Algebra – Practical session 15

We will play Question 15.1 as a game. There are no prizes but it should be fun.

• Each of you should work out f^{-1}, then decrypt your favourite letter in the message, and then announce it to the class (let's say *A decrypts to B,* for example).

• The winner of the first letter should not announce further letters, and let the others continue playing the game (except for possibly announcing that you decrypted the whole message, see below). So someone else please decrypt and announce a second letter. Then continue in this way, each time with someone announcing a letter that has not already been found by others.

• At some point someone will have decrypted the whole message (or guessed it from a portion). Please announce that you did for recognition, but do not reveal the decrypted message to others, so they can continue playing.

• If you are in the first practical group (at 10AM), please do not spoil the game for the second group (at 11AM) by disclosing the answer to them.

15.1. A message was turned into a sequence of integers modulo 29 (that is, elements of $\mathbb{Z}/29\mathbb{Z}$) according to the correspondence

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	?	!	⟨*blank*⟩
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Then the message was encrypted according to the affine map $x \mapsto y \equiv 4x + 10 \pmod{29}$ or, just in different notation, $x \mapsto y = [4] \cdot x + [10]$ in $\mathbb{Z}/29\mathbb{Z}$, and became

KZF?OUKGNYGFU?K␣C

(Note that there is one blank character (or space) before the final C.)

(a) Find the decryption map.

(b) Decrypt the message.

15.2. [Use a pocket calculator to answer this question.]
The integer 1441733 is the product of two primes which are not too far apart. Apply the Fermat factorisation trick to find those primes.

15.3. Suppose we have a long string of ciphertext (say made of thousands of letters), in the same 29-letter alphabet as in the previous question. We know that the plaintext was enciphered (or encrypted) using an affine transformation $x \mapsto y \equiv ax + b \pmod{29}$ (after translating it into numbers, and then translating the result back into letters). Suppose we count how many times each letter appears in the ciphertext, and we find that the most frequently occurring letter of ciphertext is "T", and the second most frequently occurring letter is "F". It is then reasonable to assume that these are the encryptions of " " (blank) and "E", respectively, which are the first and second most frequently occurring letters in an English language text written in our 29-letters alphabet.

(a) Find a and b, that is, discover the encrypting transformation.

(b) Find the inverse transformation, that is, the decrypting transformation.

15.4. [Use a pocket calculator to answer this question.]
The integer $n = 363697$ is the product of two primes p and q which are not very close. Hence the Fermat factorisation trick may take a long time (dozens of attempts in this particular example).

However, q happens to be quite close to $3p$. Apply the Fermat factorisation trick to $3n$ and find the primes p and q.