Math Circles - Number Theory

Tyrone Ghaswala - ty.ghaswala@gmail.com

27th March, 3rd April, 2013

Introduction

This instalment of math circles is intended to give you a taste of number theory, in all its beauty and glory. The idea is to present you with some ideas and questions, and have you work things out getting your hands dirty with some questions. The questions are both computational and exploratory, some have well defined answers, and some don't. You are not expected to answer all of them, but you are expected to explore to your heart's content. The more you explore, the more beauty you will find hidden away.

Clock Arithmetic

We are all familiar with number systems (whatever they are), say for example, the real numbers $\mathbb{R}$, or the rational numbers $\mathbb{Q}$, or the integers $\mathbb{Z}$. What all of these things have in common is not only that we're quite familiar with them, but that if you take any two things in one of these and multiply or add them together, you get another member of the number system. We might ask ourselves, what else could we consider?

Well that's simple, a clock of course!

Consider a clock with seven numbers, 0 through 6, with the 0 at the top. What we're going to do now, is to try to imitate arithmetic operations on this clock. We will call this clock *the integers modulo 7*. We denote it $\mathbb{Z}_7$ and it consists of the seven elements

$$\mathbb{Z}_7 := \{0, 1, 2, 3, 4, 5, 6\}.$$

But how do we do math in $\mathbb{Z}_7$? Well, kind of as you would expect to do math on a clock. For example,

$$\begin{aligned} 3 + 4 &\equiv 0 \mod 7 \\ 1 + 2 &\equiv 3 \mod 7 \\ 5 + 6 &\equiv 4 \mod 7. \end{aligned}$$

So addition is just what you would do on a clock! So what is $-3 \mod 7$? Well -3 does not live in $\mathbb{Z}_7$ (since it's not one of 0,1,2,3,4,5 or 6), so which element is it? Whatever it is, call it Bob, it better have the property that $\text{Bob} + 3 \equiv 0 \mod 7$. Therefore we have

$$-3 \equiv 4 \mod 7.$$

Alternatively, we could just count backwards around the clock, either way will work and no harm will come to you! Let's do some more examples. What about 22 + 11? Well we have

$$22 + 11 = 33 \equiv 5 \mod 7 \quad \text{OR} \quad 22 + 11 \equiv 1 + 4 \equiv 5 \mod 7.$$

Look at that, it doesn't seem to matter if we convert 22 and 11 to mod 7 before or after doing the addition. It turns out that this is always the case. It doesn't matter when you reduce things to live inside $\mathbb{Z}_7$, no harm will come to you.

Ok, so we've dealt with addition and subtraction (since subtraction doesn't really exist, it's just adding by negative numbers), but what about multiplication and division? Well multiplication will work as we expect. Given two numbers, multiply them together and then keep subtracting (or adding) multiples of 7 until you end up in $\mathbb{Z}_7$. Piece of cake! For example

$$\begin{aligned} 3 \cdot 4 &\equiv 5 \mod 7 \\ 5 \cdot 3 &\equiv 1 \mod 7 \\ 2 \cdot 3 &\equiv 6 \mod 7. \end{aligned}$$

So, what about division or inverses? What is $\frac{1}{3} \mod 7$? Well, let's think about it for a moment. The element that equals $\frac{1}{3}$, whatever it is, call it Jenny, had better have the property that $(\text{Jenny}) \cdot 3 \equiv 1 \mod 7$. Well, since $3 \cdot 5 \equiv 1 \mod 7$, and $2 \cdot 4 \equiv 1 \mod 7$, we see

$$\frac{1}{3} \equiv 5 \mod 7 \quad \text{and} \quad \frac{1}{2} \equiv 4 \mod 7.$$

Let's draw up a table of inverses for $\mathbb{Z}_7$.

x	0	1	2	3	4	5	6
x^{-1}	$*$	1	4	5	2	3	6

Notice here that every non-zero element appears exactly once in both rows.

Now, let's change our attention to $\mathbb{Z}_{15}$ for a change of scenery. Everything works as before and we ask the same questions. What is $\frac{1}{2}$ in $\mathbb{Z}_{15}$? Well, since $2 \cdot 8 \equiv 1 \mod 15$, we see $\frac{1}{2} \equiv 8 \mod 15$. Let's have a look at the table for $\mathbb{Z}_{15}$.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^{-1}	$*$	1	8	$*$	4	$*$	$*$	13	2	$*$	$*$	11	$*$	7	14

Now that's weird, a whole bunch of non-zero elements don't actually have inverses in $\mathbb{Z}_{15}$. Notice that the numbers which appear in the second row are exactly the numbers which appear in the first row that have an inverse. Also, 14 is its own inverse in $\mathbb{Z}_{15}$ and 6 is its own inverse in $\mathbb{Z}_7$. Does this always happen?

Before we do some questions, we make a quick definition.

Definition. If a in $\mathbb{Z}_n$ has an inverse for all $a \neq 0$, then we say $\mathbb{Z}_n$ is a **field**.

Now go ahead and try some questions from group 1, and question 3 is certainly one to devote some time to and think long and hard about.

Group 1 Questions

1. Find the following elements, if they exist.
   (a) In $\mathbb{Z}_{11}$: $\frac{1}{5}$, -92, $\frac{1}{3} + \frac{7-9}{10}$, $\sqrt{5}$.
   (b) In $\mathbb{Z}_{13}$: $\frac{1}{5}$, -92, $\frac{1}{3} + \frac{7-9}{10}$, $\sqrt{5}$.
   (c) In $\mathbb{Z}_{17}$: $\frac{1}{5}$, -92, $\frac{1}{3} + \frac{7-9}{10}$, $\sqrt{5}$.

(d) In $\mathbb{Z}_{12}$: $\frac{1}{5}$, -92, $\frac{1}{3} + \frac{7-9}{10}$, $\sqrt{5}$.

(e) In $\mathbb{Z}_7$: $\sqrt{-1}$. What about in $\mathbb{Z}_{13}$?

2. Find integers x, y, if possible, that solve the following equations. Equations like this are called *Diophantine equations*.

   (a) $8x + 13y = 1$

   (b) $8x + 13y = 11$

   (c) $6x + 4y = 1$

   (d) $6x + 4y = 2$

   (e) $23x + 29y = 1$

   Guess when an equation $ax + by = c$, with a, b, c in $\mathbb{Z}$, has integer solutions x and y. Try to prove your conjecture.

3. Write out an inverse table for $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_{11}$ and $\mathbb{Z}_{12}$. When do elements have an inverse? For which n is $\mathbb{Z}_n$ a field? Prove both your assertions.

4. We know that sometimes we can choose different ways of representing the same thing in $\mathbb{Z}_n$. For example, in $\mathbb{Z}_6$ we can represent 1 by 1, or 7, or -5. In fact, there are an infinite number of ways we can represent the number 1!

   We've already seen an example (11 + 22 in $\mathbb{Z}_7$) where it doesn't matter which representative we work with. Prove that for any $\mathbb{Z}_n$, during addition, subtraction, multiplication and division (when division makes sense), it doesn't matter which choices we make, we always get the same answer! That is, prove that no harm will ever come to you when doing clock arithmetic!

Greatest Common Divisors and Euclid

So we now shift our attention (seemingly randomly, but it won't be so random after all) to the greatest common divisor of two numbers. This is exactly what it sounds like. For example the greatest common divisor, or gcd, of 12 and 15 is

$$\gcd(12, 15) = 3$$

since 3 is the largest number that goes into both 12 and 15. One way to do this is to write out the divisors of 12 and 15, for which we get

$$\{1, 2, 3, 4, 6, 12\} \quad \text{and} \quad \{1, 3, 5, 15\}$$

and we notice that 3 is the largest number that appears in both. This method is fine, and given enough time will always work. What if I asked you to calculate $\gcd(2625, 15015)$? Well, here's where Euclid comes in.

This algorithm is best illustrated by an example. Say we wanted $\gcd(26, 38)$. Staring at it, we know it's 2, but let's use Euclid to reinforce this.

$$38 = (1)26 + 12 \tag{1}$$

$$26 = (2)12 + 2 \tag{2}$$

$$12 = (6)2 + 0. \tag{3}$$

Start with the largest number and write it as some multiple times the smaller number plus a remainder. Take the smaller number and the remainder (26 and 12 in the case of equation 1) and repeat. Keep going until your remainder is 0, and the last non-zero remainder is your greatest common divisor. Magic!

Let's do another example, $\gcd(13, 8)$.

$$13 = (1)8 + 5 \tag{4}$$
$$8 = (1)5 + 3 \tag{5}$$
$$5 = (1)3 + 2 \tag{6}$$
$$3 = (1)2 + 1 \tag{7}$$
$$2 = (2)1 + 0 \tag{8}$$

so $\gcd(13, 8) = 1$. So, this is all well and good, but let's do something radical. Let's do the Euclidean algorithm backwards! Why would we want to do this you ask? Well, it will give us solutions to diophantine equations as in question 2 above!

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \quad \text{from equation 7} \\
&= 3 - 1(5 - 1 \cdot 3) \quad \text{from equation 6} \\
&= 2 \cdot 3 - 1 \cdot 5 \\
&= 2(8 - 1 \cdot 5) - 1 \cdot 5 \quad \text{from equation 5} \\
&= 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3(13 - 1 \cdot 8) \quad \text{from equation 4} \\
&= 5 \cdot 8 - 3 \cdot 13.
\end{aligned}$$

This might seem pointless, but if we recall question 2a), we have now found integers $x = 5$ and $y = -3$ that solve the diophantine equation $8x + 13y = 1$. Why do we care, well the questions below will answer that!

Before we do the next batch of questions, we have a simple definition to make.

Definition. The set of elements in $\mathbb{Z}_n$ which have inverses is called the **group of units** and it is denoted $\mathbb{Z}_n^*$.

For example, we have

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} \quad \text{and} \quad \mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Now it's time to do some questions from group 2 below. Questions 9 and 12 are worth pushing yourselves to think about.

Group 2 Questions

5. Find an integer solution to $26x + 38y = 6$.

6. Find 8^{-1} in $\mathbb{Z}_{13}$. *Hint: There's a quick way to do this using the solution to the diophantine equation we just found on the board.*

7. (a) Calculate $\gcd(23, 29)$ using the Euclidean algorithm.
   (b) Find an integer solution to the Diophantine equation $23x + 29y = 1$.

(c) Find 23^{-1} in $\mathbb{Z}_{29}$.

8. What is 411^{-1} in $\mathbb{Z}_{757}$?

9. This question is to guide you through working out when inverses exist and when they do not.

   (a) Prove $\gcd(a, b) = 1$ **if and only if** there are integers x and y such that $ax + by = 1$. Think carefully about what "if and only if" means.

   (b) Prove that if $\gcd(a, b) = 1$ then a has an inverse in $\mathbb{Z}_b$.

   (c) Prove that if a has an inverse in $\mathbb{Z}_b$, then $\gcd(a, b) = 1$.

   (d) For which n is $\mathbb{Z}_n$ a field? Prove it.

   It is worth taking a look back at question 3 and seeing if things agree with question 9.

10. We say $\mathbb{Z}_n$ is a **domain** if whenever $ab = 0$, either $a = 0$ or $b = 0$ (or both). For which n is $\mathbb{Z}_n$ a domain? Can you prove your conjecture?

11. Prove the Euclidean algorithm always gives you the greatest common divisor.

12. List all the squares in $\mathbb{Z}_7^*$. How many are there? How about $\mathbb{Z}_{11}^*$, $\mathbb{Z}_{13}^*$ and $\mathbb{Z}_{15}^*$? Do you notice any patterns?

Before we begin the next section, it is worth noting here that question 9 guides you through a proof that $\mathbb{Z}_n$ is a field if an only if n is a prime number. From here on in, we will only really be paying attention to $\mathbb{Z}_p$ for p prime.

Squares in $\mathbb{Z}_p^*$

This section is all about finding squares in $\mathbb{Z}_p^*$. If we spend a bit of time on question 1e) above, we notice that $\sqrt{-1}$ exists in $\mathbb{Z}_7$ but not in $\mathbb{Z}_{13}$. This is kind of strange, and it raises the question of when does $\sqrt{-1}$ exist in $\mathbb{Z}_p$? What about $\sqrt{2}$ or $\sqrt{-3}$. Now the fun begins!

Let's see which squares actually exist in $\mathbb{Z}_7^*$ and $\mathbb{Z}_{13}^*$. We respectively have the tables

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

x	1	2	3	4	5	6	7	8	9	10	11	12
x^2	1	4	9	3	12	10	10	12	3	9	4	1

.

Looking at this we that since $12 \equiv -1 \mod 13$, -1 has a square root (in fact it has two, 5 and 8). Well, let's do some more examples, and this time we will write the elements of $\mathbb{Z}_p^*$ slightly differently.

For $\mathbb{Z}_{11}^* = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$ we have

x	± 1	± 2	± 3	± 4	± 5
x^2	1	4	-2	5	3

so we see

$$\begin{aligned} \text{Squares in } \mathbb{Z}_{11}^* \text{ are: } & 1, 4, -2, 5, 3, \quad \text{and} \\ \text{Non-squares in } \mathbb{Z}_{11}^* \text{ are: } & -1, -4, 2, -5, -3. \end{aligned}$$

Interesting. Let's do some more examples. For $\mathbb{Z}_{13}^* = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6\}$ we have

x	± 1	± 2	± 3	± 4	± 5	± 6
x^2	1	4	-4	3	-1	-3

so we see

$$\begin{aligned} \text{Squares in } \mathbb{Z}_{13}^* \text{ are: } & \pm 1, \pm 3, \pm 4, \quad \text{and} \\ \text{Non-squares in } \mathbb{Z}_{13}^* \text{ are: } & \pm 2, \pm 5, \pm 6. \end{aligned}$$

So the squares in $\mathbb{Z}_{11}^*$ act a little different to the squares in $\mathbb{Z}_{13}^*$. Okay, so what's so special about primes? Well, let's see. For $\mathbb{Z}_{15}^* = \{\pm 1, \pm 2, \pm 4, \pm 7\}$ we have

x	± 1	± 2	± 4	± 7
x^2	1	4	1	4

so we see

$$\begin{aligned} \text{Squares in } \mathbb{Z}_{15}^* \text{ are: } & 1, 4, \quad \text{and} \\ \text{Non-squares in } \mathbb{Z}_{15}^* \text{ are: } & -1, \pm 2, -4, \pm 7. \end{aligned}$$

From these examples, what do we notice?

- In the cases for $\mathbb{Z}_p^*$ where p is a prime, exactly half of the elements are squares and the other half are not.
- When p is a prime, each square in $\mathbb{Z}_p^*$ has two square roots. This doesn't happen in $\mathbb{Z}_{15}^*$ since 4 has four square roots, namely ± 2 and ± 7.

Let's try and figure out why the second point is true. First notice that in $\mathbb{Z}_p$, if $ab \equiv 0 \mod p$ then $a \equiv 0 \mod p$ or $b \equiv 0 \mod p$ (note this doesn't happen if p is not prime, since in $\mathbb{Z}_{15}$ we have $3 \cdot 5 \equiv 0 \mod 15$). Why is this?

Well, assume $ab \equiv 0$ and $a \neq 0 \mod p$. We are going to force $b \equiv 0 \mod p$. Since $\mathbb{Z}_p$ is a field, a^{-1} exists so we have

$$\begin{aligned} & ab \equiv 0 \mod p \\ \implies \quad & a^{-1}ab \equiv a^{-1}0 \mod p \\ \implies \quad & b \equiv 0 \mod p \end{aligned}$$

and we're done! Now we can try our hand at proving the first statement above thoroughly. Remember, a proof is simply an argument that is just about impossible to disagree with.

Theorem. *Let $p \geq 3$ be a prime and suppose a in $\mathbb{Z}_p^*$ is a square, that is $a \equiv b^2 \mod p$ for some b in $\mathbb{Z}_p^*$. Then a has exactly 2 square roots, namely b and $-b$.*

Proof. Suppose that a is a square, that is $a = b^2$ for some b. Then we know that $a = (-b)^2$, so we see that if a is a square, it certainly has at least the two square roots that we want. Now we will argue that there are no more by assuming there is another one, and showing it is actually either b or $-b$.

Assume $c^2 \equiv a \mod p$. Then we have $a \equiv b^2 \equiv c^2 \mod p$. Rearranging we get

$$c^2 - b^2 \equiv 0 \mod p$$

which after factoring we have

$$(c-b)(c+b) \equiv 0 \mod p.$$

Now, since we're in $\mathbb{Z}_p$ for some prime p, we know this means that either $c - b \equiv 0 \mod p$ or $c + b \equiv 0 \mod p$. Therefore we have $c \equiv b \mod p$ or $c \equiv -b \mod p$, and we have shown that if there is a square root, it had better be either b or $-b$. ■

What we have shown here is actually quite powerful. If a number has a square root, then there are exactly two! This is the kind of behaviour that we would like, because it is the behaviour we see on the real numbers.

We now have the tools to attack the group three problems. Definitely spend some time on questions 13, 16, and 17 and look carefully for patterns.

Group 3 Questions

13. List all the squares and non-squares in $\mathbb{Z}_7$, $\mathbb{Z}_{17}$ and $\mathbb{Z}_{19}$. Which of $\mathbb{Z}_7$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$, $\mathbb{Z}_{17}$ and $\mathbb{Z}_{19}$ have -1 as a square? Which of the primes $\{7, 11, 13, 17, 19\}$ can be written as $x^2 + y^2$ for some integers x and y?

14. (a) Prove Wilson's theorem: if p is a prime then $(p-1)! \equiv -1 (\text{mod } p)$.
    Hint: pair up each element of $\mathbb{Z}_p^*$ with its inverse. Which elements are their own inverses? Try it for small primes first to look for patterns.

    (b) If $p \equiv 1 (\text{mod } 4)$, prove $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 (\text{mod } p)$, and thus $\sqrt{-1}$ is in $\mathbb{Z}_p$.

15. Prove that for an odd prime, $\mathbb{Z}_p^*$ has exactly $\frac{p-1}{2}$ squares.

16. For each prime $p < 100$, determine whether p can be written in the form $x^2 + 3y^2$ for integers x and y.

17. For each prime $p < 100$, determine whether -3 is a square in $\mathbb{Z}_p^*$. Do you notice anything? Can you prove it?

Euler's Criterion

As we can see from the problems, finding squares in $\mathbb{Z}_p^*$ is difficult. However, we do have a nice tool called Euler's criterion. To get there, we first need to define the Legendre symbol as follows.

Let p be an odd prime and a and element of $\mathbb{Z}_p^*$. Then we define the **Legendre symbol** as

$$\left(\frac{a}{b}\right) := \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is a non-square mod } p \end{cases}.$$

For example, we know -1 is not a square in $\mathbb{Z}_{13}$ but it is in $\mathbb{Z}_7$. So we have

$$\left(\frac{-1}{7}\right) = -1 \quad \text{and} \quad \left(\frac{-1}{13}\right) = 1.$$

So how do we calculate the Legendre symbol in general without looking for the squares in $\mathbb{Z}_p^*$? Well, lucky for us, we have Euler's criterion which tells us that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

For example, the calculation

$$\left(\frac{3}{11}\right) \equiv 3^5 \equiv 243 \equiv 1 \mod 11$$

tells us that 3 is a square in $\mathbb{Z}_{11}$.

Now we have the machinery to look at the last group of questions.

Group 4 Questions

18. Use Euler's criterion to calculate $\left(\frac{2}{101}\right)$ by hand.

19. Let p be a prime and prove that if a, b in $\mathbb{Z}_p^*$ are non-squares, then ab is a square in $\mathbb{Z}_p^*$.

20. (a) We will now try to calculate $\left(\frac{2}{p}\right)$. Let's do an example using Euler's criterion, but we will calculate it slightly cleverly! Let $p = 13$. Then the calculation

$$2^6 \equiv \frac{2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 5} \equiv \frac{2 \cdot 4 \cdot 6 \cdot (-5) \cdot (-3) \cdot (-1)}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} \equiv (-1)^3 \equiv -1 \mod 13$$

shows us that $\left(\frac{2}{13}\right) = -1$. Generalise this to determine $\left(\frac{2}{p}\right)$ for all primes $p \geq 3$.

(b) Use a similar method to part (a) to calculate $\left(\frac{-2}{p}\right)$ for all primes $p \geq 3$.

(c) For each prime less than 100, determine whether or not p can be written as $x^2 + 2y^2$ for integers x, y. Are these the primes you expected? Any conjectures?

(d) How far can you push the method in parts (a) and (b)? Can you calculate $\left(\frac{a}{p}\right)$ for any a and any primes p?

21. Prove Euler's criterion. You will need to use the following fact (which you can try to prove as well if you're bored over breakfast tomorrow morning), called Fermat's Little Theorem.

Fermat's Little Theorem. *Let a be in $\mathbb{Z}_p^*$ for some prime p. Then $a^{p-1} \equiv 1 \mod p$.*

So this is all we have managed to get through, but it has barely scratched the surface of finding squares in $\mathbb{Z}_p$, let alone number theory as a whole. There are so many more questions to ask and so many more to be resolved. If you want to learn more about this stuff, the book

Primes of the form $a^2 + nb^2$: Fermat, Class Field Theory and Complex Multiplication

by David Cox is an excellent place to start. The first few chapters of the book are definitely accessible to you. Good luck!