Math Circles - Number Theory

Tyrone Ghaswala - ty.ghaswala@gmail.com

16th, 23rd November, 2016

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!

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?

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?

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 $a^{p-1} \equiv 1 \mod p$.*

We have barely scratched the surface in this tiny little corner of number theory. There are plenty more questions to ask, and plenty of answers to be found. If you're curious, some things to look up are **quadratic reciprocity** and **quadratic forms**. If you want to learn more about this area of mathematics, whilst getting a fantastic historical recount of these kinds of problems, the book

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

is an excellent place to start, and the first few chapters of the book are definitely accessible to you. Good luck!