M311S24 Problem Set 2 *Franchi-Pereira, Philip*

Problem 1.a Let S be a semigroup with some (not necessarily unique) left neutral element e_L, and such that any element a has a left inverse b_L with respect to e_L. Show that S is in fact a group.

Proposition 1: All left inverses b_L with respect to e_L in S are also right inverses

Note that since $b_L \in S$, then it too has an inverse, denoted by b_L^{-1}, such that $b_L^{-1} b_L = e_L$. Then by associativity and the definition of our inverses:

$$\begin{aligned} b_L a = e_L = b_L^{-1} b_L = b_L^{-1}(e\, b_L) = b_L^{-1}((b_L a) b_L) \\ = (b_L^{-1} b_L)(a b_L) = e(a b_L) = a b_L \end{aligned}$$

Proposition 2: If $e_L$is a left neutral of S, then it is also a right neutral.

It follows from Prop 1 that $b e_L = b(b^{-1} b) = (b b^{-1}) b = e_L b = b$

Proposition 3: The every element $a \in S$ has a two inverses b and b', then $b = b'$, and b is unique.

Similarly to the previous proof, $b = eb = (b'a)b = b'(ab) = b'$, so we see that $b = b'$, and all inverses of b are equal to each other, so they are all the same. So, b is unique.

Proof: Since the semigroup S has an associative operation, contains a unique identity element, and every element in S has a unique inverse, then by definition S is a group.

1.b Let S be a semigroup which has a left neutral e_L and such that any element a has a right inverse b_R with respect to e_L. Is S necessarily a group? Prove or give a counter-example.

Counter Example: Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \phi(a, b) \mapsto b$. We will show that ϕ is associative

$$(ab)c = (b)c = (bc) = c$$

$$a(bc) = a(c) = (ac) = c$$

So $\mathbb{Z}, \phi$ is a semigroup. Furthermore, every integer can be a left neutral element, since for any $b \in \mathbb{Z}$, all elements $a \in \mathbb{Z}$ by definition give $\phi(a, b) = b$. Finally, every element $a \in \mathbb{Z}$ has a right inverses with respect to e_L. Since e_L can be any integer, any $a, b \in \mathbb{Z}$ produces $\phi(a, b) = b$ and for any $c \in S$ we have $\phi(b, c) = c$.

However, ϕ is not a group, since there is no unique neutral element. Any element in the group can be left neutral, but there is no e such that $a, b \in S,\ a \neq b$, where $\phi(a, e) = a$ and $\phi(b, e) = b$.

Problem 2.a Let G be a group such that for all $g \in G,\ g^2 = e$. Prove that G is abelian.

Proof: Let $a, b \in G$. To show that $ab = ba$, note that the inverse of ab is ba, since $(ba)(ab) = b(aa)b = bb = e$. Note also that $ba \in G$, so by assumption $(ba)^2 = e$. It follows that $ab = e(ab) = ((ba)(ba))(ab) = (ba)((ba)(ab)) = (ba)e = ba$.

2.b Suppose, instead we have for all $g \in G,\ g^3 = e$. Is G necessarily abelian? Prove or give a counterexample.

Counter Example: Take the subset of $GL_3(\mathbb{Z}_3)$ of upper triangular, invertible matrices of the form:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

where $a, b, c \in \mathbb{Z}_3$.

By BB 3.2.4, we only need to show that the operation is also closed under the subgroup.

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & e & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+e & ag+b+f \\ 0 & 1 & c+g \\ 0 & 0 & 1 \end{bmatrix}$$

Note that for any $g \in G$, we have $g^3 = e$.

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2a & ac+2b \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{bmatrix}$$

And then

$$\begin{bmatrix} 1 & 2a & ac+2b \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3a & 3(ac+b) \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{bmatrix}$$

Since $3|3a,\ 3|3(ac+b)$, and $3|3c$, all become 0 under the field $\mathbb{Z}_3$, and we are left with the identity.

It is not abelian however, since

$$\begin{bmatrix} 1 & e & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+e & b+ec+f \\ 0 & 1 & c+g \\ 0 & 0 & 1 \end{bmatrix}$$

Problem 3 Let G be finite group and let $2|o(G)$. Prove that G has an odd number of elements of order 2. In particular G has at least one element of order 2.

Proposition: Let $n = o(g)$. If $g = g^{-1}$, then $n \leq 2$.

Since $g = g^{-1}$, then $g^2 = e$, and so by definition of order, n cannot be greater than 2. Then it can either be $o(g) = 2$, or $o(g) = 1$. In the case where $n = 1$, then $g^1 = e$, and so $g = e$.

Proof: First, we will partition G into a collection of disjoint subsets. Since G is a group, by definition for all $g \in G$, there exists a unique inverse g^{-1}. So, we will partition G into subsets such that for all $g \in G$, $S_g = \{g, g^{-1}\}$. It is clear that these partitions are covering, and that there are no empty partitions. We will show that they are also disjoint.

For any other $b \in G$, b is in the partition $S_b = \{b, b^{-1}\}$. Suppose $b = g$, then $b^{-1} = g^{-1}$, and so $S_b = \{b, b^{-1}\} = \{g, g^{-1}\} = S_g$. So if any element in S_g is in a different partition, those two are actually the same partition. Suppose instead that $b \neq g$ then $b^{-1} \neq g^{-1}$ since by the definition of an inverse in a group each inverse is unique. Therefore $S_g \cap S_b = \emptyset$. Since every $g \in G$ is in a partition, and every partition is either disjoint or equal to one another, then

$$G = \bigcup_{g \in G} \{g, g^{-1}\}$$

By ClassNotes 2.2.12, $o(G)$ is equal to the sum of the order of each partition. To find $o(G)$ we will re-partition G into two subsets:

$$M = \{\{m, m^{-1}\} : o(m) > 2, \text{ and } m, m^{-1} \in G\}$$
$$L = \{\{l, l^{-1}\} : o(l) \leq 2, \text{ and } l, l^{-1} \in G\}$$

By our lemma, for all $H = \{h, h^{-1}\}$, $H \in M$, since $o(H) > 2$, then $h \neq h^{-1}$ and so $o(H) = 2$. We also have for all $K = \{l, l^{-1}\}$, $K \in L$, $o(K) \leq 2$ and $l = l^{-1}$, so $K = \{l, l\} = \{l\}$. We may redefine L to see

$$L = \{\{l\} : o(l) \leq 2, \text{ and } l \in G\}$$

So, all subsets in M have two elements, and all subsets in L have one element. Therefore $o(G) = 2(|M|) + |L|$.

Every $K \in L$ has only one element, and therefore by our lemma has either order 1 or 2. Let L^1 and L^2 be the partitions of order 1 and 2 respectively. Then $|L| = |L^1| + |L^2|$. But there is only one partition of order 1, e. Therefore, $|L^2| = |L| - 1$ and since $|L|$ must be even, $|L^2|$ must be odd, so there are an odd number of partitions of order 2. Since each partition is just one element, then there are an odd number of elements of order 2.

Finally, we show that if $2|o(G)$ then there is always at least one element with order 2 in G. By definition every group has an identity, and therefore $|L^1| = 1$. Since $2M + |L^2| + 1$ must be even, then $|L^2| + 1$ must be even, and so $|L^2|$ must be an odd integer. The smallest $|L^2|$ could be is 1, so there must always be at least one element of order 2 in G.

Problem 4 Let H and K be subgroups of a group. Prove that $H \cap K$ is a subgroup of G.

Proof: For all $a, b \in H \cap K,\ a, b \in H$. Since H is also a group, then clearly $ab \in H$. Likewise, $a, b \in K$, so $ab \in K$. Since ab is in both H and K, $ab \in H \cap K$. Therefore by BB.Corollary 3.2.4, $H \cap K$ is a subgroup of G.

Problem 5 Fill out the table. The first row of the table was computed using software, and the rest using the Sign Change Identities listed in ClassNotes 5.1.9.

(m,n)	md(m,n)	qt(m,n)
(987654321, 7531)	1326	131145
(987654321, -7531)	1326	-131145
(-987654321, 7531)	-1326	-131146
(-987654321, -7531)	6205	131146

Problem 6 Let a and b be positive integers. Let $a = h(a, b),\ b = k(a, b)$. Take any pair ω, γ with $\omega a + \gamma b = (a, b)$. Show that $(\omega, \gamma) = 1$ and $(h, k) = 1$.

Proof: Let $d = gcd(a, b)$. Then $a = hd,\ b = kd$ and $\omega a + \gamma b = d$. It follows that $\omega a + \gamma b = \omega(hd) + \gamma(kd) = (\omega h + \gamma k)d = d$. Since we are operating on integers, we may cancel d from both sides, and get $(\omega h + \gamma k) = 1$. But then this is definition of the greatest common denominator, and we have $(\omega, \gamma) = 1$ and $(h, k) = 1$.

Problem 7 Let a, b, a_1, b_1 be non-zero integers. Assume that $(a, b) = 1$ and $(a_1, b_1) = 1$ and that $ab_1 = a_1 b$. Show that either $a = a_1,\ b = b_1$ or $a = -a_1,\ b = -b_1$.

Proposition: If $(a, b) = 1$, then $(a, -b) = 1$.

If $(a, b) = 1$, then there exist some $\lambda, \omega \in \mathbb{Z}$ such that $\lambda a + \omega b = 1$. For $(a, -b)$ to equal one, there must be $\lambda', \omega' \in \mathbb{Z}$ such that $\lambda' a + \omega'(-b) = 1$. Letting $\lambda' = \lambda$ and $\omega' = -\omega$, we see that $\lambda' a + \omega'(-b) = \lambda a + \omega(b)$ which equals 1, which is the definition of the GCD $(a, -b) = 1$.

Proof: Since $ab_1 = a_1 b$, it follows that $ab_1 | a_1 b$ and $a_1 b | ab_1$. Since $a | ab_1$, then $a | a_1 b$. By BB Prop 1.2.3b, since $(a, b) = 1$, then $a | a_1$. Similarly, $a_1 | a_1 b$ and so $a_1 | ab_1$. Since $(a_1, b_1) = 1$, then $a_1 | a$. An similar argument shows that $b | b_1$ and $b_1 | b$. Therefore, $a = a_1$ and $b = b_1$.

Note however, that $a_1 b = (1)(a_1 b) = (-1)(-1)(a_1 b) = (-a_1)(-b)$, in which case we see that since $a | ab_1$ and $ab_1 | (-a_1)(-b)$, then $a | (-a_1)(-b)$, and since $(a, -b) = 1$, $a | -a_1$. A similar argument yields $a_1 | -a,\ b | -b_1$, and

$b_1| - b$, which results in a second solution, $a = -a_1,\ b = -b_1$. Therefore either $a = a_1$ and $b = b_1$, or $a = -a_1$ and $b = -b_1$.

Problem 8 Find (a, b) and ω and γ such that $(\omega, \gamma) = (a, b)$ for (1) $a = 26460, b = 126000$ and (2) $a = 12091, b = 8439$

Note: The role of qt was performed by $a//b$ in Python, and md by $a\%b$ in Python.

1. $a = 26460, b = 126000$. As provided, this is 0. Assuming instead that a is the larger value of the two, then instead we have:

$$\begin{aligned} 126000 &= 26460(4) + 20160 \\ 26460 &= 20160(1) + 6300 \\ 20160 &= 6300(3) + 1260 \\ 6300 &= 1260(5) + 0 \end{aligned}$$

   So $\gcd(126000, 26460) = 1260$.

2. $a = 12091, b = 8439$

$$\begin{aligned} 12091 &= 8439(1) + 3652 \\ 8439 &= 3652(2) + 1135 \\ 3652 &= 1135(3) + 247 \\ 1135 &= 247(4) + 147 \\ 247 &= 147(1) + 100 \\ 147 &= 100(1) + 47 \\ 100 &= 47(2) + 6 \\ 47 &= 6(7) + 5 \\ 6 &= 5(1) + 1 \\ 5 &= 1(5) + 0 \end{aligned}$$

   Therefore these two numbers are relatively prime, $(12091, 8439) = 1$.

Problem 9.a The set $a\mathbb{Z} \cap b\mathbb{Z}$ is by definition the set of common multiples of a and b. Cite a result that shows that $a\mathbb{Z} \cap b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Why is this subgroup non-trivial?

Proof: In Problem 4 we proved that the intersection of two subgroups is itself a subgroup. Next we show that it is not trivial. Considering a as an element in $a\mathbb{Z}$ and b as a multiple, we have $ab, -ab \in a\mathbb{Z}$ and similarly we have $b \in b\mathbb{Z}$, with a multiple a such that $ab, -ab \in b\mathbb{Z}$. So $ab \in a\mathbb{Z}$ and $ab \in b\mathbb{Z}$, so $a\mathbb{Z} \cap b\mathbb{Z}$ is not empty.

But since $a \notin b\mathbb{Z}$ and $b \notin a\mathbb{Z}$, not every element in $a\mathbb{Z}$ and $b\mathbb{Z}$ is in the subgroup either, so it is not trivial.

9.b Use our results on subgroups of $\mathbb{Z}$ to show that the smallest positive common multiple of a and b is in fact the least common multiple.

Proof: Let $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, the set of all multiples of both a and b. This set is clearly not empty, since both $a\mathbb{Z}$ and $b\mathbb{Z}$ contain ab. Take $m\mathbb{Z} \cap \mathbb{N}$, denoted $m\mathbb{Z}^+$. Clearly every element in it is positive, and so by the Well Ordering Principle, this set has a smallest element, l, such that for all $x \in m\mathbb{Z}^+,\ l \leq x$. By construction, every element of $m\mathbb{Z}$ is a multiple of a and b, and smallest, then it is a least common multiple of a and b.

It is unique, since if there was another element s in $m\mathbb{Z}$ such that for all $m \in m\mathbb{Z}$, $s|m$, then we would have $s|l$, but since we also have $l|s$ by the construction of l, then $s = l$.

9.c Take $a = h(a, b)$ and $b = k(a, b)$. Which previous result shows that h and k are relatively prime?

This was shown directly in Problem 6.

9.d Let c be a common multiple of a and b. Certainly $(a, b)|c$ so we have $c = n(a, b)$. Show that $k|n$ and $h|n$. What result allows us to conclude that $hk|n$?

Proof: Since c is a multiple of a and $a = h(a, b)$, then there must exist some m_1 such that $c = n(a, b) = m_1 h(a, b)$. Likewise c is a multiple of b and so there must be an m_2 such that $c = n(a, b) = m_2 k(a, b)$. Cancelling (a, b) we get $n = hm_1 = km_2$, so $h|n$, and $k|n$. Since $(h, k) = 1$ by BB Prop 1.2.3c, $hk|n$.

9.e Show that $[a, b] = hk(a, b)$.

Proof: For any common positive multiple c of a, b, we have $c = pa = qb$ for some $p, q \in \mathbb{Z}$. Then we can see that $c = ph(a, b) = qk(a, b)$. Cancelling (a, b) we see that $ph = qk$. Since $(h, k) = 1$, then $k|p$ and $h|q$, so $p = xk$ and $q = yh$. Substituting those values back we see $c = ph(a, b) = xkh(a, b)$. So all multiples of a and b take the form $xkh(a, b)$, with $x \in \mathbb{Z}$. Then the smallest such common positive multiple has $x = 1$, which means $lcm = hk(a, b)$.

Problem 10 The positive numbers a and b are such that $a + b = 57$ and $[a, b] = 680$. What are a and b?

The solution is $a = 17$ and $b = 40$. First, find all the prime factors of 680. This is made easier by the fact that 680 is even, and so $680/2/2/2 = 85$. Then, factoring out 5, $85/5 = 17$, so $680 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 17$. Since $a + b = 57,\ a = 17$ and $b = 40$. Since a and b do not share factors, $(a, b) = 1$ and $[a, b] = \frac{|ab|}{(a,b)} = \frac{|ab|}{1} = 680$.

Problem 11.a Show that if p is prime then $p \neq (a/b)^2$ for a and b integers.

Note: This proof follows closely from the proof given on BB.pxix.

Proof: Suppose for sake of contradiction that p is prime and $p = (a/b)^2$. Then we can write $\sqrt{p} = \frac{m}{n}$ for some integers m, n with $n \neq 0$. Assume that m and n have been reduced to their lowest forms.

Multiplying both sides by n and squaring yields $pn^2 = m^2$, and since $p|pn^2$ then $p|m^2$. By Class Notes Proposition 5.2.3, p divides some factor of m^2, and since $m^2 = m \cdot m$, then $p|m$ by Euclid's Lemma (BB.12.5). So $m = pk$ for some $k \in \mathbb{Z}$ and $m^2 = p^2k^2$. Substituting back we see $pn^2 = p^2k^2$ and cancelling p from both sides, we get $n^2 = pk^2$, so $p|n^2$ and then $p|n$. Since $p|n$ and $p|m$, we have a contradiction, since m and n were given in their reduced forms.

11.b Show that the the set $\mathrm{S} = \{a + b\sqrt{p} : \{a, b\} \subset \mathbb{Q}\}$ is a field.

Addition:

Associativity For $\alpha, \omega, \lambda \in S$, we have

$$\begin{aligned}(\alpha + \omega) + \lambda &= ((a_\alpha + b_\alpha\sqrt{p}) + (a_\omega + b_\omega\sqrt{p})) + \lambda \\ &= ((a_\alpha + a_\omega) + (b_\alpha + b_\omega)\sqrt{p}) + (a_\lambda + b_\lambda\sqrt{p}) \\ &= ((a_\alpha + a_\omega + a_\lambda) + (b_\alpha + b_\omega + b_\lambda)\sqrt{p}) \\ &= (a_\alpha + b_\alpha\sqrt{p}) + ((a_\omega + a_\lambda) + (b_\omega + b_\lambda)\sqrt{p}) \\ &= \alpha + ((a_\omega + b_\omega\sqrt{p}) + (a_\lambda + b_\lambda\sqrt{p})) \\ &= \alpha + (\omega + \lambda)\end{aligned}$$

Commutativity For $a, b, c, d \in \mathbb{Q}$, we have $(a+b\sqrt{p})+(c+d\sqrt{p}) = (a+c)+(b+d)\sqrt{p} = (c+a)+(d+b)\sqrt{p} = (c+d\sqrt{p})+(a+b\sqrt{p})$.

Inverse For $a, b \in \mathbb{Q}$, the inverse to $(a + b\sqrt{p})$ is $-a + -b\sqrt{p}$, such that $(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a - a) + (b - b)\sqrt{p} = 0 + 0\sqrt{p} = 0$.

Identity The element $0 + 0\sqrt{p}$ is the identity for addition, since $(a + b\sqrt{p}) + (0 + 0\sqrt{p}) = (a+) + (b + 0)\sqrt{p} = a + b\sqrt{p}$.

Multiplication:

Identity The element $1 + 0\sqrt{p}$ is the identity for addition, since $(a + b\sqrt{p}) \cdot (1 + 0\sqrt{p}) = (a \cdot 1) + (b \cdot 1)\sqrt{p} + (a \cdot 0\sqrt{p}) + (b\sqrt{p} \cdot 0\sqrt{p}) = a + b\sqrt{p}$.

Associativity For $\alpha = (a + b\sqrt{p}),\ \omega = (c + d\sqrt{p}),\ \lambda = (e + f\sqrt{p})$, we have

$$\begin{aligned}(\alpha \cdot \omega) \cdot \lambda &= ((a + b\sqrt{p}) * (c + d\sqrt{p})) * (e + f\sqrt{p}) \\ &= ((ac + bdp) + (bc + ad)\sqrt{p}) \cdot (e + f\sqrt{p}) \\ &= (padf + pbcf + pebd + eac) + (acf + ead + ebc + bdfp)\sqrt{p} \\ &= (a + b\sqrt{p}) \cdot ((ec + dfp) + (cf + ed)\sqrt{p}) \\ &= \alpha \cdot (\omega \cdot \lambda)\end{aligned}$$

Commutativity For $\alpha = (a + b\sqrt{p}),\ \omega = (c + d\sqrt{p})$ we have

$$\begin{aligned}\alpha \cdot \omega &= (a + b\sqrt{p}) \cdot (c + d\sqrt{p}) \\ &= (ac + bdp) + (ad + bc)\sqrt{p} \\ &= (ca + dbp) + (da + cb)\sqrt{p} \\ &= (c + d\sqrt{p}) \cdot (a + b\sqrt{p}) \\ &= \omega \cdot \alpha\end{aligned}$$

Inverses For any $\alpha = (a + b\sqrt{p})$, we have $\alpha^{-1} = \frac{a - b\sqrt{p}}{a^2 - b^2\sqrt{p}}$

Since $(a + b\sqrt{p}) \cdot (a - b\sqrt{p}) = (a^2 - b^2\sqrt{p})$, then $\alpha \cdot \alpha^{-1} = (a + b\sqrt{p}) \cdot \frac{a - b\sqrt{p}}{a^2 - b^2\sqrt{p}} = \frac{a^2 - b^2\sqrt{p}}{a^2 - b^2\sqrt{p}} = 1$.

Distributive For $\alpha = (a + b\sqrt{p}),\ \omega = (c + d\sqrt{p}),\ \lambda = (e + f\sqrt{p})$, we have

$$\begin{aligned}\alpha \cdot (\omega + \lambda) &= (a + b\sqrt{p}) \cdot ((c + d\sqrt{p}) + (e + f\sqrt{p})) \\ &= (a + b\sqrt{p}) \cdot ((c + e) + (d + f\sqrt{p})) \\ &= (ac + ae + bdp + bfp) + (bc + ad + be + af)\sqrt{p} \\ &= ((ca + dbp) + (da + cb)\sqrt{p}) + ((ea + fbp) + (ea + fb)\sqrt{p}) \\ &= ((a + b\sqrt{p}) \cdot (c + d\sqrt{p})) + ((a + b\sqrt{p}) \cdot (e + f\sqrt{p})) \\ &= \alpha \cdot \omega + \alpha \cdot \lambda\end{aligned}$$

11.c A number n is a perfect square if there is some number m with $n = m^2$. Show that $n = (\frac{a}{b})^2$ if and only if n is a perfect square.

Proof: First, if n is a perfect square then by definition $n = m^2$ for some integer m. Taking $a = m$ and $b = 1$, then $\frac{a}{b} = \frac{m}{1}$, so $n = (\frac{a}{b})^2$. Conversely, if $n = (\frac{a}{b})^2$, then $\frac{a}{b}$ must be an integer, and so $a = kb$ for some integer k. Then, $\frac{a}{b} = k$, and so $n = k^2$.

11.d Let h and k be relatively prime, with hk a perfect square. Show that h and k are perfect squares.

Proposition: An integer x is a perfect square if and only if for all $p \in \Pr(x),\ \epsilon(x, p)$ is even.

If x is a perfect square then there exists an integer m such that $x = m^2$. Consider m in terms of its unique prime factorization,

$$m = \prod_{p \in \Pr(m)} p^{\epsilon(m,p)}$$

And for m^2 we have

$$m^2 = \prod_{p \in \Pr(m)} p^{\epsilon(m,p)} \cdot p^{\epsilon(m,p)}$$

Since $p^{\epsilon(m,p)} \cdot p^{\epsilon(m,p)} = p^{2\epsilon(m,p)}$ then for all primes $p \in \Pr(m)$, we have $\epsilon(n,p) = 2 \cdot \epsilon(m,p)$, and so for all $p \in \Pr(x)$, $\epsilon(x,p)$ is even.

Conversely if for some number x, for all $p \in \Pr(x)$ if $\epsilon(x,p)$ is even then x is a perfect square. Let $e_i = \epsilon(x,p_i)$ for all $p_i \in \Pr(x)$. If e_i is even, there there exists an integer such that $2k_i = e_i$. Then

$$\begin{aligned} x &= (p_1^{2k_1})(p_2^{2k_2}) \cdots (p_n^{2k_n}) \\ &= (p_1^{k_1})^2 (p_2^{k_2})^2 \cdots (p_n^{k_n})^2 \\ &= ((p_1^{k_1})(p_2^{k_2}) \cdots (p_n^{k_n}))^2 \end{aligned}$$

Since $(p_1^{k_1})(p_2^{k_2}) \cdots (p_n^{k_n})$ is clearly an integer, x is a perfect square.

Proof: First note that since $(h,k) = 1$, and every prime is greater than 1, then there are no primes factors in both $\Pr(h)$ and $\Pr(k)$. In other words,$\Pr(h) \cap \Pr(k) = \emptyset$.

Consider the prime factors of hk. For each $p \in \Pr(hk)$, $\epsilon(hk,p) = \epsilon(h,p) + \epsilon(k,p)$ and is even. However, since h and k do not share factors, then either $\epsilon(hk,p) = \epsilon(h,p)$ and so $\epsilon(h,p)$ is even, or $\epsilon(hk,p) = 0 + \epsilon(k,p)$ and so $\epsilon(k,p)$ is even. Since $\Pr(h) \subset \Pr(hk)$ and $\Pr(k) \subset \Pr(hk)$ then all prime factors of h and k are even, and so both are perfect squares.

Problem 12 We are given that $n(n+30)$ a perfect square. What are the possible values of n?

Since $n(n+30)$ is a perfect square, we have $n^2 + 30n = m^2$. Completing the square to shows that

$$\begin{aligned} n^2 + 30n &= m^2 \\ n^2 + 30n + 255 &= m^2 + 255 \\ (n+15)^2 - m^2 &= 255 \\ (n + 15 + m)(n + 15 - m) &= 3 \cdot 3 \cdot 5 \cdot 5 \end{aligned}$$

The possible values for $(n + 15 + m)$ and $(n + 15 - m)$ are therefore combinations of the factors of 255, and all possible pairs are listed in the table below.

(n + 15 - m)	(n + 15 + m)	n	m
1	225	98	112
3	75	24	±36
5	45	10	±20
9	25	2	±8
15	15	0	0
-1	-225	-128	112
-3	-75	-54	±36
-5	-45	-40	±20
-9	-25	-32	±8
-15	-15	-30	0

For completeness, the computation involved in the first row is shown below. The rest are omitted for the sake of brevity. First, $n + 15 - m = 3$ so $m = n + 12$. Then $n + 15 + m = 75$ and substituting for m yields $2n + 27 = 75$ so $n = 24$. Therefore $n(n + 30) = 24(24 + 30) = 1296$ and $\sqrt{1296} = \pm 36$.

In total, there are 10 unique values for n.