Exercises and Investigations: Set 5

The "Exercises and Investigations" sets for this class are designed both to reinforce mathematical concepts and to lead you to think creatively about problems. You should clearly explain what you tried and how approached each item, even if you do not get to a final solution. Also, it often happens that you gain new insight into an old problem as time goes on and you are thinking about things from a new angle. So, as weeks go on, you may choose to go back and re-explore old problems in place of new ones.

1. Recall Fermat's little Theorem from earlier this quarter. In this exercise, you will develop and explore a related statement. Let $p \neq q$ be prime numbers throughout the exercise.

   (a) Show that if b and c are integers and $1 + pb = 1 + qc$, then p divides c and q divides b. [Hint: You may use the fact that if a prime number divides a product of two integers, then it also divides at least one of the factors.]

   (b) Let a be an integer, and suppose $a \equiv 1 \mod p$ and $a \equiv 1 \mod q$. Show that $a \equiv 1 \mod pq$. [Hint: Use the previous part of the problem.]

   (c) Use Fermat's little Theorem to show that if a is an integer that is divisible by neither p nor q (i.e. $\gcd(a, pq) = 1$), then $a^{(p-1)(q-1)} \equiv 1 \mod pq$. Even if you know *Euler's Theorem* or *group theory* from a previous class, you are not allowed to use them here. This exercise shows that you can derive this result without more advanced mathematics courses! [Hint: Use the previous part of the problem.]

2. Let n be an integer. Let a be an integer that has no prime factors in common with n, i.e. $\gcd(a, n) = 1$. Show that there is an integer b such that $ab \equiv 1 \mod n$. Once again, even if you know *Euler's Theorem* or *group theory* from a previous class, you are not allowed to use them here. This exercise shows that you can derive this result without more advanced mathematics courses! [Hint: Consider $1, a, a^2, a^3, \ldots$. Show that $a^k \equiv a^m \mod n$ for some integers $k \geq m \geq 0$, so $a^m(a^{k-m} - 1) \equiv 0 \mod n$. Now, use the fact that a and n have no prime factors in common to show that n divides $(a^{k-m} - 1)$.]

3. Remember that day near the beginning of the quarter when we all clicked on the lock icon in the address bar in our web browsers near the beginning of class? To remind yourself what we saw, go to `https://www.uoregon.edu`, and click on the lock icon in your address bar. Then click on the Show Certificate button. It should indicate that you are using *RSA*.

   When you transmit information electronically, the letters get converted to numbers (which computers find more palatable). Then, to keep your information secure (which you absolutely care about if you are, for example, transmitting your credit card information as you make a purchase over the internet), those numbers get converted into other numbers, through a process called *encryption*. In case a malicious person intercepts your encrypted data, you want it to be really, really, really hard (essentially impossible) for them to figure out what your original numbers were. You also need it to be quick and easy, though, for someone who needs your information (such as the entity processing your credit card information so

that you can make an online purchase) to be able to figure out what your original numbers were.

RSA is a recipe that makes this happen. In this exercise, we are going to see how RSA works.

When your family and friends inevitably ask you what the math you've been learning "is good for," you can mention RSA encryption.

Let $p \neq q$ be really large prime numbers, and let $N = pq$. Choose an integer e such that $\gcd(e, (p-1)(q-1)) = 1$. Now, broadcast N and e to the world. This is your *public key*. Anytime anyone wants to securely send you a positive integer m less than N, tell them to send you the remainder of $m^e \mod N$, i.e., $m^e \mod N$.

(a) Using the previous two exercises, explain how you can figure out what m is when they send you $m^e \mod N$. What data do you need to calculate and keep secret so that you can easily decrypt the message but an evil person who intercepts your message cannot easily decrypt it? (This information is your *private key*.)

(b) If you now want to send someone a positive integer m less than N, and they already know e and N, what could you send them so that they get your message securely and are still able to decrypt it (without your having to reveal your private key)?

4. An open interval of length d, centered at a point a, on the real number line consists of all points x such that $|x - a| < \frac{d}{2}$. If we replace the usual absolute value by the p-adic absolute value, we get p-adic intervals.

(a) Show that if I and J are p-adic intervals and there is a point a that is contained in both I and J, then one of these intervals is contained in the other. How is this different from the situation for intervals with the usual absolute value?

(b) Show that if I is a p-adic interval and a is in I, then I is centered at a. How is this different (really, really different!!!) from the situation for intervals with the usual absolute value? [Note: If you really want to be blown away, read the link I posted on Canvas about using the p-adic absolute value to show that a square cannot be dissected into an odd number of triangles of equal area.]

5. (Optional Bonus Exercises, Not Required) These are some of the exercises suggested by students in the optional, bonus exercise in Exercises and Investigations 4, as a way to introduce other students to aspects of their collaborative projects for this course. (Note that I have edited some of them for clarity.)

(a) Consider a degree 1 polynomial with integer coefficients. This is a polynomial of the form $f(x) = ax + b$, where a and b are integers. What x gives us $f(x) = 0$? Try writing more such polynomials. Is there something all the zeroes of those polynomials have in common? (Suggested by Nitan)

(b) Find all the zeroes of $2x^3 - 9x^2 + 7x + 6$ that are rational numbers. [Hint: Find out what the *rational root theorem* says, and use it to solve for the zeroes.] (Suggested by Chloe)

(c) Newton's method is used to approximate the roots (i.e. zeros) of a given polynomial $f(x)$, starting from a guess α_0 and using a formula to improve the accuracy of the guess. Let m be the slope of the tangent line of $y = f(x)$ at the point $(\alpha_0, f(\alpha_0))$. So $y = f(\alpha_0) + m(x - \alpha_0)$ is the tangent line to $f(x)$ at α_0. Now you can find a new approximation α_1 by solving

$$0 = f(\alpha_0) + m(\alpha_1 - \alpha_0). \tag{1}$$

This process can be iterated over and over again to find more and more accurate approximations of a root for $f(x)$. Looking at Equation (1), break apart the pieces to understand what each part does in terms of the approximation. Additionally, formulate an explanation for why/how this provides such an accurate approximation for the roots of a polynomial. (Suggested by Morgan)

(d) Suppose you are asked to find the roots of the quadratic function $x^2 + 3x - 3$.You would normally solve this by first looking at c and b (-3 and 3 here), seeing if you could make the trinomial with some trivial binomial multiplication. Finding that there was none, you would use the quadratic equation. Suppose I said you could find a good approximation without using the quadratic equation. You can solve it using iterations of Newton's Method. If you were to graph the equation, you would see that there's a root around 1. Take your first guess, 1, and subtract away $f(1)/f'(1)$.This will give us: $1 - 15 = 45$. Then, we take the second number, and subtract away $f(45)/f'(45)$. This yields: $45 - .044.6 = .7913$. We can continue and continue this process until more and more numbers past the decimal point remain the same, which means that we have gotten a very close approximation to the root. So find an even better approximation, by repeating this process. (Suggested by Hunter)