Fermat's Little Theorem and Related Results
UCI Math Circle

1 Introduction

Tonight we will be learning about a theorem known as Fermat's Little Theorem which can help us answer questions like *"What is the remainder of* 8^{103} *when divided by 13?"* without even needing to use a calculator, or help us prove statements like *"15 divides* $n^{33} - n$ *for any integer* n*."* While these problems may seem intimidating at first, Fermat's Little Theorem gives us techniques that allow us to quickly find solutions using little more than modular arithmetic. We will begin by going over the basics of modular addition and multiplication, and then explore a number of example problems that will lead up to the statement of the theorem and the solutions of the examples above.

1.1 Acknowledgment

The two main examples in the lesson as well as the challenge problem are taken from Section 20 in Fraleigh's *A First Course in Abstract Algebra.*

2 Directions for the Instructor

Work through the background information portion of the student worksheet together as a class. If the class has little experience with modular arithmetic, it may be helpful to solve some additional examples together or write out addition and multiplication tables for small fields like $\mathbb{Z}_3$ and $\mathbb{Z}_5$. It may be helpful to work only in $\mathbb{Z}_p$ for p prime since all examples in this lesson are done modulo p. The challenge problem in particular requires the existence of a multiplicative inverse for a non-zero element, and introducing rings with zero divisors may cause confusion/ need explanations that are outside the scope of this lesson.

Some problems on the worksheet involve writing an element modulo n as the "negative" of its additive inverse (e.g. 4 is equivalent to -1 modulo 5.) This has the potential to cause confusion for the students, and using addition and multiplication tables to explain additive and multiplicative inverses could prove to be useful, if more explanation is needed than what is provided in the lesson.

3 Worksheet for Students

3.1 Background Information

Suppose you were asked to show that for any integer n it is true that $n^{33} - n$ is divisible by 15. Or suppose instead you were asked to calculate the remainder of 8^{103} when divided by 13. Without knowing the right tools to use, both of the questions look extremely difficult. The first question in particular appears to be a very powerful statement; how could that be possibly true for every single integer n? Perhaps you could use computation software like Mathematica or Wolfram Alpha to help you figure out the answer to the second question, but it still cannot help us answer the first. What if there was an easier way to approach these problems, a method where we could easily find the answer without even needing to use a calculator? As we will see today, there is a very powerful theorem known as *Fermat's Little Theorem* that can help us answer these questions much more easily than we may initially think.

Before we introduce the theorem, let's go over some basics of modular addition and multiplication. Modular addition and multiplication is very similar to the addition and multiplication we are already familiar with. The main difference is that we record the remainder as our answer. This will make more sense with an example. If you were asked to compute $5 + 2$ modulo 6 this means that we add 5 and 2 how we normally would and get 7, then we take the remainder of 7 divided by 6, which is 1. In symbols we would write $5 + 2 \equiv 1 \pmod 6$. The "$\equiv$" symbol is very similar to the "$=$" symbol. It tells us that our solution is not one single number, but a family of them. Notice that 1, 7, 13, and 19 all have a remainder of 1 when we divide them by 6. $5 + 2 \equiv 1 \pmod 6$ just means that 7 is a part of the family of integers that have remainder 1 when divided by 6.

Multiplication modulo n, where n is an integer, is very similar to addition modulo n. We will look at an example. To compute 5×2 modulo 7 we first multiply 5 and 2 how we normally would and get 10. Then, we divide 10 by 7 and record the remainder, which is 3. In symbols, this is $5 \times 2 \equiv 3 \pmod 7$. We are now ready to start working on the problem set. The first few questions are meant to help us prepare for the theorem.

3.2 Problem Set

1. What is a prime number? [Hint: Some examples of prime numbers include 7 and 11. An integer is prime if its only divisors are 1 and ...]

2. Circle the prime numbers in the following list.

1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 12 , 13 , 14 , 15 , 16 , 17 , 18 , 19 , 20

3. What is the prime factorization of 15? [Recall that the prime factorization of an integer is how we may write it as a product of powers of prime numbers. For example, $8 = 2 \times 2 \times 2 = 2^3$.]

4. We know that 15 divides 30. Using your answer to the previous question, what else must divide 30? [Hint: We can write 15 as a product of prime numbers. These numbers must also divide 30. What are they?]

5. Suppose we want to show that an integer is divisible by 15. One way to do it is to show that the remainder of the integer when divided by 15 is 0. What is another way we could show the integer is divisible by 15 using the prime factorization of 15?

6. If a is divisible by b, what is the remainder of a divided by b? [Hint: It might help to think of an easier example at first. We know that 6 is divisible by 3, so the remainder of 6 divided by 3 is...]

7. If a is **not** divisible by b, then what are the possible remainders of a divided by b? [Hint: Think of an easier example first. What integers between 0 and 7 (inclusive) are not divisible by 7? If we try to divide these integers by 7, what are the remainders?]

8. One of the very nice properties the integers have is that given any integer a and any integer b not equal to zero, we may write $a = bq + r$ where q is an integer and r is the remainder of a divided by b. Possible values of r are given by $0, 1, 2 \ldots, |b - 1|$. The two vertical bars around $b - 1$ mean absolute value, or the distance from 0 to $b - 1$. For example, if we let $a = 9$ and $b = 5$ then $9 = 5 \times 1 + 4$. Notice that in this example $q = 1$ and $r = 4$.

   (a) Let $a = 10$ and $b = 2$. What are q and r? Verify that $10 = 2q + r$.

   (b) Let $a = 10$ and $b = 3$. What are q and r? Verify that $10 = 3q + r$.

   (c) Explain why if a is divisible by b that there exists some integer q such that we can write $a = bq$. [Hint: Using the fact that we can always write $a = bq + r$ and your answer to Problem 6, what must r be in this case?]

   (d) Using your answer to part (b), what is 10 modulo 3? That is, what is the remainder of 10 divided by 3. [Hint: Your answer to part (b) already contains the answer. You shouldn't have to do any more work!]

We are now ready for the statement of Fermat's Little Theorem! Don't worry if this seems confusing at first, we will do an example with it shortly.

Theorem 1 (Fermat's Little Theorem)**.** *Let a be an integer and let p be a prime number that does not divide a. Then the remainder of a^{p-1} divided by p is equal to 1. In symbols, we write $a^{p-1} \equiv 1 \pmod{p}$.*

Let's go back to the question that asked us to compute the remainder of 8^{103} when divided by 13.

9. (Fraleigh 20.3) We will compute the remainder of 8^{103} when divided by 13 using the following steps.

   (a) Is 13 a prime number? 13 is a small enough number that you can check this by hand if you are unsure. Pick integers between 2 and 12 inclusive and test each one to see if it divides 13.

   (b) Does 13 divide 8? Have we satisfied the conditions of the theorem?

   (c) Find q and r such that $103 = 12q + r$.

   (d) Write $8^{103} = (8^{12})^q 8^r$ using your values for q and r found above. [Remember the rule that $x^{ab+c} = (x^a)^b x^c$.]

   (e) What can we conclude about the remainder of 8^{12} when divided by 13? Using this, what is the remainder of $(8^{12})^q$ when divided by 13 for the value of q you found above?

(f) You should have found above that $(8^{12})^8 \equiv 1 \pmod{13}$. We have left to determine what 8^7 is equivalent to modulo 13 since $1 \times 8^7 = 8^7$. Notice that $8 + 5 = 13 \equiv 0 \pmod{13}$, so 5 is the additive inverse of 8. That means we can write $8 \equiv -5 \pmod{13}$. Then, $(-5)^7 = (-5)^6(-5)^1 = (25)^3(-5)$. The remainder of 25 modulo 13 is -1, so substituting -1 for 25 above shows us that $(25)^3(-5) \equiv (-1)^3 \times (-5) \pmod{13} \equiv (-1)(-5) \pmod{13}$. Using this, what is the remainder of 8^7 when divided by 13?

(g) Putting everything together, what is the remainder of 8^{103} when divided by 13? [Hint: Look at your answer to the previous question. Why are we done at this step?]

10. (Fraleigh 20.5) We will now show that $n^{33} - n$ is divisible by 15 for any integer n using the following steps.

(a) 15 is not a prime number. Its prime factorization is $15 = 3 \times 5$. To show that $n^{33} - n$ is divisible by 15 it suffices to show that 5 divides $n^{33} - n$ and 3 divides $n^{33} - n$. Let's start with 3. Remember that if we want to use the theorem we have to make sure that 3 does not divide n. Let's see what happens if 3 **does** divide n. Factor $n^{33} - n$ by dividing out one power of n. Why does it follow that 3 divides $n^{33} - n$ for every n?

(b) Suppose now that 3 **does not** divide n. Then since $n^{33} - n = n(n^{32} - 1)$, if we want to show that $n^{33} - n$ is divisible by 3, it must divide $n^{32} - 1$ since it doesn't divide n. Find q and r such that $32 = 2q + r$.

(c) Write n^{32} as $(n^2)^q n^r$ using the values for q and r you found above. Using the theorem, what is this equivalent to modulo 3?

(d) Explain why it follows from the previous question that $n^{32} - 1$ is divisible by 3. [Hint: Remember that if it is divisible by 3 it must have remainder zero. Why does $n^{32} - 1$ have remainder 0?]

(e) Repeat the steps we used above to show that 3 always divides $n^{33} - n$ to show that 5 always divides $n^{33} - n$.

4 Challenge/Take-Home Problem

The challenge problem will make use of another theorem that can be used to prove all kinds of interesting results. It is called Wilson's Theorem and it is stated below.

Theorem 2 (Wilson's Theorem)**.** *Let p be a prime number. Then the remainder of* $(p-1)!$ *when divided by p is $p-1$. Notice that since $p-1+1 \equiv 0 \pmod{p}$, this is the same as saying that the remainder of* $(p-1)!$ *when divided by p is -1. In symbols, if p is prime then* $(p-1)! \equiv -1 \pmod{p}$.

Note that the notation "n!" is read as "n-factorial" and it means to multiply all positive integers less than or equal to n together. For example, $6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1$. Here is your question.

(Fraleigh Ex.20.19) Let p be a prime number greater than or equal to 3. Find the remainder of $(p-2)!$ when divided by p.

5 Solutions to Worksheet

1. A prime number is an integer greater than 1 whose only divisors are one and itself. For example, 4 is not a prime number since we may write it as the product 2×2, but 5 is a prime number since it can only be written as the product 1×5.

2. Here are all the prime numbers between 1 and 20: 2,3,5,7,11,13,17,19.

3. The prime factorization of 15 is 3×5. Notice that $15 = 3 \times 5$ where both 3 and 5 are prime numbers.

4. Since $15 = 3 \times 5$ we know that both 3 and 5 must divide 30. This follows from a more general statement that if a and b are integers such that the greatest common divisor (gcd) of a and b is 1 and a divides c and b divides c, then ab divides c. For those who are interested, here is a proof of the general statement. Since a divides c there exists some integer d such that $c = ad$. Similarly, since b divides c there exists some integer e such that $c = be$. Since the gcd of a and b is 1, there exists f and g such that $af + bg = 1$. Multiplying both sides by c, we have that $caf + cbg = c$. Substituting $c = ad$ and $c = be$, we see that $beaf + adbg = c$ and since ab divides the left hand side of this equation, it must divide c.

5. If we want to show that an integer is divisible by 15, it is enough to show that it is divisible by 3 and 5, since the gcd of 3 and 5 is 1, the previous answer shows that if 3 divides n and 5 divides n, then $3 \times 5 = 15$ divides n.

6. If a is divisible by b, then the remainder of a divided by b must be zero, since $\frac{a}{b}$ is an integer.

7. If a is not divisible by b then the possible remainders of a divided by b are $1, 2, 3, \dots |b-1|$, where $|b-1|$ means the absolute value of $b-1$, or the distance from $b-1$ to 0. Notice that these are all the integers less than $|b|$. Since they are smaller than $|b|$ and not equal to 0, they cannot be divisible by b.

8. (a) Notice that $10 = 2 \times 5 + 0$. We see that $q = 5$ and $r = 0$.

   (b) Notice that $10 = 3 \times 3 + 1$, so $q = 3$ and $r = 1$.

   (c) For any integers a and $b \neq 0$ we can write $a = bq + r$ for some integer q and some remainder r. If b divides a, then b must divide $bq + r$, which means $r = 0$, since the remainder is strictly less than $|b|$. If $r \neq 0$, then a would not be divisible by b since b would not divide r. Hence, we can write $a = bq$ for some integer q.

   (d) All we need to do for this question is look at the remainder in part (b). We see that $10 = 3 \times 3 + 1$, which means that when we try to divide 10 by 3 we get a remainder of 1.

9. (a) 13 is a prime number.

   (b) 13 does not divide 8. We have satisfied all conditions of the theorem since we want to look at the remainder of 8^{103} and have acknowledged that 13 is a prime number that does not divided 8.

   (c) We know that $12 \times 8 = 96$ and $12 \times 9 = 108$, so 8 is the maximum possible value for q. The difference between 103 and 96 is 7, so we see that $103 = 12 \times 8 + 7$. That is, $q = 8$ and $r = 7$.

   (d) We notice that $8^{103} = 8^{12\times 8+7} = 8^{12\times 8} \times 8^7 = \left(8^{12}\right)^8 8^7$.

   (e) Remember that by Fermat's Little Theorem we have that if p is a prime that does not divide a, then a^{p-1} has remainder 1 when divided by p. In this case, $p = 13$ and $a = 8$. Notice that $12 = 13 - 1$, so 8^{12} has remainder 1 when divided by 13. Now, $(8^{12})^8 \equiv (1)^8 \equiv 1 \pmod{13}$. Hence, we see that $(8^{12})^8 \equiv 1 \pmod{13}$.

(f) All we have left to do is compute what the remainder of $(-1)(-5)$ is modulo 13. We know that $(-1)(-5) = 5$, which is still 5 modulo 13. We see that 8^7 has remainder 5 when divided by 13.

(g) Let's put everything together. We showed that $8^{103} = (8^{12})^8 8^7$. Now, when we divide this by 13 we know that $(8^{12})^8$ has remainder 1, so $(8^{12})^8 8^7 \equiv 1 \times 8^7 \pmod{13}$. But we also know that 8^7 has remainder 5 when divided by 13. Hence, $8^{103} \equiv 5 \pmod{13}$.

10. (a) We can factor $n^{33} - n$ as $n^{33} - n = n(n^{32} - 1)$. Since 3 divides n, we know that $n = 3q$ for some integer q. Then $n^{33} - n = 3q(n^{32} - 1)$ and we see that $n^{33} - n$ is a multiple of 3 for any n, so it must be divisible by 3.

(b) Observe that $32 = 2 \times 16 + 0$, so $q = 16$ and $r = 0$.

(c) We write n^{32} as $n^{2\times 16} = (n^2)^{16}$. Because 3 is a prime number, and because we assumed that 3 does not divided n, we know that $n^2 \equiv 1 \pmod 3$, so $n^{32} \equiv 1^{16} \equiv 1 \pmod 3$.

(d) Notice that since $n^{32} \equiv 1 \pmod 3$, we have that $n^{32} - 1 \equiv 1 - 1 \equiv 0 \pmod 3$. This means that when we divide $n^{32} - 1$ by 3 we get a remainder of zero. This means that $n^{32} - 1$ is divisible by 3. Notice that when we try to divide $n(n^{32} - 1)$ by 3 we get that $n(n^{32} - 1) \equiv n \times 0 \pmod 3 \equiv 0 \pmod 3$, so $n^{33} - n$ has zero remainder when we divide by 3 for any n.

(e) suppose that 5 divides n. Then $n = 5q$ for some integer q and we may write $n^{33} - n = 5q(n^{32} - 1)$, so it is a multiple of 5 and thus divisible by 5. If 5 does not divide n, then since 5 is a prime number which does not divide n, we know that $n^4 \equiv 1 \pmod 5$. Since $32 = 8 \times 4$, we know that $n^{32} = (n^4)^8 \equiv 1^8 \equiv 1 \pmod 5$. Hence, $n(n^{32} - 1) \equiv n(1 - 1) \equiv 0 \pmod 5$. Because $n^{33} - n$ is divisible by 5 and 3, and since the gcd of 5 and 3 is 1, we know that $5 \times 3 = 15$ must divide $n^{33} - n$ as well.

6 Solution to Challenge/Take-Home Problem

We know from Wilson's Theorem that $(p-1)! \equiv -1 \pmod p$. Writing out the terms of $(p-1)!$ we see that $(p-1)! = 1 \times 2 \times \cdots \times (p-3) \times (p-2) \times (p-1)$. Notice that if we remove the $(p-1)$ term in the above product then we have $(p-2)!$ Putting this together, we see that following.

$$(p-1)! = \underbrace{1 \times 2 \times \cdots \times (p-3) \times (p-2)}_{=(p-2)!} \times (p-1) \equiv -1 \pmod p$$

$$1 \times 2 \times \cdots \times (p-3) \times (p-2)(p-1)(p-1)^{-1} \equiv -1 \times (p-1)^{-1} \pmod p \text{ (multiply by inverse of } p-1)$$
$$(p-2)! \equiv -1 \times (p-1)^{-1} \pmod p.$$

Notice that $(p-1)(p-1) = p^2 - 2p + 1$ has remainder 1 when divided by p. This means that $(p-1)$ is its own multiplicative inverse when we're working modulo p. In symbols, $(p-1)^{-1} \equiv p - 1 \pmod p$. We substitute this in the equations above.

$$\begin{aligned}(p-2)! &\equiv -1 \times (p-1)^{-1} \pmod p\\ &\equiv -1 \times (p-1) \pmod p\\ &\equiv p + 1 \equiv 1 \pmod p.\end{aligned}$$

Hence, we see that for a prime number p greater than or equal to 3 that $(p-2)! \equiv 1 \pmod p$.