Cryptology - Week 3 worksheet

These exercises are to aid your learning on the lecture material from week 3. They build up in difficulty, and a slightly harder version of the final exercise will be on the exam. If you have handed in your homework sheet and understood any feedback given, that should be sufficient revision for the relevant exam question.

1. For each calculation, where possible please give your answer as $a \pmod{n}$ where $0 \leq a < n$.

   (a) Compute $5 + 8 \pmod{10}$. $3 \pmod{10}$

   (b) Compute $8 - 19 \pmod{23}$. $12 \pmod{23}$

   (c) Compute $13 \times 16 \pmod{25}$. $8 \pmod{25}$

(d) Compute the inverse of $6 \pmod{11}$, if it exists.

inverse of $6 \pmod{11}$:

$11 = 1(6) + 5$

$6 = 1(5) + 1$ ← last nonzero remainder = gcd = 1

$5 = 5(1)$ ← continue until remainder = 0

- - - - - - - - - - - -

$1 = 6 - 1(5)$

$= 6 - 1(11 - 1(6))$

$= 6 - 1(11 - 6)$

$= 2(\underline{6}) - 1(\underline{11})$ ← rewrite in terms of 6 and 11

$\Rightarrow 1 = 2 * 6 \pmod{11}$

$\Rightarrow \boxed{2 =}\ 6^{-1} \pmod{11}$

(e) Compute the inverse of 6 (mod 9), if it exists.

$\underline{9} = 1(\underline{6}) + \underline{3}$ ← last nonzero remainder is not 1, so $\boxed{\text{no inverse exists}}$

$\underline{6} = 2(\underline{3})$

(f) Which a (mod 5) have an inverse?

all those for which $\gcd(a,5)=1$

$\Rightarrow$ $\boxed{\text{all numbers except 5,}}$ since 5 is prime

(g) Which a (mod 6) have an inverse?

all those for which $\gcd(a,6)=1$

$\Rightarrow$ $\boxed{a \text{ not divisible by } 2, 3, \text{ or } 6}$

2. (a) Using Euclid's algorithm, find the greatest common divisor (gcd) d of 754 and 512.

$754 = 1(512) + 242$

$512 = 2(242) + 28$

$242 = 8(28) + 18$

$28 = 1(18) + 10$

$18 = 1(10) + 8$

$10 = 1(8) + 2$ ← greatest common divisor is $\boxed{2}$

$8 = 4(2)$

(b) Following the method in the proof of Euclid's corollary, find integers a and b such that $754a + 512b = d$.

$$
\begin{aligned}
2 &= 10 - 8 \\
&= 10 - (18 - 10) \\
&= 2(10) - 18 \\
&= 2(28 - 18) - 18 \\
&= -3(18) + 2(28) \\
&= -3(242 - 8(28)) + 2(28) \\
&= 26(28) - 3(242) \\
&= 26(512 - 2(242)) - 3(242) \\
&= -55(242) + 26(512) \\
&= -55(754 - 512) + 26(512) \\
&= \boxed{-55(754) + 81(512)}
\end{aligned}
$$

3. From this point on, we will write

- $\mathbb{Z}/n\mathbb{Z}$ to denote the set of integers modulo n.
- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ to denote the set of integers modulo p when p is a prime.
- $\mathbb{F}_p^* = \mathbb{Z}/p\mathbb{Z} - \{0 \pmod p\}$ to denote the set of non-zero integers modulo p when p is a prime.

Determine whether or not each of the following are groups G under $*$:

(a) $G = \mathbb{R}$ and $* = +$ (addition).

Yes: 0 is the identity, the inverse of any $x \in \mathbb{R}$ is $-x$, and of course addition is associative. Also the real numbers are closed under addition.

(b) $G = \mathbb{C}$ and $* = \times$ (multiplication).

No: 1 would have to be the identity, but there's no inverse for 0, i.e. no $x \in \mathbb{C}$ s.t. $0x = 1$.

(c) $G = \mathbb{Z}/4\mathbb{Z}$ and $* = + \pmod 4$ (addition mod 4).

yes:
- 0 is the identity
- the inverse of any $x \in \mathbb{Z}/4\mathbb{Z}$ is $-x \pmod 4$
- modular addition is still associative
- $\mathbb{Z}/4\mathbb{Z}$ is closed under addition mod 4

(d) $G = \mathbb{Z}/4\mathbb{Z} - \{0 \pmod 4\}$ and $* = \times \pmod 4$ (multiplication mod 4).

no: it's not closed under $(*)$, since $2 \in G$, but $2 * 2 \equiv 0 \pmod 4$, which isn't in G

(e) $G = \mathbb{F}_5^*$ and $* = \times \pmod 5$ (multiplication mod 5).

yes:
- closed under multiplication mod 5
- 1 is the identity
- all elems have inverses:

  $1 * 1 \equiv 1$
  $2 * 3 \equiv 1$
  $3 * 2 \equiv 1$
  $4 * 4 \equiv 1$
- modular multiplication is associative

(f) $G = \mathbb{F}_p^*$, for p prime, and $* = \times \pmod p$ (multiplication mod p).
Hint: use Fermat's Little Theorem.

yes:
- $\mathbb{F}_p^*$ is closed under multiplication
- 1 is the identity
- by Fermat's Little theorem, for any $a \in \mathbb{F}_p^*$, its inverse is given by a^{p-2}.
- modular multiplication is associative

4. (a) Let φ be the Euler φ-function. Prove that:

(i) If p is prime, the $\varphi(p) = p - 1$.

Let p be prime. Then for any $0<n<p$, we must have $\gcd(p,n)=1$, since the only divisors of p are 1 and p, and p can't be a divisor of any number strictly less than p.

Thus $\varphi(p) = |\{n \in \mathbb{Z} \mid 0<n<m\}| = p-1$.

(ii) If p and q are distinct primes, then $\varphi(pq) = (p - 1)(q - 1)$.

Let p, q be distinct primes.

Then the only divisors of pq are 1, p, q, and pq.

Thus the only numbers $0<n<pq$ with $\gcd(n,pq) \neq 1$ are those divisible by either p or q, i.e. ap for $0<a<q$, and bq for $0<b<p$.

Note $ap \neq bq$ for all $0<a<q$ and $0<b<p$, since

(not sure how to prove this)

$$\begin{aligned}
\text{Thus } \varphi(pq) &= |\{n \in \mathbb{Z} \mid 0<n<pq\}| \\
&\quad - |\{ap \mid 0<a<q\}| - |\{bq \mid 0<b<p\}| \\
&= (pq-1) - (q-1) - (q-1) \\
&= (p-1)(q-1).
\end{aligned}$$

(iii) If p is prime, then $\varphi(p^2) = p(p-1)$.

Since p is prime, the only divisors of p^2 are 1, p, and p^2. Thus

$$\varphi(p^2) = |\{n \in \mathbb{Z} \mid 0 < n < p^2\}| - |\{kp \mid 0 < k < p\}| \leftarrow \text{multiples of } p$$

$$= (p^2 - 1) - (p - 1)$$

$$= p(p-1).$$

(b) Which elements should you remove from $G = \mathbb{Z}/pq\mathbb{Z}$ in order for $(G, * = \times \pmod{pq})$ to be a group? What is the resulting size of G?

You should remove 0, kp for all $0 < k < q$, and kq for all $0 < k < p$.

The resulting size of G is

$$\cancel{|G|} = \varphi(pq) \cancel{-1} \quad \nwarrow \text{from removing } 0$$

$$= \cancel{pq - (p-1)(q-1)} - 1$$

$$= \boxed{\cancel{p + q - 2}}$$

5. (a) Determine whether or not 4 (mod 5) is a generator for the group $\mathbb{F}_5^*$ under operation $* = \times \pmod 5$.

No: $4 \equiv 4 \pmod 5$, but also $4^3 \equiv 64 \equiv 4 \pmod 5$.
Thus 4 cannot generate $\mathbb{F}_5^*$, as the set $\{4, 4^2, \ldots, 4^{|G|}\}$ can have at most $|G|-1$ elements.

(b) Give a generator g for the group $\mathbb{F}_{17}^*$ under operation $* = \times \pmod{17}$. Justify your answer.

k	$3^k \pmod{17}$
1	3
2	9
3	10
4	13
5	5
6	15
7	11
8	16
9	14
10	8
11	7
12	4
13	12
14	2
15	6
16	1

As we can ~~se~~ from the table, $g=3$ works, since all numbers between 1 and 16 have been generated.
Not sure if there was a way to find this besides guess-and-check.

(c) Using Euclid's corollary, find the inverse of g.

$$\underline{17} = 5(\underline{3}) + \underline{2}$$
$$\underline{3} = 1(\underline{2}) + \underline{1}$$
$$\Downarrow$$
$$\begin{aligned} \underline{1} &= \underline{3} - \underline{2} \\ &= \underline{3} - (\underline{17} - 5(\underline{3})) \\ &= 6(\underline{3}) - \underline{17} \end{aligned}$$
$$\Downarrow$$
$$1 = 6 * 3 \pmod{17}$$
$$\Downarrow$$
$$\boxed{g^{-1} = 6.}$$

(d) Using Sun-Tzu's Remainder Theorem, find $x \pmod{17g}$ such that $x \equiv 5 \pmod{17}$ and $x \equiv 2 \pmod{g}$.

Following Thm 3.3, we set $a=5$, $b=2$, $m=17$, $n=3$.

From pt. (c):

$$-1(17)+6(3)=1.$$

Thus $c=-1$, $d=6$, so

$$x = bcm + adn \pmod{mn}$$

$$= 2(-1)(17) + (5)(6)(3) \pmod{51}$$

$$= 56 \pmod{51}$$

$$= 5.$$

And indeed, $5 \equiv 5 \pmod{17}$ and $5 \equiv 2 \pmod{3}$.