Notes for 31st Jan (Thursday)

1 The road so far...

1. Proved that Hamiltonian cycles exist if the degree of every vertex is large ($\geq \frac{n}{2}$).
2. "Proved" Euler's formula for planar graphs.

2 Number theory - The basics

First we have the division theorem :

Theorem 1. *Given two non-negative integers $a > 0$ and b, there exist two unique integers $q \geq 0, 0 \leq r < a$ such that $b = aq + r$.*

Proof.
1. Existence : Let $S = \{b - ax| \ x \in \mathbb{N} \ b - ax \geq 0\}$. This set is nonempty ($0 \in S$). By well-ordering it has a least element r. Let the corresponding x be denoted as $q \geq 0$. If $r > a$, then $b - a(q + 1) \geq 0$ contradicting the assumption of minimality on r. Hence $0 \leq r < a$.
2. Uniqueness : If $aq_1 + r_1 = aq_2 + r_2$ then $a(q_1 - q_2) = r_1 - r_2$ where $r_1 \geq r_2$. Since $0 \geq r_1 - r_2 < a$ we have a contradiction unless $r_1 = r_2$ and $q_1 = q_2$.

This theorem is the basis for number systems, i.e., decimal, binary, hexadecimal, etc. □

Now we prove the fundamental theorem of arithmetic (also called the unique factorisation property) :

Theorem 2. *Every natural number > 1 can be written uniquely as $2^{a_1}3^{a_2}\dots$ where $a_i \geq 0$, i.e., uniquely factored into a finite product of primes (upto permutation).*

Proof.
1. Existence : For $n = 2$ it is trivial. If true for $2, 3 \dots, n - 1$, then either n is a prime or $n = n_1n_2$ for two natural numbers $< n$. Using the induction hypothesis we are done.
2. Uniqueness : For $n = 2$ it is trivial. If true for $2, 3 \dots, n - 1$, then either n is a prime (in which case it cannot be factored further by definition) or $n = p_1p_2 \dots p_k$. Suppose there is another factorisation $n = q_1q_2 \dots q_m$. If there exists a j so that $q_j = p_1$, then indeed $p_2 \dots p_k = q_1 \dots q_{j-1}q_{j+1} \dots q_m$. By the induction hypothesis, we are done. Indeed, the desired result follows from the following lemma and induction.

Lemma 2.1. *If p is a prime and p divides ab, then p divides either a or b.*

Proof. (CORRECTED PROOF) Unfortunately, I shall use Bezout's identity (proven a little later). If $pk = ab$ then if p does not divide a, $gcd(a, p) = 1$ because p is a prime. By Bezout's identity, $pn+am = 1$ and hence $pnb+abm = b \Rightarrow p(nb+km) = b$ meaning that b is divisible by p. $\square$

$\square$

It is computationally very hard to factor numbers. Many encryption algorithms like RSA rely on this fact. (Although quantum computers can factor numbers quickly - See Shor's algorithm.) It is an easy exercise to show that

Lemma 2.2. *a divides b iff the exponents of the prime factors of a are smaller than those of b.*

Here is an application of the above.

Theorem 3. $|\mathbb{N}^2| \leq |\mathbb{N}|$, *i.e., there is an injective map from $\mathbb{N}^2$ to $\mathbb{N}$.*

Proof. The map is $(n_1, n_2) \to 2^{n_1}3^{n_2}$. By the fundamental theorem of arithmetic this is a $1-1$ map. (This is called Gödel numbering.) $\square$

Let $a, b \in \mathbb{N}, a \neq 0$. A common divisor of a, b is a natural number c that divides both, a, and b. A common divisor d of a, b is called the greatest common divisor (gcd) of a and b if no other common divisor is larger than d. There exists a gcd of any two numbers by well-ordering. (Indeed, take the set $S = \{\frac{a}{c} | \frac{a}{c}, \frac{b}{c} \in \mathbb{N}\}$. It is non-empty ($a \in S$) and hence has a least element d. The gcd is $\frac{a}{d}$.). Two numbers are said to be coprime if their gcd is 1.

Lemma 2.3. *If $a = 2^{a_1}3^{a_2}\ldots$ and $b = 2^{b_1}3^{b_2}\ldots$, then $c = gcd(a, b) = 2^{\min(a_1,b_1)}3^{\min(a_2,b_2)}\ldots$.*

Proof. c clearly divides a, b. If d divides a, b then by a lemma above, its exponents have to be $\leq a_i, b_i$. Therefore c is the greatest such integer. $\square$

The above process is clearly computationally inefficient. Here is a very old (dating to Euclid) but efficient algorithm -
Let $c = \min(a, b)$ and $d = \max(a, b)$. If $c = 0$ return d. If $c \neq 0$ return $gcd(c, r)$ where $d = cq + r$. Here is the proof that this algorithm works : Induct on c. The base case is trivial. If the algorithm works for all integers $< c$, then $d = cq + r$. Therefore, the gcd of (c, r) divides c and d and is hence less than $gcd(c, d)$. If u divides c, r, then it divides d as well and hence is less than $gcd(c, r)$. So $gcd(c, d) \leq gcd(c, r)$. Therefore we are done.

More clearly, $b = aq_1 + r_1$, $a = q_2r_1 + r_2$, $r_1 = q_3r_2 + r_3 \ldots r_{n-1} = q_{n+1}r_n$. The gcd is r_n. Here is a useful identity.

Theorem 4. *(Bezout's identity) If $d = gcd(a, b)$, then $d = ax + by$ where $a, b \in \mathbb{Z}$.*

Proof. Induct on the number of steps in Euclid's algorithm. If $n = 1$, then $b = aq$ and hence $d = a = a.1 + b.0$. If true for $1, 2, \ldots, n$, then as above since $gcd(a, b) = gcd(a, r_1)$, and $gcd(a, r_1)$ can be computed in n steps, we see that $d = a\alpha + r_1\beta$. Hence $d = a\alpha + (b - aq_1)\beta = ax + by$. $\square$

This solution of $d = ax + by$ for x, y is called the extended Euclidean algorithm.