**Question 1:**

Show that the integer $n > 2$ with prime decomposistion $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ is a square if, and only if, each of the exponents $k_i$ is even.

$$\begin{aligned} n &= p_1^{2l_1} p_2^{2l_2} ... p_r^{2l_r} \\ &= (p_1^{l_1} p_2^{l_2} ... p_r^{l_r})^2 \end{aligned}$$

but

$$\begin{aligned} n &= p_1^{2l_1+1} p_2^{2l_2+1} ... p_r^{2l_r+1} \\ &= (p_1^{1_1} p_2^{l_2} ... p_r^{l_r})^2 \cdot p_1 p_2 ... p_r \end{aligned}$$

as $p_1 \neq p_2 \neq p_r$, hence not a square

**Question 2:**

Show that $p|hcf(a^2, b)$if and only if$p|(a, b^2)$

Using the definition of hcf;

Forward direction;

$$p|hcf(a^2, b) \implies p|a^2 \text{ and } p|b$$

$$\implies p|a \text{ and } p|b$$

$$\implies p|hcf(a, b)$$

Backward direction;

$$p|hcf(a, b^2) \implies p|a \text{ and } p|b$$

$$\implies p|a^2 \text{ and } p|b^2$$

Using Theorem 1.4 euclides lemma for prime numbers;

$$\implies p|hcf(a^2, b^2)$$

$$\implies p|hcf(a^2, b) \text{ and } p|hcf(a, b^2)$$

**Question 3:**

Show that $p \mid gcd(a^2, b)$ if and only if $p \mid gcd(a, b^2)$.

*Proof.* Let $p$ be a prime number.

**(⇒)** Suppose $p \mid \gcd(a^2, b)$. Then, by the definition of greatest common divisor,

$$p \mid a^2 \quad \text{and} \quad p \mid b.$$

Since $p$ is prime and $p \mid a^2$, by Euclid's lemma we have $p \mid a$. Hence,

$$p \mid a \quad \text{and} \quad p \mid b,$$

which implies $p \mid \gcd(a, b^2)$ because $p \mid b \Rightarrow p \mid b^2$.

**(⇐)** Conversely, suppose $p \mid \gcd(a, b^2)$. Then

$$p \mid a \quad \text{and} \quad p \mid b^2.$$

By Euclid's lemma again, $p \mid b^2 \Rightarrow p \mid b$. Therefore,

$$p \mid a \quad \text{and} \quad p \mid b,$$

which implies $p \mid a^2$ as well. Hence $p \mid \gcd(a^2, b)$.

Thus, we have shown both directions, and so

$$p \mid \gcd(a^2, b) \iff p \mid \gcd(a, b^2).$$

□

**Question 4:**

Show that $p \mid hcf(a^2, b)$ if and only if $p \mid hcf(a, b^2)$.

*Proof.*

Let $p$ be a prime number.

Forward direction ($\Rightarrow$):

Assume $p \mid hcf(a^2, b)$.

By the definition of highest common factor,

$$p \mid a^2 \quad \text{and} \quad p \mid b.$$

Since $p$ is prime, using Euclid's lemma,

$$p \mid a^2 \implies p \mid a.$$

Hence,

$$p \mid a \quad \text{and} \quad p \mid b,$$

and therefore

$$p \mid b \implies p \mid b^2.$$

Thus, $p \mid hcf(a, b^2)$.

Backward direction ($\Leftarrow$):

Assume $p \mid hcf(a, b^2)$.

Then

$$p \mid a \quad \text{and} \quad p \mid b^2.$$

Applying Euclid's lemma again,

$$p \mid b^2 \implies p \mid b.$$

Hence

$$p \mid a \quad \text{and} \quad p \mid b,$$

and so

$$p \mid a^2 \quad \text{and} \quad p \mid b.$$

Therefore, $p \mid hcf(a^2, b)$.

Since both directions hold, we conclude that

$$p \mid hcf(a^2, b) \iff p \mid hcf(a, b^2)$$

□

**Question 5:**

If a nd b are positive integers and m and n are defined as

$$m = 3a + b \quad \text{and } n = 5a + 2b$$

Then

$$hcf(m, n) = hcf(a, b)$$

*Proof.* Let $d = \gcd(a, b)$. Then we can write $a = da'$ and $b = db'$ for some integers $a'$ and $b'$ such that $\gcd(a', b') = 1$.

Now, substituting these into the expressions for $m$ and $n$:

$$m = 3a + b = 3(da') + (db') = d(3a' + b')$$
$$n = 5a + 2b = 5(da') + 2(db') = d(5a' + 2b')$$

Thus, both $m$ and $n$ are multiples of $d$, which implies that $d$ is a common divisor of $m$ and $n$.

Next, we need to show that a common divisor of $m$ and $n$ must also divide $d$.

Let $c$ be a common divisor of $m$ and $n$. Then $c \mid m$ and $c \mid n$, which means:

$$c \mid d(3a' + b')$$
$$c \mid d(5a' + 2b')$$

Definition 4.6 *Interger combination*

Since $c$ divides both $d(3a' + b')$ and $d(5a' + 2b')$, it must also divide any integer linear combination of these two expressions. In particular, we can form the following combinations:

$$5m - 3n = 5d(3a' + b') - 3d(5a' + 2b') = d(15a' + 5b' - 15a' - 6b') = d(-b')$$

$$2n - m = 2d(5a' + 2b') - d(3a' + b') = d(10a' + 4b' - 3a' - b') = d(7a' + 3b')$$

Definition 4.8 *Coprime*

Since $c$ divides both $d(-b')$ and $d(7a' + 3b')$, it follows that $c$ must divide $d$ because $a', b'$ are coprime, implies that $c$ cannot divide $a'$ or $b'$ unless it divides $d$. Thus, we have shown that any common divisor $c$ of $m$ and $n$

must also divide $d$. Therefore, the greatest common divisor of $m$ and $n$ is equal to $d$:

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

□

**Question 6:**

If $a$ and $b$ are positive integers and $m, n$ are defined by

$$m = 3a + b \quad \text{and} \quad n = 5a + 2b,$$

show that

$$\gcd(m, n) = \gcd(a, b).$$

*Proof.* Let $d = \gcd(a, b)$. Then $a = da'$ and $b = db'$ for some integers $a', b'$ such that $\gcd(a', b') = 1$.

Substitute $a = da'$ and $b = db'$

Substituting into the definitions of $m$ and $n$,

$$m = 3a + b = 3(da') + (db') = d(3a' + b'),$$

$$n = 5a + 2b = 5(da') + 2(db') = d(5a' + 2b').$$

Thus, $d$ divides both $m$ and $n$, so $d$ is a common divisor of $m$ and $n$.

Any common divisor of $m, n$ also divides $d$

Let $c$ be any common divisor of $m$ and $n$. Then

$$c \mid d(3a' + b') \quad \text{and} \quad c \mid d(5a' + 2b').$$

By the property of integer linear combinations, $c$ must also divide any integer combination of these two:

$$5m - 3n = 5d(3a' + b') - 3d(5a' + 2b') = d(-b'),$$

$$2n - m = 2d(5a' + 2b') - d(3a' + b') = d(7a' + 3b').$$

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

Since $a'$ and $b'$ are coprime, the only common divisors of $(-b')$ and $(7a' + 3b')$ are $\pm 1$. Hence, any divisor $c$ of both expressions must divide $d$.

Thus, every common divisor of $m, n$ divides $d$, and $d$ divides both $m, n$. Therefore,

$$\gcd(m, n) = d = \gcd(a, b).$$

□

**Question 7:**

Given a positive integer in the form $14a + 3$ there is a prime divisor of the form $14b + 3$.

*Proof.* Let $n = 14a + 3$ be a posistive integer.

If $n$ is prime, then $n$ must also be a prime divisor of the form $14b + 3$ for some integer $b$.

Hence;

$$a = b$$

If $n$ is not prime, then it must have a prime factor $p$, such that $p \mid n$. By the properties of modular arithmetic, we have:

$$n \equiv 3 \pmod{1)4}$$

Since $p \mid n$, it follows that:

$$p \equiv 3 \pmod{1)4}$$

Thus, $p$ is a prime divisor of $n$ of the form $14b + 3$ for some integer $b$. Euclid's lemma

Therefore, in either case, whether $n$ is prime or not, there exists a prime divisor of $n$ of the form $14b + 3$. □

**Question 8:**

If $n$ is divisible by $15$ but not by $9$ or $25$, the $\tau(n)$ is divisible by $4$.

*Proof.* If $n$ is divisble by 15, then its prime factorisation must be of the form;

$$n = 3^{k_1} \cdot 5^{k_2} \cdot p_1^{k_3} \cdot p_2^{k_4} \dots$$

$k_1, k_2 = 1$ as $n$ is not divisble by $9$ or $25$.

Hence we can write;

$$n = 3^1 \cdot 5^1 \cdot p_1^{k_3} \cdot p_2^{k_4} \dots$$

Where $k_i > 1$

The number of divisors function $\tau(n)$ is given by;

$$\tau(n) = (1+1)(1+1)(k_3+1)(k_4+1)\dots$$

$$\tau(n) = 4(k_3+1)(k_4+1)\dots$$

Thus, $\tau(n)$ is divisible by $4$.

□

This one–check **Question 9:**

Given a positive integer in the form $14a + 3$, determine whether there must exist a prime divisor of the form $14b + 3$.

*Proof.* Let $n = 14a + 3$ for some integer $a$. We consider two cases.

Case 1: $n$ is prime

If $n$ is prime, then it is itself a prime divisor of the form $14b + 3$ (taking $b = a$).

Case 2: $n$ is composite

If $n$ is not prime, then it has at least one prime factor $p$ such that $p \mid n$. However, it does *not* follow that $p \equiv 3 \pmod{14}$ simply because $n \equiv 3 \pmod{14}$. The congruence relation does not, in general, transfer from a number to all of its factors.

To see this, consider a counterexample:

$$n = 185 = 14 \times 13 + 3.$$

Then

$$185 = 5 \times 37.$$

Checking each prime factor modulo 14:

$$5 \equiv 5 \pmod{14}, \quad 37 \equiv 9 \pmod{14}.$$

Neither of these primes is congruent to $3 \pmod{14}$. Therefore, $n = 185$ is a counterexample to the claim.

Conclusion

Hence, the statement is **false**: not every integer of the form $14a + 3$ has a prime divisor of the form $14b + 3$.

□

**Question 10:**

If $n$ is divisible by $15$ but not by $9$ or $25$, then $\tau(n)$ is divisible by $4$.

*Proof.* If $n$ is divisible by 15, its prime factorisation must be of the form

$$n = 3^{k_1} \cdot 5^{k_2} \cdot p_1^{k_3} \cdot p_2^{k_4} \dots$$

Since $n$ is not divisible by 9 or 25, we must have $k_1 = k_2 = 1$.

Hence

$$n = 3^1 \cdot 5^1 \cdot p_1^{k_3} \cdot p_2^{k_4} \dots$$

where each $k_i \geq 0$.

The number of divisors function is given by

$$\tau(n) = (k_1 + 1)(k_2 + 1)(k_3 + 1)(k_4 + 1) \dots$$

Substituting $k_1 = k_2 = 1$,

$$\tau(n) = (1 + 1)(1 + 1)(k_3 + 1)(k_4 + 1) \dots = 4 \times (k_3 + 1)(k_4 + 1) \dots$$

Since the remaining factors are integers, $\tau(n)$ is a multiple of 4.

Conclusion

Therefore, $\tau(n)$ is divisible by 4 whenever $n$ is divisible by 15 but not by 9 or 25.

□

**Question 11:**

Given a positive integer in the form $14a + 3$, determine whether there must exist a prime divisor of the form $14b + 3$.

*Proof.* Let $n = 14a + 3$ for some integer $a$. We consider two cases.

Case 1: $n$ is prime

If $n$ is prime, then it is itself a prime divisor of the form $14b + 3$ (taking $b = a$).

Case 2: $n$ is composite

If $n$ is not prime, then it has at least one prime factor $p$ such that $p \mid n$. However, it does *not* follow that $p \equiv 3 \pmod{14}$ simply because $n \equiv 3 \pmod{14}$. The congruence relation does not, in general, transfer from a number to all of its factors.

To see this, consider a counterexample:

$$n = 185 = 14 \times 13 + 3.$$

Then

$$185 = 5 \times 37.$$

Checking each prime factor modulo 14:

$$5 \equiv 5 \pmod{14}, \quad 37 \equiv 9 \pmod{14}.$$

Neither of these primes is congruent to $3 \pmod{14}$. Therefore, $n = 185$ is a counterexample to the claim.

Conclusion

Hence, the statement is **false**: not every integer of the form $14a + 3$ has a prime divisor of the form $14b + 3$.

□

**Question 12:**

If $n$ is divisible by $15$ but not by $9$ or $25$, then $\tau(n)$ is divisible by $4$.

*Proof.* If $n$ is divisible by 15, its prime factorisation must be of the form

$$n = 3^{k_1} \cdot 5^{k_2} \cdot p_1^{k_3} \cdot p_2^{k_4} \dots$$

Since $n$ is not divisible by 9 or 25, we must have $k_1 = k_2 = 1$.

Hence

$$n = 3^1 \cdot 5^1 \cdot p_1^{k_3} \cdot p_2^{k_4} \dots$$

where each $k_i \geq 0$.

The number of divisors function is given by

$$\tau(n) = (k_1 + 1)(k_2 + 1)(k_3 + 1)(k_4 + 1) \dots$$

Substituting $k_1 = k_2 = 1$,

$$\tau(n) = (1 + 1)(1 + 1)(k_3 + 1)(k_4 + 1) \dots = 4 \times (k_3 + 1)(k_4 + 1) \dots$$

Since the remaining factors are integers, $\tau(n)$ is a multiple of 4.

Conclusion

Therefore, $\tau(n)$ is divisible by 4 whenever $n$ is divisible by 15 but not by 9 or 25.

□