Abstract Algebra by Pinter, Chapter 22

Amir Taaki

Chapter 22 on Factoring Into Primes

Contents

A. Properties of the Relation "a" divides "b"

Q1

If $a|b$ and $b|c$, then $a|c$.

$$a|b \implies b = ka$$
$$b|c \implies c = lb$$

$$c = l(ka) = (kl)a \implies a|c$$

Q2

$a|b$ iff $a|(-b)$ iff $(-a)|b$.

$$b = ka \iff -b = (-k)a \iff b = (-k)(-a)$$
$$a|b \iff a|(-b) \iff (-a)|b$$

Q3

$1|a$ and $(-1)|a$.

$a = 1 \cdot a = (-1) \cdot (-a)$ thus $1|a$ and $(-1)|a$

Q4

$a|0$.

$$0 = 0a \therefore a|0$$

Q5

If $c|a$ and $c|b$, then $c|(ax + by)$ for all $x, y \in \mathbb{Z}$.

$c|a$ and $c|b \implies a = kc$ and $b = lc$

$$ax + by = kcx + lcy = c(kx + ly)$$
$$\implies c|(ax + by)$$

Q6

If $a > 0$ and $b > 0$ and $a|b$, then $a \leq b$.

Let $b = ka$

$k \neq 0$ because $0a = 0 = b$ but $b > 0$

If $k < 0$ then $-k > 0$ or $-k \geq 1 \implies 1 \leq -ka = -b$ which is a contradiction since $b > 0$.

Thus $k > 0$

$$\begin{aligned} 0 &< k \\ 1 &\leq k \\ a &\leq ka = b \end{aligned}$$

Q7

$a|b$ iff $ac|bc$, when $c \neq 0$.

$bc = kac \implies b = ka$ by the cancellation property.

Q8

If $a|b$ and $c|d$, then $ac|bd$.

$$b = ka \qquad d = lc$$

$$bd = (ka)(lc) = (kl)ac$$

Q9

Let p be a prime. If $p|a^n$ for some $n > 0$, then $p|a$.

$$a^n = (p_1 \cdots p_r)(p_1 \cdots p_r)(p_1 \cdots p_r)$$

$$p|a^n \implies a^n = kp$$

Since a^n factors uniquely $\implies p|a$

B. Properties of the gcd

Prove the following, for any integers a, b, and c. For each of these problems, you will need only the definition of the gcd.

Q1

If $a > 0$ and $a|b$, then $\gcd(a, b) = a$.

$$b = ka$$

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

$$\begin{aligned} t &= ax + by \\ &= ax + (ka)y \\ &= a(x + ky) \end{aligned}$$

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

a is the gcd because it is the biggest divisor in a.

Q2

$gcd(a,0) = a$, if $a > 0$.

$$a|a \text{ and } a|0 \implies \gcd(a,0) = a$$

Q3

$\gcd(a,b) = \gcd(a, b+xa)$ for any $x \in \mathbb{Z}$.

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

$$t = ka + lb$$

$$a = wu \qquad b + xa = vu \text{ from } \gcd(a, b+xa)$$

$$b + xa = b + x(wu) = vu$$
$$b = u(v - xw)$$

but

$$\begin{aligned} t &= ka + lb \\ &= k(wu) + lu(v - xw) \\ &= u(kw + l(v - xw)) \end{aligned}$$

therefore it follows $u|t$

Since $\gcd(a, b+xa) = \bar{k}a + \bar{l}(b+xa) = \bar{k}(tr) + \bar{l}(ts + x(tr))$

Therefore t is also the gcd of a and $bx + a$.

$$\gcd(a,b) = \gcd(a, b+xa) \qquad \forall x \in \mathbb{Z}$$

Q4

Let p be a prime. Then $\gcd(a,p) = 1$ or p. (Explain.)

a is a composite of primes.

That is $a = p_1 \cdots p_r$

If $a = pk$ for some k, then

1. $p|p$ and $p|a$.
2. for any integer u, since p is prime, u does not divide p.

Thus according to the definition $\gcd(a,p) = p$

Otherwise $\gcd(a,p) = 1$ because p is indivisible and does not divide a.

Q5

Suppose every common divisor of a and b is a common divisor of c and d, and vice versa. Then $\gcd(a,b) = \gcd(c,d)$.

$$\gcd(a,b) > \gcd(c,d)$$

$$\implies p_1 \cdots p_i p_j \cdots p_r > p_1 \cdots p_i$$

where $p_1 \cdots p_i$ are the prime common factors of $\gcd(a,b)$ and $\gcd(c,d)$ or $\gcd(\gcd(a,b),\gcd(c,d))$.

Then this implies that a and b have common factors $p_j \cdots p_r$ which are not in c and d.

Hence $\gcd(a,b) = \gcd(c,d)$.

Q6

If $\gcd(ab,c) = 1$*, then* $\gcd(a,c) = 1$ *and* $\gcd(b,c) = 1$*.*

Let $ab = (p_1 \cdots p_r)(q_1 \cdots q_s)$

$$\gcd(ab,c) = 1 \implies \forall p_i, q_j \qquad p_i \nmid c, q_j \nmid c$$

$$\forall p_i \nmid c \implies \gcd(a,c) = 1$$

Likewise for b.

Q7

Let $\gcd(a,b) = c$*. Write* $a = ca'$ *and* $b = cb'$*. Then* $\gcd(a',b') = 1$*.*

Let $\gcd(a',b') = x$

$$a = ca' = ckx$$
$$b = cb' = clx$$
$$\gcd(a,b) = cx$$

but $\gcd(a,b) = c \implies x = 1$

$$\therefore \gcd(a',b') = 1$$

C. Properties of Relatively Prime Integers

Q1

From theorem 3,

$$\gcd(a,b) = ra + sb \text{ for some integers } r \text{ and } s$$

But $a \perp b$, so $\gcd(a,b) = 1$. That is,

$$ra + sb = 1$$

Q2

$$\gcd(a,c) = 1 \implies a \perp c \implies a \nmid c$$

But $c \mid ab$ so $ab = ch$ for some integer h. And $\gcd(a,c) = 1$

$$\implies ka + lc = 1$$

$$\implies kab + lcb = b$$

However $ab = ch$, so

$$kch + lcb = b$$
$$c(kh + lb) = b$$

Thus $c \mid b$

Q3

$$d = pa = qc$$
$$\gcd(a, c) = 1 \implies ka + lc = 1$$
$$kad + lcd = d$$
$$ka(qc) + lc(pa) = d$$
$$ac(kq + lp) = d$$
$$ac \mid d$$

Q4

$$ka + lc = 1$$
$$kab + lcb = b$$
$$k(pd) + l(qd) = b$$
$$d(kp + lq) = b$$
$$d \mid b$$

Q5

$$d = ka + lb$$
$$a = dr \qquad b = ds$$

$$\begin{aligned} d &= kdr + lds \\ &= d(kr + ls) \end{aligned}$$

$$kr + ls = 1 \implies \gcd(r, s) = 1$$

Q6

$$ka + lc = 1$$
$$hb + jc = 1$$

$$ka(hb + jc) + lc = 1$$
$$kh(ab) + (j + l)c = 1 \implies gcd(ab, c) = 1$$

D. Further Properties of gcd's and Relatively Prime Integers

Q1

$$b = ma = nc$$
$$ka + lc = d$$
$$b(ka + lc) = bd$$
$$bka + blc = bd$$
$$(nc)ka + (ma)lc = bd$$
$$nk \cdot ac + ml \cdot ac = bd$$
$$\implies ac \mid bd$$

Q2

$$b = mac = nad$$
$$kc + ld = 1$$
$$bkc + bld = b$$
$$(nad)kc + (mac)ld = b$$
$$acd(nk + ml) = b$$

Q3

From theorem 3,

$$J = \{ua + vb : u, v \in \mathbb{Z}\}$$

J is a principal ideal of $\mathbb{Z}$ and $J = \langle d \rangle$.

Since $x \in J$, then x is a multiple of d and so $d \mid x$.

Likewise $d \mid x \implies x \in J$ and so x is a linear combination of a and b.

Q4

Let J be a linear combination of a and b.

$t = \gcd(a, b)$ and $J = \langle t \rangle$

Thus $t = ka + lb$ but $x \mid a$ and $x \mid b$ so $x \mid t$.

But $t \mid c$, so $c \in J$ and so c is a multiple of t (which is the biggest divisor of a and b).

$$t \leq c$$

$c \mid c \implies c \mid a$ and $c \mid b$, and c is the greatest divisor of c. So $c = \gcd(a, b) = t$.

See also here

Q5

$$\forall n > 0, \text{ if } \gcd(a, b) = 1 \text{ then } \gcd(a, b^n) = 1$$

$\gcd(a, b) = 1$ means there is only the shared divisor of 1 between a and b.

That there is no $u > 1$ such that $a = xu$ and $b = yu$.

Assume $\gcd(a, b^k) = 1$, then there is no common divisor between a and b^k and also a and b. This means that a and b^{k+1} also share no prime factors, hence

$$\gcd(a, b^{k+1}) = 1$$

Q6

Suppose $\gcd(a, b) = 1$ *and* $c|ab$*. Then there exist integers* r *and* s *such that* $c = rs, r|a, s|b,$ *and* $\gcd(r, s) = 1$.

$$a = p_1 \cdots p_n$$
$$b = q_1 \cdots q_m$$

Since $\gcd(a, b) = 1$, a and b share no factors as their prime factors are unique and distinct.

$$c \mid ab \implies ab = kc$$

Since c divides ab, it consists of some number of factors of ab such that

$$c = (p_1 \cdots p_i)(q_1 \cdots q_j)$$

that divides ab.

Let $r = (p_1 \cdots p_i)$ and $s = (q_1 \cdots q_j)$.

Then $c = rs$, $r \mid a$, $s \mid b$ and $\gcd(r, s) = 1$.

E. A Property of the gcd

Q1

Suppose a is odd and b is even, or vice versa. Then $\gcd(a, b) = \gcd(a + b, a - b)$.

$a + b$ and $a - b$ is odd.

t is a common divisor of $a - b$ and $a + b$. Since they are both odd, then t is odd.

Sum of $a + b$ and $a - b$ is $2a$, and difference is $2b$.

Since $a + b = tx$ and $a - b = ty$, then

$$(a + b) + (a - b) = tx + ty = t(x + y)$$

Likewise

$$(a + b) - (a - b) = t(x - y)$$

Since t is odd, $t \mid 2a \implies t \mid a$, and also $t \mid b$ thus if $t = \gcd(a + b, a - b)$, then

$$\gcd(a, b) = \gcd(a + b, a - b)$$

Q2

Suppose a and b are both odd. Then $2\gcd(a, b) = \gcd(a + b, a - b)$.

a and b are both odd.

$a + b$ and $a - b$ are thus even.

t is a common divisor of $a + b$ and $a - b$. So t is even.

$$(a + b) + (a - b) = 2a = t(x + y)$$
$$(a + b) - (a - b) = 2b = t(x - y)$$

That is $2|t$ and so $t = 2\gcd(a, b)$ but $t = \gcd(a + b, a - b)$

$$2\gcd(a, b) = \gcd(a + b, a - b)$$

Q3

If a and b are both even, explain why either of the two previous conclusions are possible.

$$a = 2n \qquad b = 2m$$
$$\gcd(a, b) = t = 2x$$
$$a + b = 2(n + m) \qquad a - b = 2(n - m)$$
$$\gcd(a + b, a - b) = s = 2y$$

$$2a = t(x + y) \qquad 2b = t(x - y)$$

a and b are even, so is t.

Thus either case is true: $t \mid a$ or $t \mid 2a$.

There isn't enough information to infer whether $t = \gcd(a, b)$ or $t = 2\gcd(a, b)$.

F. Least Common Multiples

Q1

Prove: The set of all the common multiples of a and b is an ideal of $\mathbb{Z}$.

$$I = \{n \cdot \mathrm{lcm}(a, b) : n \in \mathbb{Z}\}$$

$$x, y \in I, x + y = i \cdot \mathrm{lcm}(a, b) + j \cdot \mathrm{lcm}(a, b) = (i + j) \cdot \mathrm{lcm}(a, b)$$
$$-x = -i \cdot \mathrm{lcm}(a, b) \in I$$

because if $a \mid c$ then $a \mid -c$

Lastly let $w \in \mathbb{Z}$

$$w \cdot x = (wi) \cdot \mathrm{lcm}(a, b)$$

and since $wi \in \mathbb{Z}$, so $w \cdot x \in I$.

So I is an ideal of $\mathbb{Z}$.

Q2

Prove: Every pair of integers a and b has a least common multiple.

Every ideal of $\mathbb{Z}$ is principal.

That means there exists a generator

$$I = \{n \cdot \mathrm{lcm}(a, b) : n \in \mathbb{Z}\} = \langle t \rangle$$

which is a least value.

By the well ordering principle $t = 1 \cdot \mathrm{lcm}(a, b) = \mathrm{lcm}(a, b)$.

Since $x \mid xy$ for integers $x, y \in \mathbb{Z}$ where $x \neq 0$ and $y \neq 0$, then I must contain xy and is non-trivial.

Q3

Prove $a \cdot \mathrm{lcm}(b, c) = \mathrm{lcm}(ab, ac)$.

$$l = \mathrm{lcm}(ab, ac)$$

then

$$l = abx = acy$$

for some integers x and y.

So a is a factor of l

$$l = am$$

$$am = abx = acy$$

thus

$$m = \mathrm{lcm}(b, c)$$

$$a \cdot \mathrm{lcm}(b, c) = \mathrm{lcm}(ab, ac)$$

Q4

If $a = a_1 c$ *and* $b = b_1 c$ *where* $c = \gcd(a, b)$*, then* $\operatorname{lcm}(a, b) = a_1 b_1 c$*.*

$$\operatorname{lcm}(a, b) = \operatorname{lcm}(a_1 c, b_1 c) = c \cdot \operatorname{lcm}(a_1, b_1)$$

But $\gcd(a, b) = c$ and $\gcd(a_1 c, b_1 c) = c$ so $\gcd(a_1, b_1) = 1$. Since there is no q such that both $q \mid a_1$ and $q \mid b_1$, then

$$\begin{aligned}
\operatorname{lcm}(a, b) &= ax = by \\
&= a_1 cx = b_1 cy \\
&= cm \\
m &= a_1 x = b_1 y
\end{aligned}$$

We know that $\gcd(a_1, b_1) = 1$, which means a_1 and b_1 contain unique prime factors. That is that $x = b_1$ and $y = a_1$.

$$\operatorname{lcm}(a, b) = a_1 b_1 c$$

Q5

Prove $\operatorname{lcm}(a, ab) = ab$

$$\begin{aligned}
\operatorname{lcm}(a, ab) &= a \cdot \operatorname{lcm}(1, b) \\
&= ab
\end{aligned}$$

Q6

If $\gcd(a, b) = 1$ *then* $\operatorname{lcm}(a, b) = ab$*.*

From 4,

$$a = a_1 \gcd(a, b) \qquad\qquad = a_1 \cdot 1 = a_1$$

and also $b = b_1$, so

$$\begin{aligned}
\operatorname{lcm}(a, b) &= a_1 b_1 c \\
&= ab \cdot \gcd(a, b) \\
&= ab
\end{aligned}$$

Q7

If $\operatorname{lcm}(a, b) = ab$ *then* $\gcd(a, b) = 1$*.*

$$\begin{aligned}
\operatorname{lcm}(a_1 c, b_1 c) &= c \cdot \operatorname{lcm}(a_1, b_1) \\
ab &= c \cdot \operatorname{lcm}(a_1, b_1) \\
(a_1 c)(b_1 c) &= c \cdot \operatorname{lcm}(a_1, b_1) \\
a_1 b_1 c &= \operatorname{lcm}(a_1, b_1)
\end{aligned}$$

But $\gcd(a_1, b_1) = 1 \implies \operatorname{lcm}(a_1, b_1) = a_1 b_1$ so

$$\begin{aligned}
a_1 b_1 c &= a_1 b_1 \\
c &= 1 \\
\gcd(a, b) &= 1
\end{aligned}$$

Q8

Let $\gcd(a, b) = c$. *Then* $\operatorname{lcm}(a, b) = ab/c$.

$$\begin{aligned}\operatorname{lcm}(a, b) &= \operatorname{lcm}(a_1 c, b_1 c) \\ &= c \cdot \operatorname{lcm}(a_1, b_1)\end{aligned}$$

but $\gcd(a, b) = \gcd(a_1 c, b_1 c) = c \implies \gcd(a_1, b_1) = 1$ so $\operatorname{lcm}(a_1, b_1) = a_1 b_1$.

$$\begin{aligned}\operatorname{lcm}(a, b) &= c \cdot \operatorname{lcm}(a_1, b_1) \\ &= c a_1 b_1 \\ &= (a_1 c)(b_1 c)/c \\ &= ab/c\end{aligned}$$

Q9

Let $\gcd(a, b) = c$ *and* $\operatorname{lcm}(a, b) = d$. *Then* $cd = ab$.

$$\operatorname{lcm}(a, b) = d = ab/c$$

$$cd = ab$$

G. Ideals in $\mathbb{Z}$

Q1

$\langle n \rangle$ is a prime ideal iff n is a prime number.

Prime ideal:

if $ab \in J$ then $a \in J$ or $b \in J$.

Let $J = \langle n \rangle$ be a prime ideal in $\mathbb{Z}$.

Then $J = \{nx : x \in \mathbb{Z}\}$

Let $y \in J$, then $y = nx$ and $n \in J$.

Let $J = \langle n = uv \rangle$ where n is non-prime.

Then $uv \in J$ but $u \notin J$ and $v \notin J$, so n must be prime.

Q2

Every prime ideal of is a maximal ideal.

$\langle p \rangle \subseteq \langle a \rangle$ so $p \in \langle a \rangle$ but $\langle p \rangle \neq \langle a \rangle \implies p \neq a$ and so $p = a \cdot n$ for some $n \in \mathbb{Z}$.

But p is prime and since $\langle p \rangle \subseteq \langle a \rangle$, then $a < p$, but $a \nmid p$ and $\gcd(a, p) = 1$.

$p \in \langle a \rangle \implies p = a \cdot n$ for some $n \in \mathbb{Z}$ but $\gcd(a, p) = 1 \implies n = p$, therefore $a = 1$ and so $\langle a \rangle = \mathbb{Z}$. Thus every prime ideal $\langle p \rangle$ of $\mathbb{Z}$ is a maximal ideal.

Q3

For every prime number p, $\mathbb{Z}_p$ is a field.

Prime ideal:

if $ab \in J$ then $a \in J$ or $b \in J$.

Definition of a field: a commutative ring with unity where every nonzero element is invertible.

Every field is an integral domain.

Definition of an integral domain: a commutative ring with unity having the cancellation property. That is $ab = ac \implies b = c$.

From the end of chapter 19 on quotient rings, we have J is a maximal ideal of A (proven above).

$A = \mathbb{Z}$ is a commutative ring with unity so the coset $J + 1$ is the unity of A/J since $(J + 1)(J + a) = J + a$.

Now finally to prove A/J is a field we must show for every a, there exists x such that

$$(J + a)(J + x) = J + 1$$

$$K = \{xa + j : x \in A, j \in J\}$$

K is an ideal, $a \in K$ because $a = 1a + 0$ and $\forall j \in J$, $j \in K$ because $j = 0a + j$.

K is an ideal and contains J, but also $a \notin J$ and $a \in K$ so K is bigger than J.

But J is maximal so $K = A$.

Therefore $1 \in K$ so $1 = xa + j$ for some $x \in A$ and $j \in J$, that is $1 - xa = j \in J$.

$$J + 1 = J + xa = (J + x)(J + a)$$

So $J + x$ is the multiplicative inverse of $J + a$.

Thus A/J is a field.

Q4

If $c = \operatorname{lcm}(a, b)$*, then* $\langle a \rangle \cap \langle b \rangle = \langle c \rangle$*.*

$$c = \operatorname{lcm}(a, b)$$

$\langle c \rangle = \{n \cdot c : n \in \mathbb{Z}\}$ therefore $\langle c \rangle$ contains all the multiples of a and b.

$\langle a \rangle$ is all the multiples of a, $\langle b \rangle$ contains all the multiples of b, and $\langle a \rangle \cap \langle b \rangle$ are all the multiples of a and b.

Any $x \in \langle a \rangle \cap \langle b \rangle$ is both in $\langle a \rangle$ and $\langle b \rangle$ and so is a multiple of both a and b. Therefore $x \in \langle c \rangle$.

$$\langle a \rangle \cap \langle b \rangle = \langle c \rangle$$

Q5

Let ϕ be a homomorphism such that

$$\phi : \mathbb{Z} \to A$$

And let J be the ideal of ϕ.

Every ideal of $\mathbb{Z}$ is principal. By the well ordering principle pick the least value $n \in J$, and let m be any element of J. By the division algorithm $m = nq + r$ where $0 \leq r < n$. Since $n \in J$ and $m \in J$, then $r = m - nq \in J$. So either $r = 0$ or $r > 0$. But n is the least value in J, so $r = 0$. So $m = nq$.

$$J = \langle n \rangle$$

$$\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$$

Since the ideal of ϕ is $\langle n \rangle$, so

$$A \cong \mathbb{Z}/\langle n \rangle$$

Every homomorphic image of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ for some n.

Q6

Let G be a group and let $a, b \in G$. Then $S = \{n \in \mathbb{Z} : ab^n = b^n a\}$ is an ideal of $\mathbb{Z}$.

S is an ideal of $\mathbb{Z}$ if it satisfies the following conditions:

1. $(S, +)$ is a subgroup of $(\mathbb{Z}, +)$
2. For every $r \in \mathbb{Z}$ and every $x \in S$, the product rx is in S

Prove S is closed under addition for $x, y \in S$:

$$\begin{aligned} ab^{x+y} &= ab^x b^y = b^x ab^y \\ &= b^x b^y a \\ &= b^{x+y} a \end{aligned}$$

Prove that for any $x \in S$, that $-x \in S$:

$$\begin{aligned} ab^n &= b^n a \\ b^{-n} ab^n &= a \\ b^{-n} a &= ab^{-n} \end{aligned}$$

Lastly prove that for any $r \in \mathbb{Z}$ and every $x \in S$, the product $rx \in S$.

Observe firstly that $ab^n = b^n a$ and then note that $ab^{nx} = a \underbrace{b^n b^n \cdots b^n}_{x \text{ times}}$. But $b^n = a^{-1} b^n a$.

$$\begin{aligned} ab^{nx} &= a \underbrace{(a^{-1} b^n a)}_{b^n} b^n \cdots b^n \\ &= (b^n a) b^n \cdots b^n \\ &= (b^n a)(a^{-1} b^n a) \cdots b^n \\ &= b^n (b^n a) \cdots b^n \\ &= b^{nx} a \end{aligned}$$

And so S is an ideal of $\mathbb{Z}$.

Q7

Let G be a group, H a subgroup of G, and $a \in G$. Then

$$S = \{n \in \mathbb{Z} : a^n \in H\}$$

is an ideal of $\mathbb{Z}$.

Let $x, y \in S$, then $a^{x+y} = a^x a^y \in H$ since H is a group. Also $a^x \in H \implies a^{-x} \in H$.

Finally for any $z \in \mathbb{Z}, a^{xz} = \underbrace{(a^x)(a^x) \cdots (a^x)}_{z \text{ times}} \in H$.

So $S = \{n \in \mathbb{Z} : a^n \in H\}$ is an ideal of $\mathbb{Z}$.

Q8

Prove if $\gcd(a, b) = d$, then $\langle a \rangle + \langle b \rangle = \langle d \rangle$.

Let there be homomorphisms from $\mathbb{Z}$ onto $\langle a \rangle$ and $\langle b \rangle$ defined by

$$\phi(x) = \bar{x}$$

Then $\langle a \rangle \cong \mathbb{Z}/J$ and $\langle b \rangle \cong \mathbb{Z}/K$.

Then $\langle a \rangle + \langle b \rangle = J + K$

$$J + K = \{x + y : x \in J, y \in K\}$$

All ideals of $\mathbb{Z}$ are principal so there exists a generator t such that $J + K = \langle t \rangle$.

But $t = x + y$ for some $x \in J$ and $y \in K$. And $x = ka$ where $k \in \mathbb{Z}$ and $y = lb$ where $l \in \mathbb{Z}$. Thus $t = ka + lb$.

Since $\gcd(a, b) = d$ and $\langle t \rangle = J + K$ is the set of linear combinations of a and b, we know from theorem 3, that $\langle t \rangle$ is an ideal and the $\gcd(a, b)$.

Thus $J + K = \langle d \rangle$ and so

$$\langle a \rangle + \langle b \rangle = \langle d \rangle$$

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

H. The gcd and the lcm as Operations on $\mathbb{Z}$

For any two integers a and b, let $a \star b = \gcd(a, b)$ and $a \circ b = \operatorname{lcm}(a, b)$. Prove the following properties of these operations:

Q1

$\star$ and $\circ$ are associative.

First we prove $(a \star b) \star c = a \star (b \star c)$ or that $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$

$$\gcd(a, b) \implies a = a_1 r, b = b_1 r$$

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

$$\gcd(\gcd(a, b), c) = \gcd(r, c) \implies r = r_1 u, c = c_1 u$$

$$\gcd(\gcd(a, b), c) = u$$

Now note that $b = b_1 r = b_1 r_1 u$ so

$$\gcd(b, c) = \gcd(b_1 r_1 u, c_1 u) = u$$

and

$$\gcd(a, \gcd(b, c)) = \gcd(a_1 r_1 u, u) = u$$

so

$$(a \star b) \star c = a \star (b \star c)$$

Secondly we prove $(a \circ b) \circ c = a \circ (b \circ c)$ or that $\operatorname{lcm}(\operatorname{lcm}(a, b), c) = \operatorname{lcm}(a, \operatorname{lcm}(b, c))$

Note that $t = \operatorname{lcm}(a, \operatorname{lcm}(b, c))$ then $a \mid t$ and $\operatorname{lcm}(b, c) \mid t$. And $r = \operatorname{lcm}(b, c)$ then $b \mid r$ and $c \mid r$, but also $r \mid t \implies b \mid t$ and $c \mid t$.

Therefore $a \mid t$, $b \mid t$ and $c \mid t$.

Likewise through the same method we can conclude $\operatorname{lcm}(\operatorname{lcm}(a, b), c) \mid \operatorname{lcm}(a, \operatorname{lcm}(b, c))$ and so they are equal.

That is given they are the *least* multiple of a, b, c and so should divide the other value which is also a multiple of a, b and c.

From this we conclude they are equal.

We can also use the fact that

$$\begin{aligned}
\operatorname{lcm}(a, \operatorname{lcm}(b, c)) &= \operatorname{lcm}(a, 1^{\max(b_1, c_1)} \cdot 2^{\max(b_2, c_2)} \cdot 3^{\max(b_3, c_3)} \cdot 5^{\max(b_4, c_4)} \cdot 7^{\max(b_5, c_5)} \ldots) \\
&= 1^{\max(a_1, b_1, c_1)} \cdot 2^{\max(a_2, b_2, c_2)} \cdot 3^{\max(a_3, b_3, c_3)} \cdot 5^{\max(a^4, b^4, c^4)} \cdot 7^{\max(a^5, b^5, c^5)} \ldots
\end{aligned}$$

since the max operation is associative.

Q2

There is an identity element for $\circ$, but not for $\star$ (on the set of positive integers).

Let there be an identity element e for $\star$, then $\gcd(a, e) = a \implies a \mid e$ but also $\gcd(n \cdot a, e) = n \cdot a \implies n \cdot a \mid e$. So every number divides e, and it contains every prime number an infinite number of times as its factor.

Thus there is no identity for $a \star b = \gcd(a, b)$.

For the lcm note that

$$a \circ b = \operatorname{lcm}(a, b) = ab/\gcd(a, b)$$

For the identity operation

$$ae/\gcd(a, e) = \operatorname{lcm}(a, e) = a$$

$$ae = a\gcd(a, e)$$

$$e = \gcd(a, e)$$

So e divides all natural numbers

$$e = 1$$

Q3

Which integers have inverses with respect to $\circ$?

Only 1 has an inverse because

$$\operatorname{lcm}(a, b) = 1$$

$$\gcd(a, b) = ab/\operatorname{lcm}(a, b) = ab$$

that is

$$\begin{aligned} a &= a_1(ab) \\ &= a_1((a_1ab)b) \\ &= a_1a_1 \cdots b \cdot b \end{aligned}$$

$$\implies a, b = 1$$

Q4

Prove: $a \star (b \circ c) = (a \star b) \circ (a \star c)$.

$$\begin{aligned} a \star (b \circ c) &= \gcd(a, \operatorname{lcm}(b, c)) \\ (a \star b) \circ (a \star c) &= \operatorname{lcm}(\gcd(a, b), \gcd(a, c)) \end{aligned}$$

Let $a = a_1fg$, $b = b_1fx$, and $c = c_1gx$.

$$\begin{aligned} \gcd(a, bc/\gcd(b, c)) &= \gcd(a, bc/x) \\ &= gcd(a_1fg, b_1fxc_1gx/x) \\ &= fg \end{aligned}$$

$$\begin{aligned} \operatorname{lcm}(\gcd(a, b), \gcd(a, c)) &= \gcd(a, b) \cdot \gcd(a, c)/\gcd(\gcd(a, b), \gcd(a, c)) \\ &= fg/\gcd(f, g) = fg \end{aligned}$$