MATH1050 Examples: Divisibility, Division Algorithm, rationals and irrationals.

1. Prove the statements below:
   (a) *Let $x, n \in \mathbb{Z}$. Suppose x is divisible by n. Then for any $y \in \mathbb{Z}$, $(x+2y)^3 + (x-2y)^3$ is divisible by $2n$.*
   (b) *Let $x, n \in \mathbb{Z}$. Suppose x is divisible by n. Then for any $y \in \mathbb{Z}$, $(3x+y)^5 + (3x-y)^5$ is divisible by $6n$.*
   (c) *Let $x, n \in \mathbb{Z}$. Suppose x is divisible by n. Then for any $y \in \mathbb{Z}$, $(5x+y)^7 + (5x-y)^7$ is divisible by $10n$.*
   (d) *Let $x, y, n \in \mathbb{Z}$. Suppose x is divisible by n and y is divisible by n. Then, for any $r, s, t \in \mathbb{Z}$, $rx^2+sxy+ty^2$ is divisible by n^2.*

2. Let n be an integer greater than 1.
   (a) Prove that $\begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} - \begin{pmatrix} 2n-1 \\ n-2 \end{pmatrix} = \dfrac{(2n)!}{(n!)[(An+B)!]}$. Here A, B are appropriate positive integers whose respective values you have to determine explicitly.
   (b) Hence, or otherwise prove that $\begin{pmatrix} 2n \\ n \end{pmatrix}$ is divisible by $n+1$.

3. Let n be a positive integer.
   (a) Prove that $2\begin{pmatrix} 3n+1 \\ n \end{pmatrix} - \begin{pmatrix} 3n+1 \\ n+1 \end{pmatrix} = \dfrac{(3n+1)!}{[(n+A)!][(2n+B)!]}$. Here A, B are appropriate positive integers whose respective values you have to determine explicitly.
   (b) Hence, or otherwise prove that $\begin{pmatrix} 3n+1 \\ n \end{pmatrix}$ is divisible by $n+1$, and $\begin{pmatrix} 3n+1 \\ n+1 \end{pmatrix}$ is divisible by $2n+1$.

4. Apply mathematical induction to justify each of the statements below:
   (a) *$n(2n^2+1)$ is divisible by 3 for any $n \in \mathbb{N}$.*
   (b) *$(2n+1)(2n+3)(2n+5)$ is divisible by 3 for any $n \in \mathbb{N}$.*
   (c) *$(2n+1)(2n+3)(2n+5)(2n+7)(2n+9)$ is divisible by 5 for any $n \in \mathbb{N}$.*
   (d) *$2^{4n+3} + 3^{3n+1}$ is divisible by 11 for any $n \in \mathbb{N}$.*
   (e) *$2^{n+1} + 3^{2n-1}$ is divisible by 7 for any positve integer n.*
   (f) *$3^{4n+2} + 2^{6n+3}$ is divisible by 17 for any $n \in \mathbb{N}$.*

5. Apply mathematical induction to justify each of the statements below. You have to think carefully which proposition is to be formulated and proved by mathematical induction. (This will become apparent when you are attempting to work out the 'inductive argument'.)
   (a) For any $n \in \mathbb{N}$, $(\sqrt{3}+1)^{2n+1} - (\sqrt{3}-1)^{2n+1}$ is an integer which is divisible by 2^{n+1}.
   (b) For any $n \in \mathbb{N}$, $(3+\sqrt{5})^{n+1} + (3-\sqrt{5})^{n+1}$ is an integer which is divisible by 2^{n+1}.

6. Prove the statements below:
   (a) *Let x be a positive real number, r be a positive rational number, and n be an integer greater than 1. Suppose x is an irrational number. Then $\sqrt[n]{x+r}$ is an irrational number.*
   (b) *Let $r, s, t \in \mathbb{R}$. Suppose r is a non-zero rational number and s is an irrational number. Then at least one of $rs+t$, $rs-t$ is an irrational number.*

7. Prove the statements below. *Take for granted the validity of Euclid's Lemma.*
   (a) *$\sqrt[5]{7}$ is irrational.*
   (b) *Let p be a positive prime number, and Q be an integer greater than 1. The number $\sqrt[Q]{p}$ is irrational.*

8. *In this question, take for granted the validity of Euclid's Lemma.*
   (a) Prove the statement (♯):
   (♯) *Suppose p, q are distinct positive prime numbers. Then $\sqrt{pq}$ is irrational.*
   Remark. You may need to apply Euclid's Lemma for several times.
   (b) i. Prove the statement (†):

(†) *Let a, b, c be rational numbers. Suppose a, c are positive and $\sqrt{a}, \sqrt{c}$ are irrational numbers. Further suppose $\sqrt{a} = b + \sqrt{c}$. Then $b = 0$.*

ii. Hence, or otherwise, prove the statement (‡):

(‡) *Let s, t, u, v be rational numbers. Suppose t, v are positive and $\sqrt{t}, \sqrt{v}$ are irrational numbers. Further suppose $s + \sqrt{t} = u + \sqrt{v}$. Then $s = u$ and $t = v$.*

(c) Let A, B, p, q be positive integers. Suppose $\sqrt{B}$ is an irrational number. Further suppose p, q are distinct prime numbers. Prove the statements below:

i. $\sqrt{A + 2\sqrt{B}} = \sqrt{p} + \sqrt{q}$ *iff* ($A = p + q$, $B = pq$, *and* $A > 2\sqrt{B}$).

ii. $\sqrt{A + 2\sqrt{B}} = \sqrt{p} + \sqrt{q}$ *iff* $\sqrt{|A - 2\sqrt{B}|} = |\sqrt{p} - \sqrt{q}|$.

9. Apply mathematical induction to justify the statements below:

(a) *For any integer n greater than 1, n is a prime number or a product of at least two prime numbers.*

(b) *For any integer n greater than 1, if $p_1, p_2, \cdots, p_s$, $q_1, q_2, \cdots, q_t$ are prime numbers, $0 < p_1 \leq p_2 \leq \cdots \leq p_s$, $0 < q_1 \leq q_2 \leq \cdots \leq q_t$, $n = p_1 p_2 \cdot \ldots \cdot p_s$ and $n = q_1 q_2 \cdot \ldots \cdot q_t$, then $s = t$ and $p_1 = q_1$, $p_2 = q_2$, ... , $p_s = q_s$.*

Remark. In the argument for the second statement, take for granted Euclid's Lemma.

Further remark. The two statements are respectively the existence part and the uniqueness part of the **Fundamental Theorem of Arithmetic**, which can be formulated (in a compact manner) as:

For any integer n greter than 1, there are some unique positive prime numbers $p_1, p_2, \cdots, p_s$ such that $p_1 \leq p_2 \leq \cdots \leq p_s$ and $n = p_1 p_2 \cdot \ldots \cdot p_s$.

In plain words, this result says that every integer greater than 1 can be 'factorized' into a product of prime numbers in one and only one way, up to re-ordering of the factors in the product.

10. (a) Prove the statement (♯):

(♯) *Let n be a non-negative integer, and $a_0, a_1, a_2, \cdots, a_{n-1}$ be integers.*
Suppose α is a rational number, and $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$.
Then α is an integer.

Remark. Take for granted Euclid's Lemma and the existence part of the Fundamental Theorem of Arithmetic.

Further remark. The statement (♯) can be re-formulated in terms of polynomials and their roots:

- *Let $f(x)$ be a polynomial whose coefficients are integers and whose leading coefficient is 1. Suppose α is a rational root of $f(x)$. Then α is an integer.*

(b) i. By applying the statement (♯), or otherwise, prove that $\cos\left(\frac{2\pi}{9}\right)$ is irrational.

ii. Hence, or otherwise, deduce that each of the real numbers below is irrational:

A. $\cos\left(\frac{\pi}{9}\right)$ C. $\cos\left(\frac{\pi}{18}\right)$ E. $\cos\left(\frac{4\pi}{9}\right)$ G. $\sin\left(\frac{2\pi}{9}\right)$

B. $\sin\left(\frac{\pi}{9}\right)$ D. $\sin\left(\frac{\pi}{18}\right)$ F. $\sin\left(\frac{4\pi}{9}\right)$

11. Prove the statements below. *You may take Euclid's Lemma for granted.*

(a) *Suppose $m, n \in \mathbb{Z}$. Then $m^2 - n^2$ is divisible by 2 iff $m - n$ is divisible by 2.*

(b) *Suppose $m, n \in \mathbb{Z}$. Then $m^3 - n^3$ is divisible by 3 iff $m - n$ is divisible by 3.*

(c) *Suppose $m, n \in \mathbb{Z}$. Then $m^5 - n^5$ is divisible by 5 iff $m - n$ is divisible by 5.*

Remark. What if $2, 3, 5$ respectively is replaced by 7? Or 11? Or 13? Can you formulate an appropriate conjecture which generalize the statements considered here? How about proving the conjecture?

12. We recall/introduce the definition for the notion of *congruence modulo n*:

Let n be a positive integer, and x, y be integers. We say that x is congruent to y modulo n if $x - y$ is divisible by n. We write $x \equiv y (\mathsf{mod}\ n)$.

Let p be a positive prime number. Prove the statements below:

(a) *For any* $r \in [\![1, p-1]\!]$, $\begin{pmatrix} p \\ r \end{pmatrix}$ *is divisible by* p.

(b) *For any* $x, y \in \mathbb{Z}$, $(x+y)^p \equiv x^p + y^p (\mathsf{mod}\ p)$.

(c) *For any* $x \in \mathbb{N}\backslash\{0\}$, $x^p \equiv x (\mathsf{mod}\ p)$.

(d) *For any* $x \in \mathbb{Z}$, $x^p \equiv x (\mathsf{mod}\ p)$.

Remark. In part (a), you may need Euclid's Lemma at some stage of the argument. In part (b), apply the Binomial Theorem. In part (c), apply mathematical induction. The statement in part (d) is a 'generalization' of the result in part (c), and is known as **Fermat's Little Theorem**. To prove it, make good use of part (c) where applicable.

13.♣ Prove the statement (♯):

(♯) *Let* p, m, n *be positive integers. Suppose* $p > 1$ *and* $m > n > 1$. *Suppose* r *is the remainder in division of* m *by* n. *Then the remainder in the division of* $\dfrac{p^m - 1}{p-1}$ *by* $\dfrac{p^n - 1}{p-1}$ *is* $\dfrac{p^r - 1}{p-1}$.

Remark. It looks obvious that the result is a consequence of Division Algorithm. The question is: how do you apply it in the argument?

14. (a) Take for granted the validity of the statement below:

(♯) *Let* $n \in \mathbb{N}$. *Let* $x, y, u, v \in \mathbb{Z}$. *Suppose* $x \equiv u (\mathsf{mod}\ n)$ *and* $y \equiv v (\mathsf{mod}\ n)$. *Then* $x + y \equiv u + v (\mathsf{mod}\ n)$ *and* $xy \equiv uv (\mathsf{mod}\ n)$.

Let $n \in \mathbb{N}$. Apply mathematical induction to prove each of the statements below:

i. *Let* $t \in \mathbb{N}\backslash\{0,1\}$. *Let* $k_1, k_2, \cdots, k_t, \ell_1, \ell_2, \cdots, \ell_t \in \mathbb{Z}$. *Suppose* $k_i \equiv \ell_i (\mathsf{mod}\ n)$ *for each* i. *Then* $k_1 + k_2 + \cdots + k_t \equiv \ell_1 + \ell_2 + \cdots + \ell_t (\mathsf{mod}\ n)$.

ii. *Let* $t \in \mathbb{N}\backslash\{0,1\}$. *Let* $k_1, k_2, \cdots, k_t, \ell_1, \ell_2, \cdots, \ell_t \in \mathbb{Z}$. *Suppose* $k_i \equiv \ell_i (\mathsf{mod}\ n)$ *for each* i. *Then* $k_1 k_2 \cdots k_t \equiv \ell_1 \ell_2 \cdots \ell_t (\mathsf{mod}\ n)$.

(b) i. Let $m, n, r \in \mathbb{Z}$. Suppose $n \neq 0$ and $0 \leq r < n$. Prove that r is the remainder in the division of m by n iff $m \equiv r (\mathsf{mod}\ n)$.

ii. A. What is the remainder in the division of 10^{100} by 7?

B. What is the remainder in the division of 10^{100} by 13?

Remark. You can make use of the definition of 'congruence modulo n' and the results of the previous part carefully to obtain the answer very quickly.

15. (a) Prove the statements below:

i. *For any* $x \in \mathbb{N}$, *there exist some* $p \in \mathbb{N}$, $a_0, a_1, \cdots, a_p \in [\![0, 9]\!]$ *such that* $x = \sum_{k=0}^{p} a_k 10^k$ *and* $a_p \neq 0$.

ii. *For any* $x \in \mathbb{N}$, *there are at most one* $p \in \mathbb{N}$, *and for each* $j = 0, 1, 2 \cdots, p$, *at most one* $a_j \in [\![0, 9]\!]$ *such that* $x = \sum_{k=0}^{p} a_k 10^k$ *and* $a_p \neq 0$.

Remark. So altogether the existence-and-uniqueness statement below holds:

(♯) *For any* $x \in \mathbb{N}$, *there exist some unique* $p \in \mathbb{N}$, $a_0, a_1, \cdots, a_p \in [\![0, 9]\!]$ *such that* $x = \sum_{k=0}^{p} a_k 10^k$ *and* $a_p \neq 0$.

By virtue of this existence-and-uniqueness statement, each natural number x may be presented as the chain of symbols $a_p a_{p-1} \cdots a_1 a_0$, understood as the sum $x = \sum_{k=0}^{p} a_k 10^k$, in which $a_0, a_1, \cdots, a_p$ are the uniquely determined integers amongst $0, 1, \cdots, 9$ according to (♯). The presentation $x = a_p a_{p-1} \cdots a_1 a_0$ is referred to as the **decimal notation** of the natural number n. We refer to $a_0, a_1, \cdots, a_p$ as the digits of x; a_0 is the last digit, a_1 as the second-last digit, et cetera.

(b) i. Prove the statements below:

A. *Let* $n \in \mathbb{N}$. *Suppose the last digit of* n *in its decimal notation is divisible by* 2. *Then* n *is divisible by* 2.

B. *Let* $n \in \mathbb{N}$. *Suppose the number defined as expressed by the last two digits of* n *in its decimal notation is divisible by* 4. *Then* n *is divisible by* 4.

C. *Let $n \in \mathbb{N}$. Suppose the number defined as expressed by the three digits of n in its decimal notation is divisible by 8. Then n is divisible by 8.*

ii. Can you generalize the above results? Formulate a conjecture for the general situation and prove the conjecture.

(c) Prove the statements below.

i. *Let $n \in \mathbb{N}$. Suppose the sum of the digits of n is divisible by 3. Then n is divisible by 3.*

ii. *Let $n \in \mathbb{N}$. Suppose the sum of the digits of n is divisible by 9. Then n is divisible by 9.*

16. Consider each of the pairs of integers below. Apply the Euclidean Algorithm to find their greatest common divisor.

(a) $14, 35$ (b) $11, 15$ (c) $180, 252$ (d) $1368, 1278$

17. (a) Apply the Euclidean Algorithm to prove the statements below:

i. *Suppose $n \in \mathbb{N}\backslash\{0,1\}$. Then $\gcd(n, n+1) = 1$.*

ii. *Suppose $n \in \mathbb{N}\backslash\{0,1\}$. Then $\gcd(2n-1, 2n+1) = 1$.*

(b) Conjecture what can be said about $\gcd(3n-1, 3n+1)$ for each $n \in \mathbb{N}\backslash\{0,1\}$. Formulate your conjecture appropriately as a mathematical statement.
Prove your conjecture.

18. (a) Let $a, b \in \mathbb{Z}$. Suppose a, b are not both zero.
Let $I = \{x \in \mathbb{Z} :$ There exist some $h, k \in \mathbb{Z}$ such that $x = ha + kb\}$.
Define $S = I \cap (\mathbb{N}\backslash\{0\})$. Apply the Well-Ordering Principle for Integers on the set S to prove that $\gcd(a, b) \in I$.
Remark. This is a 'clean' argument for '**Bezôut's Identity**'; the trade-off is that it does not tell us how to perform the calculations to pick out $\gcd(a, b)$. The set I will be referred to as the 'ideal generated by a, b in the commutative ring $\mathbb{Z}$'.

(b) For any integers p, q, we define

$$\begin{aligned} \langle p \rangle &= \{x \in \mathbb{Z} : \text{ There exists some } h \in \mathbb{Z} \text{ such that } x = hp\}, \\ \langle p, q \rangle &= \{x \in \mathbb{Z} : \text{ There exist some } h, k \in \mathbb{Z} \text{ such that } x = hp + kq\} \end{aligned}$$

Prove that $\langle a, b \rangle = \langle \gcd(a, b) \rangle$ for any $a, b \in \mathbb{Z}$.

19. (a) Prove the statement below:

- *Suppose $a, b, c \in \mathbb{Z}$. Then c is a common divisor of a, b iff $\gcd(a, b)$ is divisible by c.*

(b) Let $\ell, m, n \in \mathbb{Z}$. Write $g = \gcd(\gcd(\ell, m), n)$. Prove the statements below:

i. *Each of ℓ, m, n is divisible by g.*

ii. *For any $d \in \mathbb{Z}$, if each of ℓ, m, n is divisble by d then $|d| \leq g$.*

iii. *If $\ell = m = n = 0$ then $g = 0$.*

iv. *Suppose $c \in \mathbb{Z}$. Then c is a common divisor of ℓ, m, n iff g is divisible by c.*

Remark. Because of the above, it makes sense to refer to the number $\gcd(\gcd(\ell, m), n)$ as the greatest common divisor of ℓ, m, n, and simply write $\gcd(\gcd(\ell, m), n)$ as $\gcd(\ell, m, n)$. We may further inductively define the greatest common divisor for four, five, six, ... integers. Moreover, to compute the greatest common divisor of n integers $a_1, a_2, \cdots, a_n$, we may iteratively compute $\gcd(a_1, a_2)$, $\gcd(\gcd(a_1, a_2), a_3)$, ..., and $\gcd(...\gcd(\gcd(a_1, a_2), a_3)..., a_n)$ in succession. The last number will turn out to be $\gcd(a_1, a_2, \cdots, a_n)$.

(c) Prove the statement below:

- *Suppose $\ell, m, n \in \mathbb{Z}$. Then there exist some $r, s, t \in \mathbb{Z}$ such that $\gcd(\ell, m, n) = r\ell + sm + tn$.*

Remark. It will turn out that when ℓ, m, n are not all zero, $\gcd(\ell, m, n)$ is the smallest positive integer in the set

$$I = \{x \in \mathbb{N} : \text{ There exist some } u, v, w \in \mathbb{Z} \text{ such that } x = u\ell + vm + wn\}.$$

20. We introduce the definitions below:

- *Let $a, b, m \in \mathbb{Z}$. We say m is a* **common multiple** *of a, b if m is divisible by each of a, b.*
- *Let $a, b \in \mathbb{Z}$.*
  - *Suppose both of a, b are non-zero. Then the* **least common multiple** *of a, b is defined to be the multiple of a, b of least value amongst all positive common multiples of a, b. It is denoted by $\text{lcm}(a, b)$.*
  - *Suppose $a = 0$ or $b = 0$. Then the least common multiple of a, b is defined to be 0, and we write $\text{lcm}(a, b) = 0$.*

Without applying the Fundamental Theorem of Arithmetic, prove that for any $a, b \in \mathbb{N}$, $\text{lcm}(a, b)\gcd(a, b) = ab$.