DISCRETE MATH 37181 TUTORIAL WORKSHEET 8

INSTRUCTIONS. Complete these problems in groups of 3-4 at the whiteboard. Partial solutions at the end of the PDF.

1. Suppose someone tells you that

$$451 \cdot 577 = 260221$$

Use congruences (*i.e.* mod *something*) to prove them wrong. [1]

2. Complete these definitions, and give an example for each.

(a) Two numbers $a, b \in \mathbb{Z}$ are *relatively prime* if

Eg:

(b) Euler's Phi function[2] $\varphi : \mathbb{N}_+ \to \mathbb{N}$ is defined by

Eg:

3. (a) Compute $\varphi(x)$ for $x = 9, 17, 21, 27, 30, 34$.

(b) Test the conjecture that $\varphi(ab) = \varphi(a)\varphi(b)$.
What if a, b are both prime?
What if a, b are both relatively prime?

4. Check digits are used for credit cards too, using the *Luhn algorithm* which is described as follows:

The check digit is computed as follows:
If the number already contains the check digit, drop that digit to form the "payload."
The check digit is most often the last digit.
With the payload, start from the rightmost digit. Moving left, double the value of every second digit (including the rightmost digit).
Sum the digits of the resulting value in each position.
Sum the resulting values from all positions, s.
The check digit is calculated by $10 - (s \mod 10)$.

Date: Week 8 workshop (Wednesday 20, Thursday 21, Friday 22 April).
[1] Try $[\cdot]_d$ for $d = 2, 3, 7, 11, \ldots$.
[2] You will see two styles for the Greek letter "phi": ϕ, φ in lecture slides and problem sheets. Both are okay.

[3]

(a) Find the missing last digit of my Visa card 4321 1234 5678 901x

(b) Check that your own credit card is valid.

(c) Show that if y is a 2-digit number $y = d_1d_2$, then $[d_1 + d_2]_9 = [y]_9$. That is, summing the digits is the same as taking the remainder mod 9.

(d) Check your phone SIM card serial number is valid. [4]

5. Recall the definition of an *affine cipher* with encipherment function $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ defined by $f(X) = [\alpha X + \beta]_{26}$ [5].

(a) Think of a secret word, encode it using $f(X) = 11X + 4$, then write down the encoded word on the whiteboard for your classmates to decode. [6]

(b) Encipher `ilovediscretemath` and `ihatediscretemath` using the affine cipher $f(X) = [13X + 5]_{26}$. What is the decipherment function?

(c) Under what conditions (on α, β) is the encipherment function the same as the decipherment function? [7]

6. (a) Using repeated squaring, compute $4^{129} \mod 13$.

(b) Using repeated squaring, compute $121^{12} \mod 13$.

7. (a) Find $\gcd(126, 95)$.

(b) Find a number $d \in \mathbb{Z}$ so that $95 \cdot d \equiv 1 \mod 126$. [8]

8. (a) Find $\gcd(1261, 195)$.

(b) Find a number d so that $195.d \equiv 1 \mod 1261$. (That is, the multiplicative inverse of 195 in $\mathbb{Z}_{1261}$.)

---

[3] See https://en.wikipedia.org/wiki/Luhn_algorithm or other web search result.

[4] https://www.hologram.io/blog/whats-an-iccid-number-and-why-does-it-matter-for-cellular-iot but just kidding, do the rest of the worksheet and quiz first.

[5] Remember from the lecture, the decipherment function is $g(X) = [\alpha^{-1}(X - \beta)]_{26}$, assuming α has a multiplicative inverse mod 26.

[6] This might be useful:

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
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

[7] that is, find α, β so that $f(X) = [\alpha X + \beta]_{26} \equiv g(X) = [\alpha^{-1}(X - \beta)]_{26}$ for all $X \in \mathbb{Z}_{26}$.

[8] That is, the multiplicative inverse mod 126 of 95.

Brief solutions:

1. $451 = 150.3 + 1, 577 = 192.3 + 1, 260221 = 86740.3 + 1$ so $[]_3$ is not useful. (Neither is $[]_2$ since they are all odd numbers.) $[451]_5 = 1, [577]_5 = 2$ so $[[451]_5.[577]_5]_5 = 2$ but $[260221]_5 = 1$ so the computation is not correct.

3. (a) $\varphi(9) : |\{1, 2, 4, 5, 7, 8\}| = 6$.

   (b) $\varphi(9) \neq \varphi(3)\varphi(3)$ so the conjecture won't work if $a = b$ in general (prime or not). It works when $\gcd(a, b) = 1$. We will prove it next week (but you can try now!)

4. (a) 4321 1234 5678 901x Drop x, then double every second digit:
   2.4, 2.2, 2.1, 2.3, 2.5, 2.7, 2.9, 2.1
   Now add the digits together if they become 2-digits long:
   8, 4, 2, 6, $10 = 1$, $14 = 5$, $18 = 9$, 2
   3, 1, 2, 4, 6, 8, 0
   Now sum all the digits, call this s: $8 + 4 + 2 + 6 + 1 + 5 + 9 + 2 + 3 + 1 + 2 + 4 + 6 + 8 + 0$ and $s = 1 \mod 10$ so the check digit $x = 10 - x = 9$.
   The correct credit card number is 4321 1234 5678 9019. Note that when you repeat the procedure including the check digit (doubling every second after it) the last digit of the result is 0. This is another way the algorithm is described.

5. (a) `hello`
   is $7, 4, 11, 11, 14$. Its not a great choice because of the double ℓ.

   $f(7) = 77 + 4 = 81 \equiv 3$ which is "d".

   $f(4) = 44 + 4 = 48 \equiv 22$ which is "w".

   $f(11) = 121 + 4 = 125 \equiv 21$ which is "v".

   $f(14) = 154 + 4 = 158 \equiv 2$ which is "c".

   `dwvvc`

   (b) 13 is a bad choice because it doesn't have an inverse in $\mathbb{Z}_{26}$ (it is a *zero divisor*), because $13.2 = 26$. So $f(2n) = [26n + 5]_{26} = 5$ which is "f", and $f(2n + 1) = [13(2n + 1) + 5]_{26} = [13 + 5] = 18$ which is "s", so
   `ilovediscretemath`
   becomes
   `fsfsfsfffsfsfffssf`
   and so does
   `ihatediscretemath`

   There is no decipherment function because $\alpha = 13$ does not have an inverse mod 26.

(c) $f(X) = \alpha X + \beta, g(X) = \alpha^{-1}(X - \beta)$ only when α has an inverse, so

$$\alpha = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.$$

Equate (mod 26):

$$\alpha X + \beta \equiv \alpha^{-1}(X - \beta) = \alpha^{-1}X - \alpha^{-1}\beta$$

$$(\alpha - \alpha^{-1})X + \beta(1 + \alpha^{-1}) \equiv 0.$$

This must be true for all values of $X \in \mathbb{Z}_{26}$, so when $X = 0$ we get

$$\beta(1 + \alpha^{-1}) \equiv 0,$$

and when $X = 1$ we get

$$(\alpha - \alpha^{-1}) \equiv 0,$$

but since α ranges between 1 and 25 the only multiple of 26 this can be is 0. Thus for the two functions to be equal we would need $\alpha = \alpha^{-1}$.

Checking the inverses of all α (each member of the class could check one each) we see the only possibilities are $\alpha = 1, 25$.

If $\alpha = 1$ then $f(X) = X + \beta, g(X) = X - \beta$ so $X + \beta \equiv X - \beta$ if and only if $\beta \equiv -\beta$ and the only values this is true are 0 and 13.

So we have $(1, 0)$ and $(1, 13)$ as two possibilities.

If $\alpha = 25 \equiv -1$ then $f(X) = 25X + \beta, g(X) = 25(X - \beta)$ so $25X + \beta \equiv 25X - 25\beta$ if and only if $\beta \equiv -25\beta$ but $-25 = 1$ so the condition is $\beta = \beta$ which is true for any $\beta \in \mathbb{Z}_{26}$.

So we get $(25, b)$ for all $b \in \{0, 1, 2, \ldots, 25\}$.

Final answer:

$$(1, 0), (1, 13), (25, b) \text{ for } b \in \{0, 1, 2, \ldots, 25\}$$

An alternative approach would be just try all pairs (α, β) brute force (there is just a finite list to check).

6. (a) $129 = 128 + 1 = 2^7 + 1$ (as a binary number 1000001).
4
$4^2 = 16 \equiv 3$
$4^4 = 4^2.4^2 \equiv 3.3 = 9$
$4^8 = 4^4.4^4 \equiv 9.9 = 81 \equiv 3$
$4^{16} = 4^8.4^8 \equiv 3.3 = 9$
$4^{32} \equiv 3$
$4^{64} \equiv 9$
$4^{128} \equiv 3$
so $4^{129} = 4^{128}.4^1 \equiv 3.4 = 12$ which is also equivalent to -1 mod 13.

(b) $12 = 8 + 4$ (as a binary number it is 1100). Recall that $[xy]_d = [[x]_d[y]_d]_d$ so to compute $121.121.121.\ldots.121 \mod 13$ we can instead compute $4.4.4.\ldots.4$ because $121 = 9.13 + 4$.
Now $4^{12} = 4^{8+4} = 4^8.4^4$ so
$4^2 = 16 \equiv 3$
$4^4 = 4^2.4^2 \equiv 3.3 = 9$
$4^8 = 4^4.4^4 \equiv 9.9 = 81 = 6.13 + 3 \equiv 3$
so $4^{12} \equiv 9.3 = 27 = 26 + 1 \equiv 1$.

We could also use *Fermat's little theorem*: $a^{p-1} \equiv 1 \mod p$ for any prime p and any $a \in \mathbb{N}$, so $121^{(13-1)} \equiv 1 \mod 13$.

7. (a) $126 = 1.95 + 31$
$95 = 3.31 + 2$
$31 = 15.2 + 1$ so gcd $= 1$.

   (b) Backwards: $1 = 31 - 15(2)$
$= 31 - 15(95 - 3.31) = 46(31) - 15(95)$
$= 46(126 - 95) - 15(95) = 46(126) - 61(95)$ so inverse is $-61 \equiv 126 - 61 = 65$.

   Check: $65.95 = 6175 = 49.126 + 1$

8. (a) 13

   (b) Does not exist.

   Proof: suppose (for contradiction) that there was some $d \in \mathbb{Z}_{1261}$ with $195.d \equiv 1 \mod 1261$. Then
$$1 = d.195 + e.1261$$
then divide everything by 13:
$$\frac{1}{13} = \frac{d.195}{13} + \frac{e.1261}{13}$$
but since 13 divides both 195 and 1261, the RHS is a whole number but the LHS is a fraction $\frac{1}{13}$, contradiciton.

   So in general, a number α has a multiplicative inverse mod n if and only if $\gcd(\alpha, n) = 1$.