Nathan Bickel
MATH 574: Section H01
Professor: Dr. Luo
November 14, 2022

MATH 574 Homework 12

Collaboration: I discussed some of the problems with Jackson Ginn and Sam Maloney.

Problem 1 Let $m, n, c \in \mathbb{Z}$. Prove that if $c \mid m$ and $c \mid n$ then $c \mid \gcd(m, n)$.
Hint: Bézout's identity.

Solution.

Assume $c \mid m$ and $c \mid n$. Then, there exist $k_1, k_2 \in \mathbb{Z}$ such that $ck_1 = m$ and $ck_2 = n$.

From Bézout's identity, we have that there exist $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = sm + tn$. Substituting from above, we have $\gcd(m, n) = sck_1 + tck_2 = c\,(sk_1 + tk_2)$. Since $sk_1 + tk_2$ is an integer, $c \mid \gcd(m, n)$. □

Problem 2 For nonzero integers $m, n, \ell \in \mathbb{Z}$ let $\gcd(m, n, \ell)$ denote the largest positive integer that divides all of m, n, and ℓ. Prove that $\gcd(m, n, \ell) = \gcd(\gcd(m, n), \ell)$.
Hint: the previous problem may be useful.

Solution.

Let $m, n, \ell \in \mathbb{Z} - \{0\}$, and let $\gcd(m, n, \ell) = d$. So by definition, $d \mid m$, $d \mid n$, $d \mid \ell$. From (1), this implies that $d \mid \gcd(m, n)$, so d is a common factor of ℓ and $\gcd(m, n)$.

Now assume that there exists $d' > d$ such that d' is a common factor of $\gcd(m, n)$ and ℓ. So $d' \mid \gcd(m, n)$ and $d' \mid \ell$, and thus there exists some $k \in \mathbb{Z}$ such that $d'k = \gcd(m, n)$. By definition then, $d'k \mid m$ and $d'k \mid n$, so $d' \mid m$ and $d' \mid n$. But then d' is a common factor of m, n, and ℓ, so $\gcd(m, n, \ell)$ cannot equal d since we assumed $d' > d$. This is a contradiction, so no such d' can exist.

Therefore, since $d = \gcd(m, n, \ell)$ is a common factor of $\gcd(m, n)$ and ℓ and no larger common factor can exist, we have that $\gcd(m, n, \ell) = \gcd(\gcd(m, n), \ell)$. □

Problem 3 Use the previous problem to prove that for nonzero integers $m, n, \ell \in \mathbb{Z}$, there exists integers $a, b, c \in \mathbb{Z}$ such that $am + bn + c\ell = \gcd(m, n, \ell)$. (Similarly we can define the notion of gcd for any number of integers. From this we can also prove geralizations of Bézout's Theorem and Chinese Remainder Theorem for more than 2 integers. In particular, this method can be used to prove the full Euler's Theorem: if $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$. This is left as an exercise to the interested reader.)

Solution.

Let $m, n, \ell \in \mathbb{Z} - \{0\}$. From Bézout's identity, we have that there exist $c, d \in \mathbb{Z}$ such that $\gcd(\gcd(m, n), \ell) = d\gcd(m, n) + c\ell$. Reapplying Bézout, there exist $a', b' \in \mathbb{Z}$ such that $\gcd(\gcd(m, n), \ell) = d(a'm + b'n) + c\ell = a'dm + b'dn + c\ell$. Let $a = a'd$ and $b = b'd$. Since $a', b', d \in \mathbb{Z}$, $a, b \in \mathbb{Z}$. From (2), we have that $\gcd(m, n, \ell) = \gcd(\gcd(m, n), \ell)$, so there exist $a, b, c \in \mathbb{Z}$ such that $\gcd(\gcd(m, n), \ell) = \gcd(m, n, \ell) = am + bn + c\ell$. □

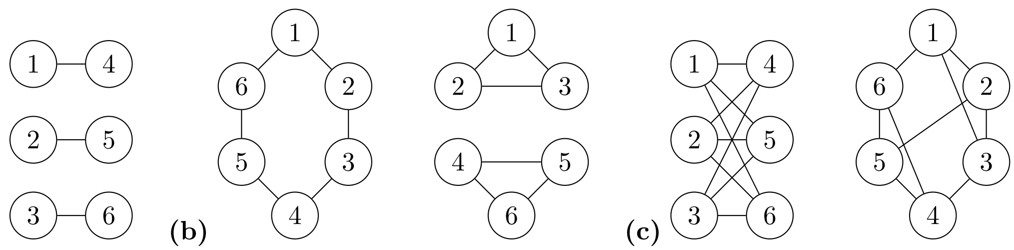
Problem 4 Alice has RSA public key $(13, 85)$. You intercept the encrypted message "39" which was sent to Alice from Bob. Decrypt the message to obtain the plaintext message that Bob sent. You may use a calculator.

Solution.

Our $n = 85$ and $e = 13$, and we note that if we let $p = 5$ and $q = 17$ that $n = pq$. We need to find a d such that d is an inverse of e mod $(p-1)(q-1)$, so in our case we need d to be an inverse of 13 mod 64. We note that $(13)(5) = 65 \equiv 1 \pmod{64}$, so $d = 5$. Our message will be $M = 39^d = 39^5 = 90224199 \mod 85$, which is 14.

Problem 5 For a positive integer k, we say a graph G is k-regular if every vertex in G has degree k.
(a) Draw a graph on 6 vertices that is 1-regular.
(b) Draw two distinct graphs on 6 vertices that are 2-regular. (Here distinct means non-isomorphic.)
(c) Draw two distinct graphs on 6 vertices that are 3-regular.
(d) Prove that if k is odd, then there cannot exist a k-regular graph with an odd number of vertices.

Solution.


(a) **(b)** **(c)**

(d) Let k be an odd integer. Assume that we have a k-regular graph G with an odd number of vertices n. From the handshake lemma, we have that

$$\sum_{v \in V(G)} d(v) = 2|E(G)|.$$

Since $d(v) = k$ for all $v \in V(G)$ and we have n vertices, the sum is nk and thus $nk = 2|E(G)|$. But since both n and k are odd, so is nk, and since $2|E(G)|$ must be even this is a contradiction. So there cannot exist a k-regular graph with an odd number of vertices if k is odd. $\square$

Problem 6 Let G be a bipartite graph with bipartition $X \cup Y$. Prove that if G is k-regular for some $k \in \mathbb{N}$, then $|X| = |Y|$.

Solution.

Assume G is a k-regular bipartite graph with bipartition $X \cup Y$. Let $|X| = m$ and $|Y| = n$. Because G is k-regular, each vertex has an edge to k other vertices. Since G is bipartite, all m vertices in X connect to k vertices in Y so there are mk edges involving vertices in X. Similarly, all n vertices in Y connect to k vertices in X so there are nk edges involving vertices in Y.

Since G is bipartite, every edge in $E(G)$ involves a vertex in X and similarly every edge involves a vertex in Y, so $|E(G)| = mk = nk$. Therefore, $m = n$ and $|X| = |Y|$. $\square$

Problem 7 Prove or disprove the following statements.
(a) If G is a graph in which every vertex has degree at least $\lceil (n-1)/2 \rceil$, then G is connected.
(b) If G is a graph in which every vertex has degree at least $\lfloor (n-2)/2 \rfloor$, then G is connected.

Solution.

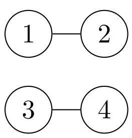
(a) We claim this is true. Let G be a graph where every vertex has degree at least $\lceil (n-1)/2 \rceil$, where $n = |V(G)|$. Assume (to the contrary) that G is not connected. Then, there will be at least 2 connected components with no connections between them.

Case 1: Suppose n is even. Then, $\lceil (n-1)/2 \rceil = \frac{n}{2}$, so every vertex has degree at least $\frac{n}{2}$. We also know that there will be a connected component with at most $\frac{n}{2}$ vertices (there cannot be more than one component with more than half of the vertices). Call this component g, and let $v \in V(G)$. Then, there are $\frac{n}{2} - 1$ other vertices in g. Since v has degree at least $\frac{n}{2}$, even if it connects to every vertex in the component it must connect to at least one vertex in the other component. This is a contradiction (components are defined to not be connected to each other).

Case 2: Suppose n is odd. Then $\lceil (n-1)/2 \rceil = \frac{n-1}{2}$. We also know that there will be a connected component with at most $\frac{n-1}{2}$ vertices (even if the components are equally distributed as much as possible, there will be one with one fewer vertex). A contradiction then follows in the same way as in case 1: any vertex must connect to a vertex in the other component because $\frac{n-1}{2} > \frac{n-1}{2} - 1$.

Therefore, if G is a graph in which every vertex has at least $\lceil (n-1)/2 \rceil$, then G is connected. □

(b) We claim that this is not true for all such graphs. Let $n = 4$. Suppose G is a graph with 4 vertices such that every vertex has degree at least $\lfloor (4-2)/2 \rfloor = 1$. For example, G could take the form:



But this is not connected because there is no path from 1 to 3. So if G is a graph in which every vertex has degree at least $\lfloor (n-2)/2 \rfloor$, it does not necessarily follow that G is connected. □

Problem 8 Suppose that G is a graph with in which every vertex has degree at least $k \geq 2$.
(a) Prove that G contains a cycle with at least $k+1$ vertices.
(b) For each $k \geq 2$, give an example of a graph G in which every vertex has degree at least k but there does not exist a cycle of length $k+2$ or greater.

Solution.

(a) Let $k \in \mathbb{N}$, $k \geq 2$, and let G be a graph where each vertex has degree at least k. Let $v \in V(G)$. Then, we begin traversing a path P starting at v. At each vertex, we arbitrarily choose a vertex to go to next that we have not already visited. We stop when we get to a vertex that only has edges to vertices that we have already visited. This process will stop, at minimum, when our path contains $k+1$ vertices: each vertex has at least k neighbors, so we cannot possibly reach a vertex that connects only to vertices we've already visited unless we've already visited k vertices. Call this last vertex v_f.

Once we reach v_f, it follows that we've found a cycle with at least $k+1$ vertices. A cycle is defined as a path where the last vertex connects to the first vertex, so we need v_f to have an edge to a vertex k or more steps behind v_f in P. We know it must, because v_f connects to at least k vertices in P (every vertex in v_f connects to a vertex in P because of how we chose it and there are at least k neighbors because that defines the graph). So even if v_f connects to the vertex 1 step, 2 steps, and so on before it in P, it still must connect to a vertex k or more steps before it. Thus, we have found a cycle of length $k+1$. □

(b) Take the complete graph K_{k+1}. Then, each vertex will be connected to k other vertices, but there cannot be a cycle of length $k+2$ or greater because there are only $k+1$ vertices.