CODING THEORY

EDWARD O'CALLAGHAN

Contents

1. Prelude

TODO: Fix notation here...

2. Introduction

In this course we builds up the rudiments of the theoretical framework that unpins many modern day coding methodology. Applications such as ISBN, RSA, bar codes and error correcting with polynomials over finite groups, typically used in things such as wifi IEEE 802.11*. Historical context is given where possible to provide the motivation behind the developments in cryptography.

3. Arithmetic

3.1. **Divisibility.** If a and b ($b \neq 0$) are integers, we say b *divides* a, or b is a divisor of a, if a/b is an integer. We shall denote by $b \mid a$ and conversely $b \nmid a$.

Example 3.1. $2 \mid 4$, however $3 \nmid 4$.

Example 3.2. If $a \in \mathbb{Z}$, then $1 \mid a$ and, for $a \neq 0$, then $a \mid a$; furthermore, $\forall a \in \mathbb{Z}^*$, $a \mid 0$.

Definition 3.3. Given $x, y \in \mathbb{Z}^*$, then $d \in Z$ is called the **greatest common divisor** of x and y if,

- $d > 0$,
- $d \mid x$ and $d \mid y$,
- $\forall f \in Z^* : f \mid x$ and $f \mid y$ then $f \mid d$.

We denote the greatest common divisor d of both x and y by the $d = gcd(x, y)$.

Example 3.4. $gcd(341, 527) = 31$.

Lemma 3.5 (Euclid's Division Lemma)**.**

$$\forall m(m > 0), p \in \mathbb{Z}\exists!q, r \in \mathbb{Z} : 0 \leq r < m \text{ and } p = qm + r$$

Note that we have simply rewritten a division problem in terms of multiplication and addition. Where, p is the dividend; m, the divisor; q, the quotient; and r, the remainder.

By Euclid's lemma we get the oldest known numerical algorithm still in use, Euclid's algorithm. Euclid's algorithm is simply the repeated application of Euclid's lemma.

Example 3.6. To find $gcd(341, 527)$ we do the following;

$$\underline{527} = \underline{341} \cdot 1 + \underline{186}$$

$$\underline{341} = \underline{186} \cdot 1 + \underline{155}$$

$$\underline{186} = \underline{155} \cdot 1 + \underline{31}$$

$$\underline{155} = \underline{31} \cdot 5 + \underline{0}$$

Hence, $31 \mid 341$ and $31 \mid 527$ so $gcd(341, 527) = 31$.

3.2. **Modular arithmetic.** Modular arithmetic is the arithmetic of forgetting. This notion of forgetful arithmetic will become apparent though the following examples given with integers. Note however, that we do not necessarily have to ”read modulo” an integer (e.g., read modulo a polynomial) and we shall explore this in more depth later.

Here are some motivating examples:

Example 3.7.

$$6 \equiv 1 \pmod 5 \tag{1}$$

$$7 \equiv 2 \pmod 5 \tag{2}$$

$$13 \equiv 3 \pmod{10} \tag{3}$$

TODO...

3.3. **Primality testing.** TODO.

3.4. **Prime number generation.** TODO.

3.5. **Random number generation.** TODO.

3.6. **Factorising.** TODO.