Homework 3

1a) Let a, b, c be integers such that

$a \mid c$, $b \mid c$ and $\gcd(a,b) = 1$,

show that $ab \mid c$.

b) Show that $\gcd(a,b) = 1$ is necessary.

Find a, b, c such that $a \mid c$ and $b \mid c$

but $ab \nmid c$.

b)

$a = 6$

$b = 8$

$c = 24$

$\gcd(a,b) = 2$

$ab = 48 \nmid 24 = c$

a)

$c = \prod p_i^{a_i} a'$

$c = \prod q_i^{b_i} b'$

Let $a = \prod p_i^{a_i}$

$b = \prod q_i^{b_i}$ p_i, q_i are primes

Since $\gcd(a,b) = 1$, $p_i \neq q_j \ \forall i, j$

Since $a \mid c$ and $b \mid c$,

$\prod p_i^{a_i}$ and $\prod q_i^{a_i}$ are in the prime factorization of c.

Hence $ab \mid c$.

if $a|c$, $b|c$ and $ab|c$

then is $\gcd(a,b)=1$?

No. Counterexample.

$a=3$

$c=18$

$b=6$

$\gcd(a,b)=3\neq 1$

c) Let $ord(g)$ denote the order of g in a group.
Complete the tables:

In $(\mathbb{Z}_2, +)$

a	$ord(a)$
0	
1	

In $(\mathbb{Z}_3, +)$

b	$ord(b)$
0	
1	
2	

In $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$

(a,b)	$ord(a,b)$
$(0,0)$	
$(0,1)$	
$(0,2)$	
$(1,0)$	
$(1,1)$	
$(1,2)$	

Observe that $ord((a,b)) = ord(a)\,ord(b)$

Prove that this is true for all $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$ where m and n are coprime.

---

c) Let $ord(g)$ denote the order of g in a group.
Complete the tables:

In $(\mathbb{Z}_2, +)$

a	$ord(a)$
0	1
1	2

In $(\mathbb{Z}_3, +)$

b	$ord(b)$
0	1
1	3
2	3

In $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$

(a,b)	$ord(a,b)$
$(0,0)$	
$(0,1)$	3
$(0,2)$	3
$(1,0)$	2
$(1,1)$	6
$(1,2)$	6

Observe that $ord((a,b)) = ord(a)\, ord(b)$

Prove that this is true for all $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$

where m and n are coprime.

$$\boxed{ord((a,b)) = \frac{ord(a)\, ord(b)}{\gcd(ord(a), ord(b))}}$$

Let $d = \text{ord}((a, b))$.

$d \cdot (a, b) = (0, 0)$

$d \cdot a = 0$ and $d \cdot b = 0$

Hence, $\text{ord}(a) \mid d$

$\text{ord}(b) \mid d$

If $\gcd(\text{ord}(a), \text{ord}(b)) = 1$,

then $\text{ord}(a) \cdot \text{ord}(b) \mid d$

Let $e = \text{ord}(a)\,\text{ord}(b)$

$e \cdot (a, b) = (ea, eb) = (0, 0)$

Hence, $d \mid e$

Since $e \mid d$ and $d \mid e$, $d = e$

$\gcd(\text{ord}(a), \text{ord}(b)) = 1$

because $\gcd(m, n) = 1$ and $\text{ord}(a) \mid m$ and $\text{ord}(b) \mid n$

2. Prove the Extended Euclidean algorithm:

For all integers a, b, there exists integers u, v such that

$$au + bv = \gcd(a, b)$$

Extended Euclidean algorithm

Find u, v such that $au + bv = \gcd(a, b)$

1. Set $u = 1$, $g = a$, $x = 0$, and $y = b$
2. If $y = 0$, set $v = (g - au)/b$ and return the values (g, u, v)
3. Divide g by y with remainder, $g = qy + t$, with $0 \leq t < y$
4. Set $s = u - qx$
5. Set $u = x$ and $g = y$
6. Set $x = s$ and $y = t$
7. Go To Step (2)

In general, if a and b are relatively prime and if $q_1, q_2, \ldots, q_t$ is the sequence of quotients obtained from applying the Euclidean algorithm to a and b as in Figure 1.2 on page 13, then the box has the form

$$\begin{array}{cc|c|c|c|c|c}
 & & q_1 & q_2 & \cdots & q_{t-1} & q_t \\
\hline
0 & 1 & P_1 & P_2 & \cdots & P_{t-1} & a \\
\hline
1 & 0 & Q_1 & Q_2 & \cdots & Q_{t-1} & b
\end{array}$$

The entries in the box are calculated using the initial values

$$P_1 = q_1, \qquad Q_1 = 1, \qquad P_2 = q_2 \cdot P_1 + 1, \qquad Q_2 = q_2 \cdot Q_1,$$

and then, for $i \geq 3$, using the formulas

$$P_i = q_i \cdot P_{i-1} + P_{i-2} \qquad \text{and} \qquad Q_i = q_i \cdot Q_{i-1} + Q_{i-2}.$$

The final four entries in the box satisfy

$$a \cdot Q_{t-1} - b \cdot P_{t-1} = (-1)^t.$$

Multiplying both sides by $(-1)^t$ gives the solution $u = (-1)^t Q_{t-1}$ and $v = (-1)^{t+1} P_{t-1}$ to the equation $au + bv = 1$.

Figure 1.3: Solving $au + bv = 1$ using the Euclidean algorithm

3. a) Given integers a, b. Show that if there exists integers u, v such that

$au + bv = 1$

then $\gcd(a, b) = 1$

b) If there exists integers u, v such that $au + bv = 6$, is it always true that $\gcd(a, b) = 6$?

If no, provide a counterexample.

b)

$$a\ u + b\ v = 6$$

$$7 \cdot 1 + 1 \cdot (-1) = 6$$

$$\gcd(a,b) = \gcd(7,1) = \underline{1}$$

4. Find a value x that simultaneously solves the congruences or show that no such value x can exist.

a) $x \equiv 3 \mod 7$

$x \equiv 4 \mod 9$

b) $x \equiv 13 \mod 71$

$x \equiv 41 \mod 97$

c) $x \equiv 7 \mod 9$

$x \equiv 3 \mod 6$

a) $\left.\begin{aligned} x &\equiv 3 \bmod 7 \\ x &\equiv 4 \bmod 9 \end{aligned}\right\}$ $x = 31$

b) $\left.\begin{aligned} x &\equiv 13 \bmod 71 \\ x &\equiv 41 \bmod 97 \end{aligned}\right\}$ $x = 5764$

c) $x \equiv 7 \bmod 9$

$x \equiv 3 \bmod 6$

$$\boxed{\text{Use Exteded Euclidean Algorithm to find } n_1, n_2 \quad m_1 n_1 + m_2 n_2 = 1.}$$

Then $x = x_1 m_2 n_2 + x_2 m_1 n_1$

c) $x \equiv 7 \mod 9$
$x \equiv 3 \mod 6$
$\Bigg\}$ If $\gcd(9,6) = 3$ then no solution ?! NO

Proof:

If x exists, then $\exists\, q, q' \in \mathbb{Z}$

$$x = 9q + 7$$
$$x = 6q' + 3$$

$$0 = 3(3q - 2q') + 4$$

$$4 = (2q' - 3q)3$$

$3 \mid (2q' - 3q)3$ but $3 \nmid 4$

So, there can't be solution

Lemma: $x \equiv a \mod m$
$x \equiv b \mod n$

has a solution for all a, b

iff $\gcd(m, n) = 1$

if $\gcd(m,n) \neq 1$ there could still be a, b s.t. it has solution

$$x \equiv 3 \bmod 7$$
$$x \equiv 4 \bmod 9$$

$x = 31$

Find u, v s.t.

$$7u + 9v = 1$$

Euclidean: $9 = 7 \cdot 1 + 2$

$7 = 2 \cdot 3 + 1$

$$\begin{aligned}
1 &= 7 - 2 \cdot 3 \\
&= 7 - (9 - 7) \cdot 3 \\
&= 7 - 9 \cdot 3 + 7 \cdot 3 \\
&= 7(4) - 9 \cdot (3)
\end{aligned}$$

$u = 4$, $v = -3$

$$x = 3 \cdot 9 \cdot v + 4 \cdot 7 \cdot u$$