Number Theory Exercises 3

Jason Sass

July 17, 2023

Prime Numbers and Fundamental Theorem of Arithmetic

Exercise 1. There exists an even prime number.

Proof. Observe that 2 is an even prime number. □

Exercise 2. There is a prime number between 90 and 100.

Proof. Observe that 97 is a prime number. □

Exercise 3. Compute the least common multiple of 3054 and 12378.

Solution. Observe that $lcm(3054, 12378) = (3054)(12378)/\gcd(3054, 12378) = 3054 * 12378/6 = 6300402$. □

Exercise 4. Prove or disprove $\forall(n \in \mathbb{N})$, the integer $n^2 - n + 11$ is prime.

Solution. We just use Java to write an algorithm(tiny computer program) to decide if the formula $f(n) = n^2 - n + 11$ really only generates primes. Using the computer, we find there are several counter examples that demonstrate the conjecture is false.

For example, when $n = 11$, then $f(11) = 121 = 11 \cdot 11$.

Another example, when $n = 12$, then $f(12) = 143 = 11 \cdot 13$

Another example, when $n = 15$, then $f(15) = 221 = 13 \cdot 17$.

Another example, when $n = 20$, then $f(20) = 391 = 17 \cdot 23$.

We could identify many more examples that demonstrate this conjecture is false.

But, to disprove the conjecture, it suffices to just show one counterexample.

Thus, we can write up the proof below. □

Proof. The statement is false.

For $n = 11$, the integer $f(11) = 121 = 11 \cdot 11$ is not prime. □

Exercise 5. Prove or disprove $\forall(n \in \mathbb{N})$, the integer $2n^2 - 4n + 31$ is prime.

Solution. We just use Java to write an algorithm(tiny computer program) to decide if the formula $f(n) = 2n^2 - 4n + 31$ really only generates primes.

Using the computer, we find there are several counter examples that demonstrate the conjecture is false.

For example, when $n = 30$, then $f(30) = 1711 = 29 \cdot 59$.

Another example, when $n = 31$, then $f(31) = 1829 = 31 \cdot 59$

Another example, when $n = 33$, then $f(33) = 2077 = 31 \cdot 67$.

Another example, when $n = 36$, then $f(36) = 2479 = 37 \cdot 67$.

We could identify many more examples that demonstrate this conjecture is false.

But, to disprove the conjecture, it suffices to just show one counterexample.

Thus, we can write up the proof below. □

Proof. The statement is false.

For $n = 30$, the integer $2(30)^2 - 4(30) + 31 = 1711 = 29 \cdot 59$ is not prime. □

Exercise 6. Disprove the conjecture: There exist two prime numbers p and q such that $p - q = 97$.

Proof. Suppose for the sake of contradiction that the conjecture is true.

Let p and q be prime numbers such that $p - q = 97$.

The difference between two odd integers is even.

Since $p - q = 97$ is odd, then p and q cannot be both odd.

Hence, at least one of p and q is not odd, so at least one of p and q is even.

Thus, either p is even or q is even.

We consider each case separately.

Case 1: Suppose p is even.

Since p is prime and p is even and the only even prime is 2, then $p = 2$.

Thus, $97 = 2 - q$, so $q = -95$.

Since $-95 = 5(-19)$, then $q = -95$ is not prime.

Case 2: Suppose q is even.

Since q is prime and q is even and the only even prime is 2, then $q = 2$.

Thus, $p - 2 = 97$, so $p = 99$.

Since $99 = 9 \cdot 11$, then $p = 99$ is not prime.

Both cases show that one of p or q is not prime, so this contradicts the assumption that both p and q are prime.

Therefore, the conjecture is false. □

Proposition 7. ***Any prime greater than 2 is odd.***

If p is a prime greater than 2, then p is odd.

Proof. Let $p > 2$ be prime.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $p > 2$, then $p \neq 2$.

Since $2 \neq 1$ and $2 \neq p$, then 2 cannot be a divisor of p, so $2 \not| p$.

Therefore, p is not even, so p must be odd. □

Lemma 8. ***Sieve of Eratosthenes lemma1***

Let $n \in \mathbb{Z}^+$.

If n is composite, then there exists $d \in \mathbb{Z}^+$ such that $d|n$ and $1 < d \leq \sqrt{n}$.

Proof. Suppose n is composite.

Since a composite is composed of smaller positive factors, then there exist integers a, b with $1 < a < n$ and $1 < b < n$ such that $n = ab$.

Since $n = ab$, then $a|n$ and $b|n$.

If both $a > \sqrt{n}$ and $b > \sqrt{n}$, then $n = ab > \sqrt{n} \cdot \sqrt{n} = (\sqrt{n})^2 = n$, so $n > n$, a contradiction.

Thus, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$, so either $1 < a \leq \sqrt{n}$ or $1 < b \leq \sqrt{n}$.

Therefore, either $1 < a \leq \sqrt{n}$ and $a|n$, or $1 < b \leq \sqrt{n}$ and $b|n$. □

Lemma 9. ***Sieve of Eratosthenes lemma2***

Let $n \in \mathbb{Z}^+$.

If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof. Suppose n is composite.

Then there exists $d \in \mathbb{Z}^+$ such that $d|n$ and $1 < d \leq \sqrt{n}$ by lemma 8.

Since $1 < d \leq \sqrt{n}$, then $1 < d$ and $d \leq \sqrt{n}$.

Since $d > 1$, then d has a prime factor p, since every integer greater than one has a prime factor.

Hence, $p|d$ and $1 < p \leq d$.

Since $p|d$ and $d|n$, then $p|n$.

Since $p \leq d$ and $d \leq \sqrt{n}$, then $p \leq \sqrt{n}$.

Therefore, p is prime and $p|n$ and $p \leq \sqrt{n}$. □

Exercise 10. Any prime of the form $3n + 1$ is also of the form $6m + 1$.

Proof. Let p be a prime such that $p = 3n + 1$ for some $n \in \mathbb{Z}^+$.

We must prove $p = 6m + 1$ for some $m \in \mathbb{Z}$.

Since p is prime, then $p \geq 2$, so either $p > 2$ or $p = 2$.

Suppose $p = 2$.

Then $2 = 3n + 1$, so $3n = 1$.

Hence, 3 divides 1, a contradiction.

Thus, $p \neq 2$, so $p > 2$.

Since p is prime and $p > 2$, then p is odd, so $p - 1 = 3n$ is even.

Since $3n$ is even, then $2|3n$.

Since $2|3n$ and $\gcd(2, 3) = 1$, then $2|n$, so $n = 2m$ for some integer m.

Hence, $p = 3n + 1 = 3(2m) + 1 = 6m + 1$.

Therefore, there exists an integer m such that $p = 6m + 1$. □

Proof. Let $p = 3n + 1$ be a prime for some $n \in \mathbb{Z}^+$.

We must prove $p = 6m + 1$ for some $m \in \mathbb{Z}$.

Since p is prime, then $p \geq 2$, so either $p > 2$ or $p = 2$.

Suppose $p = 2$.

Then $2 = 3n + 1$, so $3n = 1$.

Hence, 3 divides 1, a contradiction.

Thus, $p \neq 2$, so $p > 2$.
Since p is prime and $p > 2$, then p is odd, so $p - 1$ is even.
Hence, $3n$ is even, so $2|3n$.
Since 2 is prime and $2|3n$, then either $2|3$ or $2|n$, by Euclid's lemma.
Since $2 \not| 3$, then $2|n$, so $n = 2m$ for some integer m.
Thus, $p = 3n + 1 = 3(2m) + 1 = 6m + 1$.
Therefore, there exists an integer m such that $p = 6m + 1$. □

Exercise 11. Every integer of the form $3n + 2$ has a prime factor of this form.

Proof. We prove by contradiction.
Suppose there is a positive integer $a = 3n + 2$ that has no prime factor $p = 3m + 2$.
Since $a|a$ and $a = 3n + 2$, then a cannot be a prime.
Since $a \in \mathbb{Z}^+$, then $a \geq 1$.
If $1 = a = 3n + 2$, then $3n = -1$, so $3|(-1)$, a contradiction.
Hence, $a \neq 1$, so $a > 1$.
Thus, by FTA, $a = p_1^{e_1} p_2^{e_2} ... p_k^{e_s}$ for primes $p_1, p_2, ..., p_k$ and positive integers $e_1, e_2, ..., e_k$.

Let p be an arbitrary prime factor of a.
Since $a = 3n + 2$, then $3 \not| a$, so $p \neq 3$.
By the division algorithm, either $p = 3b$ or $p = 3b + 1$ or $p = 3b + 2$.
Since a has no prime factors of the form $3b + 2$, then $p \neq 3b + 2$.

Suppose $p = 3b$.
Then $3|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Thus, p must be 3, so $p = 3$.
But, this contradicts $p \neq 3$.
Therefore, $p \neq 3b$.

Hence, $p = 3b + 1$, so every prime factor p of a must be of the form $3b + 1$.
Thus, $p_1 = 3b_1 + 1$ and $p_2 = 3b_2 + 1$ and ... $p_k = 3b_k + 1$.

If $p = 3b + 1$ and $q = 3c + 1$, then the product is $pq = (3b + 1)(3c + 1) = 9bc + 3b + 3c + 1 = 3(3bc + b + c) + 1 = 3m + 1$ for some integer m.
Hence, the product of any two integers of the form $3b + 1$ is always of the same form.
This applies to a finite number of integers of this form. We should prove this by induction.
Therefore, the product of all of these prime factors of a will be an integer of the form $3b + 1$, so $p_1^{e_1} \cdot p_2^{e_2} \ldots p_k^{e_k} = 3b + 1 = a = 3n + 2$.
Thus, $3b + 1 = 3n + 2$, so $3b - 3n = 1 = 3(b - n)$.
Hence, $3|1$, a contradiction.

Consequently, there is no positive integer $a = 3n+2$ that has no prime factor $p = 3m + 2$.

Therefore, every positive integer $a = 3n + 2$ has at least one prime factor $p = 3m + 2$. □

Exercise 12. **7 is the only prime of the form $n^3 - 1$.**

Let $n \in \mathbb{Z}^+$.

Then $n^3 - 1$ is prime iff $n = 2$.

Proof. We prove if $n = 2$, then $n^3 - 1$ is prime.

Suppose $n = 2$.

Then $n^3 - 1 = 2^3 - 1 = 7$ is prime. □

Proof. Conversely, suppose $p = n^3 - 1$ is prime.

We must prove $n = 2$.

Observe that $p = n^3 - 1 = (n - 1)(n^2 + n + 1)$.

Since $n \in \mathbb{Z}^+$, then $n \geq 1$.

If $n = 1$, then $p = 1^3 - 1 = 0$, so 0 is a prime, a contradiction.

Hence, $n \neq 1$, so $n > 1$.

Thus, $n - 1 > 0$.

Since p is prime, then $p > 1 > 0$.

Since $n - 1 > 0$ and $p > 0$ and $p = (n - 1)(n^2 + n + 1)$, then $n^2 + n + 1 > 0$.

Since p is prime, then the only positive divisors of p are 1 and p.

Thus, either $1 = n - 1$ or $1 = n^2 + n + 1$.

If $1 = n^2 + n + 1$, then $0 = n^2 + n = n(n + 1)$, so either $n = 0$ or $n + 1 = 0$.

Hence, either $n = 0$ or $n = -1$.

But, $n > 1$, so n cannot be either 0 or -1.

Therefore, $1 = n - 1$, so $n = 2$, as desired. □

Exercise 13. Let $p \in \mathbb{Z}^+$.

The only prime p such that $3p + 1$ is a perfect square is $p = 5$.

Solution. We must prove

1. If $p = 5$, then $3p + 1$ is a perfect square.
2. If p is prime and $3p + 1$ is a perfect square, then $p = 5$. □

Proof. Suppose $p = 5$.

Then $3p + 1 = 3 \cdot 5 + 1 = 16 = 4^2$ is a perfect square. □

Proof. Conversely, suppose p is prime and $3p + 1$ is a perfect square.

We must prove $p = 5$.

Since $3p + 1$ is a perfect square, then $3p + 1 = m^2$ for some integer m.

Thus, $3p = m^2 - 1 = (m - 1)(m + 1)$.

Since p is prime, then $p > 1$, so $3p > 3 > 1$.

Hence, $(m - 1)(m + 1) = 3p > 1$, so $(m - 1)(m + 1)$ has a unique prime factorization, by FTA.

Therefore, either $3 = m - 1$ or $3 = m + 1$.

Suppose $3 = m + 1$.
Then $m = 2$, so $4 = 2^2 = 3p + 1$.
Thus, $3 = 3p$, so $p = 1$.
But, p is prime, so $p > 1$.
Hence, $p \neq 1$.
Therefore, $3 \neq m + 1$.
Thus, we must conclude $3 = m - 1$.
Hence, $m = 4$, so $16 = 4^2 = 3p + 1$,
Therefore, $15 = 3p$, so $p = 5$. □

Lemma 14. *Let $p \in \mathbb{Z}^+$.*
If p is prime and $p \geq 5$, then either $p = 6k + 1$ or $p = 6k + 5$ for some integer k.

Proof. Suppose p is prime and $p \geq 5$.
Since $p \geq 5 > 2$, then $p > 2$.
Since p is prime and $p > 2$, then p must be odd, so $2 \nmid p$.
Since $p \geq 5 > 3$, then $p > 3$.
We must prove there exists an integer k such that $p = 6k + 1$ or $p = 6k + 5$.
By the division algorithm, there is a unique integer k such that either $p = 6k$ or $p = 6k + 1$ or $p = 6k + 2$ or $p = 6k + 3$ or $p = 6k + 4$ or $p = 6k + 5$.
We consider each case separately.
Case 1: Suppose $p = 6k$.
Then $p = 6k = 2 \cdot 3k$, so $2|p$.
Thus, we have $2|p$ and $2 \nmid p$, a contradiction.
Therefore, $p \neq 6k$.
Case 2: Suppose $p = 6k + 2$.
Then $p = 2(3k + 1)$, so $2|p$.
Thus, we have $2|p$ and $2 \nmid p$, a contradiction.
Therefore, $p \neq 6k + 2$.
Case 3: Suppose $p = 6k + 3$.
Then $p = 3(2k + 1)$, so $3|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since $3|p$, then this implies either $3 = 1$ or $3 = p$.
Since $3 \neq 1$, then this implies $3 = p$.
But, $p > 3$, so $p \neq 3$.
Therefore, we must conclude $p \neq 6k + 3$.
Case 4: Suppose $p = 6k + 4$.
Then $p = 2(3k + 2)$, so $2|p$.
Thus, we have $2|p$ and $2 \nmid p$, a contradiction
Therefore, $p \neq 6k + 4$.

Since $p \neq 6k$ and $p \neq 6k + 2$ and $p \neq 6k + 3$ and $p \neq 6k + 4$ and either $p = 6k$ or $p = 6k + 1$ or $p = 6k + 2$ or $p = 6k + 3$ or $p = 6k + 4$ or $p = 6k + 5$, then we must conclude either $p = 6k + 1$ or $p = 6k + 5$, as desired. □

Exercise 15. Let $p \in \mathbb{Z}^+$.

If p is prime and $p > 3$, then $p^2 + 2$ is composite.

Proof. Suppose p is prime and $p > 3$.

By the division algorithm, $p = 3q + r$ for some unique integers q and r with $0 \leq r < 3$, so either $p = 3q$ or $p = 3q + 1$ or $p = 3q + 2$.

Suppose $p = 3q$.

Then $3|p$.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $p > 3$, then $p \neq 3$.

Thus, $3 \not| p$.

But, this contradicts $3|p$.

Therefore, we conclude $p \neq 3q$.

Hence, either $p = 3q + 1$ or $p = 3q + 2$.

We consider each case separately.

Case 1: Suppose $p = 3q + 1$.

Observe that

$$\begin{aligned} p^2 + 2 &= (3q + 1)^2 + 2 \\ &= 9q^2 + 6q + 1 + 2 \\ &= 9q^2 + 6q + 3 \\ &= 3(3q^2 + 2q + 1). \end{aligned}$$

Therefore, $3|(p^2 + 2)$.

Case 2: Suppose $p = 3q + 2$.

Observe that

$$\begin{aligned} p^2 + 2 &= (3q + 2)^2 + 2 \\ &= 9q^2 + 12q + 4 + 2 \\ &= 9q^2 + 12q + 6 \\ &= 3(3q^2 + 4q + 2). \end{aligned}$$

Therefore, $3|(p^2 + 2)$.

Hence, in all cases, $3|(p^2 + 2)$.

Since $p > 3$, then $p^2 > 9$, so $p^2 + 2 > 11 > 0$.

Thus, $p^2 + 2 > 0$, so $p^2 + 2$ is a positive integer.

Since $1 < 3 < 11 < p^2 + 2$, then $1 < 3 < p^2 + 2$.

Since $p^2 + 2$ is a positive integer and $1 < 3 < p^2 + 2$ and $3|(p^2 + 2)$, then $p^2 + 2$ is composite, since a composite number has a positive divisor other than 1 or itself. □

Lemma 16. *Let $a, b \in \mathbb{Z}$.*

If $a|b$, then $a^n|b^n$ for all $n \in \mathbb{Z}^+$.

Proof. We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : \text{if } a|b, \text{ then } a^n|b^n\}$.

Basis:
Suppose $a|b$.
Then $a^1|b^1$, so $1 \in S$.
Induction:
Suppose $k \in S$.
Then $k \in \mathbb{Z}^+$ and if $a|b$, then $a^k|b^k$.
Since $k \in \mathbb{Z}^+$, then $k+1 \in \mathbb{Z}^+$.
Suppose $a|b$.
Then, by the induction hypothesis, $a^k|b^k$.
Since $a|b$ and $a^k|b^k$, then $aa^k|bb^k$, so $a^{k+1}|b^{k+1}$.
Since $k+1 \in \mathbb{Z}^+$ and $a|b$ implies $a^{k+1}|b^{k+1}$, then $k+1 \in S$.
Therefore, by PMI, if $a|b$, then $a^n|b^n$ for all $n \in \mathbb{Z}^+$. □

Exercise 17. Let $a, n, p \in \mathbb{Z}^+$.
If p is prime and $p|a^n$, then $p^n|a^n$.

Proof. Let $r(n)$ be the predicate : if p is prime and $p|a^n$, then $p^n|a^n$ defined over $\mathbb{Z}^+$.
We prove $r(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Let $n = 1$.
If p is prime and $p|a^1$, then $p|a$, so $p^1|a^1$.
Therefore, $r(1)$ is true.
Induction:
Suppose $r(k)$ is true for any positive integer k.
Then if p is prime and $p|a^k$, then $p^k|a^k$.

Suppose p is prime and $p|a^{k+1}$.
Since $a \in \mathbb{Z}^+$, then $a \geq 1$, so either $a > 1$ or $a = 1$.
If $a = 1$, then $p|(1)^{k+1}$, so $p|1$.
Since the only positive divisor of 1 is 1, then $p = 1$.
But, p is prime, so $p > 1$.
Therefore, $a \neq 1$, so $a > 1$.
Thus, by the Fundamental Theorem of Arithmetic, a has a unique canonical prime factorization.
Hence, there exist primes p_i and positive integers e_i such that $a = p_1^{e_1} \cdot p_2^{e_2} \dots p_t^{e_t}$ and $p_1 < p_2 < \dots p_s$ and $1 \leq i \leq t$.
Consequently, $a^{k+1} = (p_1^{e_1} \cdot p_2^{e_2} \dots p_t^{e_t})^{k+1} = p_1^{e_1(k+1)} \cdot p_2^{e_2(k+1)} \dots p_t^{e_t(k+1)}$.
Since $p|a^{k+1}$, then this implies p divides $p_1^{e_1(k+1)} \cdot p_2^{e_2(k+1)} \dots p_t^{e_t(k+1)}$.
Since p is prime, then p divides p_m for some integer m with $1 \leq m \leq t$, by corollary to Euclid's lemma.
Since $p|p_m$ and $p_m|a$, then $p|a$.
Hence, p divides any multiple of a, so $p|(a^{k-1})a$.
Therefore, $p|a^k$.
Since p is prime and $p|a^k$, then $p^k|a^k$, by the induction hypothesis.

Since $p|a$ and $p^k|a^k$, then the product pp^k divides the product aa^k, so $p^{k+1}|a^{k+1}$.

Therefore, if p is prime and $p|a^{k+1}$, then $p^{k+1}|a^{k+1}$, so $r(k+1)$ is true.

Thus, $r(k)$ implies $r(k+1)$ for all $k \in \mathbb{Z}^+$.

By induction, we conclude $r(n)$ is true for all $n \in \mathbb{Z}^+$.

Therefore, if p is prime and $p|a^n$, then $p^n|a^n$ for all $n \in \mathbb{Z}^+$. □

Exercise 18. Let $a, b, p \in \mathbb{Z}^+$.

If p is prime and $\gcd(a, b) = p$, what are the possible values of $\gcd(a^2, b^2)$?

Solution. Based on some computations run in SageMath, we conjecture that $\gcd(a^2, b^2) = p^2$.

So, let's prove the statement: If p is prime and $\gcd(a, b) = p$, then $\gcd(a^2, b^2) = p^2$. □

Proof. Suppose p is prime and $\gcd(a, b) = p$.

Since p is prime, then $p > 1$.

Since $\gcd(a, b) = p$, then $p|a$ and $p|b$.

Since $p|a$, then $p \leq a$, so $a \geq p > 1$.

Hence, $a > 1$.

Since $p|b$, then $p \leq b$, so $b \geq p > 1$.

Hence, $b > 1$.

Since $a > 1$, then a has a unique canonical prime factorization, by FTA.

Thus, $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ for primes p_i and $e_i \in \mathbb{Z}^+$ and $p_1 < p_2 < ... < p_r$ and $1 \leq i \leq r$.

Since $b > 1$, then b has a unique canonical prime factorization, by FTA.

Thus, $b = q_1^{f_1} q_2^{f_2} \dots q_s^{f_s}$ for primes q_j and $f_j \in \mathbb{Z}^+$ and $q_1 < q_2 < ... < q_s$ and $1 \leq j \leq s$.

Since p is prime and $p|a$ and $p|b$, then p is a common prime factor of both a and b, so p must be one of the primes in the prime factorization of both a and b.

Thus, $p = p_k = q_m$ for some integers k and m with $1 \leq k \leq r$ and $1 \leq m \leq s$ and $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \dots p_r^{e_r}$ and $b = q_1^{f_1} q_2^{f_2} \dots q_m^{f_m} \dots q_s^{f_s}$.

Hence, $a = p_1^{e_1} p_2^{e_2} \dots p^{e_k} \dots p_r^{e_r}$ and $b = q_1^{f_1} q_2^{f_2} \dots p^{f_m} \dots q_s^{f_s}$.

If we square a, then $a^2 = (p_1^{e_1} p_2^{e_2} \dots p^{e_k} \dots p_r^{e_r})^2 = p_1^{2e_1} p_2^{2e_2} \dots p^{2e_k} \dots p_r^{2e_r}$.

If we square b, then $b^2 = (q_1^{f_1} q_2^{f_2} \dots p^{f_m} \dots q_s^{f_s})^2 = q_1^{2f_1} q_2^{2f_2} \dots p^{2f_m} \dots q_s^{2f_s}$.

Since $\gcd(a, b) = p = p^1$, then either $e_k = 1$ or $f_m = 1$.

We consider these cases separately.

Case 1: Suppose $e_k = 1$.

Since $f_m \in \mathbb{Z}^+$, then $f_m \geq 1$, so $2f_m \geq 2$.

Thus, $\min(2e_k, 2f_m) = \min(2 \cdot 1, 2f_m) = \min(2, 2f_m) = 2$.

Case 2: Suppose $f_m = 1$.

Since $e_k \in \mathbb{Z}^+$, then $e_k \geq 1$, so $2e_k \geq 2$.

Thus, $\min(2e_k, 2f_m) = \min(2e_k, 2 \cdot 1) = \min(2e_k, 2) = 2$.

Hence, in all cases, $\min(2e_k, 2f_m) = 2$.

Therefore, the highest power of p that is common to both a^2 and b^2 is p^2.

Suppose p is not the only common prime factor of both a^2 and b^2.

Then there exists another prime factor q of both a^2 and b^2.

Since p and q are distinct primes, then $q \neq p$.

Since q is a factor of both a^2 and b^2, then $q|a^2$ and $q|b^2$.

Since q is prime and $q|a^2$, then $q|a$, by Euclid's lemma.

Since q is prime and $q|b^2$, then $q|b$, by Euclid's lemma.

Since $q|a$ and $q|b$, then q is a common divisor of both a and b, so q must divide $\gcd(a, b) = p$.

Hence, $q|p$.

Since p is prime, then the only positive divisors of p are 1 and p, so either $q = 1$ or $q = p$.

Since q is prime, then $q > 1$, so $q \neq 1$.

Hence, $q = p$.

But, this contradicts $q \neq p$.

Therefore, there is no other prime factor q of both a^2 and b^2, so p is the only common prime factor of both a^2 and b^2.

Thus, the greatest common factor of both a^2 and b^2 must be p^2.

Therefore, $\gcd(a^2, b^2) = p^2$. □

Exercise 19. Let $a, b, p \in \mathbb{Z}^+$.

If p is prime and $\gcd(a, b) = p$, what are the possible values of $\gcd(a^2, b)$?

Solution. Based on some computations run in SageMath, we conjecture that $\gcd(a^2, b)$ is either p or p^2.

So, let's prove the statement: If p is prime and $\gcd(a, b) = p$, then either $\gcd(a^2, b) = p$ or $\gcd(a^2, b) = p^2$. □

Proof. Suppose p is prime and $\gcd(a, b) = p$.

Since p is prime, then $p > 1$.

Since $\gcd(a, b) = p$, then $p|a$ and $p|b$.

Since $p|a$, then $p \leq a$, so $a \geq p > 1$.

Hence, $a > 1$.

Since $p|b$, then $p \leq b$, so $b \geq p > 1$.

Hence, $b > 1$.

Since $a > 1$, then a has a unique canonical prime factorization, by FTA.

Thus, $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ for primes p_i and $e_i \in \mathbb{Z}^+$ and $p_1 < p_2 < ... < p_r$ and $1 \leq i \leq r$.

Since $b > 1$, then b has a unique canonical prime factorization, by FTA.

Thus, $b = q_1^{f_1} q_2^{f_2} \dots q_s^{f_s}$ for primes q_j and $f_j \in \mathbb{Z}^+$ and $q_1 < q_2 < ... < q_s$ and $1 \leq j \leq s$.

Since p is prime and $p|a$ and $p|b$, then p is a common prime factor of both a and b, so p must be one of the primes in the prime factorization of both a and b.

Thus, $p = p_k = q_m$ for some integers k and m with $1 \leq k \leq r$ and $1 \leq m \leq s$ and $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \dots p_r^{e_r}$ and $b = q_1^{f_1} q_2^{f_2} \dots q_m^{f_m} \dots q_s^{f_s}$.

Hence, $a = p_1^{e_1} p_2^{e_2} \dots p^{e_k} \dots p_r^{e_r}$ and $b = q_1^{f_1} q_2^{f_2} \dots p^{f_m} \dots q_s^{f_s}$.

If we square a, then $a^2 = (p_1^{e_1} p_2^{e_2} \dots p^{e_k} \dots p_r^{e_r})^2 = p_1^{2e_1} p_2^{2e_2} \dots p^{2e_k} \dots p_r^{2e_r}$.

Since $\gcd(a, b) = p = p^1$, then either $e_k = 1$ or $f_m = 1$.

We consider these cases separately.

Case 1: Suppose $e_k = 1$.

Since $f_m \in \mathbb{Z}^+$, then $f_m \geq 1$, so either $f_m > 1$ or $f_m = 1$.

If $f_m = 1$, then $\min(2e_k, f_m) = \min(2 \cdot 1, 1) = \min(2, 1) = 1$.

If $f_m > 1$, then $f_m \geq 2$.

Thus, $\min(2e_k, f_m) = \min(2 \cdot 1, f_m) = \min(2, f_m) = 2$.

Therefore, $\min(2e_k, f_m)$ is either 1 or 2.

Case 2: Suppose $f_m = 1$.

Since $e_k \in \mathbb{Z}^+$, then $e_k \geq 1$, so $2e_k \geq 2$.

Thus, $\min(2e_k, f_m) = \min(2e_k, 1) = 1$.

Hence, in all cases, either $\min(2e_k, f_m) = 1$ or $\min(2e_k, f_m) = 2$.

Therefore, the highest power of p that is common to both a^2 and b is either $p^1 = p$ or p^2.

Suppose p is not the only common prime factor of both a^2 and b.

Then there exists another prime factor q of both a^2 and b.

Since p and q are distinct primes, then $q \neq p$.

Since q is a factor of both a^2 and b, then $q|a^2$ and $q|b$.

Since q is prime and $q|a^2$, then $q|a$, by Euclid's lemma.

Since $q|a$ and $q|b$, then q is a common divisor of both a and b, so q must divide $\gcd(a, b) = p$.

Hence, $q|p$.

Since p is prime, then the only positive divisors of p are 1 and p, so either $q = 1$ or $q = p$.

Since q is prime, then $q > 1$, so $q \neq 1$.

Hence, $q = p$.

But, this contradicts $q \neq p$.

Therefore, there is no other prime factor q of both a^2 and b, so p is the only common prime factor of both a^2 and b.

Thus, the greatest common factor of both a^2 and b must be either p or p^2.

Therefore, $\gcd(a^2, b) = p$ or $\gcd(a^2, b) = p^2$. □

Exercise 20. Let $a, b, p \in \mathbb{Z}^+$.

If p is prime and $\gcd(a, b) = p$, what are the possible values of $\gcd(a^3, b^2)$?

Solution. Based on some computations run in SageMath, we conjecture that $\gcd(a^3, b^2)$ is either p^2 or p^3.

So, let's prove the statement: If p is prime and $\gcd(a, b) = p$, then either $\gcd(a^3, b^2) = p^2$ or $\gcd(a^3, b^2) = p^3$. □

Proof. Suppose p is prime and $\gcd(a, b) = p$.

Since p is prime, then $p > 1$.

Since $\gcd(a, b) = p$, then $p|a$ and $p|b$.

Since $p|a$, then $p \leq a$, so $a \geq p > 1$.

Hence, $a > 1$.

Since $p|b$, then $p \leq b$, so $b \geq p > 1$.

Hence, $b > 1$.

Since $a > 1$, then a has a unique canonical prime factorization, by FTA.

Thus, $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ for primes p_i and $e_i \in \mathbb{Z}^+$ and $p_1 < p_2 < ... < p_r$ and $1 \leq i \leq r$.

Since $b > 1$, then b has a unique canonical prime factorization, by FTA.

Thus, $b = q_1^{f_1} q_2^{f_2} \dots q_s^{f_s}$ for primes q_j and $f_j \in \mathbb{Z}^+$ and $q_1 < q_2 < ... < q_s$ and $1 \leq j \leq s$.

Since p is prime and $p|a$ and $p|b$, then p is a common prime factor of both a and b, so p must be one of the primes in the prime factorization of both a and b.

Thus, $p = p_k = q_m$ for some integers k and m with $1 \leq k \leq r$ and $1 \leq m \leq s$ and $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \dots p_r^{e_r}$ and $b = q_1^{f_1} q_2^{f_2} \dots q_m^{f_m} \dots q_s^{f_s}$.

Hence, $a = p_1^{e_1} p_2^{e_2} \dots p^{e_k} \dots p_r^{e_r}$ and $b = q_1^{f_1} q_2^{f_2} \dots p^{f_m} \dots q_s^{f_s}$.

If we cube a, then $a^3 = (p_1^{e_1} p_2^{e_2} \dots p^{e_k} \dots p_r^{e_r})^3 = p_1^{3e_1} p_2^{3e_2} \dots p^{3e_k} \dots p_r^{3e_r}$.

If we square b, then $b^2 = (q_1^{f_1} q_2^{f_2} \dots p^{f_m} \dots q_s^{f_s})^2 = q_1^{2f_1} q_2^{2f_2} \dots p^{2f_m} \dots q_s^{2f_s}$.

Since $\gcd(a, b) = p = p^1$, then either $e_k = 1$ or $f_m = 1$.

We consider these cases separately.

Case 1: Suppose $e_k = 1$.

Since $f_m \in \mathbb{Z}^+$, then $f_m \geq 1$, so either $f_m > 1$ or $f_m = 1$.

If $f_m = 1$, then $\min(3e_k, 2f_m) = \min(3 \cdot 1, 2 \cdot 1) = \min(3, 2) = 2$.

If $f_m > 1$, then $2f_m > 2$, so $2f_m \geq 3$.

Thus, $\min(3e_k, 2f_m) = \min(3 \cdot 1, 2f_m) = \min(3, 2f_m) = 3$.

Therefore, $\min(3e_k, 2f_m)$ is either 2 or 3.

Case 2: Suppose $f_m = 1$.

Since $e_k \in \mathbb{Z}^+$, then $e_k \geq 1$, so $3e_k \geq 3$.

Thus, $\min(3e_k, 2f_m) = \min(3e_k, 2 \cdot 1) = \min(3e_k, 2) = 2$.

Hence, in all cases, either $\min(3e_k, 2f_m) = 2$ or $\min(3e_k, 2f_m) = 3$.

Therefore, the highest power of p that is common to both a^3 and b^2 is either p^2 or p^3.

Suppose p is not the only common prime factor of both a^3 and b^2.

Then there exists another prime factor q of both a^3 and b^2.

Since p and q are distinct primes, then $q \neq p$.

Since q is a factor of both a^3 and b^2, then $q|a^3$ and $q|b^2$.

Since q is prime and $q|a^3$, then $q|a$, by Euclid's lemma.

Since q is prime and $q|b^2$, then $q|b$, by Euclid's lemma.

Thus, q is a common divisor of both a and b, so q must divide $\gcd(a, b) = p$.

Hence, $q|p$.

Since p is prime, then the only positive divisors of p are 1 and p, so either $q = 1$ or $q = p$.

Since q is prime, then $q > 1$, so $q \neq 1$.

Hence, $q = p$.

But, this contradicts $q \neq p$.

Therefore, there is no other prime factor q of both a^3 and b^2, so p is the only common prime factor of both a^3 and b^2.

Thus, the greatest common factor of both a^3 and b^2 must be either p^2 or p^3.

Therefore, $\gcd(a^3, b^2) = p^2$ or $\gcd(a^3, b^2) = p^3$. □

Exercise 21. Let $n \in \mathbb{Z}^+$.

If $n > 1$, then every integer of the form $n^4 + 4$ is composite.

Solution. The statement to prove is: $(\forall n \in \mathbb{Z}^+, n \geq 2)(n^4 + 4$ is composite).

We observe that 4 is a factor of $n^4 + 4$ if n is even.

If n is odd, we conjecture that $n^4 + 4$ has a least prime factor p such that $p = 4k + 1$ for some integer k. □

Proof. Suppose $n > 1$.

Since $n \in \mathbb{Z}$, then $n^4 + 4 \in \mathbb{Z}$.

Observe that $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$.

Since $n > 1$, then $n^2 > 1$ and $n + 1 > 2$, so $n^2(n + 1) > 2$.

Thus, $n^2(n + 1) - 2 > 0$.

Since $n > 1$, then $n - 1 > 0$.

Since $n - 1 > 0$ and $n^2(n + 1) - 2 > 0$, then $(n - 1)[n^2(n + 1) - 2] > 0$.

Thus, $(n-1)(n^3+n^2-2) > 0$, so $n^4 - n^2 - 2n + 2 > 0$, so $n^4 > n^2 + 2n - 2$.

Therefore, $n^4 + 4 > n^2 + 2n + 2$.

Since $n > 1$, then $n + 1 > 2$, so $n + 1 > 0$.

Hence, $(n + 1)^2 > 0$, so $n^2 + 2n + 1 > 0$.

Therefore, $n^2 + 2n + 2 > 1$.

Since $n^4+4 > n^2+2n+2$ and $n^2+2n+2 > 1$, then $n^4+4 > n^2+2n+2 > 1$, so $1 < n^2 + 2n + 2 < n^4 + 4$.

Since $n^2 > 1$, then $n^2 > 0$.

Since $n - 1 > 0$ and $n^2 > 0$, then $n^2(n - 1) > 0 > -2$, so $n^2(n - 1) > -2$.

Thus, $n^2(n - 1) + 2 > 0$.

Since $n > 1$, then $n + 1 > 2 > 0$, so $n + 1 > 0$.

Since $n + 1 > 0$ and $n^2(n - 1) + 2 > 0$, then $(n + 1)[n^2(n - 1) + 2] > 0$, so $(n + 1)(n^3 - n^2 + 2) > 0$.

Thus, $n^4 - n^2 + 2n + 2 > 0$, so $n^4 > n^2 - 2n - 2$.

Therefore, $n^4 + 4 > n^2 - 2n + 2$.

Since $n > 1$, then $n - 1 > 0$, so $(n - 1)^2 > 0$.

Therefore, $n^2 - 2n + 1 > 0$, so $n^2 - 2n + 2 > 1$.

Since $n^4+4 > n^2-2n+2$ and $n^2-2n+2 > 1$, then $n^4+4 > n^2-2n+2 > 1$, so $1 < n^2 - 2n + 2 < n^4 + 4$.

Since $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$ and $1 < n^2 + 2n + 2 < n^4 + 4$ and $1 < n^2 - 2n + 2 < n^4 + 4$ and a composite number is composed of smaller positive factors, then the integer $n^4 + 4$ is composite. □

Exercise 22. Let $n \in \mathbb{Z}^+$.

If $n > 4$ and n is composite, then n divides $(n-1)!$.

Proof. Suppose $n > 4$ and n is composite.

Then

TODO: FINISH THIS PROOF. □

Exercise 23. Let $n \in \mathbb{Z}^+$.

Every integer of the form $8^n + 1$ is composite.

Proof. Since $n \in \mathbb{Z}^+$, then $8^n + 1 \in \mathbb{Z}$ and $n \geq 1$.

Observe that $8^n + 1 = (2^{2n} - 2^n + 1)(2^n + 1)$.

Since $n \geq 1$, then $n > 0$.

Therefore, $2^n > 0$, so $2^n + 1 > 1$.

Since $3 > 1$ and $n > 0$, then $3n > n$, so $2^{3n} > 2^n$.

Since $8^n = 2^{3n}$, then $8^n > 2^n$, so $8^n + 1 > 2^n + 1$.

Since $8^n + 1 > 2^n + 1$ and $2^n + 1 > 1$, then $8^n + 1 > 2^n + 1 > 1$, so $1 < 2^n + 1 < 8^n + 1$.

Since $n > 0$, then $4^n > 2^n$, so $4^n - 2^n > 0$.

Since $4^n - 2^n > 0 > -1$, then $4^n - 2^n > -1$, so $4^n > 2^n - 1$.

Since $2^n > 0$, then $2^n(4^n) > 2^n(2^n - 1)$, so $8^n > 2^{2n} - 2^n$.

Therefore, $8^n + 1 > 2^{2n} - 2^n + 1$.

Since $n > 0$, then $2n > n$, so $2^{2n} > 2^n$.

Therefore, $2^{2n} - 2^n > 0$, so $2^{2n} - 2^n + 1 > 1$.

Since $8^n + 1 > 2^{2n} - 2^n + 1$ and $2^{2n} - 2^n + 1 > 1$, then $8^n + 1 > 2^{2n} - 2^n + 1 > 1$, so $1 < 2^{2n} - 2^n + 1 < 8^n + 1$.

Since $8^n + 1$ is an integer and $1 < 2^n + 1 < 8^n + 1$ and $1 < 2^{2n} - 2^n + 1 < 8^n + 1$ and $8^n + 1 = (2^{2n} - 2^n + 1)(2^n + 1)$ and a composite number is composed of smaller positive factors, then we conclude $8^n + 1$ is composite. □

Exercise 24. Every integer $n > 11$ can be written as the sum of two composite numbers.

Solution. We observe that each even composite $c = 2k$ for $k \geq 3$ can be added so that $2c = 2k + 2k = 4k$.

Since $k \geq 3$, then $2k \geq 6$, so $4k \geq 12 > 11$.

Thus, one case occurs when $2k$ is added to itself and the sum is greater than 11 and $2k$ is even, so $2k$ is composite.

Let $U = \{n \in \mathbb{Z}^+ : n \geq 12\} = \{12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, ...\}$.

Let $A = \{4k : k \geq 3\} \subset 4\mathbb{Z} = \{12, 16, 20, 24, 28, 32, 36, 40, 44, ...\}$.

Let $B = \{4+b : b \geq 8 \text{ and } b \text{ is composite}\} = \{12, 13, 14, 16, 18, 19, 20, 22, 24, 25, 26, 28, 29, 30, 31, 32, 34, 36, 3$

Let $C = U - A - B = \{15, 17, 21, 23, 27, 33, 35, 41, 45, ...\}$.

Then $U = A \cup B \cup C$.

How can we characterize set C?

Maybe $C = \{2x + 3y : x \geq 3, y \geq 3\}$, so C is perhaps a set of linear combinations of 2 and 3?

We know $\gcd(2, 3) = 1$, so any linear combination of 2 and 3 is a multiple of 1 and $2x$ and $3y$ are both composite numbers.

Since $x \geq 3$, then $2x \geq 6$.

Since $y \geq 3$, then $3y \geq 15$.

Hence, $2x + 3y \geq 6 + 9 = 15$, so 15 would be possibly the least element of C.

Each element of C is odd or prime.

We see that $15 = 6+9, 17 = 8+9, 21 = 6+15, 23 = 9+14, 27 = 12+15$, *etc.*

Can we prove $U = A \cup B \cup C$?

We know each of A, B, C are subsets of U, so their union is also a subset of U.

Hence, $A \cup B \cup C \subset U$.

But, is $U \subset A \cup B \cup C$?

Let $n \in U$.

Then $n \geq 12$.

Can we consider n divided by 4 and use the division algorithm? □

Proof. TODO FINISH PROOF. □

Exercise 25. Compute all prime numbers that divide 50!.

Solution. The prime factorization is $50! = 2^{47} \cdot 3^{22} \cdot 5^{12} \cdot 7^8 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47$.

Therefore, the set of primes that divide 50! is $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$. □

Lemma 26. ***Any prime other than*** 3 ***is of the form*** $3k + 1$ ***or*** $3k + 2$

Let $p \in \mathbb{Z}^+$.

If p is prime and $p \neq 3$, then either $p = 3k + 1$ or $p = 3k + 2$ for some integer k.

Proof. Suppose p is prime and $p \neq 3$.

By the division algorithm, there exist unique integers q and r such that $p = 3q + r$ with $0 \leq r < 3$.

Hence, either $p = 3q$ or $p = 3q + 1$ or $p = 3q + 2$.

Suppose $p = 3q$.

Then $3|p$.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $p \neq 3$, then 3 cannot be a divisor of p, so $3 \not| p$.

But, this contradicts $3|p$.

Therefore, $p \neq 3q$.

Hence, either $p = 3q + 1$ or $p = 3q + 2$.

Therefore, there exists an integer q such that either $p = 3q + 1$ or $p = 3q + 2$. □

Lemma 27. ***Any prime other than*** 2 ***is of the form*** $8k+1$ ***or*** $8k+3$ ***or*** $8k+5$ ***or*** $8k+7$

Let $p \in \mathbb{Z}^+$.

If p is prime and $p \neq 2$, then either $p = 8k + 1$ or $p = 8k + 3$ or $p = 8k + 5$ or $p = 8k + 7$ for some integer k.

Proof. Suppose p is prime and $p \neq 2$.

By the division algorithm, there exist unique integers q and r such that $p = 8q + r$ with $0 \leq r < 8$.

Hence, either $p = 8q$ or $p = 8q + 1$ or $p = 8q + 2$ or $p = 8q + 3$ or $p = 8q + 4$ or $p = 8q + 5$ or $p = 8q + 6$ or $p = 8q + 7$.

Suppose $p = 8q$.
Then $8|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since p is prime, then $p \neq 8$, so 8 cannot be a divisor of p.
Hence, $8 \nmid p$.
But, this contradicts $8|p$.
Therefore, $p \neq 8q$.

Suppose $p = 8q + 2$.
Then $p = 8q + 2 = 2(4q + 1)$, so $2|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since $p \neq 2$, then 2 cannot be a divisor of p, so $2 \nmid p$.
But, this contradicts $2|p$.
Therefore, $p \neq 8q + 2$.

Suppose $p = 8q + 4$.
Then $p = 8q + 4 = 4(2q + 1)$, so $4|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since p is prime, then $p \neq 4$, so 4 cannot be a divisor of p.
Hence, $4 \nmid p$.
But, this contradicts $4|p$.
Therefore, $p \neq 8q + 4$.

Suppose $p = 8q + 6$.
Then $p = 8q + 6 = 2(4q + 3)$, so $2|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since $p \neq 2$, then 2 cannot be a divisor of p.
Hence, $2 \nmid p$.
But, this contradicts $2|p$.
Therefore, $p \neq 8q + 6$.

Hence, either $p = 8q + 1$ or $p = 8q + 3$ or $p = 8q + 5$ or $p = 8q + 7$.

Therefore, there exists an integer q such that either $p = 8q + 1$ or $p = 8q + 3$ or $p = 8q + 5$ or $p = 8q + 7$. □

Exercise 28. Let $p, q \in \mathbb{Z}^+$.

If $p \geq q \geq 5$ and p and q are both primes, then $24|(p^2 - q^2)$.

Solution. By a previous lemma, we know that any prime $p \neq 3$ is of the form $3k + 1$ or $3k + 2$ for some integer k.

Also, by a previous lemma, we know that any prime $p \neq 2$ is of the form $8m + 1$ or $8m + 3$ or $8m + 5$ or $8m + 7$ for some integer m.

We shall prove $3|(p^2 - q^2)$ and $8|(p^2 - q^2)$.

Then, this means $p^2 - q^2$ is a common multiple of 3 and 8.

Since $p^2 - q^2$ is a common multiple of 3 and 8 and $\gcd(3, 8) = 1$, then another proposition guarantees that $p^2 - q^2$ is a multiple of the product $3 \cdot 8 = 24$.

Therefore, this implies $24|(p^2 - q^2)$. □

Proof. Suppose $p \geq q \geq 5$ and p is prime and q is prime.

Since $p \geq q \geq 5$, then $p \geq 5$, so $p \neq 3$.

Since p is prime and $p \neq 3$, then either $p = 3k + 1$ or $p = 3k + 2$ for some integer k, by a previous lemma.

Since $p \geq q \geq 5$, then $q \geq 5$, so $q \neq 3$.

Since q is prime and $q \neq 3$, then either $q = 3m + 1$ or $q = 3m + 2$ for some integer m, by a previous lemma.

Thus,
either $p = 3k + 1$ and $q = 3m + 1$ or
either $p = 3k + 1$ and $q = 3m + 2$ or
either $p = 3k + 2$ and $q = 3m + 1$ or
either $p = 3k + 2$ and $q = 3m + 2$.
Without loss of generality, we consider only
either $p = 3k + 1$ and $q = 3m + 1$ or
either $p = 3k + 1$ and $q = 3m + 2$ or
either $p = 3k + 2$ and $q = 3m + 2$, since $p^2 - q^2 = -(q^2 - p^2)$.
We consider these cases separately.
Case 1: Suppose $p = 3k + 1$ and $q = 3m + 1$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (3k + 1)^2 - (3m + 1)^2 \\ &= 3(3k + 3m + 2)(k - m). \end{aligned}$$

Therefore, $3|(p^2 - q^2)$.
Case 2: Suppose $p = 3k + 1$ and $q = 3m + 2$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (3k + 1)^2 - (3m + 2)^2 \\ &= 3(3k - 3m - 1)(k + m + 1). \end{aligned}$$

Therefore, $3|(p^2 - q^2)$.

Case 3: Suppose $p = 3k + 2$ and $q = 3m + 2$.

Observe that

$$\begin{aligned} p^2 - q^2 &= (3k+2)^2 - (3m+2)^2 \\ &= 3(3k + 3m + 4)(k - m). \end{aligned}$$

Therefore, $3|(p^2 - q^2)$.

In all cases, we conclude $3|(p^2 - q^2)$. □

Proof. Suppose $p \geq q \geq 5$ and p is prime and q is prime.

Since $p \geq q \geq 5$, then $p \geq 5$, so $p \neq 2$.

Since p is prime and $p \neq 2$, then either $p = 8k+1$ or $p = 8k+3$ or $p = 8k+5$ or $p = 8k + 7$ for some integer k, by a previous lemma.

Since $p \geq q \geq 5$, then $q \geq 5$, so $q \neq 2$.

Since q is prime and $q \neq 2$, then either $q = 8m + 1$ or $q = 8m + 3$ or $q = 8m + 5$ or $q = 8m + 7$ for some integer m, by a previous lemma.

Thus,
either $p = 8k + 1$ and $q = 8m + 1$ or
either $p = 8k + 1$ and $q = 8m + 3$ or
either $p = 8k + 1$ and $q = 3m + 5$ or
either $p = 8k + 1$ and $q = 3m + 7$ or
either $p = 8k + 3$ and $q = 8m + 1$ or
either $p = 8k + 3$ and $q = 8m + 3$ or
either $p = 8k + 3$ and $q = 3m + 5$ or
either $p = 8k + 3$ and $q = 3m + 7$ or
either $p = 8k + 5$ and $q = 8m + 1$ or
either $p = 8k + 5$ and $q = 8m + 3$ or
either $p = 8k + 5$ and $q = 3m + 5$ or
either $p = 8k + 5$ and $q = 3m + 7$ or
either $p = 8k + 7$ and $q = 8m + 1$ or
either $p = 8k + 7$ and $q = 8m + 3$ or
either $p = 8k + 7$ and $q = 3m + 5$ or
either $p = 8k + 7$ and $q = 3m + 7$.

Without loss of generality, we consider only
either $p = 8k + 1$ and $q = 8m + 1$ or
either $p = 8k + 1$ and $q = 8m + 3$ or
either $p = 8k + 1$ and $q = 8m + 5$ or
either $p = 8k + 1$ and $q = 8m + 7$ or
either $p = 8k + 3$ and $q = 8m + 3$ or
either $p = 8k + 3$ and $q = 8m + 5$ or
either $p = 8k + 3$ and $q = 8m + 7$ or
either $p = 8k + 5$ and $q = 8m + 5$ or
either $p = 8k + 5$ and $q = 8m + 7$ or

either $p = 8k + 7$ and $q = 8m + 7$,
since $p^2 - q^2 = -(q^2 - p^2)$.
We consider these cases separately.
Case 1: Suppose $p = 8k + 1$ and $q = 8m + 1$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+1)^2 - (8m+1)^2 \\ &= 16(4k + 4m + 1)(k - m) \\ &= 8 * 2(4k + 4m + 1)(k - m). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.
Case 2: Suppose $p = 8k + 1$ and $q = 8m + 3$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+1)^2 - (8m+3)^2 \\ &= 8(8k + 1)(8m + 3). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.
Case 3: Suppose $p = 8k + 1$ and $q = 8m + 5$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+1)^2 - (8m+5)^2 \\ &= 8(4k + 4m + 3)(2k - 2m - 1). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.
Case 4: Suppose $p = 8k + 1$ and $q = 8m + 7$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+1)^2 - (8m+7)^2 \\ &= 16(4k - 4m - 3)(k + m + 1) \\ &= 8 * 2(4k - 4m - 3)(k + m + 1). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.
Case 5: Suppose $p = 8k + 3$ and $q = 8m + 3$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+3)^2 - (8m+3)^2 \\ &= 16(4k + 4m + 3)(k - m) \\ &= 8 * 2(4k + 4m + 3)(k - m). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.
Case 6: Suppose $p = 8k + 3$ and $q = 8m + 5$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+3)^2 - (8m+5)^2 \\ &= 16(4k - 4m - 1)(k + m + 1) \\ &= 8 * 2(4k - 4m - 1)(k + m + 1). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.
Case 7: Suppose $p = 8k + 3$ and $q = 8m + 7$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+3)^2 - (8m+7)^2 \\ &= 8(4k + 4m + 5)(2k - 2m - 1). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.
Case 8: Suppose $p = 8k + 5$ and $q = 8m + 5$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+5)^2 - (8m+5)^2 \\ &= 16(4k + 4m + 5)(k - m) \\ &= 8 * 2(4k + 4m + 5)(k - m). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.
Case 9: Suppose $p = 8k + 5$ and $q = 8m + 7$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+5)^2 - (8m+7)^2 \\ &= 8(4k - 4m - 1)(2k + 2m + 3). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.
Case 10: Suppose $p = 8k + 7$ and $q = 8m + 7$.
Observe that

$$\begin{aligned} p^2 - q^2 &= (8k+7)^2 - (8m+7)^2 \\ &= 16(4k + 4m + 7)(k - m) \\ &= 8 * 2(4k + 4m + 7)(k - m). \end{aligned}$$

Therefore, $8|(p^2 - q^2)$.

In all cases, we conclude $8|(p^2 - q^2)$.

Since $3|(p^2 - q^2)$ and $8|(p^2 - q^2)$, then $p^2 - q^2$ is a common multiple of 3 and 8.

Since $p^2 - q^2$ is a common multiple of 3 and 8 and $\gcd(3, 8) = 1$, then another proposition guarantees that $p^2 - q^2$ is a multiple of the product $3 \cdot 8 = 24$.

Therefore, $24|(p^2 - q^2)$. □

Exercise 29. Let $p \in \mathbb{Z}^+$.
If p is prime and $p \neq 5$ and p is odd, then either $10|(p^2 - 1)$ or $10|(p^2 + 1)$.

Proof. Suppose p is prime and $p \neq 5$ and p is odd.
Since p is odd, then p^2 is odd, so $p^2 - 1$ and $p^2 + 1$ are both even.
Hence, $2|(p^2 - 1)$ and $2|(p^2 + 1)$.

Since p is prime and odd, then $p > 2 > 0$, so $p > 2$ and $p > 0$.

Since $p > 0$, then $p^2 > 0$, so $p^2 + 1 > 1$.

Since $p > 2$, then $p^2 > 4$, so $p^2 - 1 > 3 > 1$.

Hence, $p^2 - 1 > 1$.

Since $p^2 + 1 > 1$ and $p^2 - 1 > 1$, then both $p^2 + 1$ and $p^2 - 1$ have unique canonical prime factorizations, by FTA.

By the division algorithm, there are unique integers q and r such that $p = 5q + r$ with $0 \leq r < 5$, so either $p = 5q$ or $p = 5q + 1$ or $p = 5q + 2$ or $p = 5q + 3$ or $p = 5q + 4$.

Suppose $p = 5q$.

Then $5|p$.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $p \neq 5$, then 5 cannot divide p, so $5 \not| p$.

But, this contradicts $5|p$, so $p \neq 5q$.

Thus, either $p = 5q + 1$ or $p = 5q + 2$ or $p = 5q + 3$ or $p = 5q + 4$.

We consider these cases separately.

Case 1: Suppose $p = 5q + 1$.

Then $p^2 - 1 = (5q + 1)^2 - 1 = 25q^2 + 10q + 1 - 1 = 25q^2 + 10q = 5q(5q + 2)$, so $5|(p^2 - 1)$.

Case 2: Suppose $p = 5q + 2$.

Then $p^2 + 1 = (5q + 2)^2 + 1 = 25q^2 + 20q + 4 + 1 = 25q^2 + 20q + 5 = 5(5q^2 + 4q + 1)$, so $5|(p^2 + 1)$.

Case 3: Suppose $p = 5q + 3$.

Then $p^2 + 1 = (5q + 3)^2 + 1 = 25q^2 + 30q + 9 + 1 = 25q^2 + 30q + 10 = 5(5q^2 + 6q + 2)$, so $5|(p^2 + 1)$.

Case 4: Suppose $p = 5q + 4$.

Then $p^2 - 1 = (5q + 4)^2 - 1 = 25q^2 + 40q + 16 - 1 = 25q^2 + 40q + 15 = 5(5q^2 + 8q + 3)$, so $5|(p^2 - 1)$.

Therefore, in all cases, either $5|(p^2 - 1)$ or $5|(p^2 + 1)$.

Since $2|(p^2 - 1)$ and $2|(p^2 + 1)$ and either $5|(p^2 - 1)$ or $5|(p^2 + 1)$, then either both $2|(p^2 - 1)$ and $5|(p^2 - 1)$ or both $2|(p^2 + 1)$ and $5|(p^2 + 1)$.

We consider these cases separately.

Case 1: Suppose $2|(p^2 - 1)$ and $5|(p^2 - 1)$.

Then 2 and 5 are both prime factors of $p^2 - 1$, so both 2 and 5 occur in the prime factorization of $p^2 - 1$.

Hence, the product $2 \cdot 5 = 10$ is a factor of $p^2 - 1$, so $10|(p^2 - 1)$.

Case 2: Suppose $2|(p^2 + 1)$ and $5|(p^2 + 1)$.

Then 2 and 5 are both prime factors of $p^2 + 1$, so both 2 and 5 occur in the prime factorization of $p^2 + 1$.

Hence, the product $2 \cdot 5 = 10$ is a factor of $p^2 + 1$, so $10|(p^2 + 1)$.

Therefore, either $10|(p^2-1)$ or $10|(p^2+1)$, as desired. □

Exercise 30. Let $k \in \mathbb{Z}^+$.
Let $p = 2^k - 1$.
If p is prime and $k > 2$, then k is odd.

Proof. Suppose p is prime and $k > 2$.

Suppose k is not odd.
Then k is even, so $k = 2n$ for some integer n.
Thus, $p = 2^k - 1 = 2^{2n} - 1 = (2^n)^2 - 1 = (2^n - 1)(2^n + 1)$.
Since $2 < k = 2n$, then $2 < 2n$, so $1 < n$.
Hence, $n > 1$, so $n > 0$.

Since $n > 0$ and $1 < 2$, then $n < 2n$, so $2^n < 2^{2n}$.
Hence, $2^n - 1 < 2^{2n} - 1$.

Since $n > 1$, then $2^n > 2$, so $2^n - 1 > 1$.
Since $1 < 2^n - 1$ and $2^n - 1 < 2^{2n} - 1$, then $1 < 2^n - 1 < 2^{2n} - 1$.

Since $2^n > 2$, then $2^n + 2^n > 2^n + 2$.
Hence, $2(2^n) = 2^{n+1} > 2^n + 2$.
Since $2^n > 2$ and $2^n > 0$, then $2^n \cdot 2^n > 2 \cdot 2^n = 2^{n+1} > 2^n + 2$.
Thus, $(2^n)^2 > 2^n + 2$, so $2^{2n} > 2^n + 2$.
Therefore, $2^{2n} - 1 > 2^n + 1$.

Since $n > 0$, then $2^n > 0$, so $2^n + 1 > 1$.
Since $1 < 2^n + 1$ and $2^n + 1 < 2^{2n} - 1$, then $1 < 2^n + 1 < 2^{2n} - 1$.

Since $1 < 2^n - 1 < 2^{2n} - 1$ and $1 < 2^n + 1 < 2^{2n} - 1$ and $p = (2^n - 1)(2^n + 1)$, then p is composite.
But, this contradicts p is prime.
Therefore, k is odd. □

Exercise 31. $(\forall n \in \mathbb{Z}^+)(3|4^n - 1)$.

Proof. Let $p(n)$ be the predicate : $3|(4^n - 1)$ defined over $\mathbb{Z}^+$.
We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Since $4^1 - 1 = 3$ and $3|3$, then $3|(4^1 - 1)$, so $p(1)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then $3|(4^k - 1)$, so $4^k - 1 = 3x$ for some integer x.

Observe that

$$\begin{aligned} 4^{k+1}-1 &= 4\cdot 4^k - 1 \\ &= 4\cdot 4^k - 4 + 4 - 1 \\ &= 4(4^k-1)+3 \\ &= 4(3x)+3 \\ &= 3(4x+1). \end{aligned}$$

Thus, $3|(4^{k+1}-1)$, so $p(k+1)$ is true.

Since $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then, we conclude $p(n)$ is true for all $n \in \mathbb{Z}^+$, by induction.

Therefore, $3|(4^n-1)$ for all $n \in \mathbb{Z}^+$. □

Exercise 32. Let $S = \{3k+1 : k \in \mathbb{Z}^+ \vee k = 0\}$.

Let $a \in S$.

Define $a > 1$ to be prime if a cannot be factored into two smaller integers in S.

Example is 10 and 25 are prime, but $16 = 4 * 4$ and $28 = 4 * 7$ are not prime.

a. Prove any member of S is either prime or a product or primes.

b. Give an example to show that it is possible for an integer in S to be factored into primes in more than one way.

Proof. TODO FINISH PROOF □

Exercise 33. It is conjectured that every even integer can be written as the difference of two consecutive primes in infinitely many ways.

For example, $6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \ldots$.

Express the integer 10 as the difference of two consecutive primes in fifteen ways.

Solution. TODO Try this one. this is computational exercise. □

Exercise 34. Let $a \in \mathbb{Z}^+$.

Then $a > 1$ is a perfect square iff in the canonical form of a all the exponents of the primes are even integers.

Proof. TODO We've already done this. So find the proof in one of the exercises and copy it here and clean up the proof to make it coherent, clear. □

Lemma 35. ***Each prime factor of a square number greater than one has even exponent.***

Let $n \in \mathbb{Z}^+$ and $n > 1$.

Then each prime factor of n^2 has even exponent.

Proof. Since $n > 1$, then by FTA, n has a unique canonical prime decomposition $n = p_1^{e_1} * p_2^{e_2} * * * p_k^{e_k}$ for primes $p_1, p_2, ..., p_k$ and positive integers $e_1, e_2, ..., e_k$ such that $p_1 < p_2 < ... < p_k$.

Observe that $n^2 = (p_1^{e_1} * p_2^{e_2} * * * p_k^{e_k})^2 = p_1^{2e_1} * p_2^{2e_2} * * * p_k^{2e_k}$.

Therefore, each of the exponents $2e_i$ is even. □

Exercise 36. Any integer n can be expressed as $n = 2^k m$, where $k \geq 0$ and m is an odd integer.

Proof. TODO □

Exercise 37. It is conjectured that there are infinitely many primes p such that $p + 50$ is also prime.

Find 15 of these primes.

Solution. We use SageMath to write a simple function to compute primes p and $p + 50$.

Below is a list of some primes.

$$\begin{array}{r} \text{prime } p | p+50 \\ 3 \to 53 \\ 9 \to 59 \\ 11 \to 61 \\ 17 \to 67 \\ 21 \to 71 \\ 23 \to 73 \\ 29 \to 79 \\ 33 \to 83 \\ 39 \to 89 \\ 47 \to 97 \\ 51 \to 101 \\ 53 \to 103 \\ 57 \to 107 \\ 59 \to 109 \\ 63 \to 113 \end{array}$$

□

Exercise 38. Show that the sums $1+2+4$, $1+2+4+8$, $1+2+4+8+16, ...$ are not alternately prime and composite.

Solution. Observe that $S_1 = 1 + 2 + 4 = 2^0 + 2^1 + 2^2 = \sum_{k=0}^{2} 2^k$ and $S_2 = 1+2+4+8 = 2^0+2^1+2^2+2^3 = \sum_{k=0}^{3} 2^k$ and $S_3 = 1+2+4+8+16 = 2^0+2^1+2^2+2^3+2^4 = \sum_{k=0}^{4} 2^k$ and in general, $S_n = 2^0+2^1+2^2+...+2^n+2^{n+1} = \sum_{k=0}^{n+1} 2^k$.

We usage SageMath to write a program to compute the sums S_n for various $n \in \mathbb{Z}^+$.

We find the following results:

$S_1 = 7$ is prime.

$S_2 = 15 = 3 * 5$ is composite.

$S_3 = 31$ is prime.
$S_4 = 63 = 3^2 * 7$ is composite.
$S_5 = 127$ is prime.
$S_6 = 255 = 3 * 5 * 17$ is composite.
$S_7 = 511 = 7 * 73$ is composite.
Hence, the sums do alternate between prime and composite up to S_7.
But, S_6 and S_7 are both composite. □

Exercise 39. Disprove the statement:
$(\forall n \in \mathbb{Z}^+)$ either $6n + 1$ or $6n - 1$ is prime.

Solution. We use SageMath to write a program to compute $6n + 1$ and $6n - 1$ for each $n \in \mathbb{Z}+$ until we can find a counter-example. □

Proof. Let $n = 20$.
Then $6 * 20 + 1 = 121 = 11^2$ is composite and $6 * 20 - 1 = 119 = 7 * 17$ is composite.
Therefore, the statement is false. □

Exercise 40. The difference of two consecutive cubes is not divisible by 2.

Proof. Let $n \in \mathbb{Z}$.
We must prove the difference $(n + 1)^3 - n^3$ is not divisible by 2.
Observe that $(n + 1)^3 - n^3 = 3n^2 + 3n + 1 = 3n(n + 1) + 1$.
Since the product of two consecutive integers is even, then $n(n + 1)$ is even, so $2|n(n + 1)$.
Thus, $2|3n(n + 1)$, so $3n(n + 1)$ is even.
Therefore, $3n(n + 1) + 1 = (n + 1)^3 - n^3$ is odd, so $(n + 1)^3 - n^3$ is not divisible by 2. □

Proof. Let $n \in \mathbb{Z}$.
We must prove $(n + 1)^3 - n^3$ is odd.
Observe that $(n + 1)^3 - n^3 = 3n^2 + 3n + 1 = 3n(n + 1) + 1$.
By the division algorithm, either $n = 2q$ or $n = 2q + 1$ for some integer q.
We consider each case separately.
Case 1: Suppose $n = 2q$.
Then

$$\begin{aligned}(n+1)^3 - n^3 &= 3n(n+1) + 1 \\ &= 3(2q)(2q+1) + 1 \\ &= 2(3q)(2q+1) + 1.\end{aligned}$$

Therefore, $(n + 1)^3 - n^3 = 2k + 1$ for some integer $k = 3q(2q + 1)$, so $(n + 1)^3 - n^3$ is odd.
Case 2: Suppose $n = 2q + 1$.
Then

$$\begin{aligned}(n+1)^3 - n^3 &= 3n(n+1)+1 \\ &= 3(2q+1)((2q+1)+1)+1 \\ &= 3(2q+1)(2q+2)+1 \\ &= 3(2q+1)(2)(q+1)+1 \\ &= 2(3)(2q+1)(q+1)+1.\end{aligned}$$

Therefore, $(n+1)^3 - n^3 = 2k+1$ for some integer $k = 3(2q+1)(q+1)$, so $(n+1)^3 - n^3$ is odd.

Therefore, in all cases, $(n+1)^3 - n^3$ is odd, so $(n+1)^3 - n^3$ is not divisible by 2. □

Exercise 41. Let $n \in \mathbb{Z}^+$ and p is a prime number.
Then p cannot divide both n and $n+1$.

Proof. Suppose p divides both n and $n+1$.
Then p divides any linear combination of n and $n+1$.
Since $1 = (n+1) - n = (-1)n + (1)(n+1)$ is a linear combination of n and $n+1$, then p divides 1.
The only positive integer that divides 1 is 1, so $p = 1$.
But, p is prime, so $p > 1$.
Therefore, p cannot divide both n and $n+1$. □

Exercise 42. Let $n \in \mathbb{Z}^+$.
Then $n(n+1)$ is not a square.

Proof. TODO FINISH PROOF
If $n = 1$, then $1(1+1) = 2$ is not a square.

Suppose $n(n+1)$ is a square.
Then $n \neq 1$, so $n > 1$, and there exists an integer m such that $n(n+1) = m^2$.
We may assume $m > 0$, since $(-m)^2 = m^2$.
If $m = 1$, then $1 = 1^2 = m^2 = n(n+1)$, so $n|1$.
Hence, $n = 1$.
But, this contradicts the fact $n > 1$.
Therefore, $m \neq 1$.
Since $n > 1$, then $n \geq 2$, so $n+1 \geq 3$.
Thus, $m^2 = n(n+1) \geq 6$.
If $m = 2$, then $m^2 = 4 < 6 \leq m^2$, a contradiction.
Thus, $m \neq 2$, so $m > 2$.
Suppose m is prime.
Since $m > 2$, then m is odd, so m^2 is odd.
Hence, $n(n+1) = m^2$ is odd.

But, this contradicts the fact that the product of two consecutive integers is even and $n(n+1)$ is even.

Therefore, m cannot be prime.

Since $m \neq 1$, then this implies m must be composite.

Since $n(n+1) = m^2$ is even, then m is even, so $2|m$. □

Exercise 43. Let p be a prime.

For what primes p is $17p + 1$ a perfect square?

Solution. Using SageMath we find $p = 19$ implies $17(19) + 1 = 324 = 18^2$ is a perfect square.

We try other larger primes and still we only get $p = 19$, so we conjecture that $17p + 1$ is a square iff $p = 19$.

We shall prove $17p + 1$ is a square iff $p = 19$. □

Proof. We first prove if $p = 19$, then $17p + 1$ is a square.

Suppose $p = 19$.

Then $17p + 1 = 17(19) + 1 = 324 = 18^2$ is a perfect square. □

Proof. Conversely, suppose $17p + 1$ is a square.

Then $17p + 1 = n^2$ for some integer n.

Hence, $17p = n^2 - 1 = (n-1)(n+1)$.

Since p is prime, then $p > 1$, so $17p > 17 > 1$.

Thus, by the Fundamental Theorem of Arithmetic, $17p = (n-1)(n+1)$ has a unique prime factorization.

Hence, either $17 = n - 1$ or $17 = n + 1$.

Suppose $17 = n + 1$.

Then $n = 16$, so $256 = 16^2 = 17p + 1$.

Hence, $255 = 17p$, so $p = 15 = 3 \cdot 5$, a composite number.

But, this contradicts that p is a prime number.

Consequently, $17 \neq n + 1$, so $17 = n - 1$.

Thus, $n = 18$, so $324 = 18^2 = 17p + 1$.

Therefore, $323 = 17p$, so $p = 19$, as desired. □

Exercise 44. Find the smallest positive integer n such that $n + 1, n + 2, n + 3$ are all composite.

a. If $n = 5! + 1$, show that $n + 1, n + 2, n + 3, n + 4$ are composite.

b. Find a sequence of 100 consecutive composite numbers.

Solution. We see that $n = 7$ is the smallest positive integer for which $7 + 1 = 8 = 2^3$ and $7 + 2 = 9 = 3^2$ and $7 + 3 = 10 = 2 * 5$ are all composite.

a. Let $n = 5! + 1 = 120 + 1 = 121$.

Then $n + 1 = 121 + 1 = 122 = 2 * 61$ is composite and $n + 2 = 121 + 2 = 123 = 3 * 41$ is composite and $n + 3 = 121 + 3 = 124 = 4 * 31$ is composite and $n + 4 = 121 + 4 = 125 = 5 * 25$ is composite. So, we have a sequence of 4 consecutive composite numbers.

b. Using SageMath we write a program to find a sequence of consecutive composite numbers. The sequence starts with $n = 370262$ to 370361. □

Exercise 45. Let $n \in \mathbb{Z}^+$ be composite and p be the least prime factor of n.

If $p^3 > n$, then $\frac{n}{p}$ is prime.

Solution. Try $n = 11 * 17$ and $p = 11$.

Then $11^3 = 11 * 11 * 11 > 11 * 17$ and $\frac{11*17}{11} = 17$ is prime. □

Proof. Suppose $p^3 > n$.

Since p is a factor of n, then $p|n$, so $p \leq n$.

Since n is composite and p is prime, then $p \neq n$.

Thus, $p < n$.

Since p is prime, then $p > 0$, so $1 < \frac{n}{p}$.

Since $\frac{n}{p} > 1$, then $\frac{n}{p}$ is either prime or composite.

Suppose $\frac{n}{p}$ is composite.

Since $\frac{n}{p} > 1$, then by FTA, $\frac{n}{p}$ has a unique canonical prime factorization, so $\frac{n}{p} = q_1^{e_1} * q_2^{e_2} * \ldots q_s^{e_s}$ for primes q_i and positive integers e_i with $1 \leq i \leq s$.

Since $n = p \cdot \frac{n}{p}$ and p is the least prime factor of n, then $n = p \cdot q_1^{e_1} * q_2^{e_2} * \ldots q_s^{e_s}$, so $p \leq q_1 < q_2 < ... < q_s$.

Since $p \leq q_1$ and $p < q_2$, then $p^2 < q_1 q_2$.

Thus, $p^2 < q_1 q_2 \ldots q_s$, so $p^2 < q_1^{e_1} * q_2^{e_2} * \ldots q_s^{e_s}$.

Since $p^3 > n$ and $p > 0$, then $p^2 > \frac{n}{p} = q_1^{e_1} * q_2^{e_2} * \ldots q_s^{e_s}$, so $p^2 > q_1^{e_1} * q_2^{e_2} * \ldots q_s^{e_s}$.

Hence, we have $p^2 > q_1^{e_1} * q_2^{e_2} * \ldots q_s^{e_s}$ and $p^2 < q_1^{e_1} * q_2^{e_2} * \ldots q_s^{e_s}$, a contradiction.

Therefore, $\frac{n}{p}$ is not composite, so $\frac{n}{p}$ is prime. □

Exercise 46. Let $N \in \mathbb{Z}^+$ be odd.

Then there exists $a \in \mathbb{Z}$ such that $N + a^2 = b^2$ for some $b \in \mathbb{Z}$.

Solution. For $N = 1$, let $a = 0$. Then $1 + 0^2 = 1 = 1^2$, so $b = 1$.

For $N = 3$, let $a = 1$. Then $3 + 1^2 = 4 = 2^2$, so $b = 4$.

For $N = 5$, let $a = 2$. Then $5 + 2^2 = 9 = 3^2$, so $b = 9$.

For $N = 7$, let $a = 3$. Then $7 + 3^2 = 16 = 4^2$, so $b = 16$. □

Proof. Let $a = \frac{N-1}{2}$ and let $b = \frac{N+1}{2}$.

Since N is odd, then $N - 1$ and $N + 1$ are both even.

Thus, $\frac{N-1}{2}$ and $\frac{N+1}{2}$ are integers, so $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$.

Observe that

$$\begin{aligned} N + a^2 &= N + (\frac{N-1}{2})^2 \\ &= N + \frac{N^2 - 2N + 1}{4} \\ &= \frac{4N + N^2 - 2N + 1}{4} \\ &= \frac{N^2 + 2N + 1}{4} \\ &= \frac{(N+1)^2}{4} \\ &= (\frac{N+1}{2})^2 \\ &= b^2. \end{aligned}$$

□

Exercise 47. Let $p, q \in \mathbb{Z}^+$.
If p and q are prime and $p|q$, then $p = q$.

Proof. Suppose p and q are prime and $p|q$.
Since q is prime, then the only positive divisors of q are 1 and q.
Since $p \in \mathbb{Z}^+$ and $p|q$, then this implies either $p = 1$ or $p = q$.
Since p is prime, then $p > 1$, so $p \neq 1$.
Therefore, $p = q$. □

Exercise 48. Let $p, a, n \in \mathbb{Z}^+$.
If p is prime and $p|a^n$, then $p^n|a^n$.

Proof. Suppose p is prime and $p|a^n$.
Then by a corollary to Euclid's lemma, $p|a$.
By the previous lemma, we know if $p|a$, then $p^n|a^n$.
Since $p|a$, then we conclude $p^n|a^n$. □

Exercise 49. There do not exist positive integers a and b such that $a^2 = 2b^2$.
This implies that $\sqrt{2}$ cannot be a rational number.

Proof. Suppose there exist positive integers a and b such that $a^2 = 2b^2$.
Then $2|a^2$, so a^2 is even and 2 is a prime factor of a^2 and $2 \leq a^2$.
Since $a^2 \geq 2$, then $a^2 > 1$.
Since a^2 is even, then a is even, so $a = 2k$ for some integer k.
Therefore, $2b^2 = a^2 = (2k)^2 = 4k^2$, so $b^2 = 2k^2$.
Thus, $2|b^2$, so 2 is a prime factor of b^2 and $2 \leq b^2$.
Since $b^2 \geq 2$, then $b^2 > 1$.
By lemma 35, each prime factor of a square number greater than one has even exponent, so b^2 has 2^{2e_1} prime factor for some positive integer e_1.
Since $a^2 = 2b^2$, then a^2 has prime factor $2 * 2^{2e_1} = 2^{2e_1+1}$.

But, $2e_1 + 1$ is an odd integer which means the prime factor 2 has odd exponent for the square number a^2.

This contradicts the fact that each prime factor of a square number greater than one has even exponent.

Therefore, there do not exist integers a and b such that $a^2 = 2b^2$. □

Proof. Suppose there exist positive integers a and b such that $a^2 = 2b^2$ and $\gcd(a, b) = 1$.

Since $a^2 = 2b^2$, then $b|a^2$.

Since $b \in \mathbb{Z}^+$, then $b \geq 1$, so either $b > 1$ or $b = 1$.

Suppose $b = 1$.

Then $a^2 = 2(1)^2 = 2$, so 2 is a square integer.

But, there is no integer whose square is 2, so $b \neq 1$.

Suppose $b > 1$.

Since every integer greater than 1 has a prime factor, then b has a prime factor p, so $p|b$.

Since $p|b$ and $b|a^2$, then $p|a^2$.

Since p is prime and $p|a^2$, then by Euclid's lemma, $p|a$.

Since $p|a$ and $p|b$, the p is a common divisor of a and b, so $p|\gcd(a, b)$.

Since $\gcd(a, b) = 1$, then this implies $p|1$, so $p = 1$.

But, p is prime, so $p > 1$.

Thus, we have $p = 1$ and $p > 1$, a contradiction.

Hence, b cannot be greater than 1.

Since $b \neq 1$ and b cannot be greater than 1, then b cannot exist, so a cannot exist.

Therefore, there are no positive integers a and b such that $a^2 = 2b^2$ and $\gcd(a, b) = 1$. □

Exercise 50. Let $n \in \mathbb{Z}^+$.

If $n \geq 4$ and n divides $2^n - 2$, then $\frac{2^n-2}{n}$ is not prime.

Proof. Suppose $n \geq 4$ and n divides $2^n - 2$.

Since n divides $2^n - 2$, then $2^n - 2 = nk$ for some integer k and $\frac{2^n-2}{n} \in \mathbb{Z}$.

Hence, $\frac{nk}{2} = 2^{n-1} - 1$.

Since $n \geq 4$, then $n > 1$, so $n - 1 > 0$.

Thus, $2^{n-1} \in \mathbb{Z}$, so $2^{n-1} - 1 \in \mathbb{Z}$.

Consequently, $\frac{nk}{2} \in \mathbb{Z}$, so $2|nk$.

Suppose n is even.

Then $n = 2m$ for some integer m, so $2|n$.

We prove $gcd(2^n - 2, n) = 2$ because $n \geq 4$.

Since $2|2^n$ and $2|2$, then 2 divides the difference $2^n - 2$.

Since $2|n$ and 2 divides $2^n - 2$, then 2 is a common divisor of $2^n - 2$ and n.

Let c be any common divisor of $2^n - 2$ and n.

Then $c|2^n - 2$ and $c|n$, so $2^n - 2 = cx$ and $n = cy$ for some integers x and y.

We prove $c|2$.

TODO FINISH PROOF.

Then we divide by 2 to get $\frac{2^n-2}{2} = 2^{n-1} - 1$ and this we would like to conclude that the numerator when divided by 2 and the denominator when divided by 2 would be relatively prime.

We must also show that this must be a fraction and cannot be an integer, so we must also show that $2^n - 1 \neq 0$ and $2^n - 1 \neq m$ and $m \neq 1$.

This would imply the ratio is actually not an integer which means n cannot be even, so n must be odd.

Since n is odd, then 2 cannot divide n.

Since 2 is prime and $2|nk$, then either $2|n$ or $2|k$, by Euclid's lemma.

Since 2 does not divide n, then we conclude $2|k$.

Thus, $\frac{k}{2} \in \mathbb{Z}$.

Since $2^{n-1} - 1 = (n)\frac{k}{2}$, then n divides $2^{n-1} - 1$.

Thus, $2n$ divides $2(2^{n-1} - 1)$, so $2n$ divides $2^n - 2$.

Hence, $2^n - 2 = 2na$ for some integer a, so $\frac{2^n-2}{n} = 2a$.

Therefore, 2 divides $\frac{2^n-2}{n}$, so $\frac{2^n-2}{n}$ is not prime.

But, we must also show that $\frac{2^n-2}{n} \neq 2$, too!

Thus, we must also prove $2^n > 2n + 2$ for all $n \geq 4$ (by induction).

This would show that $\frac{2^n-2}{n} > 2$ for all $n \geq 4$, so $\frac{2^n-2}{n} \neq 2$. □

Definition 51. Mersenne prime

A prime number of the form $2^p - 1$ is a **Mersenne prime** iff p is prime.

Mersenne primes $= \{2^p - 1 : p \text{ is prime } \} = \{3, 7, 31, 127, 8191, ...\}$

It is not known whether there are infinitely many Mersenne primes.

Exercise 52. Mersenne prime exercise

Let $n \in \mathbb{N}$.

If $2^n - 1$ is prime, then n is prime.

Solution. We can try proof by contrapositive, since direct proof doesn't seem to lead us anywhere.

If n is a natural number that is not prime, then n is either 1 or a composite number.

If n is 1, then $2^1 - 1 = 1$ which is not prime.

If n is composite, then $n > 2$, and n is either even or odd.

If n is even and $n > 2$, then $n = 2k, k \in \mathbb{Z}$. Since $2^n - 1 = 2^{2k} - 1 = (2^k)^2 - 1 = (2^k + 1)(2^k - 1)$, so $2^k - 1$ and $2^k + 1$ are integers.

If $n > 2$ and even, then $n \geq 4$, so $k \geq 2$. Thus, $2^k - 1 \geq 3$ and $2^k + 1 \geq 5$.

Thus each factor is greater than 1 and less than $2^n - 1$. Hence, $2^n - 1$ is composite if $n > 2$ and n is even.

If n is composite and odd, then $n \geq 9$ since 9 is the smallest composite odd natural number. The set of composite odd natural numbers is $\{9, 15, 21, 25, 27, 33, 35, 39, 45, ...\}$.

Thus this set consists of natural numbers that are divisible by 3 or 5 or both. If $3|n$, then $n = 3k, k \in \mathbb{Z}$. Thus, $2^n - 1 = 2^{3k} - 1$. Since $a^3 - 1 = (a-1)(a^2 + a + 1)$, then $2^n - 1 = (2^k)^3 - 1 = (2^k - 1)(2^{2k} + 2^k + 1)$. Since $n \geq 9$, then $k \geq 3$, so $2^k - 1 > 1$.

Since $2^k - 1, 2^{2k} + 2^k + 1 \in \mathbb{Z}$, then $2^n - 1$ is composite for odd composites divisible by 3.

If $5|n$, then $n = 5k, k \in \mathbb{Z}$, so $2^n - 1 = 2^{5k} - 1 = (2^k)^5 - 1$. Since $a^5 - 1 = (a-1)(a^4+a^3+a^2+a+1)$, then $2^n-1 = (2^k)^5-1 = (2^k-1)(2^{4k}+2^{3k}+2^{2k}+2^k+1)$.

Since $5|n$, then the smallest n is 15, so $k \geq 5$. Thus $2^k-1 \geq 31$, so $2^k-1 > 1$.

Thus each factor is greater than 1. Hence if n is an odd composite and $5|n$, then $2^n - 1$ is composite. We write this up in a logical coherent proof. □

Proof. We prove by contrapositive.

Suppose n is not prime.

Then either $n = 1$ or n is composite.

We consider these cases separately.

Case 1: Suppose $n = 1$.

Then $2^n - 1 = 2^1 - 1 = 1$ is not prime.

Case 2: Suppose n is composite.

Then there exist integers a and b with $1 < a < n$ and $1 < b < n$ such that $n = ab$.

Since $a \in \mathbb{Z}$, then $2^a \in \mathbb{Z}$, so $2^a - 1 \in \mathbb{Z}$.

Since $1 < a < n$, then $1 < a$ and $a < n$.

Since $a \in \mathbb{Z}$ and $a > 1$, then $2^a > 2$, so $2^a - 1 > 1$.

Since $a, n \in \mathbb{Z}$ and $a < n$, then $2^a < 2^n$, so $2^a - 1 < 2^n - 1$.

Since $1 < 2^a - 1$ and $2^a - 1 < 2^n - 1$, then $1 < 2^a - 1 < 2^n - 1$.

Since $0 < 1 < b < n$, then $0 < b$.

Since $b \in \mathbb{Z}$ and $b > 0$, then $b \in \mathbb{Z}^+$.

Since $b \in \mathbb{Z}^+$ and $2^a \in \mathbb{Z}$, then by a previous proposition, $2^a - 1$ divides $(2^a)^b - 1^b = 2^{ab} - 1 = 2^n - 1$.

Since $2^a - 1 \in \mathbb{Z}$ and $1 < 2^a - 1 < 2^n - 1$ and $2^a - 1$ divides $2^n - 1$, then $2^n - 1$ is composite, so $2^n - 1$ is not prime.

Therefore, in all cases, $2^n - 1$ is not prime, as desired. □

Proof. We use proof by contrapositive.

Suppose n is a natural number that is not prime.

Then n is either 1 or n is composite. We consider these cases separately.

Case 1: Suppose n is 1.

Then $2^1 - 1 = 1$ and 1 is not prime.

Case 2: Suppose n is composite, then $n > 2$.

Either n is even or n is odd. We consider each case separately.

Case 2a: Suppose n is even.

Then $n \geq 4$ since 4 is the least even composite natural number and $n = 2k, k \in \mathbb{Z}$.

We have $2^n - 1 = 2^{2k} - 1 = (2^k)^2 - 1 = (2^k - 1)(2^k + 1)$.

Since k is an integer, then the factors $2^k - 1$ and $2^k + 1$ are integers.

Since $n \geq 4$ then $k \geq 2$, so $2^k - 1 \geq 3$ and $2^k + 1 \geq 5$.

Hence each factor of $2^n - 1$ is greater than 1.

Therefore $2^n - 1$ is composite if n is even.

Case 2b: Suppose n is odd.

Then $n \geq 9$ since 9 is the least odd composite natural number.

The set of odd composite natural numbers is $\{9, 15, 21, 25, 27, 33, 35, 39, 45, ...\}$.

Thus this set consists of natural numbers larger than 8 that are divisible by 3 or 5 or both.

Let n be an arbitrary element of this set.

If $3|n$, then $n = 3k, k \in \mathbb{Z}$ and $n \geq 9$. Thus, $2^n - 1 = 2^{3k} - 1 = (2^k)^3 - 1 = (2^k - 1)(2^{2k} + 2^k + 1)$.

Since k is an integer, then the factors $2^k - 1$ and $2^{2k} + 2^k + 1$ are integers.

Since $n \geq 9$ then $k \geq 3$, so $2^k - 1 \geq 7$ and $2^{2k} + 2^k + 1 \geq 73$.

Hence each factor of $2^n - 1$ is greater than 1.

If $5|n$, then $n = 5k, k \in \mathbb{Z}$ and $n \geq 15$. Thus, $2^n - 1 = 2^{5k} - 1 = (2^k)^5 - 1 = (2^k - 1)(2^{4k} + 2^{3k} + 2^{2k} + 2^k + 1)$.

Since k is an integer, then the factors $2^k - 1$ and $2^{4k} + 2^{3k} + 2^{2k} + 2^k + 1$ are integers.

Since $n \geq 15$ then $k \geq 3$, so $2^k - 1 \geq 7$ and $2^{4k} + 2^{3k} + 2^{2k} + 2^k + 1 \geq 4681$.

Hence each factor of $2^n - 1$ is greater than 1.

Thus $2^n - 1$ is composite if n is odd.

Both cases show that whether n is an even composite or n is an odd composite, then $2^n - 1$ is not prime. □

Exercise 53. Fermat prime exercise

Let $n \in \mathbb{N}$.

If $2^n + 1$ is prime, then n is a power of 2.

Proof. Since $n \in \mathbb{N}$, then $n \geq 1$, so either $n > 1$ or $n = 1$.

We consider these cases separately.

Case 1: Suppose $n = 1$.

Then $2^n + 1 = 2^1 + 1 = 3$ is prime and $n = 1 = 2^0$, so n is a power of 2.

Case 2: Suppose $n > 1$.

Suppose $2^n + 1$ is prime.

To prove n is a power of 2, we must prove there exists an integer m such that $n = 2^m$.

Since $n > 1$, then $2^n > 2$, so $2^n + 1 > 3$.

Suppose for the sake of contradiction n is odd.

Since $2^n + 1 = 2^n - (-1) = 2^n - (-1)^n$, then $2 - (-1)$ divides $2^n - (-1)^n$, so 3 divides $2^n + 1$.

Since $1 < 3 < 2^n + 1$ and 3 divides $2^n + 1$, then $2^n + 1$ is composite.

But, this contradicts the fact that $2^n + 1$ is prime.
Hence, n is not odd, so n must be even.
Thus, $2|n$.

Suppose for the sake of contradiction there is a prime $p > 2$ such that $p|n$.
Since $n > 1 > 0$, then $n > 0$.
Since $p > 2 > 0$, then $p > 0$.
Since $p|n$ and $p > 0$ and $n > 0$, then $n = pq$ for some $q \in \mathbb{Z}^+$.
Since p is prime and $p > 2$, then p is odd.
Since $2^n + 1 = 2^{pq} + 1 = 2^{qp} - (-1) = (2^q)^p - (-1)^p$, then $2^q - (-1)$ divides $(2^q)^p - (-1)^p$, so $2^q + 1$ divides $2^n + 1$.
Since $q \in \mathbb{Z}^+$, then $2^q > 0$, so $2^q + 1 > 1$.
Since $n = pq$, then $q|n$, so $q \leq n$.
Hence, either $q < n$ or $q = n$.
Suppose $q = n$.
Then $n = pq = pn$, so $p = 1$.
But, $p > 2$, so $q \neq n$.
Thus, $q < n$.
Since $0 < q < n$, then $2^q < 2^n$, so $2^q + 1 < 2^n + 1$.
Since $2^q + 1 \in \mathbb{Z}$ and $1 < 2^q + 1 < 2^n + 1$ and $2^q + 1$ divides $2^n + 1$, then $2^n + 1$ is composite.
But, this contradicts the fact that $2^n + 1$ is prime, so there is no prime $p > 2$ such that $p|n$.
Since $n > 1$, then by the Fundamental theorem of Arithmetic, n has a unique prime factorization.
Since $2|n$, then 2 is a prime factor of n.
Since there is no prime $p > 2$ that divides n, then 2 is the only prime factor of n.
Hence, $n = 2^m$ for some $m \in \mathbb{Z}^+$. □

Exercise 54. Find all integer solutions of the equation $xy + 2y - 3x = 25$.

Solution. Let S be the solution set of the equation $xy + 2y - 3x = 25$.
Then $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : xy + 2y - 3x = 25\}$.
We can factor and use multiplicative properties of integers.
Thus, $y(x + 2) - 3(x + 2) = 25 - 6$.
Hence, $(x + 2)(y - 3) = 19$.
What are the factors of 19?
They are: 1,-1,19,-19.
Thus, we have 4 cases to consider.
We consider these cases separately.
Case 1: Suppose $x + 2 = 1$.
Then $x = -1$.
Hence, $1 * (y - 3) = 19$, so $y = 22$.
Substituting into the equation gives $(-1)(22) + 2(22) - 3(-1) = 25$, so $(-1, 22)$ is a solution.

Case 2: Suppose $x + 2 = -1$.

Then $x = -3$.

Hence, $-1 * (y - 3) = 19$, so $y = -16$.

Substituting into the equation gives $(-3)(-16) + 2(-16) - 3(-3) = 25$, so $(-3, -16)$ is a solution.

Case 3: Suppose $x + 2 = 19$.

Then $x = 17$.

Hence, $19(y - 3) = 19$, so $y = 4$.

Substituting into the equation gives $(17)(4) + 2(4) - 3(17) = 25$, so $(17, 4)$ is a solution.

Case 4: Suppose $x + 2 = -19$.

Then $x = -21$.

Hence,$(-19)(y - 3) = 19$, so $y = 2$.

Substituting into the equation gives $(-21)(2) + 2(2) - 3(-21) = 25$, so $(-21, 2)$ is a solution.

Therefore, $S = \{(-1, 22), (-3, -16), (17, 4), (-21, 2)\}$. □

Exercise 55. Let $x, y \in \mathbb{N}$ such that $\gcd(x, y) = 1$.

If xy is a perfect square, then x and y are perfect squares.

Proof. Either x and y are both greater than 1 or x and y are both equal to 1 or one of x and y is greater than 1 and the other of x and y equals 1.

Thus, either $x, y > 1$ or $x = y = 1$ or $x > 1, y = 1$ or $y > 1, x = 1$.

We consider each case separately.

Case 1: Suppose $x = y = 1$.

Then $xy = 1 * 1 = 1$ is a perfect square.

Since $x = 1 = 1^2 = y$, then x and y are perfect squares.

Therefore, xy is a perfect square implies x and y are perfect squares, as desired.

Case 2: Suppose $x > 1$ and $y = 1$.

Then $xy = x * 1 = x$.

Since $y = 1 = 1^2$, then y is a perfect square.

Suppose xy is a perfect square.

Then $x = xy$ is a perfect square.

Thus, xy is a perfect square and x and y are perfect squares.

Therefore, xy is a perfect square implies x and y are perfect squares, as desired.

Case 3: Suppose $x = 1$ and $y > 1$.

Then $xy = 1 * y = y$.

Since $x = 1 = 1^2$, then x is a perfect square.

Suppose xy is a perfect square.

Then $y = xy$ is a perfect square.

Thus, xy is a perfect square and x and y are perfect squares.

Therefore, xy is a perfect square implies x and y are perfect squares, as desired.

Case 4: Suppose $x > 1$ and $y > 1$.

Since $x > 1$, then by the fundamental theorem of arithmetic(FTA) there exists a unique prime factorization of x, so there exist prime factors $a_1, a_2, ..., a_r$ in the prime factorization of x.

Since $y > 1$, then by the fundamental theorem of arithmetic(FTA) there exists a unique prime factorization of y, so there exist prime factors $b_1, b_2, ..., b_s$ in the prime factorization of y.

Since $x > 1$ and $y > 1$, then $xy > 1$, so by the fundamental theorem of arithmetic(FTA) there exists a unique prime factorization of xy.

Let $a \in \mathbb{Z}$ such that $a > 1$.

Then, by FTA, there exists a unique prime factorization of a, so $a = p_1^{k_1} p_2^{k_2} ... p_n^{k_n}$ for each distinct prime factor p_i and each exponent $k_i \in \mathbb{N}$.

Hence, $a^2 = (p_1^{k_1} p_2^{k_2} ... p_n^{k_n})^2 = p_1^{2k_1} p_2^{2k_2} ... p_n^{2k_n}$, so each distinct prime factor in the prime factorization of a^2 has even power.

Therefore, each distinct prime factor in the prime factorization of any square number greater than 1 occurs an even number of times.

Since $\gcd(x, y) = 1$, then x and y have no common factors greater than 1.

Since every prime number is greater than 1, then this implies every prime factor a_i of x cannot also be a factor of y.

Since $a_i | x$ and $x | xy$, then $a_i | xy$, so each a_i is a prime factor of xy.

Since xy is a square number, then each a_i occurs an even number of times in the prime factorization of xy, so each a_i has even exponent $2d_i$ for some $d_i \in \mathbb{Z}$.

Therefore, $x = a_1^{2d_1} \cdot a_2^{2d_2} ... \cdot a_r^{2d_r} = (a_1^{d_1} \cdot a_2^{d_2} ... \cdot a_r^{d_r})^2$, so x is a perfect square.

Since x and y have no common factors greater than 1 and every prime number is greater than 1, then this implies every prime factor b_i of y cannot also be a factor of x.

Since $b_i | y$ and $y | xy$, then $b_i | xy$, so each b_i is a prime factor of xy.

Since xy is a square number, then each b_i occurs an even number of times in the prime factorization of xy, so each b_i has even exponent $2e_i$ for some $e_i \in \mathbb{Z}$.

Therefore, $y = b_1^{2e_1} \cdot b_2^{2e_2} ... \cdot b_s^{2e_s} = (b_1^{e_1} \cdot b_2^{e_2} ... \cdot b_s^{e_s})^2$, so y is a perfect square.

Hence, if xy is a perfect square greater than 1, then x and y are square numbers.

Therefore, in all cases, if xy is a perfect square, then x and y are square numbers. □

Exercise 56. There are an infinite number of primes of the form $6n + 1$.

Proof. Let $n \in \mathbb{Z}^+$.

We prove there are an infinite number of primes of the form $6n + 1$ by contradiction.

Suppose there are not an infinite number of primes of the form $6n + 1$.

Then there are a finite number of primes of the form $6n + 1$.

Let $p_1, p_2, ..., p_n$ be the primes of the form $6n + 1$ for some integer n.

Let $N = 6 * p_1 * p_2 * ... * p_n + 1$.

Since $N > 1$, then by FTA, N has a prime factorization.

Let $r_1 * r_2 * .... * r_t$ be the prime factorization of N.

Then $r_1 * r_2 * ... * r_t = N = 6 * p_1 * p_2 * ... * p_n + 1$, so $1 = r_1 * r_2 * .... * r_t - (6 * p_1 * p_2 * ... * p_n)$.

Is N prime? If so, then we have our contradiction.

So, let's prove N must be prime.

□

Proof. Let P be the set of primes.

Then $P = \{2, 3, 5, 7, 11, 13, 17, 19, ...\}$.

Let p_k be the k^{th} prime where $p_1 = 2$ and $p_2 = 3$ and $p_3 = 5$, etc.

Define predicate $S(k) : p_1 * p_2 * ... * p_k + 1$ is prime over $\mathbb{Z}^+$.

To prove there exist an infinite number of primes of the form $6n + 1$, we prove $(\forall n \in \mathbb{Z}^+, n > 1)(S(n))$.

Basis:

Since $2 * 3 + 1 = 7$ is prime, then $S(2)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ with $k \geq 2$ such that $S(k)$ is true.

Then $p_1 * p_2 * ... * p_k + 1$ is prime.

Let $a = p_1 * p_2 * ... * p_k + 1$ and $b = p_1 * p_2 * ... * p_k * p_{k+1} + 1$.

Then a is prime and $b = (a - 1)p_{k+1} + 1$.

To prove $S(k + 1)$, we must prove b is prime.

Since each prime is greater than one and $k > 0$, then $p_1 * p_2 * ... * p_k > 1$.

Thus, $p_{k+1} > 1$ and $p_1 * p_2 * ... * p_k > 1$ imply $p_1 * p_2 * ... * p_k * p_{k+1} > 1$, so $p_1 * p_2 * ... * p_k * p_{k+1} + 1 > 2$.

Hence, $p_1 * p_2 * ... * p_k * p_{k+1} + 1 > 1$.

Let $a = p_1 * p_2 * ... * p_k + 1$ and $b = p_1 * p_2 * ... * p_k * p_{k+1} + 1$.

Then a is prime and $b = (a - 1)p_{k+1} + 1$.

By FTA, b has a unique prime factorization.

We can prove that any prime factor of b cannot be $p_1, p_2, ..., p_k, p_{k+1}$.

So, to prove b is prime, we need to prove there can be no prime factor p such that $p_{k+1} < p < b$.

Suppose there exists a prime factor of b between p_{k+1} and b.

Let p be a prime factor of b such that $p_{k+1} < p < b$.

Then $p|b$, so there exists a positive integer c such that $b = pc$.

Since $p < b$, then $p < pc$, so $1 < c$.

Hence, $c > 1$, so by FTA, c has a unique prime factorization.

Can any of the prime factors of c be greater than p_k?

Can we derive a contradiction and use the induction hypothesis? □

Proof. Let P be the set of primes.

Then $P = \{2, 3, 5, 7, 11, 13, ...\}$.

Let S be the set of all primes of the form $6n + 1$ for some $n \in \mathbb{Z}^+$.

Then $S = \{x \in P : x = 6n + 1, n \in \mathbb{Z}^+\}$, so $S \subset P$.

Since $6 * 1 + 1 = 7$ is prime, then $7 \in S$, so $S \neq \emptyset$.

Suppose for the sake of contradiction S is finite.

Then there exists a greatest element $g \in S$.

Hence, $g \in P$ and $g = 6m + 1$ for some $m \in \mathbb{Z}^+$.

Since $g \in P$, then g is prime.

Since g is the greatest element of S, then $x \leq g$ for all $x \in S$.

Since $p_1 < p_2 < ... < g$, let V be the set of all primes less than or equal to g.

Then $V = \{p_1, p_2, ..., g\}$.

Let $N = (p_1 * p_2 * ... * g) + 1$.

Let T be the set of all primes less than N.

Then $T = \{p_1, p_2, ..., g, p_w...\}$.

Pick $p_1 \in T$.

Since $1 = N - (p_1 * p_2 * ... * g)$ is a linear combination of N and the primes in V.

Construct N so that $N > g$ such that N is the product of all primes less than $g + 1$.

What are all of the primes less than N?

Let $M = p_1 * p_2 * ... * p_m$ be the product of all primes less than N where $p_1 = 2$ and $p_2 = 3$ and $p_3 = 5$, etc.

Let $N = (p_1 * p_2 * ... * p_m) + 1$.

We claim N must be prime and yet also $N \in S$ and prove N is bigger than g, which contradicts that fact that g is the greatest element of S. This would then prove S is not finite, so S must be infinite.

Observe that

$$\begin{aligned} N &= (p_1 * p_2 * p_3 * ... * p_m) + 1 \\ &= (2 * 3 * p_3 * ... * p_m) + 1 \\ &= (6 * p_3 * ... * p_m) + 1. \end{aligned}$$

Therefore, $N = 6(p_3 * ... * p_m) + 1$.

How do we prove N is prime?

□

Exercise 57. Suppose p and q are prime numbers with $p \neq q$.

Then $\sqrt[3]{pq}$ is irrational.

Proof. Suppose $\sqrt[3]{pq}$ is rational.

Then there exist integers a and b with $b \neq 0$ such that $\sqrt[3]{pq} = \frac{a}{b}$.

Hence, $pq = (\frac{a}{b})^3$,

Since p is prime, then $p > 1$.

Since q is prime, then $q > 1$.

Thus, $pq > 1$.

Hence, $1 < pq = (\frac{a}{b})^3$.

Taking the cube root, we obtain $1 < \frac{a}{b}$.

Assume without loss of generality $b > 0$.

Since $1 < \frac{a}{b}$ and $b > 0$, we multiply by b to obtain $b < a$.

Thus, $0 < b < a$.

Suppose $b = 1$.

Then $pq = (\frac{a}{b})^3 = (\frac{a}{1})^3 = a^3$, so $pq = a^3$.

Since $b < a$ and $b = 1$, then $1 < a$, so $a > 1$.

By FTA, a has a unique prime factorization, so $a = x_1^{e_1} \cdot x_2^{e_2} \cdot ... \cdot x_k^{e_k}$ for distinct primes $x_1, x_2, ..., x_k$ and positive integer exponents $e_1, e_2, ..., e_k$.

Thus, $a^3 = (x_1^{e_1} \cdot x_2^{e_2} \cdot ... \cdot x_k^{e_k})^3 = x_1^{3e_1} \cdot x_2^{3e_2} \cdot ... \cdot x_k^{3e_k} = pq$.

Since $a^3 = pq$, then p is a prime factor of a^3, so p must be one of the prime factors x_i.

Since each $e_i \geq 1$, then each $3e_i \geq 3$.

Hence, each prime factor x_i occurs at least 3 times in the prime factorization of a^3.

But, p occurs only once in the prime factorization of a^3, since $p \neq q$.

Thus, we must conclude $b \neq 1$.

Since $b \in \mathbb{Z}$ and $b > 0$ and $b \neq 1$, then $b > 1$.

Since $pq = (\frac{a}{b})^3 = \frac{a^3}{b^3}$, then $pqb^3 = a^3$, so p divides a^3.

Since $a > b > 0$, then $a > 0$.

Since $a > 0$ and $a \in \mathbb{Z}$ and p is prime and p divides a^3, then by Euclid's lemma, p divides a, so $p \leq a$.

Since $1 < p \leq a$, then $1 < a$, so $a > 1$.

By FTA, a has a unique prime factorization, so $a = x_1^{e_1} \cdot x_2^{e_2} \cdot ... \cdot x_k^{e_k}$ for distinct primes $x_1, x_2, ..., x_k$ and positive integer exponents $e_1, e_2, ..., e_k$.

Thus, $a^3 = (x_1^{e_1} \cdot x_2^{e_2} \cdot ... \cdot x_k^{e_k})^3 = x_1^{3e_1} \cdot x_2^{3e_2} \cdot ... \cdot x_k^{3e_k} = pqb^3$.

Since $b > 1$, then by FTA, b has a unique prime factorization, so $b = y_1^{f_1} \cdot y_2^{f_2} \cdot ... \cdot y_m^{f_m}$ for distinct primes $y_1, y_2, ..., y_m$ and positive integer exponents $f_1, f_2, ..., f_m$.

Thus, $b^3 = (y_1^{f_1} \cdot y_2^{f_2} \cdot ... \cdot y_k^{f_m})^3 = y_1^{3f_1} \cdot y_2^{3f_2} \cdot ... \cdot y_m^{3f_m}$, so $a^3 = pq(y_1^{3f_1} \cdot y_2^{3f_2} \cdot ... \cdot y_m^{3f_m})$.

Hence, $a^3 = x_1^{3e_1} \cdot x_2^{3e_2} \cdot ... \cdot x_k^{3e_k} = pq(y_1^{3f_1} \cdot y_2^{3f_2} \cdot ... \cdot y_m^{3f_m})$.

Since p is prime and p divides a^3, then p is a prime factor of a^3, so p must be one of the primes x_i.

Let t be the number of occurrences of p in the prime factorization of a^3.

Then $t = 3e_j$ for some $e_j \in \mathbb{Z}^+$.

Since $e_j \geq 1$, then $t = 3e_j \geq 3$, so $t \geq 3$.

Either p is one of the primes y_w or not.

We consider these cases separately.

Case 1: Suppose p is not one of the primes y_w in the prime factorization of a^3.

Since $p \neq q$, then this implies p occurs exactly once in the prime factorization of a^3, so $t = 1$.

But, this contradicts the fact that $t \geq 3$.

Case 2: Suppose p is one of the primes y_w in the prime factorization of a^3.

Then $p = y_w$ for some $w \in \{1, 2, ..., m\}$.

Since $p \neq q$, then this implies p occurs $1+3f_w$ times in the prime factorization of a^3, where $f_w \in \mathbb{Z}^+$.

Hence, $t = 1 + 3f_w$.

Thus, $3e_j = t = 1 + 3f_w$, so $3e_j - 3f_w = 1$.

Therefore, $3(e_j - f_w) = 1$, so 3 divides 1, a contradiction.

Consequently, in all cases a contradiction is reached, so we are forced to conclude the assumption $\sqrt[3]{pq}$ is rational is false.

Therefore, $\sqrt[3]{pq}$ is irrational. □

Exercise 58. For every positive integer n, there exists an integer divisible by n distinct primes.

Solution. The statement to prove is below.

$(\forall n \in \mathbb{Z}^+)(\exists k \in \mathbb{Z})$ (k is divisible by n distinct primes). □

Proof. Let $n \in \mathbb{Z}^+$.

Then either $n = 1$ or $n > 1$.

We consider each case separately.

Case 1: Suppose $n = 1$.

Let $k = 2$.

Since 2 is prime and $2|2$, then k is divisible by 1 prime.

Case 2: Suppose $n > 1$.

Then $n \geq 2$.

Let S be the set of distinct primes p_i such that $p_1 < p_2 < ... < p_n$ for $i \in \{1, 2, ..., n\}$.

Then $p_1 \in S$ and $p_2 \in S$ and $|S| = n$.

Let k be the product of all the primes in S.

Since k is the product of primes and every prime is an integer and $\mathbb{Z}$ is closed under multiplication, then $k \in \mathbb{Z}$.

Since $p_1 < p_2$, then $p_1 \neq p_2$.

Since $p_1 \in S$, then $S \neq \emptyset$.

Let $p_i \in S$ be arbitrary.

Let t be the product of all primes in the set $S - \{p_i\}$.

Since $p_2 \in S$ and $p_2 \neq p_1$, then $p_2 \in S - \{p_i\}$, so $S - \{p_i\} \neq \emptyset$.

Since $p_i \in S$, then p_i is one factor of k.

Since t is the product of all primes in $S - \{p_i\}$, then t is the product of all primes of S except for the prime p_i.

Therefore, $k = p_i t$.

Since t is a product of primes and every prime is an integer and $\mathbb{Z}$ is closed under multiplication, then $t \in \mathbb{Z}$.

Since $t \in \mathbb{Z}$ and $k = p_i t$, then $p_i | k$.

Hence, if $p_i \in S$, then $p_i | k$, so $p_i | k$ for every $p_i \in S$.

Thus, every prime number of S divides k.

Since $|S| = n$, then there are n distinct primes that divide k.

Therefore, there is an integer k such that k is divisible by n distinct primes.

□