Division Algorithm, Euclid and Bezout

Andres Buritica

April 16, 2022

1 Division Algorithm

From last time:

- Prove that if a is an integer and b is a positive integer, there is a unique pair (q, r) of integers such that $0 \leq r < b$ and $a = qb + r$.

A similar result is true for polynomials: if $A(x)$ and $B(x)$ are polynomials with $B \neq 0$, then there is a unique pair of polynomials $Q(x)$ and $R(x)$ such that $\deg R < \deg B$ and

$$A(x) = Q(x)B(x) + R(x).$$

In particular, for sufficiently large n, $B(n) > R(n)$.

We can find these polynomials by *polynomial long division*.

- Prove that if there are polynomials A, B, Q, R with integer coefficients satisfying

  $$A(x) = Q(x)B(x) + R(x),$$

  then for each n we have

  $$B(n) \mid A(n) \iff B(n) \mid R(n).$$

- Find all integers n such that $n^2 + 1 \mid n^3 + n^2 - n - 15$.

2 Euclid's Algorithm

We define the *greatest common divisor* of two integers a and b, not both of which are 0, as the largest positive integer d such that $d \mid a$ and $d \mid b$. We notate it by $\gcd(a, b)$.

- Let a and b be integers. Prove that if $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.
- Find $\gcd(72, 30)$ by applying the previous result repeatedly. (This is Euclid's Algorithm.)
- Prove that if we have a function $F : \mathbb{N}^2 \to \mathbb{R}$ such that $F(a, a) = a\ \forall a,\ F(a, b) = F(b, a)\ \forall a, b,$ and $F(a, b) = F(a, b - a)\ \forall a, b$ s.t. $b < a$ then $F(a, b) = \gcd(a, b)\ \forall a, b.$
- Prove that for all positive integers a, m, n we have

  $$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1.$$

3 Bezout's Identity

- Let a and b be integers. Prove that there are integers c and d such that $ac + bd = \gcd(a, b)$.
- Prove that if n, a, b are positive integers such that $n \mid ab$ and $\gcd(n, a) = 1$ then $n \mid b$.
- Let a and b be integers with $\gcd(a, b) = 1$, and let c be an integer. Prove that if $a \mid c$ and $b \mid c$ then $ab \mid c$.
- Let a, b, c, d be positive integers with $\gcd(a, b) = 1$. Prove that there is an integer e such that $a \mid e - c$ and $b \mid f - d$.

4 Problems

1. Let a, b, c, d be positive integers with $ab = cd$. Prove that there exist positive integers p, q, r, s such that $a = pq, b = rs, c = pr, d = qs$.
2. Prove that for positive integers $m, n > 2$ we cannot have
$$2^m - 1 \mid 2^n + 1.$$
3. Find all positive integers n such that $3^{n-1} + 5^{n-1} \mid 3^n + 5^n$.
4. Let n be a composite positive integer. Calculate
$$\gcd((n-1)! + 1, n!).$$
5. Assume that $p_1, \ldots, p_m,\ q_1, \ldots, q_n$ are primes such that
$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$
Prove that the q_is are a permutation of the p_is.
6. Find all pairs of positive integers a, b such that
$$b^2 - a \mid a^2 + b \quad \text{and} \quad a^2 - b \mid b^2 + a.$$
7. Let m and n be positive integers. Prove that
$$m \mid \gcd(m, n)\binom{m}{n}.$$
8. Find all pairs of positive integers x, y such that $xy^2 + y + 7 \mid x^2y + x + y$.

5 Homework

1. (a) Find all integers x, y such that $6x + 2y = 8$.

   (b) Find all integers x, y such that $6x + 4y = 8$.

2. Let $a_1, a_2, \ldots, a_n$ be positive integers, and let d be the largest positive integer such that $d \mid a_i$ for all i.

   Prove that there are integers $b_1, b_2, \ldots, b_n$ such that

   $$d = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.$$

3. The Fibonacci sequence is defined by $F_1 = F_2 = 1$ and

   $$F_{n+1} = F_n + F_{n-1}.$$

   Prove that $\gcd(F_n, F_{n+2}) = 1$ for all n.