CISC-102 WINTER 2016

HOMEWORK 6 SOLUTIONS

(1) Prove, using the second (strong) form of mathematical induction that any integer value greater than 2 can be written as $3a + 4b + 5c$, where a, b, c are non-negative integers, that is $a, b, c \in \mathbb{Z}, a, b, c \geq 0$. (HINT: You need to use 3 base cases, that is, verify that 3,4 and 5 can be written as $3a + 4b + 5c$, where a, b, c are non-negative integers.)

We use the second form of mathematical induction.

Base: $3 = 3\times1+4\times0+5\times0$, and $4 = 3\times0+4\times1+5\times0$, and $5 = 3\times0+4\times0+5\times1$.

Induction Hypothesis: All values i such that, $2 < i \leq k$ can be written as $3a+4b+5c$, where a, b, c are non-negative integers.

Induction Step: Consider the value $k + 1$, and the value k. By the induction hypothesis $k = 3a + 4b + 5c$ for non-zero integers a, b, c. There are 3 cases to consider.

Case 1: $a > 0$ in the expression $k = 3a + 4b + 5c$,
therefore $k + 1 = 3(a - 1) + 4(b + 1) + 5c$.

Case 2: $a = 0$, $b > 0$ in the expression $k = 3a + 4b + 5c$,
therefore $k + 1 = 4(b - 1) + 5(c + 1)$.

Case 3: $a = 0$, $b = 0$, and $c > 0$ in the expression $k = 3a + 4b + 5c$,
therefore $k + 1 = 3(a + 2) + 5(c - 1)$.

(2) Let a, b, c be Integers.

(a) Prove that if $a|b$ and $b|c$ then $a|c$.
$a|b$ implies that there exists an integer p such that $b = pa$.
$b|c$ implies that there exists an integer q such that $c = qb$.
Putting the two equations above together we have $c = qpa$, and can conclude that $a|c$.

(b) Prove that if $a|b$ and $a|c$, then $a|(b + c)$.
$a|b$ implies that there exists an integer p such that $b = pa$.
$a|c$ implies that there exists an integer q such that $c = qa$.
Putting the two equations above together we have $b + c = pa + qa = a(p + q)$, and can conclude that $a|(b + c)$.

(c) Prove that if $a|b$ and $b|a$, then $|a| = |b|$, that is $a = \pm b$.

$a|b$ implies that there exists an integer p such that $b = pa$.

$b|a$ implies that there exists an integer q such that $a = qb$.

Putting the two equations above together we have $b = pqb$. Therefore the product $pq = 1$. Since both p and q are integers we conclude that $p = q = 1$, or $p = q = -1$. This in turn implies that $|a| = |b|$.

(3) Let a = 1763, and b = 42

(a) Find $\gcd(a, b)$. Show the steps used by Euclid's algorithm to find $\gcd(a, b)$.

(1763) = 41(42) + 41

(42) = 1(41) + 1

(41) = 41(1) + 0

gcd(1763,42) = gcd(42,41) = gcd(41,1)= gcd(1,0) = 1

(b) Find integers x, y such that $\gcd(a, b) = ax + by$

$$\begin{aligned} 1 &= 42 - 1(41) \\ &= 42 - 1[1763 - 41(42)] \\ &= 42(42) + (-1)1763 \end{aligned}$$

(c) Find lcm(a,b)

lcm(a,b) = $\frac{ab}{gcd(a,b)}$ = 74046

(4) Prove $\gcd(a, a + k)$ divides k.

Let $g = \gcd(a, a + k)$. Therefore $g|a$ and $g|a + k$, and this implies that $g|a + k - a$, or $g|k$.

(5) If a and b are relatively prime, that is $\gcd(a, b) = 1$ then we can always find integers x, y such that $1 = ax+by$. This fact will be useful to prove the following proposition.

Suppose p is a prime such that $p|ab$, that is p divides the product ab, then $p|a$ or $p|b$.

We can look at two possible cases.

Case 1: $p|a$ and then we are done.

Case 2: $p \nmid a$, and since p is prime we can deduce that p and a are relatively prime. Therefore, there exist integers x, y such that

$$1 = ax + py. \tag{1}$$

Now multiply the left and right hand side of equation (1), by b to get:

$$b = bax + bpy. \tag{2}$$

We know that $p|ba$ so $p|bax$, and we can also see that $p|bpy$. Therefore, $p|(bax+bpy)$, and by equation (2) we can conclude that $p|b$.