MODULAR ARITHMETIC

STUDENT:
PROF. PINEIRO

Abstract. We will introduce modular arithmetic. In particular we want to use quadratic reciprocity to determine whether or not a given number is a square modulo an odd prime. The plan is to produce a list of squares and non-squares for small prime moduli.

1. Project Description

Given an integer $n > 1$, called a modulus, two integers are said to be congruent modulo n, if n is a divisor of their difference (i.e., if there is an integer k such that $a - b = kn$). Congruence modulo n is an equivalence relation compatible with the operations of addition, subtraction, and multiplication. Congruence modulo n is denoted:

$$a \equiv b \pmod{n}.$$

Remark 1.1. Two numbers a, b are congruent mod n, if and only if they have the same remainder when divided by n. For example, $144 \equiv 74 \pmod{10}$, $18 \equiv 103 \pmod{5}$ or $-5 \equiv 4 \pmod{9}$. Any integer a mod (n) can be made congruent to an element in the set $\{0, 1, \dots, n-1\}$ by taking the remainder of the division of a by n.

Some properties of modular congruency:

(1) (addition) If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$.
(2) (subtraction) If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$.
(3) (multiplication) If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$.
(4) (inverse) There exists an integer denoted a^{-1} such that $a \cdot a^{-1} \equiv 1 \pmod{n}$ if and only if a is coprime with n (no number except 1 divide them both). This integer a^{-1} is called a modular multiplicative inverse of a modulo n.
(5) (linear equations) If $ax \equiv b \pmod{n}$ and a is coprime to n, then the solution to this linear congruence is given by $x \equiv a^{-1}b \pmod{n}$.
(6) (quadratic equations) An integer a is a quadratic residue modulo n, if there exists an integer x such that $x^2 \equiv a \pmod{n}$. The Legendre symbol $\left(\frac{a}{p}\right)$, for a number a and an odd prime p, is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } n \\ -1 & \text{if } a \text{ is a not quadratic residue mod } n \\ 0 & a \equiv 0 \pmod{p} \end{cases}$$

For example $\left(\frac{2}{7}\right) = 1$ because $2 \equiv 3^2 \equiv 9 \pmod{7}$, while $\left(\frac{5}{7}\right) = -1$ because there is not solution to $5 \equiv x^2 \pmod{7}$. Now the Legendre symbol satisfies the following properties:

(a) $\left(\frac{1}{p}\right) = 1$, $\quad$ (*b*) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\quad$ (*c*) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(d) It is completely multiplicative: $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(e) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(f) (quadratic reciprocity law) For p, q odd primes, we have $\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right)$.

This means that if $p-1$ or $q-1$ is divisible by 4, we have $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, otherwise $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

(g) (factor out squares) $\left(\frac{x^2}{p}\right) = 1$ if p does not divide x and zero otherwise.

Example 1.2. Can we find a solution to the modular equation $x^2 \equiv 60 \pmod{331}$?
To solve this question, we need to compute the Legendre symbol $\left(\frac{60}{331}\right)$. If we get 1, then answer is Yes. If we get -1, the answer is Not (the only three answers are $0, 1, -1$, and we can not get 0 because 15 is not divisible by 331).

$$\begin{aligned}\left(\frac{60}{331}\right) &= \left(\frac{2^2}{331}\right) \cdot \left(\frac{5}{331}\right) \cdot \left(\frac{3}{331}\right) \\ &= (1) \cdot \left(\frac{331}{5}\right) \cdot (-1) \cdot \left(\frac{331}{3}\right) \\ &= (1) \cdot \left(\frac{1}{5}\right) \cdot (-1) \cdot \left(\frac{1}{3}\right) = -1.\end{aligned}$$

And the answer we get is that 60 is not a square module 331. To actually check our result, we have to square each element $\{0, 1, \ldots, 330\}$ to make sure that no answer will be $\equiv 60 \pmod{331}$.

Practice Questions:

(1) Find $x \in \{0, 1, \ldots, 59\}$ such that $3333 \equiv x \pmod{60}$.
(2) If $x = 21$ and $y = 12$. What is the value of $xy \pmod{11}$?
(3) Find the value of $4^3 \pmod{15}$.
(4) If $x = 28$ and $n = 11$. Find $x^n \equiv \pmod{29}$.
(5) Express the concepts of even and odd using modular congruency.
(6) Let n be any odd number. Show that $n^2 - 1$ is always divisible by 4.
(7) Find a solution of the linear equation $9x \equiv 1 \pmod 7$. Find a multiplicative inverse for 9 modulo 7.
(8) Find a multiplicative inverse of 5 modulo 17. Use this inverse to find a solution of the linear equation $5x \equiv 3 \pmod{17}$.
(9) Follow a exhaustive method, squaring all elements in $\{0, 1, \ldots, 6\}$, to determine all elements that are square modulo 7. What is the value of $\left(\frac{3}{7}\right)$?
(10) Follow a exhaustive method, squaring all elements in $\{0, 1, \ldots, 10\}$, to determine all elements that are square modulo 11. What is the value of $\left(\frac{3}{11}\right)$?
(11) Determine the symbols $\left(\frac{11}{3}\right)$ and $\left(\frac{7}{3}\right)$ and check in each case the quadratic reciprocity law using your answers above.
(12) Follow a exhaustive method, squaring all elements in $\{0, 1, \ldots, 12\}$, to determine all elements that are square modulo 13. What is the value of the symbols $\left(\frac{2}{13}\right), \left(\frac{3}{13}\right), \left(\frac{6}{13}\right)$. Verify the completely multiplicative property.

(13) Design and implement a program to calculate the Legendre symbol of numbers for small primes. Create a table of values of $\left(\frac{a}{p}\right)$, for example, for $a = 0, \ldots, 30$ and $p = 3, 5, 7, 11, \ldots, 127$. This program can be part of a class ModuloN that mimic modular arithmetic mod N.

References

[1] Lazar, *Modular arithmetic* available at $https://www2.math.upenn.edu/\ mlazar/math170/notes06-2.pdf$

[2] J. Silverman, *A friendly introduction to Number Theory (third edition)* Pearson, (2005)

[3] Wikipedia, *Modular arithmetic* available at $https://en.wikipedia.org/wiki/Modular\_arithmetic$