**Internet Security (CI6240)**

Lab Exercise for Lecture 2: “Mathematical Revision”

**Exercise 1: Prime and Relatively Prime Numbers**

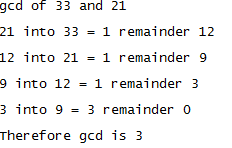
1. Use the Sieve of Eratosthenes to find all prime numbers between 101 and 150.

No highest factor than 11

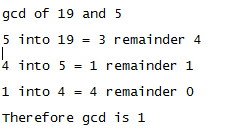
Prime numbers are:



1. Use the Euclidean algorithm to determine greatest common divisors of the following pairs of integers:
2. 33 and 21



1. 19 and 5



1. 15 and 16



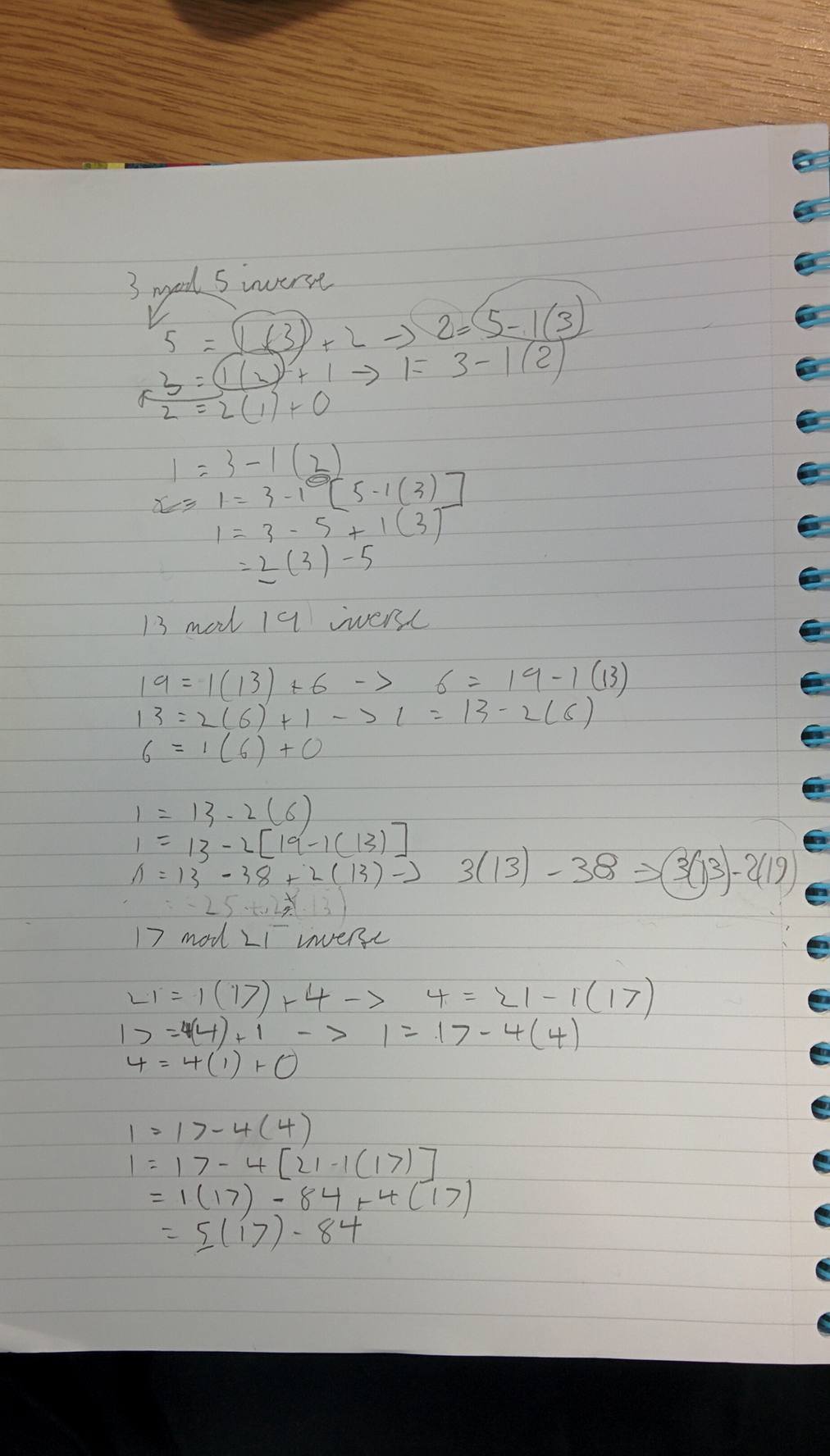
Gcd is 1

What do (b) and (c) have in common?

The gcd is 1

**Exercise 2: Modular Arithmetic**

1. Calculate the following:
2. 21 mod 5 = 1
3. -5 mod 10 = -5 (10 goes 0 times into 5, remainder -5)
4. (17+13) mod 15 = 0
5. (21-35) mod 40 = 26
6. Use the Extended Euclidean Algorithm to determine the multiplicative modular inverses of the following:
7. 3 mod 5
8. 13 mod 19
9. 17 mod 21



1. Why is it impossible to find the modular inverse of 5 mod 15?

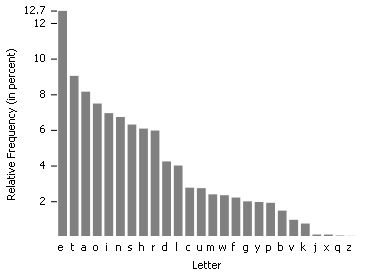
Because there is instantly a remainder of 0, so it’s impossible to divide 0 into 5

**Exercise 3: Number Bases and Logic**

1. Convert the following decimal numbers both to hexidecimal and binary:
2. 35 Hex = 0x23 (16 goes into 35 twice, remainder 3, so reading the digits bottom to top just reads 23, expressed in Hex is 0x23)
3. 25
4. 117
5. 255
6. Find A⊕B when:
7. A=1010, B=1100 (binary)
8. A=0xA5, B=0x4E (hexadecimal)
9. A=211, B=31 (decimal)
10. The decimal number A=211 is represented in 8 bits. Calculate the value of:
11. A right-shifted 4 bits.
12. A left-shifted 3 bits.
13. A right-shifted 8 bits

Giving your answers in both decimal and hexadecimal.

**Exercise 4: Frequency**



The diagram above shows a histogram of the frequencies of letters in a typical English document. You have a document which contains 158714 characters.

1. Which letter would you expect to appear most often in your document. About how many times should it appear?
2. A printer error has made the letters “r” and “g” unrecognizable, though they can still be distinguished from each other. One unreadable letter appears 9523 times and the other 4750 times. Use the histogram above to determine which letter is which.
3. Can you think of any applications this histogram may have in the deciphering of secret messages?

Full solutions will be posted online next week.