MATH 220
Discrete Mathematics and Cryptography

Tutorial 2 **Solutions**

1. If $d \mid n$ and $d \mid (n+1)$ then, by 1(c), $d \mid ((n+1)-n)$, that is, $d \mid 1$. Therefore $d = \pm 1$ are the only common divisors of n and $n+1$. So $\gcd(n+1, n) = 1$. (You can also do this via Euclid's Algorithm.)

Similarly, if $d \mid n$ and $d \mid (n+2)$, then $d \mid ((n+2)-n)$, that is, $d \mid 2$. Therefore $d = 1$ or $d = 2$. (We need only look at positive divisors.)

Two cases depending upon whether n is odd or even:

(i) If n is odd, then $2 \nmid n$ and so $\gcd(n, n+2) = 1$.

(ii) If n is even, then $2 \mid n$ and so $\gcd(n, n+2) = 2$.

In the same way, if p is prime, then $d \mid n$ and $d \mid (n+p)$ and so $d \mid ((n+p)-n)$. That is, $d \mid p$. This means that (again assuming d is positive) $d = 1$ or $d = p$. Again there are two cases:

(i) If $p \nmid n$, then $\gcd(n, n+p) = 1$.

(ii) If $p \mid n$, then $\gcd(n, n+p) = p$.

2. One way to do this is via prime factorisation. Suppose that $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$, but $\gcd(ab, m) \neq 1$. This means that ab and m have a *prime* factor p in common, that is, there is a prime p such that $p \mid ab$ and $p \mid m$. Since $p \mid ab$ and p is prime, either $p \mid a$ or $p \mid b$. This now means that either p divides both a and m, or p divides both b and m, contradicting the assumptions that $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$.

3. Using Euclid's Algorithm,

$$\begin{aligned} 173 &= 117 + 56 \\ 117 &= 2 \times 56 + 5 \\ 56 &= 11 \times 5 + 1 \end{aligned}$$

So $\gcd(173, 117) = 1$. Working backwards,

$$\begin{aligned} 1 &= 56 - 11 \times 5 \\ &= 56 - 11(117 - 2 \times 56) = 23 \times 56 - 11 \times 117 \\ &= 23(173 - 117) - 11 \times 117 \\ &= 23 \times 173 - 34 \times 117 \end{aligned}$$

So $1 = 117x + 173y$ has a solution $x = -34$ and $y = 23$.

4. Using Euclid's Algorithm,

$$\begin{aligned} 299 &= 1 \times 247 + 52 \\ 247 &= 4 \times 52 + 39 \\ 52 &= 1 \times 39 + 13 \\ 39 &= 3 \times 13 + 0 \end{aligned}$$

So $\gcd(299, 247) = 13$. Working backwards,

$$\begin{aligned} 13 &= 52 - 39 \\ &= 52 - (247 - 4 \times 52) = 5 \times 52 - 247 \\ &= 5 \times (299 - 247) - 247 \\ &= 5 \times 299 - 6 \times 247 \end{aligned}$$

So one solution of the equation $299m + 247n = 13$ is

$$m = 5, \quad n = -6.$$

The equation is the same as $23m + 19n = 1$ (dividing by the gcd). So the general solution is

$$m = 5 + 19t, \quad n = -6 - 23t,$$

where t is an integer.

5. A neat way to do this is by Euclid's algorithm.

Write $c = ka$ and $c = lb$, where k and l are integers. From Euclid's Algorithm, there exist integers m and n such that $ma + nb = 1$. (Because a and b are relatively prime.) So

$$c = mac + nbc = ma(lb) + nb(ka) = ab(ml + nk).$$

Therefore $ab \mid c$.

If a and b are not relatively prime, then ab need not divide c. For example, take $a = 4$, $b = 6$, and $c = 12$.

6. Since $m \in \{1, 2, \ldots, 12\}$ and $b \in \{1, 2, \ldots, 31\}$

$$40(m - 1) + b \leq 40 \times 11 + 31 < 500,$$

and so the final three digits 218 must refer to a male and similarly 953 to a female.

The equation $40(m - 1) + b = 218$ can be written as

$$40m + b = 258,$$

in which case

$$b \equiv 258 \bmod 40$$

So $b \equiv 18 \bmod 40$, that is $b = 18 + 40t$ for some integer t. Since $1 \leq b \leq 31$, we must have $t = 0$, so $b = 18$ and therefore $m = 6$.

Thus the date of birth is 18 June 1942.

The second case is entirely similar; the date of birth is 13 December 1953.

7. Consider the remainders when x is divided by 10.

$$\begin{array}{rcccccccccc} x & \equiv & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ x^2 & \equiv & 0 & 1 & 4 & 9 & 6 & 5 & 6 & 9 & 4 & 1 \\ x^4 & \equiv & 0 & 1 & 6 & 1 & 6 & 5 & 6 & 1 & 6 & 1 \end{array}$$

So x^4 ends in one of 0, 1, 5, or 6.

8. Now $(n+1)^3 - n^3 = 3(n^2+n) + 1 \equiv 1 \bmod 3$. Therefore $(n+1)^3 - n^3$ is never divisible by 3.

Working in $\mathbb{Z}_5$, we have

$$\begin{array}{rcccccc} n & \equiv & 0 & 1 & 2 & 3 & 4 \\ n^2 & \equiv & 0 & 1 & 4 & 4 & 1 \\ n^2+n & \equiv & 0 & 2 & 1 & 2 & 0 \\ 3(n^2+n) & \equiv & 0 & 1 & 3 & 1 & 0 \\ 3(n^2+n)+1 & \equiv & 1 & 2 & 4 & 2 & 1 \end{array}$$

Therefore $(n+1)^3 - n^3 = 3(n^2+n) + 1$ is never congruent to 0 mod 5, that is, it is never divisible by 5.

9. (a) Now $a = 0$, $t = 19$, $d = 3$, $w = 22$, and $n = 13$, so `a` is encrypted as `N`, `t` as `C`, `d` as `O`, `a` as `N`, `w` as `D`, and `n` as `A`. Thus the ciphertext is `NCONDA`.

(b) The encryption function is $f(x) = 9x + 13$, so if the ciphertext is y, then

$$9x + 13 = y \bmod 26.$$

Solving for x, we get

$$9x = y + 13 \bmod 26,$$

that is

$$x = 3y + 13 \bmod 26$$

as $9^{-1} = 3$ and $3 \cdot 13 = 13$ in $\mathbb{Z}_{26}$. Reversing the roles of x and y, the decryption function is $f^{-1}(x) = 3x + 13 \bmod 26$.

10. (a) For the transformation $y = 3x + 5$ to be legitimate, we need to be able to *invert* it, that is, to be able to find x in terms of y.

We have $3x = y - 5$ and so we need to find the inverse 3^{-1} in $\mathbb{Z}_{26}$. Since $\gcd(26, 3) = 1$, this is possible (and can be done using Euclid's Algorithm). We find that $9 \times 3 = 1$ in $\mathbb{Z}_{26}$, and so $3^{-1} = 9$.

So

$$\begin{aligned} 9 \times 3x &= 9(y - 5) \\ x &= 9(y - 5) = 9y - 45 = 9y + 7 \end{aligned}$$

(b) The transformation $y = 2x + 5$ cannot be inverted since 2^{-1} does not exist in $\mathbb{Z}_{26}$ ($\gcd(26, 2) = 2 \neq 1$).

If, for example, $x_1 = 2$ and $x_2 = 14$, then

$$2x_1 + 5 = 7 = 2x_2 + 5$$

and so x_1 and x_2 encode to the same value of y ($= 7$). This means that $y = 7$ cannot be uniquely decoded.