MTH 4104 Example Sheet I Shu SASAKI

I-1. Using extended Euclid'a algorithm, find $\gcd(186, 132)$ and find a pair (x, y) of integers such that $186x + 132y = \gcd(186, 132)$.

I-2. (a) Use Euclid's algorithm to find a pair (x, y) of integers such that $272x + 200y = 16$. (b) Prove that there are no integers x and y such that $272x + 200y = 4$.

I-3. Find at least two integer solutions for $206x + 64y = \gcd(206, 64)$.

I-4. (a) Use Euclid's algorithm to find a pair (x, y) of integers $61x + 18y = 1$. (b) Find all pairs (x, y) of integers such that $61x + 18y = 0$. (c) Find all pairs (x, y) of integers such that $61x + 18y = 1$.

I-5. Let a and b be two positive integers. (a) Prove that every integer solution to the equation $ax + by = 0$ is of the form $x = cb/\gcd(a, b)$ and $y = -ca/\gcd(a, b)$ for some integer c. (b) Suppose that $(x, y) = (r, s)$ is a pair of integer solution for $ax + by = \gcd(a, b)$. Prove that every solution to the equation $ax + by = \gcd(a, b)$ is of the form $(x, y) = (r + cb/\gcd(a, b), s - ca/\gcd(a, b))$.

I-6. Prove that $a\gcd(b, c) = \gcd(ab, ac)$ for positive integers a, b, c.

I-7. Let a, b and c be fixed integers. Prove that there is an integer solution to $ax + by = c$ if and only if $\gcd(a, b)$ divides c.

I-8. (a) Explain how to find the LCM of two positive integers using prime factorisations. (b) Prove that $\gcd(a, b)\mathrm{lcm}(a, b) = ab$ for any two positive integers a and b. (c) Describe an algorithm to compute the LCM of two positive integers, even when the integers are large.

I-9. Given a finite set S of integers and a prime number p, prove that if p divides the product of all integers in S, then there exists at lease one integer in S that is divisible by p.

I-10. There are infinitely many primes that are congruent to $-1 \bmod 4$. Fill in the argument below to prove the assertion. Suppose that the set S of prime numbers that are congruent to $-1 \bmod 4$ is finite. If this assumption leads to a contradiction, the assertion follows.

Let N_S be the product of all prime numbers p in S and let $N = 4N_S - 1$. By definition, $N < \infty$ and $N \equiv -1 \bmod 4$. (a) Prove that N is not a prime number. (b) Prove that 2 is not a factor of N. (c) Prove that none of the prime numbers in S is a factor of N either. (d) Prove that any prime factor of N is congruent to $1 \bmod 4$. (e) By observing that product of integers congruent to $1 \bmod 4$ is again congruent to $1 \bmod 4$, deduce that (d) contradicts $N \equiv -1 \bmod 4$, and therefore conclude that there are infinitely many primes $\equiv -1 \bmod 4$.