Assignment 2

Pages 15-17: 18 a, 19 a,b, 27, 35, 41 i, ii; pages 32-33: 2,7,8; and **X**: if a, b, c are natural numbers, then (1) $(ac, bc) = (a, b)c$, (2) $[ac, bc] = [a, b]c$, (3) If $g = (a, b)$ then $(a/g, b/g) = 1$.

18.(a) If $(a, b) = (a, c) = 1$ then $[a, b] = ab$ and $[a, c] = ac$, so if $a \neq 0, b \neq c$ then $[a, b] \neq [a, c]$. For example any three distinct primes p, q, r are pairwise coprime and $[p, q] = pq, [p, r] = pr, [q, r] = qr$ are all different.

(1 point)

19.(a) If $(a, b) = 1$ and $c \mid a$ then there are integers x, y, a' such that $1 = ax + by = c(a'x) + by$, hence $(b, c) = 1$.

(b) If $(a, bc) = 1$ then there are integers x, y such that $1 = ax + bcy = ax + b(cy) = ax + c(by)$, hence $(a, b) = (a, c) = 1$.

(2 points)

27. If $n + 1$ divides $n^2 + 1$ then it divides $n^2 + 1 - (n + 1)(n - 1) = 2$, so $n = 1$ if it is a positive integer.

(2 points)

35. If $(m, n) = 3$ then $\{3u : u \in \mathbb{Z}\} = \{mx + ny : x, y \in \mathbb{Z}\}$ contains $m + n$ but not 101. That is $3 \mid m + n$ but $3 \nmid 101$.

(2 points)

41. (i) Writing $a = (a, b)a', b = (a, b)b'$, we have $(a, b)^2 a'b' = ab = (a, b)[a, b]$, so $a'b' = [a, b]/(a, b) = 90/15 = 2 \cdot 3$. Then $\{a', b'\} = \{1, 6\}$ or $\{2, 3\}$, hence $\{a, b\} = \{15, 90\}$ or $\{30, 45\}$.

(ii) If $[a, b] = m$ and $(a, b) = d$, say $a = da', b = db'$, then $m = [a, b] = ab/(a, b) = da'db'/d = da'b'$, hence $d \mid m$. If $d \mid m$ then $(d, m) = d$ and $[d, m] = dm/(d, m) = dm/d = m$ (so let $a = d, b = m$).

(2 points)

2. Let r be the largest integer such that $2^r \mid n$. Then $r \geq 0$ and $n = 2^r m$ where $2 \nmid m$, that is m is odd.

(1 point)

7. We have $ab = \prod_p p^{2\nu_p}$, and since $(a, b) = 1$, $p \mid a$ implies $p \nmid b$ and vice-versa. By uniqueness of factorization, we must have that $a = \prod_{p|a} p^{2\nu_p}$ and $b = \prod_{p|b} p^{2\nu_p}$ are squares.

(2 points)

8. The hard way: $(n, n + 1) = 1$ (for $(n + 1) \cdot 1 - n \cdot 1 = 1$), so if $n(n + 1)$ is a square then n and $n + 1$ are squares by 7. But this is impossible for no two squares differ by 1, except for $(\pm 1)^2$ and 0^2. To see this, note that if $a^2 - b^2 = (a + b)(a - b) = 1$, then $a + b = a - b = \pm 1$.

The easy way: if n is positive then $n^2 < n(n + 1) < (n + 1)^2$.

(2 points)

X. (1) If $G = \{ax + by : x, y \in \mathbb{Z}\}$ then clearly $\{acx + bcy : x, y \in \mathbb{Z}\} = \{cg : g \in G\} =: cG$. If c is positive then clearly the smallest positive integer in cG is cg, where g is the smallest positive integer in G, that is $(ac, bc) = c(a, b)$. (2) $[ac, bc] = acbc/(ac, bc) = acbc/c(a, b) = cab/(a, b) = c[a, b]$. (3) By (1), $g(a/g, b/g) = (a, b) = g$, hence $(a/g, b/g) = 1$.

(3 points)

17 points, plus 3 points for a reasonable attempt at all questions = 20 points.