UBC Math Circle - Arithmetic and Higher Algebra

March 10, 2025

1. Chinese Remainder Theorem

(a) [*The Chinese Remainder Theorem*] Let $N_1, \ldots, N_n$ be pairwise coprime positive integers, here coprime means that $i \neq j$ implies $\gcd(N_i, N_j) = 1$. Let $a_1, \ldots, a_n$ be integers, show that for some $a \in \mathbb{Z}$ we have

$$a \equiv a_i \bmod N_i \text{ for } 1 \leq i \leq n$$

Further prove that a is unique modulo $\prod_1^n N_i$, i.e. If a, b both satisfy the system of congurences above, then $a \equiv b \bmod \prod_1^n N_i$.

Hint: *Use Bezout's identity to construct a solution in the case $n = 2$, proceed by induction.*

(b) [*Lagrange interpolation*] Alice is an engineering student studying robotics at the University of British Columbia, she was asked to track her robots movement through an obstacle course but fell asleep during the lab, her lab instructor is asking that she provide a plot of the robots distance from the finish line of the course as a function of time or else she will fail the lab. Luckily Alice remembers that her she programmed her robot such that its distance from the finish line is a degree 16 polynomial in terms of t, and she has data for the robots distance from the finish line and time at the 17 unique obstacles on the course. Additionally alice recalls that if two polynomials of degree n agree at $n + 1$ points, then the polynomials are equal. Alice has a dentists appointment so she has entrusted you with her data set $\{(t_1, d_1), (t_2, d_2), \ldots, (t_{17}, d_{17})\} \subset \mathbb{R}^2$ can you help Alice by writing down the degree 16 polynomial she needs to plot of her robots progress in the obstacle course?

Hint1: *Your answer should involve summation and product notation.*

Hint2: A big hint, see back of page and try a smaller example on your own first.

(c) [*Just for fun!*] Can you make a connection between the constructions in **(a)** and **(b)**?

2. Polynomial Equations

[*Pell's Equation*] Show that the equation $x^2 - 2y^2 = 1$ has infinitely many solutions, $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

Hint: *(three, two) is a solution*

3. Hensel's Lemma and Number Systems Say we want to solve the equation $x^2 + 1 = 0$ in $\mathbb{Z}$. This problem explores various approaches to this conundrum and the structures that are created in order to do so.

(a) [*Gaussian integers*] Consider the Gaussian integers $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{a + bi \mid a, b \in \mathbb{Z}\}$ where addition and multiplication are defined as in $\mathbb{C}$. Here i is "adjoined" to $\mathbb{Z}$ in order to directly add a solution to $x^2 + 1 = 0$. The resulting structure $\mathbb{Z}[i]$ actually looks quite a lot like the integers, but with a few key differences. We can define a notion of size on $\mathbb{Z}[i]$, where $N(x+iy) = x^2+y^2$, we say that an element $x + iy \in \mathbb{Z}[i]$ is prime when we cannot write $x + iy = (a + ib)(c + id)$ for $N(a + ib) \neq 1 \neq N(c + id)$. **(i)** Show there is atleast one prime number $p \in \mathbb{Z}$, such that p is not prime in $\mathbb{Z}[i]$. **(ii)** Show that if $p \in \mathbb{Z}$ is prime, and $p \equiv 3 \bmod 4$, then p is prime in $\mathbb{Z}[i]$.

(Challenge Problem)[*You can try this problem if youre interested I don't expect many people to do this one*] Show that similar to $\mathbb{Z}$, elements of $\mathbb{Z}[i]$ have unique prime factorizations, additionally, characterize all primes in $\mathbb{Z}[i]$.

(b)[*Hensel's Lemma and Projective Limits*] We know that there is a solution to $x^2 + 1 = 0 \bmod 5$, namely 2, to find a solution in $\mathbb{Z}$ is similar to finding a solution modulo ∞. We can consruct such a solution step by step, the idea here is to show that if we have a solution y_n modulo 5^n, then we can "lift" it to a (unique) solution $y_{n+1} = \ell(y_n)$ modulo 5^{n+1}, then we can consider the number system

$$\mathbb{Z}_5 := (x_1 \bmod 5, x_2 \bmod 25, \ldots)$$

where we require $x_{i+1} \equiv x_i \bmod 5^i$. Then the solution to our quadratic equation will be

$$(2 \bmod 5, \ell(2) \bmod 25, \ldots, \ell^{(n)}(5) \bmod 5^n, \ldots)$$

Hensel's lemma is the statement that we can lift these solutions. Let f be a polynomial, we will prove Hensel's lemma in two steps

(i) Show that $f(x + 5^n) \equiv f(x) + 5^n f'(x) \bmod 5^{n+1}$ (here f' denotes the derivative of f).

Hint: *Use the Binomial theorem.*

(ii) Use the result from **(i)** To prove Hensels lemma. i.e. a solution to f modulo 5^n lifts to a solution modulo 5^{n+1}

Hint: *If y_n is the lift modulo 5^n, then y_{n+1} must be of the form $y_n + 5^n t$, for some t.*

(c)[*Computation practice*] Write the first 4 digits of the solution lifting the solution 2 of $x^2 \equiv 1 \bmod 5$.

1(b) Hint2: *If the degree of the polynomial is 2 instead of 16 and we have data at 3 obstacles, $(t_1, d_1) = (1, 9), (t_2, d_2) = (2, 4), (t_3, d_3) = (3, 1)$, then the solution can be written as*

$$D(t) = 9\frac{(t-2)(t-3)}{(1-2)(1-3)} + 4\frac{(t-1)(t-3)}{(2-1)(2-3)} + \frac{(t-1)(t-2)}{(3-2)(3-1)}$$