MATHEMATICS 271 L01 FALL 2003
ASSIGNMENT 5 SOLUTION

1. In this question, a, b, d are positive integers. Prove or disprove each of the following statements.

(a) $d \mid a$ and $d \mid b$ if and only if $d \mid (xa + yb)$ for all integers x and y.

(b) $\gcd(a, b) \leq \gcd(xa + yb, ma + nb)$ for all integers x, y, m and n.

(c) For all positive integers a and b, $\gcd(a, b) = \gcd(2a + 3b, 2a + b)$.

(d) For all positive integers a and b, $\gcd(a, b) = \gcd(2a + 3b, a + 2b)$.

Solution:

(a) This statement is true and here is a proof.

($\Longrightarrow$) Suppose that $d \mid a$ and $d \mid b$. We show that $d \mid (xa + yb)$ for all integers x and y. Let $x, y \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$, there are $m, n \in \mathbb{Z}$ so that $a = dm$ and $b = dn$, and so $xa + yb = xdm + ydn = d(xm + yn)$, which implies that $d \mid (xa + yb)$ (note that $xm + yn \in \mathbb{Z}$ because $x, y, m, n \in \mathbb{Z}$).

($\Longleftarrow$) Suppose that $d \mid (xa + yb)$ for all integers x and y. It follows that $d \mid (1a + 0b)$ and $d \mid (0a + 1b)$, that is , $d \mid a$ and $d \mid b$.

(b) This statement is true and here is a proof.

Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$, and so by (a) we have for any inetegers x, y, m and n, $d \mid xa + yb$ and $d \mid ma + nb$. Thus, d is a common divisor of $xa + yb$ and $ma + nb$, and so $d \leq \gcd(xa + yb, ma + nb)$, that is, $\gcd(a, b) \leq \gcd(xa + yb, ma + nb)$.

(c) This statement is false. For example, when $a = 1$ and $b = 2$, we have $\gcd(a, b) = \gcd(1, 2) = 1 \neq 4 = \gcd(8, 4) = \gcd(2a + 3b, 2a + b)$.

(d) This statement is true and here is a proof. Let a and b be positive integers. Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(2a + 3b, a + 2b)$.

From part (b), we have $d_1 = \gcd(a, b) \leq \gcd(2a + 3b, a + 2b) = d_2$.

On the other hand, also from part (b), we have
$d_2 = \gcd(2a + 3b, a + 2b) \leq \gcd(2[2a + 3b] - 3[a + 2b], 2[a + 2b] - [2a + 3b]) = \gcd(a, b) = d_1$.

Since $d_1 \leq d_2$ and $d_2 \leq d_1$, we have that $d_1 = d_2$, that is, $\gcd(a, b) = \gcd(2a + 3b, a + 2b)$.

2. Let $n \geq 2$ be an integer. Let G_n be the graph where $V(G_n) = \{2, 3, 4, ..., n\}$ and a vertex a is connected to vertex b by an edge if and only if a and b are relatively prime. For each of the following questions from part (b) to part (e), an explanation is required to support your answer.

(a) Draw the graphs G_5 and G_6.

(b) Find the degree of the vertex 2 in G_n.

(c) Find the degree of the vertex 3 in G_n for $n \geq 3$.

(d) Is it true that G_n has a Hamiltonian path for all integers $n \geq 2$? (A Hamiltonian path of a graph G is a path that contains all the vertices of G.)

(e) Find all values of n so that G_n has a Hamiltonian cycle? (A Hamiltonian cycle of a graph G is a cycle that contains all the vertices of G.)

Solution:

(b) It is clear that $\{2, a\}$ is not an edge if and only if a is not a multiple of 2. Thus, the vertices which are not neighbours of 2 are $2, 4, 6, ..., 2\left\lfloor \frac{n}{2} \right\rfloor$, and so $d(2) = |V(G_n)| - \left\lfloor \frac{n}{2} \right\rfloor = n - 1 - \left\lfloor \frac{n}{2} \right\rfloor$

(c) Similarly, it is clear that $\{3, a\}$ is not an edge if and only if a is not a multiple of 3. Thus, the vertices which are not neighbours of 2 are $3, 6, ..., 3\left\lfloor \frac{n}{3} \right\rfloor$, and so $d(2) = |V(G_n)| - \left\lfloor \frac{n}{3} \right\rfloor = n - 1 - \left\lfloor \frac{n}{3} \right\rfloor$

(d) Yes, G_n has a Hamiltonian path for all integers $n \geq 2$. In fact, a Hamiltonian path of G_n is $2 \sim 3 \sim 4 \sim 5 \sim ... \sim n$. This is from the fact that two consecutive integers k and $k+1$ are relative prime (because $1 = (k+1) + (-1)k$) and so they are adjacent.

(e) We prove that G_n has a Hamiltonian cycle if and only if n is odd.

($\Longrightarrow$) We show that if n is even then G_n does not have a Hamiltonian cycle. Suppose that n is even. We note that two even integers are not relative prime and so they are not adjacent. Thus, in a cycle, the even integers must be separated by the odd integers. However, since n is even, the number of even integers in $V(G_n)$ is one more than the number of even integers in $V(G_n)$, so G_n can not have a Hamiltonian cycle.

($\Longleftarrow$) We show that if n is odd then G_n has a Hamiltonian cycle. Suppose that n is odd. Then a Hamiltonian cycle of G_n is $2 \sim 3 \sim 4 \sim 5 \sim ... \sim n \sim 2$.

3. (This is exercise #13 on page 376 of the text book) Let n and k be integers with $1 \leq k < n$. Let $G_{n,k}$ be the graph with $V(G_{n,k}) = \{0, 1, 2, 3, ..., n-1\}$ and $E(G_{n,k}) = \{ab : a - b \equiv \pm k \pmod{n}\}$.

(a) Draw the graphs $G_{6,1}$, $G_{6,2}$ and $G_{6,3}$.

(b) Find necessary and sufficient conditions on n and k so that G is connected. Prove your answer.

(c) Find a formula involving n and k for the number of connected components of G. Explain how you get the formula.

Solution:

(b) We prove that $G_{n,k}$ is connected if and only if n and k are relatively prime.

We note that ab is an edge of $G_{n,k}$ if and only if $a - b \equiv \pm k \pmod{n}$, if and only if $b = (a \pm k) \bmod n$, and therefore

if there is an (a, b)-walk, then $b = (a + ik) \bmod n$ for some $i \in \mathbb{Z}$. $\qquad (\star)$

($\Longrightarrow$) Suppose that $G_{n,k}$ is connected. Then there is a $(0, 1)$-path, and so by $(\star)$, we have $1 = (ik) \bmod n$ for some $i \in \mathbb{Z}$. This, means $k \otimes (i \bmod n) = 1$ in $\mathbb{Z}_n$, so k is invertible in $\mathbb{Z}_n$, and so n and k are relatively prime.

($\Longleftarrow$) Suppose that n and k are relatively prime. First, we note that

$$\begin{aligned} ab \text{ is an edge of } G_{n,k} &\iff a - b \equiv \pm k \pmod{n} \\ &\iff b = (a + k) \bmod n \text{ or } b = (a - k) \bmod n \end{aligned}$$

and so, we see that $0 \sim k \bmod n \sim (2k) \bmod n \sim (3k) \bmod n \sim ... \sim ((n-1)k) \bmod n = 0$ is a walk in $G_{n,k}$. We show that $G_{n,k}$ this walk contains all the vertices of $G_{n,k}$ by showing that 0, $k \bmod n$, $(2k) \bmod n$, $(3k) \bmod n$, ..., $((n-1)k) \bmod n$ are distinct. Suppose

that $(ik) \bmod n = (jk) \bmod n$ for some integers $0 \leq i, j < n$. Since $i, j, k \in \mathbb{Z}_n$, from $(ik) \bmod n = (jk) \bmod n$, we have $i \otimes k = j \otimes k$. However, since n and k are relatively prime, k is invetible in $\mathbb{Z}_n$, k^{-1} exists, and so $i = i \otimes k \otimes k^{-1} = j \otimes k \otimes k^{-1} = j$. Thus, the above walk contains all the vertices of $G_{n,k}$ and hence, $G_{n,k}$ is connected.

(c) We show that $G_{n,k}$ has $\gcd(n.k)$ components. In (b), we have shown that if $\gcd(n.k) = 1$ (n and $k$are relatively prime) then $G_{n,k}$ is connected and so it has 1 component. Suppose that $g = \gcd(n, k) > 1$. Since $g \mid n$, there is an integer $m > 0$ so that $n = mg$. We show that the components of $G_{n,k}$ are the induced subgraphs $G_{n,k}[A_j]$ where for $j = 0, 1, 2, .., g-1$,

$A_j = \{j, (j+k) \bmod n, (j+2k) \bmod n, (j+3k) \bmod n, ... (j+(m-1)k) \bmod n\}$

We note that $j \sim (j+k) \bmod n \sim (j+2k) \bmod n \sim (j+3k) \bmod n \sim ... \sim (j+(m-1)k) \bmod n$ are walks in $G_{n,k}$ for all $j = 0, 1, 2, .., g-1$. Thus, $G_{n,k}[A_j]$ are connected for all $j = 0, 1, 2, .., g-1$. Next, let $a \in A_r$ and $b \in A_s$, where $r \neq s$ and $0 \leq r, s \leq g-1$, we show that a and b are not connected by a contradiction proof. Suppose that a and b are connected, that is, there is an (a, b)-walk, then by $(\star)$, $b = (a + xk) \bmod n$ for some $x \in \mathbb{Z}$ and so there is $y \in \mathbb{Z}$ so that $a + xk = yn + b$. It follows that

$$a - b = yn - xk. \qquad (\clubsuit)$$

On the other hand, since $a \in A_r$ and $b \in A_s$, $a = (r + pk) \bmod n$ and $b = (s + qk) \bmod n$ for some $p, q \in \mathbb{Z}$. Thus, there are $u, v \in \mathbb{Z}$ so that $r + pk = nu + a$ and $s + qk = nv + b$. It follows that $a = r + pk - nu$ and $b = s + qk - nv$ and hence

$$a - b = r - s + (p - q)k + (v - u)n. \qquad (\spadesuit)$$

From $(\clubsuit)$and $(\spadesuit)$, we have $r - s = \alpha n + \beta k$ for some $\alpha, \beta \in \mathbb{Z}$. Now, since $g = \gcd(n, k)$, we have $g \mid n$ and $g \mid k$, and so by 1(a), $g \mid (\alpha n + \beta k)$, that is $g \mid (r - s)$. Thus, $r - s$ is a multiple of g between $-g$ and g (because $0 \leq r, s \leq g-1$) and so $r - s = 0$. This implies $r = s$ which contradicts the assumption that $r \neq s$. Thus, the components of $G_{n,k}$ are the induced subgraphs $G_{n,k}[A_j]$ where $j = 0, 1, 2, .., g-1$, and so $G_{n,k}$ has $g = \gcd(nk)$ components.