MATH220
Discrete Mathematics and Cryptography

Tutorial 2 **Week starting 2 March 2020**

1. If $n > 0$, show that $\gcd(n, n+1) = 1$. What can you say about $\gcd(n, n+2)$? More generally, what can you say about $\gcd(n, n+p)$ when p is prime?

2. Suppose that $\gcd(a, m) = 1$ and $\gcd(b, m)$=1. Show that $\gcd(ab, m) = 1$.

3. Find $\gcd(117, 173)$ and express it in the form $117x + 173y$ for integers x and y.

4. Find $\gcd(299, 247)$ and all integer solutions of the equation $299m + 247n = 13$.

5. Suppose that $a \mid c$ and $b \mid c$. If a and b are *relatively prime*, show that $ab \mid c$. Give an example where a and b are not relatively prime and ab does not divide c.

6. In one U.S. state, drivers' licences are given a five digit number. The first two digits give the year of birth. The last three digits for a male with month of birth m and day of birth b are represented by $40(m-1)+b$ and for females by $40(m-1)+b+500$.

Determine the dates of birth of two people with licence numbers 42218 and 53953.

7. What can the last digit of a fourth power be?

8. Show that the difference of two consecutive cubes is never divisible by 3 or 5.

9. Setting $a = 0$, $b = 1$, $\ldots$, $z = 25$, the plaintext `atdawn` was encrypted using the affine function $9x + 13$.

(a) What is the ciphertext?

(b) Can you work out the decryption function? This is the function that decrypts the ciphertext into plaintext.

10. The general affine transformation in $\mathbb{Z}_{26}$ is given by

$$y = \alpha x + \beta,$$

where α and β are integers between 0 and 25. But to be able to *uniquely decipher* a piece of ciphertext, there are some restrictions on α.

(a) Show that the transformation $y = 3x + 5$ is legitimate in this sense and find the inverse transformation (which is also affine), that is, find x in terms of y.

(b) Show that the transformation $y = 2x + 5$ is *not* legitimate.

(Find two numbers x_1 and x_2 which encode to the *same* value of y. This means that decoding y is impossible because it would lead to an ambiguous result.)