

## MATH 470 Solutions to Homework 1

1. Fred Formal often starts his e-mails with "Hi .....". Eve, who knows Fred uses an affine cipher, intercepts his encrypted e-mail. The first 3 letters of the codetext are AHR. Can you reconstruct Fred's key?

If the conjecture is correct then the first two letters of the ciphertext must correspond to the plaintext "hi". In this case,  $h \rightarrow A$  and  $i \rightarrow H$ . The affine cipher is  $y = \alpha x + \beta \pmod{26}$  where  $x$  is the plaintext letter and  $y$  the corresponding ciphertext letter. Thus since  $A = 0$ ,  $H = 7$ ,  $i = 8$  we have the pair of equations

$$0 = 7\alpha + \beta \quad 7 = 8\alpha + \beta$$

Subtracting immediately gives  $\alpha = 7$  and then the first gives  $\beta = -49 \pmod{26} = 3$ . Thus the cipher encoding was  $y = 7x + 3$  and since  $7 \cdot 15 \equiv 1 \pmod{26}$  we find that the inverse (decoding) transformation is  $x = \frac{1}{7}(y - 3) \equiv 15(y - 3) \equiv 15y + 7 \pmod{26}$ .

2. Ciphertext3 came from a Vigenere cipher. You have to determine the keyword. The "correct" answer should consist of the keyword + your work in how this was obtained. I assume you used some code to do this and possibly some "obvious observations". Part of the assignment is to convince a third party (here the grader) that you have actually cracked the code. Thus you should include all supporting evidence.

```
oiiqrmljtlwdowboewikcehesbjmlvpbhxyaedmylyqvvhxsmhfilauctsunyvdmtau
oghnonafhxwxabufeqaihbjtctuaflzbxbeewaabklmkmoqmtmfekatewpechcqrrvf
klcuxuoytumlrzustyaugkfxfqakvzemoaulhzdglmrefmlezgcajupaldsuloaflyok
larelesklmdbskblmktixeufrnburoktqdtafavrqlbohvsmslpoaejupaldslaulel
zjhfbobxakpfymvparatonntmhzflrhepngllxzqslzbtbhlrhxlvpbhxyerxtmiglp
vnszekhnlxaackfbttumlrzusnzunzatalaqcauuqnlgnmpxtalunolztbvzoyateivxy
tsbhtiqtbjoiioqrtyaugkfhtudyprtxlztajqnmbybufhxwalrhxpahnempocbwtek
lzckfbtbvzulleadlkwhypwapohvvztkvxselftxyeuzfimbfihupeilzdbusogdtivo
xemaqrhmfhxrqypvddbzgsxkpelwutxatilpypkvheflztivxytsbhtiqtbjoiioqrivr
tapetrwqrxtmiglpptyfitsxyobxnxymbelfoyyqnlzcrhzaefeilaqcauuqnlletavgg
aatildmsnupiljavxyqdnufiateehfegpzemlqnmoogagrr
```

[there are no spaces in the ciphertext - just there for printing purposes.]

This just has to follow the technique fo the book - calculate lots of inner products.

On the web page you will find some commented C code - vigenere\_solve.c Copy and compile (cc -o vigenere\_solve vigenere\_solve.c -lm), then run by the command  
> vigenere\_solve ciphertext