2) Number Theory

Definition of divisibility:

Suppose $n, d \in \mathbb{Z}$ with $d \neq 0$.

d divides n if and only if these exists an integer k such that $n = dk$

More formally:

"d divides n" $\iff \exists\, k \in \mathbb{Z}$ such that $n = dk$.

Notation:

$d \mid n$ denoted "d divides n"

Instead of d divides n, we can also say:

- n is a multiple of d
- d is a factor of n
- d is a divisor of n
- n is divisible by d

Notation:

$d \nmid n$ denotes "d does not divide n."

Stating defn symbolically:

$$d \mid n \iff \exists\, k \in \mathbb{Z} \text{ s.t } n = dk$$

$$d \nmid n \iff \nexists\, k \in \mathbb{Z} \text{ s.t } n = dk$$

or

$$d \nmid n \iff \forall\, k \in \mathbb{Z} \quad n \neq dk$$

Properties of divisibility:

1) If $a \mid b$ and $b \mid c$ then $a \mid c$ (Transitivity)

proof: Suppose $a \mid b$ and $b \mid c$.

$a \mid b \Rightarrow b = ak$ for some integer k

$b \mid c \Rightarrow c = bl$ for some integer l.

By substituting:

$c = \ell b \Rightarrow c = \ell(ka)$

$\Rightarrow c = (\ell k)a$

$k \in \mathbb{Z}$ and $\ell \in \mathbb{Z} \Rightarrow k\ell \in \mathbb{Z}$

Let $m = k\ell \in \mathbb{Z}$

So $c = ma$ for some integer $m \in \mathbb{Z}$.

Therefore by defn of divisibility;

$a \mid c$

■

2) If $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ $\forall x, y \in \mathbb{Z}$

proof: Suppose $a \mid b$ and $a \mid c$.

$a \mid b \Rightarrow b = ak$ for some integer k

$a \mid c \Rightarrow c = al$ for some integer l.

Multiplying $b = ak$ by x on both sides:

$$bx = xak \qquad (*1)$$

Multiplying $c = al$ by y on both sides

$$cy = yal \qquad (*2)$$

Adding equations $(*1)$ and $(*2)$

$$bx + cy = xak + yal \Rightarrow bx + cy = a(xk + yl)$$

$x, y, k, l \in \mathbb{Z} \Rightarrow xk + yl \in \mathbb{Z}$. So let $m = xk + yl$.

So $bx + cy = am$ for some integer m

Therefore by defn of divisibility:

$$a \mid (bx + cy)$$

■

3) $\forall a \neq 0,\ a \mid a$

proof: As $a = 1 \times a$, $a \mid a$ ■

4) if $a \mid b$ then $a \mid bc$ for any $c \in \mathbb{Z}$

proof: Suppose $a \mid b$.

$a \mid b \Rightarrow b = ak$ for some integer k.

Multiplying $c \in \mathbb{Z}$ on both sides gives

$$bc = (ak)c \Rightarrow bc = a(kc)$$

So by defn of divisibility:

$$a \mid bc$$

■

5) if $a|b$ and $a|c$ then $a|(b \pm c)$

proof: Suppose $a|b$ and $a|c$.

$a|b \Rightarrow b = ak$ for some integer k

$a|c \Rightarrow c = al$ for some integer l.

$b \pm c = ak \pm al \Rightarrow b \pm c = a(k \pm l)$

$k, l \in \mathbb{Z} \Rightarrow k \pm l \in \mathbb{Z}$ let $m = k \pm l \in \mathbb{Z}$.

$b \pm c = am$ for some integer m

Therefore by definition of divisibility

$a|(b \pm c)$

■

6) if $a|b$ and $b \neq 0$ then $|a| \leq |b|$

proof: Suppose $a|b$.

$a|b \Rightarrow b = ak$ for some $k \in \mathbb{Z}$.

Then $|b| = |ak| \Rightarrow |b| = |a| \cdot |k|$

As $|k| \geq 1$ as $b \neq 0$,

$|b| = |a| \cdot |k| \Rightarrow |b| \geq |a|$

$\Rightarrow |a| \leq |b|$ ■

7) if $a|b$ then $a|(-b)$

proof: Suppose $a|b$

$a|b \Rightarrow b = ak$ for some integer k.

Multiplying both sides by -1,

$-b = -(ak) \Rightarrow -b = -ak$

$\Rightarrow -b = a(-k)$

$k \in \mathbb{Z} \Rightarrow -k \in \mathbb{Z}$

Therefore by definition of divisibility:

$a \mid (-b)$

■

8) if $a \mid b$ and $c \mid d$ then $ac \mid bd$

proof: Suppose $a \mid b$ and $c \mid d$

$a \mid b \Rightarrow b = ak$ for some integer k

$c \mid d \Rightarrow d = cl$ for some integer l.

$bd = (ak)(cl) \Rightarrow bd = ac(kl)$

$k, l \in \mathbb{Z} \Rightarrow kl \in \mathbb{Z}$ and let $m = kl \in \mathbb{Z}$

So $bd = ac(m)$ for some integer m.

Therefore by defn of divisibility:

$ac \mid bd$

■

9) If $a|b$ then $a^2|b^2$

proof: Suppose $a|b$

$a|b \Rightarrow b = ak$ for some $k \in \mathbb{Z}$

Squaring both sides;

$b^2 = (ak)^2 \Rightarrow b^2 = a^2k^2$

$\Rightarrow b^2 = a^2(k^2)$

$k \in \mathbb{Z} \Rightarrow k^2 \in \mathbb{Z}$, let $m = k^2 \in \mathbb{Z}$.

So

$b^2 = a^2m$ for some $m \in \mathbb{Z}$

$\Rightarrow a^2|b^2$ by defn of divisibility.

■

The Division Theorem:

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}$ $d > 0$. Then there exists unique integers q and r such that

$$n = dq + r$$

and

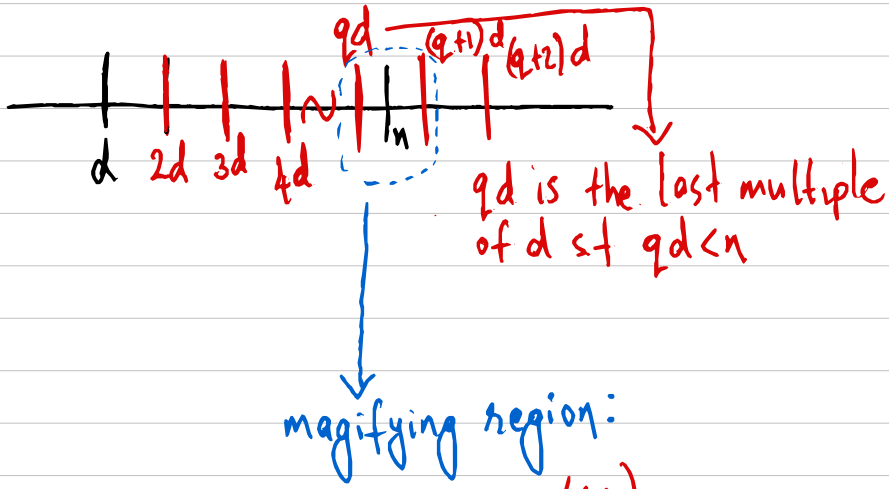
$$0 \leq r < d$$

We call the unique quantities

- $q = q(d,n)$ as quotient
- $r = r(d,n)$ as remainder

Pictorial representation of division theorem:

Place integers on straight line



$\Rightarrow r < d$

Well-Ordering Principle:

Theorem: Let S be a non-empty subset of $\mathbb{N}$, i.e. $S \neq \emptyset$ and $S \subseteq \mathbb{N}$. Then S has a least element

Assume WOP is true, no proof given.

Note: W.O.P is also holds if we take $S \subseteq \mathbb{N}_0$ or $S \subset \{M, M+1, M+2, \ldots,\}$ where M is any integer as long as it fixed.

Proof of Division Theorem:

Define $S \subseteq \mathbb{N}_0$ to be the set

$$S = \{n - kd : k \in \mathbb{Z},\ n - kd \geq 0\}$$

Need to show that $S \neq \emptyset$:

- If $n \geq 0$ then $n - 0 \times d \in S$, then $S \neq \emptyset$
- If $n < 0$ then let $k = n$, Then $n - dn = n(1-d)$
  But $d \geq 1 \Rightarrow 0 \geq 1 - d$
  $n < 0$ and $(1-d) \leq 0 \Rightarrow n(1-d) \geq 0$
  So $n - kd \in S$ exists.

So $S \neq \emptyset$

So by the well ordering principle:

S has a least element, say r.

↳ $r \leq t$ for any $t \in S$. (*1)

↳ if $t < r$ then $t \notin S$ (*2)

By definition of S, elements of S are of form $n - kd$. So for least element r, there must be a corresponding k, say $k = q$ such that

$$r = n - dq$$

Therefore

$$n = dq + r$$

Showing that $0 \leq r < d$:

As $d \geq 1$, $r - d < r$. But $r = n - dq$ So

$$r - d < r \Rightarrow n - dq - d < r$$

$$\Rightarrow n - d(q+1) < r$$

Since r is the least element of S,

$$r - d(q+1) < 0 \qquad \text{(negative)}$$

if $r - d(q+1) \geq 0$, then $r - d(q+1) \in S$ and $r - d(q+1) < r$

↳ impossible as r is the least element (by #1 and #2).

So $r - d(q+1) < 0$ ie if is negative.

$$r - d(q+1) < 0 \Rightarrow r - dq < d$$

$$\Rightarrow r < d$$

Since $r \in S$, $r \geq 0$, by definition of S

Therefore

$$0 \leq r < d$$

Claim: q and r are unique.

↳ almost all uniqueness proof use this method: proof by contradiction

Suppose that q_1, r_1 and q_2, r_2 satisfy the conditions

$$n = dq_i + r_i \quad 0 \le r_i < d$$

where $i \in \{1,2\}$

Assume $q_1 \neq q_2$
Thus without loss of generality, assume

$$q_1 > q_2$$

If $q_1 > q_2$ then $q_1 = q_2 + \alpha$ where $\alpha \ge 1$

Substituting $q_1 = q_2 + \alpha$,

$$n = dq_1 + r_1 = d(q_2 + \alpha) + r_1$$

$$= dq_2 + d\alpha + r_1$$

$$= dq_2 + d\alpha + r_1$$

$\hookrightarrow r = dq_2 + r_2 \Rightarrow r - r_2 = dq_2$

$$= r - r_2 + d\alpha + r_1$$

Thus

$r = r - r_2 + \alpha d + r_1 \Rightarrow 0 = -r_2 + \alpha d + r_1$

$\Rightarrow r_2 = r_1 + \alpha d$

Since $\alpha \geq 1$

$r_2 = r_1 + \alpha d \geq r_1 + d \geq a$ (since $d \geq 1$)

$\Rightarrow$

$r_2 \geq a.$

But by our hypothesis $0 \leq r_i < a$ for $i \in \{1, 2\}$

$\Rightarrow 0 \leq r_2 < a.$

This is a contradiction.

So we must have $q_1 = q_2$ and by substitution, it immediately follows that $r_1 = r_2$

So q and r are unique.

■

Evaluating q and r

Define the floor function

$$\lfloor \cdot \rfloor : \mathbb{Q} \to \mathbb{Z} : \alpha \mapsto K_\alpha$$

where K_α is the unique integer such that

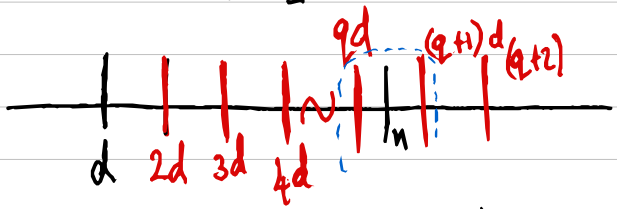
$$K_\alpha \leq \alpha < (K_\alpha + 1)$$

We can calculate q and r in division theorem as

$$\boxed{q = \left\lfloor \frac{n}{d} \right\rfloor} \qquad r = n - dq \Rightarrow \boxed{r = n - d\left\lfloor \frac{n}{d} \right\rfloor}$$

$$\hookrightarrow \left\lfloor \frac{n}{d} \right\rfloor \leq \frac{n}{d} < \left\lfloor \frac{n}{d} \right\rfloor + 1$$

$$\Leftrightarrow d\left\lfloor \frac{n}{d} \right\rfloor \leq n < d\left(\left\lfloor \frac{n}{d} \right\rfloor + 1 \right)$$



So by the line $qd = d\left\lfloor \frac{n}{d} \right\rfloor \Rightarrow q = \left\lfloor \frac{n}{d} \right\rfloor$

Common Dividors and GCD

Definition of common divisor:

Suppose that $a, b \in \mathbb{Z}$ and that atleast one integer is non-zero.

Then a common divisor of a and b is an integer d such that

$$d \mid a \text{ and } d \mid b$$

Note: Common divisors always exist since

$$1 \mid a \text{ and } 1 \mid b$$

$$-1 \mid a \text{ and } -1 \mid b$$

for any a and b. So always atleast 2 common divisors.

Definition of greatest common divisor:

The greatest common divisor denoted by $\gcd(a,b)$, of a and b is the largest positive common divisor of a and b.

i.e. let $\gcd(a,b) = d$.
if $d' \mid a$ and $d' \mid b$ then $d' < d$,
There is no d' s.t. $d' \mid a$ and $d' \mid b$ and $d' > d$.

Extend $\gcd(a,b)$ for all pairs $(a,b) \in \mathbb{Z}^2$

Define $\gcd(0,0) = 0$

Facts of divisors and gcd

1) $a \mid b \iff r = 0$ in division theorem.
2) $\gcd(a,b) = \gcd(b,a)$
3) $\gcd(0,a) = |a|$ for any $a \in \mathbb{Z}$

(with special case for $a = 0$ above)

Lemma: If $b = sa + t$ for some integers s and t then

$$\gcd(b, a) = \gcd(a, t)$$

Note: The division theorem q and r would be special cases. But the above is true for any s and t

proof: 1) $\gcd(b, a) \leq \gcd(a, t)$

Let b and a be integers and let c be the common divisor of b and a.

So $c \mid a$ and $c \mid b$

$c \mid a \Rightarrow a = mc$ for some integer m

$c \mid b \Rightarrow b = nc$ for some integer n

Substituting into $b = sa + t$,

$$nc = (mc)s + t$$

$$\Rightarrow \quad t = nc - msc$$

$$\Rightarrow \quad t = c(n - ms)$$

Now, $r - ms$ is an integer so by definition of divisibility,

$$c \mid t$$

Now the greatest common divisor of a and b are both not 0
Every common divisor of a and b is a common divisor of a and t.
So greatest common divisor of a and b divides a and t:

$\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ implies

$\gcd(a,b) \mid a$ and $\gcd(a,b) \mid t$

let greatest common divisor of a, t be $\gcd(a,t)$. By defn of gcd

$$\gcd(a,b) \leq \gcd(a,t) \qquad (*1)$$

2) $\gcd(a,t) \leq \gcd(a,b)$

Let a and b be integers. Let c be common divisors of a and t.

So $c|a$ and $c|t$

$c|a \Rightarrow a = cl$ for some integer l

$c|t \Rightarrow t = ck$ for some integer k.

Substituting into $b = as + t$,

$$b = s(cl) + ck \Rightarrow b = c(sl) + ck$$

$$\Rightarrow b = c(sl + k)$$

$sl + k$ is an integer so by defn of divisibility

$$c|b$$

Now greatest common divisor of a and t is not 0.
Every common divisor of a and t is a common divisor of a and b
So greatest common divisor of a and t divides a and b:

$\gcd(a,t) \mid a$ and $\gcd(a,t) \mid t$ implies

$\gcd(a,t) \mid a$ and $\gcd(a,t) \mid b$

Let the greatest common divisor of a and b be $\gcd(a,b)$. By defn of gcd,

$$\gcd(a,t) \leq \gcd(a,b) \qquad (*2)$$

Combining inequalities $(*1)$ and $(*2)$ we get

$$\gcd(b,a) = \gcd(s,t)$$

■

Bezout's Theorem:

Theorem: Let $a, b \in \mathbb{Z}$ both not zero. Then there exists integers $s, t \in \mathbb{Z}$ such that

$$\boxed{\gcd(a,b) = sa + tb}$$

Further, $\gcd(a,b)$ is the least positive integer expressed in this form.

proof: Let

$$S = \{ma + nb \in \mathbb{N} \mid m, n \in \mathbb{Z}\}$$

Showing that $S \neq \emptyset$.

- if $a > 0$ set $m = 1$ and $n = 0$. Then $a \in S$
- if $a < 0$ set $m = -1$, and $n = 0$, Then $(-1)a \in S$
- if $a = 0$ and $b \neq 0$, we can prove that $b \in S$ if $b > 0$ and $-b \in S$ if $b < 0$ using similar arguments.

$\therefore S \neq \emptyset$.

By the well ordering principle, S has a least element say d.

Want to prove: $d = \gcd(a, b)$

Claim: $d \mid a$ and $d \mid b$.

proof: By division theorem:

$\exists\ q, r$ s.t $a = qd + r$ and $0 \leq r < d$

If $r > 0$ then $a - qd = r < a$
But $d = sa + tb$ for some $s, t \in \mathbb{Z}$
So

$$r = a - qd = a - q(sa + tb)$$

$$= a(1 - qs) + (-tq)b$$

Since $0 \leq r = a(1-qs) + (-tq)b$,
r is a linear combination of a and b so
r must belong to S, $r \in S$

But $r < d$ and d is the least element of S
So r cannot be in $S \Rightarrow r \notin S$.

So $r > 0 \in S$ $r < d$ so $r \notin S$

This is a <u>contradiction</u>. So our initial assumption that $r > 0$ was wrong. So

$$r = 0$$

Since $r = 0$,

$$a = dq + r \Rightarrow a = dq \text{ for some integer } q$$

$$\Rightarrow \underline{d \mid a}$$

By a similar argument, assuming that

$$b = q'd + r',$$

we get that <u>$d \mid b$</u>.

So d is a common divisor of a and b.

Take any common divisor $\hat{d}$ of a and b.

Then $\hat{d} \mid sa + tb$ (by property 2)

By assumption, $sa + tb = d$. So

$$\hat{d} \mid d \Rightarrow |\hat{d}| \leq |d| \quad \text{(by property 6)}$$

$$\Rightarrow |\hat{d}| \leq d \quad \text{(since } d > 0\text{)}$$

So d is bigger than any common divisor of a and b, $\hat{d}$ so by defn,

$$d = \gcd(a, b)$$

$\Rightarrow$

$$\gcd(a, b) = sa + tb$$

■

Modular Arithmetic

Definition of Congruency

Let $m, n, d \in \mathbb{Z}$ with $d \neq 0$

We say that **m is congruent to n modulo d** and write

$$m \equiv n \pmod{d}$$

if and only if

$$d \mid m-n$$

More formally:

$$m \equiv n \pmod{d} \iff d \mid m-n$$

Theorem: Modular Equivalences

The following are equivalent:
Suppose $n, a, b \in \mathbb{Z}$, $n \neq 0$

1) $a \equiv b \pmod{n}$
2) $n \mid a-b$
3) $a = b + kn$ for some $k \in \mathbb{Z}$
4) a and b have same remainder on division by n.
5) $a \bmod n = b \bmod n$

proof: (1) $\Leftrightarrow$ (2) : immediately by defn.

(2) $\Leftrightarrow$ (3):

$n \mid a-b \Leftrightarrow a-b = nk$ for some integer k

$\Leftrightarrow a = b + kn$

(3) $\Rightarrow$ (4)

Suppose that $a = b + kn$.
By division theorem to divide a by n,

$$a = qn + r \quad \text{where } q, r \in \mathbb{Z},\ 0 \leq r < n$$

Substituting $b + kn$ gives

$$b + kn = qn + r$$

$$\Rightarrow \quad b = (q-k)n + r$$

Since $0 \leq r < n$, the uniqueness property of quotient-remainder thm r is also the remainder obtained when b is divided by n. Thus a and b have same remainder when divided by n.

(4) $\Rightarrow$ (5)

follows immediately from defn of mod

$a \bmod n = r = b \bmod n$.

(4) $\Rightarrow$ (2)

By quotient remainder thm,

$a = qn + r$ and $b = q'n + r$

(The same remainder)

So

$$a - b = qn + r - (q'n + r)$$
$$= n(q - q')$$

$\Rightarrow n \mid a - b \quad \Rightarrow a \equiv b \pmod{n}$

■

Lemma: Given that $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, there exists a unique integer r satisfying

$$0 \leq r < n$$

such that

$$a \equiv r \pmod{n}$$

proof: Follows immediately from division theorem, which states that

$\forall\, a \in \mathbb{Z}, n \in \mathbb{N}$ $\exists$ a unique r with $0 \leq r < n$ such that

$$a = qn + r$$

$$\Rightarrow \quad a - r = qn$$

$$\Rightarrow \quad n \mid a - r$$

$$\Rightarrow \quad a \equiv r \pmod{n}$$

This lemma means that any $a \in \mathbb{Z}$ is congruent to exactly one of $0, 1, 2, \ldots, (m-1)$

■

Theorem: Modular arithmetic

Let $a, b, c, d \in \mathbb{Z}$, $n \in \mathbb{N}$.

Suppose $a \equiv c \pmod{n}$ $b \equiv d \pmod{n}$

Then

1) $(a+b) \equiv (c+d) \pmod{n}$
2) $(a-b) \equiv (c-d) \pmod{n}$
3) $(ab) \equiv (cd) \pmod{n}$
4) $a^m \equiv c^m \pmod{n}$ for all positive integers m.

proof: 1) $a \equiv c \pmod{n} \Rightarrow a - c = nk$ for some $k \in \mathbb{Z}$

$\Rightarrow a = c + nk$ (*1)

$b \equiv d \pmod{n} \Rightarrow b - d = nl$ for some $l \in \mathbb{Z}$

$\Rightarrow b = d + nl$ (*2)

1) Adding (*1) and (*2)

$(a+b) = (c+d) + n(k+l)$

$\Rightarrow (a+b) - (c+d) = n(k+l)$ $\left[\begin{array}{l} k \in \mathbb{Z},\ l \in \mathbb{Z} \\ \Rightarrow k+l \in \mathbb{Z} \end{array}\right]$

$\Rightarrow n \mid [(a+b) - (c+d)]$

$\Rightarrow (a+b) \equiv (c+d) \pmod{n}$

2) Subtracting (*1) and (*2)

$(a-b) = (c+nk) - (d+nl)$

$\Rightarrow (a-b) = (c-d) + n(k-l)$

$\Rightarrow (a-b) - (c-d) = n(k-l)$

$\Rightarrow n \mid [(a-b) - (c-d)]$

$\Rightarrow (a-b) \equiv (c-d) \pmod{n}$

$\left[\begin{array}{l} k \in \mathbb{Z},\ l \in \mathbb{Z} \\ \Rightarrow k-l \in \mathbb{Z} \end{array}\right]$

Multiplying (*1) and (*2)

$$ab = (c+nk)(d+nl)$$

$$= cd + cnl + dnk + n^2kl$$

$$\Rightarrow ab - cd = n(cl + dk + kln)$$

let $m = cl + dk + kln$.

$m \in \mathbb{Z}$ as $c, l, d, n \in \mathbb{Z}$ by closure.

Thus

$$n \mid [ab - cd]$$

$$\Rightarrow (ab) \equiv (cd) \pmod{n}$$

4) By induction on $m \in \mathbb{N}$

Base case $m = 1$

property (4) is immediately true by our premise.

Inductive hypothesis:

Suppose property is true for some $m = k \in \mathbb{N}$

$$a^k \equiv c^k \pmod{n}$$

Now show that if property is true for $n = k$, then it is true for $n = k+1$

By inductive hypothesis, $a^k \equiv c^k \pmod{n}$
By base case, $a \equiv c \pmod{n}$

Therefore by part 3:

$$(a^k \cdot a) \equiv (c^k \cdot c) \pmod{n}$$

$$\Rightarrow a^{k+1} \equiv c^{k+1} \pmod{n}$$

Hence property true by induction.

4) Alternative proof:

$$a^m - c^m = (a-c)(a^{m-1} + a^{m-2}c + \cdots + ac^{m-2} + c^{m-1})$$

$$\Rightarrow (a-c) \mid a^m - c^m$$

Now by premice,

$$a \equiv c \pmod{n} \Rightarrow n \mid (a-c)$$

and $(a-c) \mid (a^m - c^m)$

Therefore by transitivity of divisibility:

$$n \mid (a^m - c^m) \Rightarrow a^m \equiv c^m \pmod{n}$$

■

Lemma: Every square number is congruent to 0 or 1 modulo 4

More formally;

$\forall n \in \mathbb{Z}, n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

proof: By lemma on page 32:

for $0 \leq r < m = 4$, $\forall n \in \mathbb{Z}$

$n \equiv r \pmod 4$

$\Rightarrow n \equiv 0 \pmod 4$ or $n \equiv 1 \pmod 4$ or

$n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$

Case 1: $n \equiv 0 \pmod n$

$n \equiv 0 \pmod 4 \Rightarrow n^2 \equiv 0^2 \pmod 4$

$\Rightarrow n^2 \equiv 0 \pmod 4$

(by laws of modular arithmatic)

case2 : $n \equiv 1 \pmod 4$

$n \equiv 1 \pmod 4 \Rightarrow n^2 \equiv 1^2 \pmod 4$

$\Rightarrow n^2 \equiv 1 \pmod 4$

(by laws of modular arithmetic)

case3 : $n \equiv 2 \pmod 4$

$n \equiv 2 \pmod 4 \Rightarrow n^2 \equiv 4 \pmod 4$

$\Rightarrow n^2 \bmod 4 = 4 \bmod 4$

$\Rightarrow n^2 \bmod 4 = 0$

(equivalence) $\Rightarrow n^2 \bmod 4 = 0 \bmod 4$

$\Rightarrow n^2 \equiv 0 \pmod 4$

case 4: $n \equiv 3 \pmod 4$

$n \equiv 3 \pmod 4 \equiv n^2 \equiv 9 \pmod 4$

$\Rightarrow n^2 - 9 = 4k$ some integer k

$\Rightarrow n^2 = 8 + 4k + 1$

$\Rightarrow n^2 = 4(k+2) + 1$

$\Rightarrow n^2 - 1 = 4(k+2)$ $\quad [k+2 \in \mathbb{Z}]$

$\Rightarrow 4 \mid n^2 - 1$

$\Rightarrow n^2 \equiv 1 \pmod 4$

In all cases,

$n^2 \equiv 0 \pmod 4$ or

$n^2 \equiv 1 \pmod 4$

■

Corollary: If $n \equiv 3 \pmod 4$, then n is not the sum of 2 squares

proof: by the previous lemma:

any square number is congruent to 0 or 1 modulo 4.

So let k^2 and l^2 be 2 square numbers.

$k^2 \equiv 0 \pmod 4$ or $k^2 \equiv 1 \pmod 4$

Similarly

$l^2 \equiv 0 \pmod 4$ or $l^2 \equiv 1 \pmod 4$

let $n = k^2 + l^2$

Case 1: $k^2 \equiv 0 \pmod 4$ and $l^2 \equiv 0 \pmod 4$

$n \equiv (k^2 + l^2) \equiv (0+0) \equiv 0 \pmod 4$

Case 2: $k^2 \equiv 0 \pmod 4$ and $l^2 \equiv 1 \pmod 4$

$n = (k^2 + l^2) \equiv (0+1) \equiv 1 \pmod 4$

Case 3: $k^2 \equiv 1 \pmod 4$ or $l^2 \equiv 0 \pmod 4$

$n \equiv (k^2 + l^2) \equiv (1+0) \equiv 1 \pmod 4$

Case 4: $k^2 \equiv 1 \pmod 4$ or $l^2 \equiv 1 \pmod 4$

$n \equiv (k^2 + l^2) \equiv (1+1) \equiv 2 \pmod 4$

In all cases, n is not congruent to 3 modulo 4.

■

Corollary: The number $\sqrt{2}$ is not rational

proof: (Using modular arithmetic by contradiction):

Suppose $\sqrt{2}$ is rational.

By defn of rational number

$\sqrt{2} = \frac{a}{b}$ for some $a \in \mathbb{Z}$, $b \in \mathbb{N}$

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

$$\sqrt{2} = \frac{a}{b} \Rightarrow a^2 = 2b^2$$

By lemma, $a^2 \equiv 0, 1 \pmod 4$

$$b^2 \equiv 0, 1 \pmod 4 \quad (\text{"}, \text{"} = \text{or})$$
$$\Rightarrow 2b^2 \equiv 0, 2 \pmod 4$$

The only possible solution to the equation

$$a^2 = 2b^2$$

is when both are congruent to 0 as if 2 numbers are equal, they are congruent to the same thing

$$a^2 = 2b^2 \equiv 0 \pmod 4$$

So $a^2 \equiv 0 \pmod 4 \Rightarrow 4 \mid a \Rightarrow 2 \mid a$

$2b^2 \equiv 0 \pmod 4 \Rightarrow 4 \mid 2b \Rightarrow 2 \mid b$

Both numbers are even which contradicts the fact that $\gcd(a, b) = 1$

They have to give same remainder when divided by same number in this case 4

■

Example: find $2^{14} \pmod{15}$

$$2^{14} = 2^7 \times 2^2 = (16)^3 \cdot 4$$

Now

$$16 \equiv 1 \pmod{15} \Rightarrow 16^3 \equiv 1^3 \pmod{15}$$

$$\Rightarrow 16^3 \equiv 1 \pmod{15}$$

$$\Rightarrow (16^3 \times 4) \equiv (1 \times 4) \pmod{15}$$

$$\Rightarrow \boxed{2^{14} \equiv 4 \pmod{15}}$$

Used modulas asithmetic laws:

$a^n \equiv b^n \pmod{m}$ if $a \equiv b \pmod{m}$

$ac \equiv bd \pmod{m}$ if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

Example: Show that $8^{4n+2} + 4^{2n} \equiv 0 \pmod 5$ i.e. a multiple of 5.

$8 \equiv 3 \pmod 5 \Rightarrow 8^{4n+2} \equiv 3^{4n+2} \pmod 5$

$\Rightarrow 8^{4n+2} \equiv 9^{2n+1} \pmod 5$

Since $9 \equiv (-1) \pmod 5$, $9^{2n+1} \equiv (-1)^{2n+1} \pmod 5$

[$9 = 2.5 + (-1)$]

$\Rightarrow 9^{2n+1} \equiv (-1) \pmod 5$

Similarly $4 \equiv (-1) \pmod 5 \Rightarrow 4^{2n} \equiv (-1)^{2n} \pmod 5$

$\Rightarrow 4^{2n} \equiv 1 \pmod 5$

Therefore

$8^{4n+2} + 4^{2n} \equiv (-1+1) \pmod 5$

$\Rightarrow$

$8^{4n+2} + 4^{2n} \equiv 0 \pmod 5$

$\Rightarrow 5k + 0 = 8^{4n+2} + 4^{2n}$

$\Rightarrow 5 \mid 4^{2n} + 8^{4n+2}$.

Congruence Equations

Example: Find solutions to $4x \equiv 3 \pmod{10}$

$4x \equiv 3 \pmod{10} \Rightarrow 10 \mid 4x-3$

$\Rightarrow 4x-3 = 10k$

$\Rightarrow 4x = 10k+3$

$4x = 2 \cdot (2x)$ which is an even numbers

$10k+3 = 2(5k+1)+1$ which is an odd number.

An odd numbers cannot be equal to an even number.

↯ There is a contradiction.

Therefore $4x \equiv 3 \pmod{10}$ has no solutions

Example: Find solutions $6x \equiv 9 \pmod{15}$

$6x \equiv 9 \pmod{15} \Rightarrow 15 \mid 6x - 9$

$\Rightarrow 6x - 9 = 15k$ for some $k \in \mathbb{Z}$

Running through all possible values of x such that $6x-9$ is a multiple of 15,

$x = 4$ or $x = 9$

Lemma (2.9): The congruence equation $ax \equiv b \pmod{m}$ has solutions if and only if

$$\gcd(a, m) \mid b$$

important

proof: Throughout the proof: let $d = \gcd(a, m)$

($\Rightarrow$): Proving forward implication:

Let $x = c$ be a solution of $ax \equiv b \pmod{m}$, which means $ac = qm + b$

$$ac \equiv b \pmod{m} \Rightarrow ac = qm + b$$

Rearranging, we get

$$b = ac - qm$$

Since d is a gcd, $d|a$ and $d|m$.

$d|a$ and $d|m \Rightarrow d|ac - qm$ (since it is a linear combination)

Thus

$$d|b$$

($\Leftarrow$): proving reverse implication:

if $d|b$ then $b = dk$ for some $k \in \mathbb{Z}$. By Bezout's thm,

$$\gcd(a,b) = sa + tm \quad \text{for some } s,t \in \mathbb{Z}$$

This means that

$$b = dk \Rightarrow b = k(sa + tm)$$

$$\Rightarrow b = k(sa) + k(tm)$$

$$\Rightarrow b = (kt)m + a(ks)$$

$\Rightarrow b \equiv a(ks) \pmod{m}$

$\Rightarrow a(ks) \equiv b \pmod{m}$

$\Rightarrow x = ks$ is a solution. ■

Remark: The proof given for lemma 2.9 even though an existence proof shows how to find a solution:

- Use Euclids Algorithm to write gcd of a and m as a linear combination of a and m
- Use that combination to find a solution

Example: There are no solutions to $6x \equiv 4 \pmod{9}$ as

$$\gcd(6,9) = 3 \text{ and } 3 \nmid 4.$$

Example: Find an x so that

$$924x \equiv 36 \pmod{1152}$$

Solution: In notes, it is given that $\gcd(924, 1152) = 12$ and that

$$12 = 5 \times 924 + (-4) \times 1152$$

by Euclidean Algorithm.

Note that

$$36 = 3 \times 12 = 3 \times (5 \times 924 + (-4) \times 1152)$$

$$= (15 \times 924) + (-12) \cdot (1152)$$

$$\Rightarrow 36 \equiv (15 \times 924) \pmod{1152}$$

$$\Rightarrow (924) \cdot (15) \equiv 36 \pmod{1152}$$

(symmetric property)

$\Rightarrow x = 15$ is a solution.

There are different solutions to this congruence equation, though.
One can check that $x=111$ is also a solution to the congruence $924x \equiv 36 \pmod{1152}$, since

$$1152 \mid (111 \times 924 - 36)$$

$115 \not\equiv 15 \pmod{1152}$ so they are genuinly "different" solutions.

The following result gives whole set of solutions.

Lemma (2.10): If $ax \equiv b \pmod{m}$ has a solution $x=c$ then any

$$x \equiv c \pmod{m/d}$$

is also a solution where $d = \gcd(a,m)$

Proof: Let $d = \gcd(a,m)$

$d = \gcd(a,m) \Rightarrow d \mid a$ and $d \mid m$

$\Rightarrow a = a'd$ for some $a' \in \mathbb{Z}$ and

$m = m'd$ for some $m' \in \mathbb{Z}$

Since there is a solution, lemma 2.9 says:

$$d \mid b \Rightarrow b = db' \text{ for some } b' \in \mathbb{Z}$$

As c is a solution;

$$ac \equiv b \pmod{m} \Leftrightarrow m \mid (ac - b)$$

$$\Leftrightarrow dm' \mid ((da')c - db') \quad \text{(by substitution)}$$

$$\Leftrightarrow m' \mid (a'c - b') \quad \text{(by dividing both sides by } d\text{)}$$

$$\Leftrightarrow a'c \equiv b' \pmod{m'} \quad \left[m' = \frac{m}{d}\right]$$

due to these implications: $ax \equiv b \pmod{m} \Leftrightarrow a'x \equiv b' \pmod{m'}$

If $x \equiv c \pmod{m'}$ then $x = rm' + c$ for some $r \in \mathbb{Z}$ and so

$$a'x = (ar)m' + a'c \Leftrightarrow a'x \equiv a'c \pmod{m'} \text{ and}$$

$$a'c \equiv b' \pmod{m'}$$

$$\Leftrightarrow a'x \equiv b' \pmod{m'}$$

(transitivity of congruence)

That is any $x \equiv c \pmod{m'}$ solves the equation $a'x \equiv b' \pmod{m}$ and hence also solves the equation $ax \equiv b \pmod{m}$ ■

Note: if $d = \gcd(a,m) > 1$ then setting

$a' = a/d$ and $m' = m/d$

implies that $\gcd(a',m') = 1$.

The next lemma shows that is essentially only one solution to $a'x \equiv b' \pmod{m'}$

Lemma (2.11): If $\gcd(a',m') = 1$ then there exists exactly one solution modulo m' to $a'x \equiv b' \pmod{m'}$

proof: By lemma 2.9 we know that the equation has solutions

Let y and x be two such solutions. so

$a'x \equiv b' \pmod{m'}$ and $a'y \equiv b' \pmod{m'}$

$\Rightarrow a'x \equiv a'y \pmod{m'} \iff m' \mid a'(x-y)$

Since $\gcd(a',m') = 1$, it must be that

find proof of general fact

$$m' \mid (x-y) \Rightarrow x \equiv y \pmod{m'}$$

That is they are the same mod m' so the same solution. ∎

Summary: To solve $ax \equiv b \pmod{m}$

1) Find $d = \gcd(a, m)$ using Euclidean Algorithm
2) If $d \nmid b$ then there are no solutions
3) If $d \mid b$, write $b = b'd$ for some $b' \in \mathbb{Z}$ and $d = as + tm$ (Bezout)
4) $x = sb'$ is a solution
5) Let $m' = m/d$

The set of numbers congruent to $sb' \pmod{m'}$ is the set of all solutions.

Example: The general solution to $70x \equiv 42 \pmod{119}$

Solution First find $\gcd(70, 119)$ (Euclidean Algorithm)

$119 = 1 \cdot 70 + 49$

$\gcd(119, 70) = \gcd(70, 49)$

$70 = 1 \cdot 49 + 21$

$\gcd(70, 49) = \gcd(49, 21)$

$49 = 2 \cdot 21 + 7$

$\gcd(49, 21) = \gcd(21, 7)$

$21 = 7 \cdot 3 + 0$

$\gcd(21, 7) = \gcd(7, 0) = 7$

$\Rightarrow \gcd(70, 119) = 7$

Since $7 \mid 42$, we know there is a solution

$42 = 7 \cdot 6$, Let $b' = 42/7 = 6$

Working back up the chain of equalities,

$$\begin{aligned} 7 &= 49 - 2 \times 21 \\ &= 49 - 2 \times (70 - 49) \\ &= 3 \times 49 - 2 \times 70 \\ &= 3 \times (119 - 70) - 2 \times 70 \\ &= 3 \times (119) - 5 \times 70 \end{aligned}$$

Therefore we have $s = -5$

Therefore $sb' = -5 \times 6 = -30$ is a solution.

The general solution is the set of all

$$x \equiv (-30) \pmod{17} \equiv 4 \pmod{17}$$

Chinese Remainder Theorem

Here is a lemma to show to help prove the chinese remainder theorem.

Lemma (*1): If $a, b, c \in \mathbb{Z}$ with $\gcd(a,b) = \gcd(a,c) = 1$ then

$$\gcd(a, bc) = 1$$

proof: By Bezout's theorem:

$\gcd(a,b) = 1 \Rightarrow 1 = sa + tb$ for some $s,t \in \mathbb{Z}$

$\gcd(a,c) = 1 \Rightarrow 1 = ua + vc$ for some $u,v \in \mathbb{Z}$

$1.1 = (sa+tb).(ua+vc)$

$$\Rightarrow 1 = sua^2 + svca + utba + vtbc$$

$$\Rightarrow 1 = a(sua + svc + utb) + (vt)bc$$

So 1 can be written as a linear combination of a and bc. So by Q6 of algebra sheet 1,

$$\gcd(a, bc) \mid 1 \Rightarrow \gcd(a, bc) \leq 1$$

Now $\gcd(a,b)=1 \Rightarrow 1|a$ and $1|b$

$\Rightarrow a=1.a$ and $b=1.b$

$\gcd(a,c)=1 \Rightarrow 1|a$ and $1|c$

$\Rightarrow 1=a.1$ and $c=1.c$

$bc=1.bc \Rightarrow 1|bc$

Now $1|bc$ and $1|a \Rightarrow 1$ is a common divisor of a and bc.

So 1 is a linear combination of a and bc and 1 is a common divisor of a and bc

So by question sheet 1 Q5

$$\gcd(a,bc)=1$$

■

Lemma (#2): If $a_1, a_2, a_3, \ldots, a_n$ are integers and b is another integer such that

$$\gcd(a_1, b) = \gcd(a_2, b) = \ldots = \gcd(a_n, b) = 1$$

then

$$\gcd(a_1 \cdot a_2 \cdots a_n, b) = 1$$

proof: (by mathematical induction):

Let property $P(n)$ be

$$\gcd(a_1 \cdot a_2 \cdots a_n, b) = 1$$

Base case: $n = 2$:

$$\gcd(a_1, b) = \gcd(a_2, b) = 1$$

$$\Rightarrow \quad \gcd(a_1 \cdot a_2, b) = 1$$

This was shown in previous lemma (#1) with

$$a \leftarrow b, \quad a_1 \leftarrow b \quad a_2 \leftarrow c$$

Inductive hypothesis:
Assume property $P(n)$ is true for some $n=k$

So $\gcd(a_1, b) = \gcd(a_2, b) = \dots \gcd(a_k, b) = 1$

$\Rightarrow$

$$\gcd(a_1 \cdot a_2 \cdot a_3 \cdots a_k, b) = 1$$

Inductive step:
Show that $\forall n \in \mathbb{N}$ with $n \geq 2$, if property is true for $n=k$, then it is true for $n=k+1$:

We have that

$$\gcd(a_1,b) = \gcd(a_2,b) = \dots = \gcd(a_k,b) = \gcd(a_{k+1},b) = 1$$

Let $A = a_1 \cdot a_2 \dots a_k$

By inductive hypothesis $\gcd(A,b) = 1$

$\gcd(A,b) = 1$ and $\gcd(a_{k+1}, b) = 1$.

So by lemma (*1), $\gcd(A \cdot a_{k+1}, b) = 1$
where

$a \leftarrow b, \quad b \leftarrow A \quad c \leftarrow a_{k+1}$.

$P(n)$ true by induction on n. ■

Theorem: Chinese Remainder Theorem:

Let $m_1, m_2, \ldots m_r$ be integers such that

$$\gcd(m_i, m_j) = 1$$

for $i \neq j$ and $1 \leq i, j \leq r$

Then the system of congruences

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2},$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

has a unique solution modulo M where

$$M = m_1 \cdot m_2 \cdots m_r$$

(proof given on next page)

proof: First we construct a simultaneous solution to the system of congruences.

To do this, let

$$M_k = \frac{M}{m_k} = m_1 \cdot m_2 \cdot m_3 \cdots m_{k-1} m_{k+1} \cdots m_r$$

By lemma (#2) $\gcd(M_k, m_k) = 1$

↳ as $(m_j, m_k) = 1$ when $j \neq k$

Therefore we can find an inverse y_k of M_k modulo m_k such that

$$M_k y_k \equiv 1 \pmod{m_k}$$

Claim:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r$$

is a simultaneous solution to the set of linear congruences.

To demonstrate this we must show that

$$x \equiv a_k \pmod{m_k} \quad \text{for } k = 1, 2, 3, \ldots, r$$

Since $m_k \mid M_j$ whenever $j \neq k$, we have

$$M_j \equiv 0 \pmod{m_k} \quad j \neq k.$$

Therefore

$$a_j M_j y_j \equiv 0 \pmod{m_k} \quad j \neq k$$

So

$$\sum_{\substack{j=1 \\ j \neq k}}^{r} a_j M_j y_j \equiv 0 \pmod{m_k}$$

by laws of modular arithmetic

$$x = a_k M_k y_k + \sum_{\substack{j=0 \\ j \neq k}}^{r} a_j M_j y_j$$

Now

$$\sum_{\substack{j=1 \\ j \neq k}}^{r} a_j M_j y_j \equiv 0 \pmod{m_k}$$

$$\Rightarrow a_k M_k y_k + \sum_{\substack{j=0 \\ j \neq k}}^{r} a_j M_j y_j \equiv a_k M_k y_k \pmod{m_k}$$

$$\Rightarrow x \equiv a_k M_k y_k \pmod{M_k}$$

Since $M_k y_k \equiv 1 \pmod{m_k}$,

$a_k M_k y_k \equiv a_k \pmod{m_k} \Rightarrow a_k \equiv a_k M_k y_k \pmod{m_k}$

So $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$

$\Rightarrow x \equiv a_k \pmod{m_k}$

Showing that x is unique solution:

We know show that any two solutions are congruent modulo M

Let x and y be both simultaneous solutions to system of n congruences.

Then for all $1 \leq k \leq n$

$$x \equiv y \equiv a_k \pmod{m_k}$$

$$\Rightarrow \quad x \equiv y \pmod{m_k}$$

$$\Rightarrow \quad m_k \mid (x-y) \qquad \text{for all } 1 \leq k \leq n$$

Since all m_k are relatively prime to each other

$$M = m_1 \cdot m_2 \cdot m_3 \cdots m_k \text{ divides } x-y$$

i.e. $M \mid (x-y)$

$$\Rightarrow \quad x \equiv y \pmod{M}$$

Hence solutions are unique modulo M. ■

☆ proof given in appendix

Example Find solution to

$$x \equiv 4 \pmod 5 \quad \text{and} \quad x \equiv 6 \pmod 7$$

Solution: Let $M = 5 \times 7 = 35$

$M_1 = 35/5 = 7 \qquad M_2 = 35/7 = 5$

$\gcd(5,7) = 1 \Rightarrow \exists\, y_2 \in \mathbb{Z}$ s.t

$$7y_2 \equiv 1 \pmod 5$$

By Bezout's thm:

$\gcd(5,7) = 1 \Rightarrow 1 = 5s + 7t$ for some $s,t \in \mathbb{Z}$

By Euclidean Algorithm

$7 = 5.1 + 2 \Rightarrow \gcd(7,5) = \gcd(5,2)$

$5 = 2.2 + 1 \Rightarrow \gcd(5,2) = \gcd(2,1)$

$2 = 2.1 + 0 \Rightarrow \gcd(2,1) = \gcd(1,0)$

$\Rightarrow \gcd(5,7) = 1.$

So $5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2$

$\Rightarrow 1 = 5 - 2(7 - 5)$

$\Rightarrow 1 = 5(3) + 7(-2)$

so $s = 3$ and $t = -2$ are possible solutions to Bezout's thm.

$1 = 5(3) + 7(-2) \Rightarrow 1 \equiv 7(-2) \pmod 5$

$\Rightarrow 7(-2) \equiv 1 \pmod 5$

observe that

$5 \mid (3 - (-2)) \Rightarrow 3 \equiv (-2) \pmod 5$

$\Rightarrow 7(3) \equiv 7(-2) \equiv 1 \pmod 5$

$\Rightarrow 7(3) \equiv 1 \pmod 5$ $\quad y_1 = 3$

similarly $\gcd(7,5) = 1 \Rightarrow \exists\, y_2 \in \mathbb{Z}$ s.t

$5 y_2 \equiv 1 \pmod 7$

$1 = 5(3) + 7(-2)$

$\Rightarrow 1 \equiv 5(3) \pmod 7$

$\Rightarrow 5(3) \equiv 1 \pmod 7$

$\Rightarrow y_2 = 3$

$x = M_1 a_1 y_1 + M_2 a_2 y_2$

$= 7 \times 4 \times 3 + 5 \times 6 \times 3$

$= 84 + 90$

$= 174$

So $x \equiv 174 \pmod{35}$

$\equiv 34 \pmod{35}$

$\Rightarrow \boxed{x \equiv 34 \pmod{35}}$

is the set of simultaneous solutions to

$x \equiv 4 \pmod 5$ and $x \equiv 6 \pmod 7$

Alternative proof to Chinese remainder theorem when $n=2$:

If m_1 and m_2 are integers such that

$$\gcd(m_1, m_2) = 1$$

then $\exists$ a unique $x \pmod{m_1 m_2}$ such that x simultaneously satisfies

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

proof: Since $\gcd(m_1, m_2) = 1$, by Bezout's thm

$$1 = s_1 m_1 + s_2 m_2 \quad \text{for some } s_1, s_2 \in \mathbb{Z}$$

claim: any integer

$$x \in \{c_1 m_2 s_2 + c_2 m_1 s_1 + q m_1 m_2 : q \in \mathbb{Z}\}$$

is the simultaneous solution.

To show this

• modulo m_1 we have:

$$x = c_1 m_2 s_2 + c_2 m_2 s_1 + q m_1 m_2$$

$$\Rightarrow x \equiv c_1 m_2 s_2 \pmod{m_1}$$

$$\Rightarrow x \equiv c_1 (1 - s_1 m_1) \pmod{m_1}$$

$$\Rightarrow x \equiv (c_1 - c_1 m_1 s_1) \pmod{m_1}$$

$$\Rightarrow x = c_1 - c_1 m_1 s_1 + k m_1$$

$$\Rightarrow x = c_1 + m_1(-c_1 s_1 + k)$$

$$\Rightarrow x \equiv c_1 \pmod{m_1}$$

• modulo m_2 we have:

$$x = c_1 m_2 s_2 + c_2 m_2 s_1 + q m_1 m_2$$

$$\Rightarrow x \equiv c_2 m_1 s_1 \pmod{m_2}$$

$$\Rightarrow x \equiv c_2 (1 - s_2 m_2) \pmod{m_2}$$

$$\Rightarrow x \equiv (c_2 - c_2 m_2 s_2) \pmod{m}$$

$$\Rightarrow x = c_2 - c_2 m_2 s_2 + k m_2$$

$$\Rightarrow x = c_2 + (-m_2 s_2 + k) m_2$$

$$\Rightarrow x \equiv c_2 \pmod{m_2}$$

To see that there are no other solutions modulo $m_1 m_2$

Let x and y be solutions.

$$x \equiv y \equiv c_1 \pmod{m_1}$$

$$\Rightarrow x \equiv y \pmod{m_1} \Rightarrow m_1 \mid (x-y)$$

Similarly

$$x \equiv y \equiv c_2 \pmod{m_2} \Rightarrow x \equiv y \pmod{m_2}$$

$$\Rightarrow m_2 \mid x-y$$

Since $\gcd(m_1, m_2) = 1$ and $m_1 \mid x-y$ and $m_2 \mid x-y$,

$$m_1 m_2 \mid x-y \qquad \text{(by lemma)}$$

$$\Rightarrow x \equiv y \pmod{m_1 m_2}$$

■

So simultaneous set of solutions to

$$x \equiv c_1 \pmod{m_1}$$

and

$$x \equiv c_2 \pmod{m_2}$$

is

$$\boxed{x \equiv (c_2 m_1 s_1 + c_1 m_2 s_2) \pmod{m_1 m_2}}$$

Appendix:

Lemma If $\gcd(m_1, m_2) = 1$ and $m_1 \mid a$ and $m_2 \mid a$ then

$$m_1 m_2 \mid a$$

proof: By Bezout's theorem:

$\gcd(m_1, m_2) = 1 \Rightarrow 1 = sm_1 + tm_2$ for some $s, t \in \mathbb{Z}$

$m_1 \mid a \Rightarrow a = m_1 k$ for some $k \in \mathbb{Z}$

$m_2 \mid a \Rightarrow a = m_2 l$ for some $l \in \mathbb{Z}$

and $m_1 k = m_2 l = a$.

Now

$$1 = sm_1 + tm_2 \Rightarrow k = sm_1 k + tm_2 k$$

$$\Rightarrow k = sm_2 l + tm_2 k$$

$$\Rightarrow k = m_2(sl + tk)$$

$$\Rightarrow m_2 \mid k$$

$m_2 \mid k \Rightarrow k = m_2 p$ for some $p \in \mathbb{Z}$

So

$$a = m_1 k \Rightarrow a = m_1 m_2 p \text{ for some } p \in \mathbb{Z}$$
$$\Rightarrow m_1 m_2 \mid a$$

■

Using this lemma and principle of induction we can prove that

$\forall n \in \mathbb{N}$ s.t $n \geq 2$, if

$$\gcd(m_i, m_j) = 1 \quad i \neq j \quad \forall\, 1 \leq i, j \leq n$$

and

$$m_i \mid a \qquad \forall\, 1 \leq i \leq n$$

then $M = m_1 \cdot m_2 \cdot m_3 \cdots m_n$ s.t

$$M \mid a$$