MATH 8: FINAL REVIEW 1

1. RSA Encryption

To bring the number theory unit to a worthwhile achievement as an endpoint for this year, I briefly introduce RSA encryption. Number theory is used in modern times to encode information so that a target recipient of the information can read it but other people can't - this concept is known as *encryption*.

RSA Encryption goes as follows:

Suppose we want to use number theory to encrypt information - a way of securing a key and a lock, but via multiplication and exponentiation instead of metal and tumblers.

To do this, we will figure out the two basic pieces of cryptography: sending information into something that (hopefully) looks like random noise (known as *encryption*), and then returning that information into readable form (known as *decryption*). Let's begin with the goal of encoding the nubers 0,1,2,3,4 (which we will pretend carry some sort of information) into unreadable format.

Propose that we take each of these numbers and examine what happens to them modulo the prime number 41. Recall that we have $x^{40} \equiv 1 \bmod 41$ from last week's theorem, and thus $x^41 \equiv x \bmod 41$. Recall also that any number coprime to 40 should be invertible mod 40 - we will use the example of 3 and 27. Notice this: $(x^3)^27 \equiv x^{81} \equiv x80 + 1 \equiv 1^2 \cdot x \equiv x \bmod 41$. Thus a message encoded from the numbers 0 through 4 should be unreadable if we cube the numbers to get 0, 1, 8, 27, and 23 mod 41, but when we put each of these numbers to the power of 27 (which we can do via several computational examples) we will receive the original numbers. We'll leave it as an exercise to check that, for example, $23^{27} \equiv 4 \bmod 41$.

2. Encryption and Decryption Mod PQ

The bulk of RSA comes from the fact that large numbers with large factors are relatively hard (often impossible) to factorize efficiently. The famous algorithm that forms a basis for the history of modern encryption is based on the simple idea of combining two of the above encryptions modulo different large prime numbers to get a combined encryption system mod the product of two primes.

3. Review Problems

This week's homework is review problems, to brush up on past topics we covered. **You may use any of the theorems we have proved, so you may want to review them.**

I'll say it one more time, *you may want to review past theorems.*

1. (a) Suppose that $ABCD$ is a parallelogram, and its diagonals are congruent (i.e., the same length). What kind of quadrilateral is $ABCD$? Prove your answer.

(b) Prove that a diameter is the longest chord of a circle. In other words, prove that any chord that is not a diameter must be shorter than a diameter of the circle.

(c) Let $ABCD$ be a quadrilateral whose vertices all lie on the same circle. Now, suppose we take the angle bisector of each of the four angles; we will get four lines, each of which intersects the circle at some point other than the vertex of the angle it is bisecting. Prove that the four resulting intersection points form a rectangle.

2. (a) Come up with a quadratic polynomial with integer coefficients such that its value (when you plug in any integer) is always a multiple of 3.

(b) Come up with a quadratic polynomial with integer coefficients such that its value (when you plug in any integer) is never a multiple of 3.

(c) Let $n > 2$ be an integer; come up with a polynomial of degree n with integer coefficients such that its value is never a multiple of 3.

3. (a) Explain why two circles with the same center but different radii cannot intersect.

(b) Prove that a line cannot intersect a circle at three distinct points.

(c) Prove that two circles cannot intersect at three distinct points.

4. (a) Prove that for any odd prime p, there is some integer $n \geq 2$ such that $p|(2^n - 1)$

(b) Prove that, for any odd prime p and integers $1 < a, b < p$, that the values of $ax + b$ are different mod p for different values of x mod p.

(c) Prove that, for any prime $p \geq 3$, it is impossible to have four different values of x mod p that satisfy $x^3 \equiv 1$.