b) The gcd(21,14) = 7 and $7|147$ so there are infinitely many solutions. One solutions is: $21(11)+14(-6) = 147$. It follows that all the solutions are in the form:

$$x = 11 + \frac{14}{7}k$$
$$y = -6 - \frac{21}{7}k$$

c) The gcd(60,18) = 6 which does not divide 97 so there are no integral solutions.

d) The gcd(738,621) = 9. Since $9|45$, there are infinitely many solutions. One of these solutions is $738(11) + 621(-12) = 45$ So from theorem 3.16 the solution sets are:

$$x = 11 + \frac{621}{9}$$
$$y = -12 + \frac{638}{9}$$