Ciphers and Number Theory Coursework 1

This is an assessed coursework, and will count towards your final grade. Solutions should be handed in to the **mathematics general office** (C123) by **2pm on Monday 8th March**. Late submissions will be penalised. You should show all necessary working.

1. Playfair encode your (full) name using the keyword BIRTHDAY. **[8]**

2. In our definition of the railfence cipher, we started writing the plaintext in the top row, going down and then up. We could instead have started writing from the bottom row, going up and then down. Decipher the message encoded using this method on four rows given by `OIRSE FDNUS ISNOR OAIMI GOUSS N`. **[8]**

3. Find all integer pairs (x, y) satisfying $92x + 28y = 120$. **[8]**

4. Recall that the Fibonacci numbers f_n are defined by setting $f_0 = f_1 = 1$ and

$$f_i = f_{i-1} + f_{i-2}$$

for $i \geq 2$.

   (a) Show that $(f_i, f_{i-1}) = 1$ for all $i \geq 1$.

   (b) Prove by induction that if r_{n+1} is the first remainder equal to 0 in the Euclidean Algorithm, then

$$r_{n+1-k} \geq f_k.$$

[9]

5. A positive integer a is usually written as a sequence of digits $a_t a_{t-1} \ldots a_1 a_0$ with $0 \leq a_i \leq 9$, so that

$$a = \sum_{i=0}^{t} a_i (10)^i.$$

   (a) Show that a is divisible by 13 if and only if the alternating sum of 3 digit numbers

$$a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \ldots$$

   is divisible by 13. (For example, 7893216 is divisible by 13 if and only if $216 - 893 + 007$ is divisible by 13.)

   (b) Which other two prime numbers satisfy the same divisibility test? **[9]**

6. (a) Determine which of the following pair of functions from $\mathbb{Z}_{26}$ to $\mathbb{Z}_{26}$ can be used to define an affine cipher:

$$f(x) = 5x + 11 \mod 26 \qquad g(x) = 6x + 9 \mod 26.$$

   (b) Use this affine cipher to encode your full name.

   (c) Determine the inverse function, and verify that it correctly decodes your name.

[8]