University of Toronto

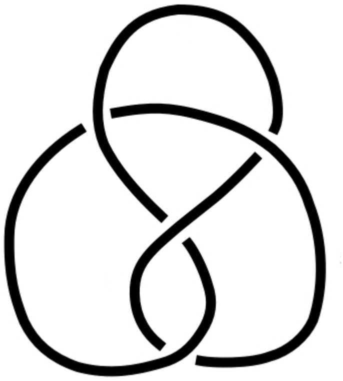
Math Academy 2021

August 13, 2024

Try to solve the most you can and explain the solution to the best of your abilities. Do not just put computations, be mindful of your arguments. Discuss with the other members of the academy and learn together!
These problems might be harder for some of you than others, I do encourage you to talk among yourselves if that's possible and to ask me for suggestions and help if you need. If you get frustrated, GOOD, is part of progress. Don't let it dominate you, look for help, think, take your time. Math is worth the challenge.

1 Problems

1. (a) The following knot is the knot 4_1, called the **eight knot**. Prove that it is equivalent to it mirror reflection (i.e it is **amphichiral**) by showing a sequence of Reidemeister movements that transform one into the other.



   (b) Prove that adding an orientation to a knot doesn't change the number of n-Fox Colourings of the knot. That is, this number is independent of orientation, and we would say it is **an invariant of unoriented knots**.

   (c) Prove or find a counterexample: The number of Fox $n-$colourings is invariant under mirror images.

2. For this exercise we will consider p a prime number.

   An $m \times n$ matrix is an array (i.e a table) of m rows and n columns, with a number in each entry, that is, on the intersection of each row and column. When $m = n$ we call the matrix a **square matrix**.

   We will consider matrices whose entries are numbers modulo p. [For some extra exercises on modular arithmetic please see the second appendix to this homework or talk with me or search online. It is not hard, just requires some practice!] In class we have made some examples modulo 5.

   We define two operations, called **row operations**, that transform one matrix into another. They are as follows:

   Exchange: Exchange two different rows from the matrix.

Linear Addition: Pick two different rows R_i and R_j. Substitute the row R_i by $R_i + xR_j$ where x is any number (modulo p).

Because we are modulo a prime number, the following is always possible: *it is always possible in this way to transform the matrix into another one such that for each nonzero row, all the numbers below its first nonzero entry and to its left, are all zero and all the rows that consist of only zeros are at the bottom of the matrix.*

A matrix of this form is said to be in **row echelon form**. Once a matrix is in this form the first nonzero terms in each row, in case they exist, are called the **pivots** of the matrix. We define number **rank of the matrix**, modulo p, as the number of pivots it has.

Note: Depending on the way you performed the operations the final echelon form might not be unique, but the number of pivots is invariant.

(a) Consider the following matrix

$$A = \begin{pmatrix} 1 & 4 & 3 \\ 2 & 4 & 5 \\ 2 & 0 & 1 \end{pmatrix}$$

Find its rank, modulo p, for the primes $p = 2, 3, 5, 7$.

(b) Consider the following matrix

$$B = \begin{pmatrix} 5 & 1 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 2 & 3 \end{pmatrix}$$

Find its rank, modulo p, for the primes $p = 2, 3, 5, 7$.

(c) Define the analogous operations for columns and say what is a column echelon form. It turns out the rank can also be computed as the number of pivots in the column echelon form and the answer is the same as when performed on rows.

Verify this for the matrices A and B of the previous exercises.

(d) We have seen in class that a system of equations with n variables and m equations corresponds to a matrix of $m \times n$ equations. We have also seen that from every knot diagram we can create a system of equations.

Prove that for every knot diagram this system always have the same number of equations as variables. Hence, the corresponding matrix is an square matrix.

(e) The following is a theorem: **A knot has a nonmonochormatic Fox p-colouring if and only if the rank modulo p of the associated matrix is $p - 1$.**

For the knots $7_i, i = 1, ..., 7$ find their rank modulo 5.

(f) (If you are familiar with linear algebra) Prove the theorem of the previous part.

3. (For this and the next part you might want to work in teams. Of course, you can also do it for the whole problem sets! I encourage you to engage with others :D)

We have defined Gauss Diagrams in class. We saw that for this we needed an orientation and a choice of fixed point (we called it the orange point in class).

(a) What happens to the Gauss Diagram if you change the orange point?

(b) What happens to the Gauss Diagram if you reverse the orientation?

(c) What happens to the Gauss Diagram if you mirror the knot?

(d) Make a new table (it must be beautiful!), just as the one of the appendix, but instead of showing the knot diagram show the Gauss Diagram. Explain, if it is necessary according to your answers of the previous parts of this question, how did you pick the orange point and the orientation.

4. (a) Based on your previous exercise, specially the last part, compute the Casson Invariant of all the knots in the appendix table.

(b) Is there any two of the knots $7_i, i = 1, ..., 7$ that you cannot distinguish via the number of $5-$Fox Colourings but you can with the Casson Invariant or Viceversa?

5. (a) We have defined the Reidemeister movements and the oriented Reidemeister movements in class. We use them to say when two knot diagrams and oriented knot diagrams are equivalent.

   Find the corresponding Reidemeister movements but in Gauss Diagram notation. That is, if two knots just differ by a single Reidemeister movement, how does the Gauss Diagram Change?.

   (b) (Harder) Prove that the Casson Invariant is indeed Invariant under Reidemeister Movements.

2 Appendix: Number Theory Exercises

1. **Divisibility** Consider the following formal definition of divisibility in the integers:

   Definition: *We say the integer a divides the integer b if and only if there exists an integer c such that*

   $$b = ac.$$

   We write this as as $a \mid b$

   Verify the following properties of divisibility without using the fundamental theorem of arithmetic or the notion of prime numbers. You are just allowed to use the definition of divisibility and the propositions proven here.

   (a) If $a|b$ and $a|c$ then $a|bx + cy$ for any integers x, y.

   (b) If $a|b$ and $b|c$ then $a|c$.

   (c) If $a|b$ and $b|a$ then $a = b$ or $a = -b$.

   (d) Two integers a and b are **relatively prime** if whenever $d|a$ and $d|b$ we must have $d = \pm 1$. Prove that if a and b are relatively prime and $a|bc$, then $a|c$.

   (e) Given two integers a and b, an integer c such that $c|a$ and $c|b$ is called a **common divisor**. Prove that there exists a unique biggest positive common divisor. We call this divisor the greatest common divisor and is usually denoted by (a, b). Do not confuse this for the pair (a, b), as coordinates, it is the same notation but it means a different thing.

   (f) Given two integers a and b, an integer c such that $a|c$ and $b|c$ is called a **common multiple**. Prove that there exists a least positive common multiple of a and b. It is usually called the least common multiple and is denoted by $[a, b]$.

   (g) Let a and b be two integers. Prove that there exists unique integers q and r such that

   $$a = bq + r$$

   and such that $0 \leq r < |b|$. We call r the residue or remainder of a when divided by b. This is called division with remainder property.

   (h) Let a and b be two integers and let r be the remainder of a when divided by b. Prove that $(a, b) = (b, r)$.

   (i) Let a and b be integers with greatest common divisor d. Prove there exists x and y such that

   $$ax + by = d.$$

   This statement is called **Bezout's Theorem**.

2. **Congruences**

   Consider the following formal definition of congruence

   Definition: *We say the integers a and b are **congruent** modulo m if and only if*

   $$m \mid a - b.$$

We write this as as $a \equiv b \pmod{m}$.

Prove the following properties of congruences. You can use the statements of the previous question if you need.

(a) We said in class that congruence behaves almost like the equal sign. Prove that adding and multiplying congruences together is possible, that is, prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

(b) Find a counterexample to the following claim: if $ac \equiv bc \pmod{m}$ then $a \equiv b \pmod{m}$ where a, b and c are all nonzero modulo m. Convince yourself that this means that cancellation is not possible modulo m.

(c) Let m be a positive integer and x an integer that is relatively prime to m (see question 1(d) for the definition of relatively prime). Prove that there exists a unique solution y modulo m such that

$$xy \equiv 1 \pmod{m}.$$

Notice that in class we mentioned this, in the case when m is a prime number, by saying that all *row of the multiplication table had a 1.*

(d) Prove that if $ac \equiv bc \pmod{m}$ and $(c, m) = 1$ then $a \equiv b \pmod{m}$. So, cancellation **is possible** when the number you want to cancel on both sides is relatively prime to the modulus m.

(e) Let a, b, c, m be integers with $(m, a) = 1$ and m odd. Suppose that $b^2 - 4ac$ is a square modulo m (we explained in class what this means). Prove that the quadratic congruence

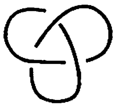
$$aX^2 + bX + c \equiv 0 \pmod{m}$$

has the following as possible solutions

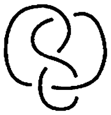
$$X = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

3 Appendix: Knot Tables

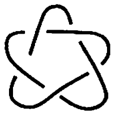
3_1



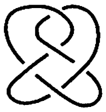
4_1



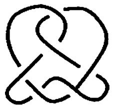
5_1



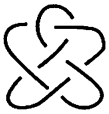
5_2



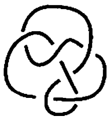
6_1



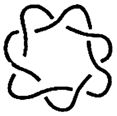
6_2



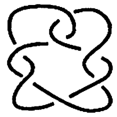
6_3



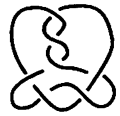
7_1



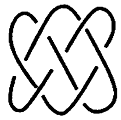
7_2



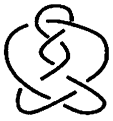
7_3



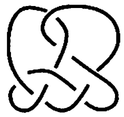
7_4



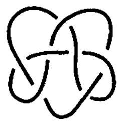
7_5



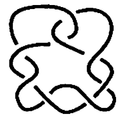
7_6



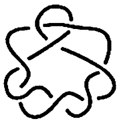
7_7



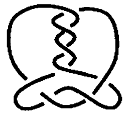
8_1



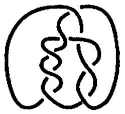
8_2



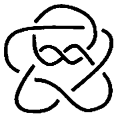
8_3



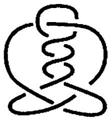
8_4



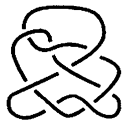
8_5



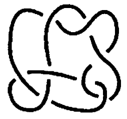
8_6



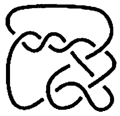
8_7



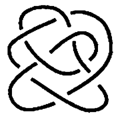
8_8



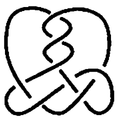
8_9



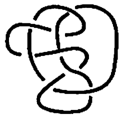
8_{10}



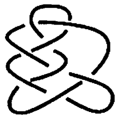
8_{11}



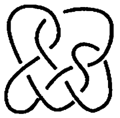
8_{12}



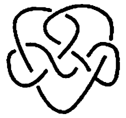
8_{13}



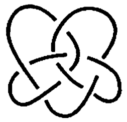
8_{14}



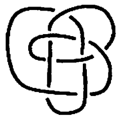
8_{15}



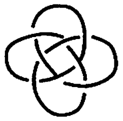
8_{16}



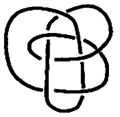
8_{17}



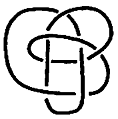
8_{18}



8_{19}



8_{20}



8_{21}