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. A $p \in Z^+ : p \neq 1$ is said to be **prime** iff p and 1 are the only divisors of p.

Example 3.4. $2, 3, 5, 7, 11, \cdots$

Definition 3.5. 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 3.6. $gcd(341, 527) = 31$.

Definition 3.7. We say that x and y are **relatively prime** or **coprime** iff $gcd(x, y) = 1$.

Note. Any two distinct primes are ofcourse coprime.

Example 3.8. Given that $gcd(27, 7) = 1$, then we see that 27 and 7 are coprime.

Lemma 3.9 (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 3.10. 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 $gcd(341, 527) = 31$.

We now note that Euclid's lemma can be interprated geometrically as a line. Where we are in actual fact asking how one line divides into another. Thus we have motivation for the following equation:

Corollary.

$$a \cdot x + b \cdot y = gcd(a, b) : x, y \in \mathbb{Z}.$$

Problem 3.11. *Solve:* $341 \cdot x + 527 \cdot y = 31$.

Thus, using the previous result of repeated application of Euclids lemma, that is, Euclids algorithm. We may extend this result as Euclids 'extended' algorithm by working backwards.

$$\begin{aligned}
\underline{31} &= \underline{186} - \underline{155} \cdot 1 && (1)\\
&= \underline{186} - (\underline{341} - \underline{186} \cdot 1) \cdot 1 && (2)\\
&= \underline{186} \cdot 2 - \underline{341} \cdot 1 && \text{(after simplifying)}\\
&= (\underline{527} - \underline{341} \cdot 1) \cdot 2 - \underline{341} \cdot 1 && (3)\\
&= \underline{527} - \underline{341} \cdot 3 && \text{(after simplifying)}
\end{aligned}$$

Hence, we see that $x = -3$ and $y = 1$, however these solutions are **particular**. To find the more general solution set we must look at the homogenous case by finding the kernel.

Notice that, if we subsitute $x = 527t$ and $y = -341t$ into the orginal equation, we have:

$$341 \cdot (527t) + 527 \cdot (-341t) = 0 \qquad \forall t \in \mathbb{Z}$$

However, note also that $31 \mid 527t$ and $31 \mid -341t$ and so we may **reduce** the kernel to $x = 107t$ and $y = -11t$. Hence we have the general solution as given by,

$$x = -3 + 107t, \tag{4}$$
$$y = 1 - 11t \qquad \forall t \in \mathbb{Z}. \tag{5}$$

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 3.12.

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

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

$$13 \equiv 3 \pmod{10} \tag{8}$$

TODO...

3.3. **Primality testing.** TODO.

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

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

3.6. **Factorising.** TODO.