MATH 220

Discrete Mathematics and Cryptography

Tutorial 1 **Solutions**

---

1. Let $f(x) = \alpha x + \beta \bmod 26$ be the affine function. Since `do` is the first two letters of the plaintext, we know that

$$\begin{aligned} 3\alpha + \beta &\equiv 10 \bmod 26 \\ 14\alpha + \beta &\equiv 17 \bmod 26 \end{aligned}$$

as `d`=3, `K`=10, `o`=14, and `R`=17. Subtracting these equations, we obtain

$$11\alpha \equiv 7 \bmod 26.$$

By trial and error, we deduce that $\alpha = 3$ and so $\beta = 1$. The encryption function is

$$f(x) = 3x + 1 \bmod 26.$$

Thus `O` decrypts to the value of x for which

$$3x + 1 \equiv 14 \bmod 26$$

as `O`=14, that is, `O` decrypts to `n`. Similarly, `N` decrypts to `e`, and the plaintex is `done`.

2. Now $a = 0$ so, as $2(0) + 1 = 1 \pmod{26}$, `a` is encrypted to `B`. But $n = 13$ so, as $2(13) + 1 = 1 \pmod{26}$, `n` is also encrypted to `B`.

3. Consider $c_1 + c_2 = m + k_A + c_1 + k_B = m + k_A + m + k_A + k_B = k_B$. So we can recover k_B. Then $m = c_3 + k_B$. This gives

$$m = 01001000\ \ 01101001\ \ 00100000\ \ 01010101\ \ 01000011.$$

Which is 48 69 20 55 43 in hex, and therefore Hi UC in ASCII.

4. (a) Since $a \mid b$, we can write $\frac{b}{a} = m$, that is, $b = ma$ for some integer m. Similarly $c = nb$ for some integer n. Then

$$c = nb = n(ma) = (nm)a.$$

So $\frac{c}{a}$ is an integer and this implies that $a \mid c$.

(b) Now $\frac{b}{a} = m$ is an integer and so $b = ma$. Therefore $bc = mac$ which implies that $ac \mid bc$.

(c) Put $b = ua$ and $c = va$, where u and v are integers. Then

$$mb + nc = mua + nva = (mu + nv)a$$

and so, as $mu + nv$ is an integer, $a \mid (mb + nc)$.

(d) Since $\frac{b}{a} = m$ is an integer and $m \neq 0$ as $b \neq 0$, it follows that

$$\frac{|b|}{|a|} = \left|\frac{b}{a}\right| = |m| \geq 1.$$

In particular, $|b| \geq |a|$.

(e) If $a \mid b$ and $b \mid a$, then $b = ma$ and $a = nb$ for some integers m and n. Therefore

$$b = ma = mnb$$

so that $mn = 1$. In particular, $m, n = \pm 1$ and this implies that $a = \pm b$.

5. Note that $n^2 - n = n(n-1)$ and so, as one of n and $n-1$ is even, $n^2 - n$ is even. Since 2 is the only even prime, this implies that $n^2 - n = 2$, that is $(n+1)(n-2) = 0$, so $n = -1$ or $n = 2$.

6. (a) $168 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 = 2^3 \cdot 3 \cdot 7$ and $192 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^6 \cdot 3$.

(b) The number of distinct positive divisors of 168 and 192 are

$$(3+1) \cdot (1+1) \cdot (1+1) = 16$$

and

$$(6+1) \cdot (1+1) = 14,$$

respectively. Furthermore,

$$\gcd(168, 192) = 2^3 \cdot 3 = 24.$$

7. (a) Since n is non-prime, we can write $n = ab$ for some integers a and b, where $1 < a \leq b$. Now a has a prime factor. Call this factor p. Then, as $p \leq a$ and $a \leq b$, we have $p^2 \leq ab = n$.

(b) If 467 is not a prime, then, by (a), it has a prime factor p such that $p^2 \leq 467$, that is, $p \leq \sqrt{467} < 22$. Since neither 20 nor 21 are prime, it follows that $p \leq 19$.

(c) To deduce that 467 is prime, it follows by (b) that we simply need to check that none of $2, 3, 5, 7, 11, 13, 17, 19$ divides 467. A routine check shows that this is indeed the case.

8. If j is an integer between 1 and $n+1$, then, since

$$(n+1)! = (n+1) \cdot n \cdot (n-1) \cdots j \cdots 1,$$

j divides $(n+1)!$ and therefore j divides $(n+1)!+j$. So $(n+1)!+j$ has a non-trivial divisor if $2 \leq j \leq n+1$ and therefore $(n+1)!+j$ is composite.

9. The key phrase is

```
a r c h i m e d e s
```

and the message reads

```
most urgent stop all members of glider team killed stop
in contact with norsk hydro informant stop red penguin frenzy stop
do not send follow up team untill i give coordinates and time for safe
landing zone end
```