CRYPTOGRAPHY HANDOUT 07

"DIVIDE AND CONQUER"

(adapted from Number Theory Through Inquiry by Marshall, Odell, and Starbird)

1. Divisibility

In addition to understanding mathematical concepts, we need to practice communicating our understanding. The next exercises will help you to practice writing mathematical explanations.

Example. Here is an example of a mathematical statement (which we write as a *theorem*) with a formal explanation of why it is true (written as a *proof*).

Theorem 1.1. *Let n be an integer. If $6 \mid n$, then $3 \mid n$.*

Proof. Suppose that $6 \mid n$. Then by definition, there exists an integer k such that $n = 6k$. We want to show that there exists another integer k' such that $n = 3k'$. Since $n = 6k = 3(2k)$, then we can choose $k' = 2k$, which concludes that $3 \mid n$. □

Now it's your turn to try writing some proofs. Instructions:

1. Read the theorem.
2. Come up with two examples with your partner(s) so that you believe it is true.
3. Individually write a mathematical proof (most of these will draw on definitions).
4. Switch papers and read your partner's proof. Discuss the good parts as well as anything that is confusing. *Don't take any criticism of your writing personally! Everyone is here to help each other, and the feedback is meant to be constructive.*

Theorem 1.2. *Let a, b, c be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

Theorem 1.3. *Let a, b, c be integers. If $a \mid b$ and $a \mid c$, then $a \mid bc$.*

Theorem 1.4. *Let a, b, c, n be integers with $n > 0$. If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.*

2. Euclidean Algorithm

First, let's get more familiar with the Euclidean Algorithm by doing some examples. Run through the algorithm, and write down the steps for the following pairs of numbers.

1. $a = 96, b = 112$
2. $a = 162, b = 31$

Recall that two integers a and b are *relatively prime* if $\gcd(a, b) = 1$. It can be shown that an equivalent statement is that we can write that there exists integers x and y such that $ax + by = 1$.

Let's do some more proof-writing practice.

Theorem 2.1. *Let a, b, c be integers. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Theorem 2.2. *Let a, b, n be integers. If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.*