Part I. Integers and Polynomials

1. A grasshopper can jump \( p \) or \( q \) inches right or left on the line. Find all points on the line the grasshopper can reach starting from the origin.

2. Prove that the minimal positive integer \( d \) of the form \( d = mp + nq \) coincides with the Greatest Common Divisor of \( p \) and \( q \), and that \( \text{GCD}(p, q) \) can be found by the following Euclidean algorithm:
   Divide \( p \) by \( q > 0 \) with the remainder \( r \):
   \[ p = lq + r \]
   where \( q > r \geq 0 \).
   If \( r > 0 \), proceed with \( q, r \) instead of \( p, q \). If \( r = 0 \), stop. The last non-zero remainder \( d \) equals \( \text{GCD}(p, q) \).

3. Find \( \text{GCD}(2^{120} - 1, 2^{100} - 1) \), \( \text{GCD}(n^{30} - 1, n^4 - 1) \).

4. Polynomials. A function of the form \( a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \) with \( a_0 \neq 0 \) is called a polynomial of degree \( n \).
   Given two polynomials \( p(x) \) and \( q(x) \neq 0 \), prove that the minimal degree polynomial of the form \( m(x)p(x) + n(x)q(x) \) is the Greatest Common Divisor of \( p(x) \) and \( q(x) \) and can be found by the following algorithm:
   Divide \( p \) by \( q \) with the remainder \( r \):
   \[ p(x) = l(x)q(x) + r(x) \]
   where \( \deg r(x) < \deg q(x) \).
   If \( r \neq 0 \), proceed with \( q \) and \( r \) instead of \( p \) and \( q \).
   If \( r = 0 \), stop. The last non-zero remainder \( d(x) \) is \( \text{GCD}(p(x), q(x)) \).

Notation: \( \mathbb{Z} \) — the set of all integer numbers.
\( \mathbb{Q} \) — the set of all rational numbers.
\( \mathbb{R} \) — the set of all real numbers.
\( \mathbb{R}[x] \) — the set of all polynomials with real coefficients.
\( \mathbb{Q}[x] \) — the set of all polynomials with rational coefficients.
\( \mathbb{Z}[x] \) — the set of all polynomials with integer coefficients.

5. In \( \mathbb{Z}[x] \), find the minimal degree polynomial of the form \( m(x)(x + 2) + n(x)x \). Apply the Euclidean algorithm to \( p = x + 2, q = x \).

6. (a) An invertible element is called a unit. Find all units in \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x] \).
   (b) An element \( a \neq 0 \) is called composite if it can be factored as \( a = bc \) where none of \( b, c \) is a unit. Is \( x^3 - 2 \) composite in \( \mathbb{Q}[x] \)? Which polynomials of the form \( ax^3 + bx^2 + cx + d \) are composite in \( \mathbb{R}[x] \)?

\(^1\) c by Berkeley Math Circle
(c) Prove that a polynomial equation of degree \( n \) has at most \( n \) solutions.

_The Fundamental Theorem of Algebra says that any polynomial in \( \mathbb{R}[x] \) of degree \( > 2 \) is composite._

**Homework.**

(a) Find the Greatest Common Divisor of 11...11 (100 ones), and 11...11 (60 ones).

(b) A Heffelump is a chess piece which moves like Knight but with \( p \) steps in one direction and \( q \) steps in the perpendicular direction. Determine for which \( p \) and \( q \) the Heffelump, starting from one cell on the infinite chess board, can reach any other cell.

(c) Prove that there exists an integer \( a \) such that \( a+1, a+2, \ldots, a+1998 \) are all composite.

(d) Prove that if \( ab \) is divisible by \( c \) but neither \( a \) nor \( b \) is divisible by \( c \) then \( c \) is composite. The same — for \( a, b, c \) in \( \mathbb{R}[x] \) or \( \mathbb{Q}[x] \). Can you prove the same statement for \( \mathbb{Z}[x] \)?

(e) Prove that any polynomial \( x^n + a_1x^{n-1} + \ldots + a_n \) of degree \( n > 0 \) can be factored into a product of linear and quadratic real polynomials (of the form \( x-b \) or \( x^2 + px + q \)), and the factorization is unique up to a permutation of the factors.

(f) Formulate and prove a “unique prime factorization theorem” for \( \mathbb{Q}[x] \).

(g) Prove a “unique prime factorization theorem” for \( \mathbb{Z}[x] \).

**Part II. Arithmetics modulo \( m \)**

1. **Find the last digit of** \( 2^{1998} \).

2. **Given a positive integer** \( m \), **two integers** \( a \) and \( b \) **are called congruent modulo** \( m \) **(write:** \( a \equiv b \pmod{m} \) **if** \( a - b \) **is divisible by** \( m \) **(in other words, if** \( a \) **and** \( b \) **have the same remainder upon division by** \( m \)).**

(a) **Suppose** \( ac \equiv bc \pmod{6} \) **and** \( c \neq 0 \pmod{6} \). **Does it mean that** \( a \equiv b \pmod{6} \)? **The same — modulo** \( 7 \)?

(b) **Prove that** \( c \) **is invertible modulo** \( m \) **if and only if** \( \text{GCD}(c, m) = 1 \).

(c) **Find the inverse to each remainder modulo** \( 7 \).

(d) **Compute** \( 5^{103} \) **modulo** \( 7 \).

(e) **Find all solutions of equation** \( x^2 = 1 \) **modulo** \( 7 \).

_Wilson’s Theorem: For any prime integer** \( p \) **1...(p-1) \equiv -1 \pmod{p}_.

_Fermat’s Little Theorem: If** \( p \) **is a prime integer then** \( a^p \equiv a \pmod{p} \) **for any** \( a \).

3. **Prove that** \( 7^{120} - 1 \) **is divisible by** \( 143 \).
4. Let \( p \) be prime.

(a) For any \( a \not\equiv 0 \pmod{p} \) the sequence \( a^k \pmod{p}, k = 0, 1, 2, \ldots \), is periodic. If \( r(a) \) is the minimal period then the remainders of \( a, a^2, \ldots, a^{r(a)} \) are distinct.

(b) If the minimal periods \( r(a) \) and \( r(b) \) of the sequences \( a^k \pmod{p} \) and \( b^k \pmod{p} \) are relatively prime, then the minimal period of \( (ab)^k \pmod{p} \) equals \( r(a)r(b) \).

(c) Let \( r \) be the Least Common Multiple of the minimal periods \( r(a) \) and \( r(b) \). Then there exists a remainder \( c \) with the minimal period \( r(c) = r \).

(d) Let \( s \) be the Least Common Multiple of the minimal periods \( r(a) \) for all \( a = 1, 2, \ldots, p - 1 \). Then there exist \( a \) with \( r(a) = s \). Deduce that \( s < p \).

5. Let \( s \) be the same as in 4(d). Prove that \( x^s - 1 \equiv (x - 1)(x - 2)\ldots(x - (p - 1)) \pmod{p} \). Deduce that \( s = p - 1 \) and that all remainders \( 1, 2, \ldots, p - 1 \) are powers \( a, \ldots, a^{p-1} \pmod{p} \) of the same \( a \).

6. For which prime numbers \( p \) the equation \( x^2 \equiv -1 \pmod{p} \) has solutions? Find such a solution when it exists.

**Homework**

(a) Find \( 3^{100} \) modulo 7 and \( 7^{77} \) modulo 11.

(b) Find \( 1^2 + \ldots + 36^2 \) modulo 37.

(c) Given a polynomial \( p(x) \) with integer coefficients such that \( p(1) = 2 \). Show that \( p(7) \) is never a perfect square.

(d) Could a perfect cube end with \( 0\ldots01 \) (100 zeroes)?

(e) Let \( A \) be the sum of digits of \( 444444444 \), \( B \) be the sum of digits of \( A \). Find the sum of digits of \( B \).

(f) Prove that there are infinitely many prime numbers congruent to 3 modulo 4.

(g) Can you generalize Fermat’s little theorem for a composite \( p \).

(h) Prove that the equation \( x^2 + y^2 = 3 \) has no rational solutions, and \( x^2 + y^2 = 1 \) has infinitely many rational solutions.

(i) Prove that a spot of area \( > 1 \) on the lattice paper can be translated in such a way that it hits at least two points of the lattice.

(k) Prove that any convex spot of area \( > 4 \) centrally symmetric with respect to the origin of the lattice paper contains a non-zero lattice point.