primes are considered secure if they are $2,048$ bits long, because the product of these two primes would be about $1,234$ decimal digits.

Prime numbers have shown its existence in nature. Cicadas insect spend most of their time hiding, only reappearing to mate every 13 or 17 years. Why this particular number? Scientists invented that cicadas reproduce in cycles that minimize possible interactions with predators. Any predator reproductive cycle that divides the cicada's cycle evenly means that the predator will hatch out the same time as the cicada at some point. For instance , if the cicada evolved towards a 12-year reproductive cycle, predators who reproduce at the 2, 3, 4 and 6 year intervals would find themselves with plenty of cicadas to eat. By using a reproductive cycle with a prime number of years, cicadas would be able to minimize contact with predators. Simulation models of $1,000$ years of cicada evolution prove that there is a major advantage for reproductive cycle times based on primes.

3.2 Primes & Fundamental Theorem of Arithmetic

Positive divisors of an integer have a great importance in the study of number theory. The integer 1 has only one positive divisor which is 1 itself. Any other integers has more than one divisor. At Least two divisors of them are 1 and the integer itself. There are integers which have divisors other than 1 and itself. The numbers which have only two divisors 1 and itself are called prime numbers.

Definition 3.2.1. *An integer $p > 1$ is said to be a prime number or prime if its only divisors are 1 and p itself.*

An integer which is not prime is known to be a composite number, having more than two(what are those?) divisors.

Among the first ten positive integers $2, 3, 5, 7$ are prime numbers whereas $4, 6, 8, 9, 10$ are examples of composite numbers. Here 1 is a special type of integer which is neither prime nor composite. Here the study of prime numbers starts with the study of prime divisors. Here 5 is prime where $5 \nmid 3$ but $5|5$ itself together implies $5|15$, leads us to the following theorem:

Theorem 3.2.1. *An integer $p > 1$ is prime if and only if $p|ab$ implies $p|a$ or $p|b$.*

Proof. Let p be a prime number such that for any two integers a and b, $p|ab$ holds. If $p|a$, then we are done. Let $p \nmid a$ then the only divisors of p are 1 and p

itself. As p is prime we have $\gcd(p, a) = 1$ implies there exists integers r, t such that $1 = rp + at$. Then $b = brp + t(ab)$. Now $p|ab$ and $p|prb$ imply $p|b$.

Conversely, let p satisfy the condition and q, r be any integers such that $p = qr$ where $q < p$. Thus $p|qr$ and by the condition we can say either $p|q$ or $p|r$. But $q|p$ shows $p|r$ only. Therefore $r = pt$ for some integer t. Hence $p = qr = qpt$ implies $qt = 1$ implies $q = 1$. So 1 and p are only divisors of p. This shows p is prime. □

Let us now generalize the above theorem for more than two terms as follows:

Theorem 3.2.2. *If p is prime and $p|a_1a_2a_3\cdots a_n$, then $p|a_i$ for some $i = 1, 2, 3, \ldots, n$.*

Proof. We will prove this by mathematical induction. The statement is true for $n = 1$. With reference to theorem (3.2.1) the statement is true for $n = 2$. Let us assume the statement is true for $n = k$. Let $n = k + 1$ holds. Then $p|a_1a_2a_3\cdots a_ka_{k+1}$. Also choose $a_1a_2a_3\cdots a_k = b$ where b is an integer, thus $p|ba_{k+1}$. Now if $p|a_{k+1}$ we are done. If $p \nmid a_{k+1}$, then from $n = 2$ we have $p|b$ implies $p|a_1a_2a_3\cdots a_k$ which further implies $p|a_i$ for some i by the induction hypothesis. Thus $p|a_i$ for $i = 1, 2, \ldots, k+1$. So the statement is true for $n = k+1$. Thus by principle of mathematical induction the theorem is proved. □

Corollary 3.2.1. *If $p, q_1, q_2, q_3, \ldots, q_n$ are all primes and $p|q_1q_2q_3\cdots q_n$ then $p = q_i$ for some $i = 1, 2, \ldots, n$.*

Proof. By virtue of above theorem, we know that if $p|q_i$ for some $i = 1, 2, \ldots, n$. But q_i being prime so q_i is not divisible by any integer other than 1 and itself. Since, $p > 1$ then we have $p = q_i$ for some $i = 1, 2, 3 \ldots, n$. □

Let us now consider few integers $35, 25, 10$ and we see that $7|35, 5|25$ and $2|10$. So the observation is that every integer has a prime factor. We now prove this result for any integer $n \geq 2$.

Theorem 3.2.3. *Every integer $n \geq 2$ has a prime factor.*

Proof. We prove the statement by mathematical induction method. Taking $n = 2$, the result is obvious as 2 itself is prime. Let us assume that each of the integers $2, 3, \ldots, n - 1$ has a prime factor. Now considering $n > 2$ we can say that the result is true if n is prime. If n is composite then $n = rs$ for some integer r, s with $1 < r, s < n$. Then by induction hypothesis r has a prime factor which is also a prime factor of n. So the theorem is proved. □

The set of all positive integers is countably infinite and the set of prime numbers is a subset of the set. So two possibilities to occur. One, the cardinality of the set is finite and the other which is countably infinite. But the set of prime numbers that are countably infinite is given in a theorem of Euclid (300 B.C.) and till the 21st century the proof is considered as an elegant proof of Mathematics.

Theorem 3.2.4. *Prime number set is countably infinite.*

Proof. Let the number of primes be finite and we write them as $p_1 = 2, p_2 = 3 \cdots p_n$. Now let us consider a composite number $m = p_1 p_2 \cdots p_n + 1$ and $m > 1$. As m is composite it has a prime factor p(say). This p obviously one of $p_1, p_2, \cdots p_n$. Now $p|p_1 p_2 \cdots p_n + 1, p|p_1 p_2 \cdots p_n$ together imply $p|1$ [Applying $x = -1, y = 1, b = p_1 p_2 \cdots p_n$ and $c = p_1 p_2 \cdots p_n + 1$ on $a|b, a|c \Rightarrow a|(bx + cy)$]. This leads to a contradiction (Why!). So our assumption is wrong and the theorem is proved. □

All the above results lead us to the fact that any integer can be factorized if it is composite. The factorized integers can be prime or composite such as $20 = 4 \times 5$ where 4 is composite whereas 5 is prime. But the most interesting fact is that $20 = 2^2 \times 5$ where both 2 and 5 are prime. This factorization is known to be prime factorization. The following Fundamental Theorem of Arithmetic or the unique factorization theorem enlighten us about the fact:

Theorem 3.2.5. *Every positive integer $n \geq 2$ can be expressed uniquely as product of primes, $n = p_1 p_2 p_3 \cdots p_r$, where each p_i is distinct for $1 \leq i \leq r$.*

Proof. If n is prime then we are done. If n is composite then there exists an integer d such that $d|n$ with $1 < d < n$. By well ordering principle, let p_1 be the smallest of them. Here p_1 must be prime otherwise t be any divisor of p_1 such that $1 < t < p_1$ then $t|p_1$ and $p_1|n$ together imply $t|n$ which is a contradiction(Why!). So we have $n = p_1 n_1$ for some integer n_1 where $1 < n_1 < n$. If n_1 is prime then we are done. If n_1 is composite then by the same argument we have another prime p_2 and integer n_2 where $1 < n_2 < n_1$ such that $n = p_1 p_2 n_2$. Continuing this way we have a decreasing sequence of integers $n > n_1 > n_2 > \cdots > 1$. This sequence is finite and after finite n_n we will get a prime p_r. This leads to prime factorization $n = p_1 p_2 \cdots p_r$.

To prove the uniqueness let there be two distinct prime factorizations of n as $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ where $r \leq s$ and each of $p_i's$ and $q_j's$ are primes. These primes are in the ordering $p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq q_3 \leq \cdots \leq q_s$. As $p_1|n$ this implies $p_1|q_1 q_2 \cdots q_s$ then by virtue of Corollary 3.2.1 $p_1 = q_j$ for some j where $1 \leq j \leq n$. This follows that $p_1 < q_1$. Now cancelling the

common factors from both the sides we have $q_2q_3\cdots q_s = p_2p_3\cdots p_r$. Continuing as above, up to r terms as $r < s$. After r-th step we have $1 = q_{r+1}q_{r+2}\cdots q_s$ which is absurd as $q_j's$ are prime. Hence $r = s$ and $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_s$. So the factorization is unique. □

Let us consider an integer 15 which can be written as 5×3 where both 5 and 3 are distinct primes. But if we take 75 it can be expressed as $5\times 5\times 3$ where we can see the representation of primes. By collecting those primes and replacing them by a single factor we can represent any integer by following corollary viz

Corollary 3.2.2. *Any positive integer can be uniquely written as* $p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ *where each* n_i *is a positive integer and* $p_i's$ *are prime for* $i = 1, 2, 3, \ldots, r$ *with* $p_1 < p_2 < p_3 < \cdots < p_r$.

From the above corollary we can assert that any arbitrary positive integer has an unique prime factorization. Now in the later part of this section we have given an alternative proof of the Theorem 2.5.1. For that we have to define the greatest common divisor and least common multiple of any two arbitrary integers in the light of prime factorization. Let us take two integers a and b with their unique prime factorizations $a = p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$, $b = p_1^{b_1}p_2^{b_2}\cdots p_n^{b_n}$ with $p_1 < p_2 < \cdots < p_n$ and a_k, b_k be non negative integers for $k = 1, 2, \cdots, n$. Then $\gcd(a, b) = p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n}$ and $lcm(a, b) = p_1^{M_1}p_2^{M_2}\cdots p_n^{M_n}$ where $M_k = \mathrm{Max}(a_k, a_k)$ and $m_k = \min(a_k, b_k)$. Here to give alternative proof of the Theorem 2.5.1 we first state and prove the lemma as follows:

Lemma 3.2.1. *If* x *and* y *are real numbers, then* $max(x, y) + min(x, y) = x + y$.

Proof. If $x < y$, then $\min(x, y) = x$ and $\max(x, y) = y$, and again we find that $\max(x, y) + \min(x, y) = x + y$. Similarly, If $x > y$, then $\min(x, y) = y$ and $\max(x, y) = x$, and again we find that $\max(x, y) + \min(x, y) = x + y$. □

Now using the above lemma, let us proceed for the alternate proof:

Proof. Let a and b have prime-power factorizations $a = p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$, $b = p_1^{b_1}p_2^{b_2}\cdots p_n^{b_n}$, where the powers are nonnegative integers and the primes $p_i's$ occurring in the prime-power factorizations of a and b. Let $M_k = \mathrm{Max}(a_k, b_k)$

and $m_k = \min(a_k, b_k)$. Then, we have

$$\begin{aligned} lcm(a,b)\gcd(a,b) &= p_1^{M_1} p_2^{M_2} \cdots p_n^{M_n} p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} \\ &= p_1^{M_1+m_1} p_2^{M_2+m_2} \cdots p_n^{M_n+m_n} \\ &= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n} \\ &= p_1^{a_1} p_1^{b_1} p_2^{a_2} p_2^{b_2} \cdots p_n^{a_n} p_n^{b_n} \\ &= ab. \end{aligned}$$

□

The numbers $2, 3, 4$ are integers and if we take $\frac{2}{3}, \frac{3}{4}$ then this type are the rational numbers of the form $\frac{p}{q}$ where $q \neq 0$ and $\gcd(p, q) = 1$. But there are numbers of the form $\sqrt{2}, \sqrt{3}$ which can not be written as above. These are said to be irrational numbers. We are now going to introduce a famous result of Pythagoras on irrational numbers viz

Theorem 3.2.6. *The number $\sqrt{2}$ is irrational.*

Proof. Let us suppose that $\sqrt{2}$ is a rational quantity. Then $\sqrt{2} = \frac{a}{b}$ where a, b are integers relatively prime to each other. Squaring we have, $2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2$ implies $b^2 | a^2$. If $b > 1$, then by fundamental theorem of arithmetic we can say that there exists a prime p such that $p|b$. Then it follows $p|a^2$ implies $p|a$ and hence $\gcd(a, b) \geq p$ which is a contradiction unless $b = 1$. But if $b = 1$ holds then $a^2 = 2$ which is impossible(Why!). Hence the proof. □

For further discussion of this chapter we will show our interest in finding extremely large primes. To do so our first aim is to check whether a given integer is prime or not. We first deal with this question by trial division of n using the following theorem viz

Theorem 3.2.7. *If n is a composite integer, then n has a prime factor not exceeding $\sqrt{n}$.*

Proof. Since n is composite, we can write $n = ab$ where a, b are integers with $1 < a \leq b < n$. There must be $a \leq \sqrt{n}$, if not then $b \geq a > \sqrt{n}$ which leads to $ab > n$, which is not possible. Now from Theorem 3.2.3 the integer a must have a prime divisor p(say). Then $p \leq a \leq \sqrt{n}$. Further if $p|a$ and $a|n$ implies $p|n$. Then p is the required prime factor of n not exceeding $\sqrt{n}$. □

We can use this theorem to find all the primes less than or equal to a given positive integer n. This procedure is called Sieve of Eratosthenes. To illustrate

the process, let us choose $n = 81$. Then by virtue of the above theorem, 81 has a prime factor less than or equal to $\sqrt{81} = 9$. Since, the only prime less than 9 are $2, 3, 5, 7$. We only have to find those integers less than 81 which can be divisible by any one of those primes. In the below table we have shown a complete list of them. The multiples of any one or two or three of $2, 3, 5, 7$ of the numbers in the table are cancelled by $/$, $\backslash$ and $\not\backslash$ respectively.

$\not 2$	$\not 3$	$\not 4$	$\not 5$	$\not 6$	$\not 7$	$\not 8$	$\not 9$
$\not 10$	11	$\not 12$	13	$\not 14$	$\not 15$	$\not 16$	17
$\not 18$	19	$\not 20$	$\not 21$	$\not 22$	23	$\not 24$	$\not 25$
$\not 26$	$\not 27$	$\not 28$	29	$\not 30$	31	$\not 32$	$\not 33$
$\not 34$	$\not 35$	$\not 36$	37	$\not 38$	$\not 39$	$\not 40$	41
$\not 42$	43	$\not 44$	$\not 45$	$\not 46$	47	$\not 48$	49
$\not 50$	$\not 51$	$\not 52$	53	$\not 54$	$\not 55$	$\not 56$	$\not 57$
$\not 58$	59	$\not 60$	61	$\not 62$	$\not 63$	$\not 64$	$\not 65$
$\not 66$	67	$\not 68$	69	$\not 70$	71	$\not 72$	73
$\not 74$	$\not 75$	$\not 76$	$\not 77$	$\not 78$	79	$\not 80$	$\not 81$

The above table indicates that there exist many primes less than 81. In fact, from theorem (3.2.4), we have infinitely many primes. A fairly natural question arises: Is it possible to estimate, how many primes are less than a positive real number x? We are fortunate enough to have the most renowned theorem of number theory, and of all mathematics, is the prime number theorem which answers this question. In 1793, Gauss speculated the theorem but it was an open problem until 1896, when a French mathematician J. Hadamard and a Belgian mathematician C. J. de la Vallée-Poussin had proved it independently. So before going to state the theorem let us begin with a simple definition.

Definition 3.2.2. *The function $\pi(x)$, where x is a positive real number, denotes the number of primes not exceeding x.*

We now state the prime number theorem, whose proof is beyond the scope of the book.

Statement 3.2.1. *In language of limits, the theorem can be stated as* $\lim_{x\to\infty} \dfrac{\pi(x)}{\ln x} = 1$.

The above stated theorem reflects the fact that for large values of x, $\dfrac{x}{\ln x}$ is a good approximation to $\pi(x)$. Further, it is to be noted that it is not necessary to find all primes not exceeding x in order to compute $\pi(x)$. By virtue of counting

argument based on the Sieve of Eratosthenes,one can compute $\pi(x)$ without finding all the primes less than x.

Our next theorem addresses that the gap between consecutive primes is arbitrarily long.

Theorem 3.2.8. *For any positive integer n, there are at least n consecutive composite positive integers. Stated otherwise, there are arbitrarily large gaps in the series of primes.*

Proof. Consider the n consecutive positive integers

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1.$$

Now, $2 \leq j \leq n+1 \Rightarrow j \big| (n+1)!$. Finally, an appeal to Proposition 2.2.1 yields the desired result. □

The following example will exemplify our foregoing theorem.

Example 3.2.1. *For $n = 5$, the smallest 5 consecutive composite integers can be found by locating the first pair of consecutive composite odd integers, 25 and 27. Hence the smallest 5 consecutive composite integers are $24, 25, 26, 27$, and 28. These are considerably smaller than the integers $(5+1)!+j = 6!+j = 720+j$ for $j = 2, 3, 4, 5, 6$. Also, the seven consecutive integers beginning with $8! + 2 = 40322$ are all composite. However, these are much larger than the smallest seven consecutive composites $90, 91, 92, 93, 94, 95$, and 96.*

Our next discussion is about the propagation of prime numbers of prime numbers. Let us choose p a prime and $\tilde{p}$ to be the product of all primes that are less than or equal to p. The numbers $\tilde{p}+1$ form are called "Euclidean numbers" as they appear in the proof of Theorem 3.2.4. For example,

$$\tilde{2}+1 = 2+1 = 3$$
$$\tilde{3}+1 = 2\cdot 3+1 = 7$$
$$\tilde{5}+1 = 2\cdot 3\cdot 5+1 = 31$$

are all prime numbers but also we can see $\widetilde{13} = 59 \cdot 509$ is not prime. From these two types of examples, we see that $\tilde{p}+1$ is not always a prime.

If we consider a sequence of integers such as,

$$\begin{aligned} n_1 &= 2 \\ n_2 &= n_1 + 1 \\ n_3 &= n_1 n_2 + 1 \\ &\vdots \\ n_k &= n_1 n_2 \cdots n_{k-1} + 1 \end{aligned}$$

where each $n_k > 1$ and they are relatively prime to each other. If not, let $\gcd(n_i, n_j) = d$ where $i < j$. Then $d|n_i \Rightarrow d\big|n_1 n_2 \cdots n_i \cdots n_{j-1}$. Since, $d|n_j$ therefore $d|n_1 n_2 \cdots n_{j-1} + 1$ together imply $d|1$, possible when $d = 1$. So our assertion, all $n_k's$ are pairwise relatively prime, is true. Now we can say that there are many distinct primes as there are integers n_k.

Let p_n be n-th prime number. Then from Euclid's proof we can estimate the rate of increase of p_n. Here we have $p_{n+1} \leq p_1 p_2 \cdots p_n + 1 < p_n^n + 1$. If $n = 5$ then $31 = p_6 = p_5^5 + 1 = 7^5 + 1 = 16808$. Thus we have the following theorem viz

Theorem 3.2.9. *If p_k be the k-th prime, then $p_k \leq 2^{2^k - 1}$.*

Proof. We will prove the theorem by Mathematical Induction on k. If $k = 1$, then the result is obvious. Let us assume $k > 1$. Then

$$\begin{aligned} p_{k+1} &\leq p_1 p_2 \cdots p_k + 1 \\ &\leq 2 \cdot 2^2 \cdots 2^{k-1} + 1 = 2^{1+2+2^2+\cdots+2^{k-1}} + 1 = 2^{2^k - 1} + 1. \end{aligned}$$

But $1 \leq 2^{2^k - 1}$ for all k. Therefore $p_{k+1} \leq 2^{2^k}$ (How!). Thus the result is true for $k + 1$. Hence the proof. □

The last inequation of the above proof gives rise to an interesting corollary stated as follows:

Corollary 3.2.3. *For $k \geq 1$ there exists at least $k + 1$ primes less than 2^{2^k}.*

Proof. left to the reader. □

Finally, we conclude this section with remarkable conjecture about primes, commonly known as Golbach's Conjecture, stated by Christian Goldbach in a letter to Euler in 1742.

Goldbach Conjecture: Every even positive integer greater than two can be written as the sum of two primes.

Let us exemplify the Conjecture with an example:

$$\begin{aligned} 10 &= 3+7 = 5+5 \\ 24 &= 5+19 = 7+17 = 11+13 \\ 100 &= 3+97 = 11+89 = 17+83 \\ &= 29+71 = 41+59 = 47+53 \end{aligned}$$

Next with the help of the following lemma, we are going to prove the fact that there exists infinitely many primes of the form $4n+3$.

Lemma 3.2.2. *The product of two or more integers of the form* $4n+3$ $(n \in \mathbb{Z})$ *results in the same form.*

Proof. It's sufficient to prove the lemma with two integers of the form $4n+1$. Set $k_1 = 4n_1 + 1,\ k_2 = 4n_2 + 1$. Multiplying we obtain,

$$\begin{aligned} k_1k_2 &= (4n_1+1)(4n_2+1) \\ &= 4(4n_1n_2 + n_1 + n_2) + 1 \\ &= 4n+1,\ [n = 4n_1n_2 + n_1 + n_2 \in \mathbb{Z}] \end{aligned}$$

which is the desired form. □

This facilitates the proof for the following theorem.

Theorem 3.2.10. *There exists infinitely many primes of the form* $4n+3$.

Proof. Suppose there exists finitely many primes $t_1, t_2, \ldots, t_s$ of the form $4n+3$. Also, consider $N = 4t_1t_2\ldots t_s - 1 = 4(t_1t_2\ldots t_s - 1) + 3$ to be a positive integer. Further, let $N = k_1k_2\ldots k_n$ be the prime factorization of N. Since N is odd, then $k_i \neq 2,\ \forall\, i$. Thus k_i is of the form, either $4n+1$ or $4n+3$. If k_i is of the form $4n+1$, then using the lemma 3.2.2 we can say that N must be of the form $4n+1$. This is not the case here. Then N must contain one prime factor k_i of the form $4n+3$. But, k_i can not be found among $t_1, t_2, \ldots, t_s$. Otherwise this leads to $k_i|1$, which is not true. Thus our assumption of finitely many primes of the form $4n+3$ is wrong. □

The last theorem inspired us to ask a fairly question: Is the number of primes of the form $(4n+1)$ also infinite? The following Dirichlet's statement, whose proof is beyond the scope of the book, is the answer to the question.

Theorem 3.2.11. *If a and b are positive integers with $\gcd(a, b) = 1$, then the arithmetic progression*

$$a, a + b, a + 2b, \ldots$$

contains infinite number of primes.

From Dirichlet's statement it can be seen that there exists infinitely many primes ending with 999, for instance 1999, 1000999, ..., they appear in arithmetic progression given by $1000n + 999$, with $\gcd(1000, 999) = 1$.

Theorem 3.2.12. *There exists no arithmetic progression of the form $a, a + b, a + 2b, \ldots$ that consists of only primes.*

Proof. To begin with, consider $a + nb = p$, p being a prime. If $n_k = n + kp$ for $k = 1, 2, 3 \ldots$ then the n_k-th term in the progression is

$$\begin{aligned} a + n_k b &= a + (n + kp)b \\ &= (a + nb) + kbp = p + kbp \\ &= p(1 + kb) \end{aligned}$$

Since, $p|p(1 + kb)$, therefore $p|(a + n_k b)$. Hence $(a + n_k b)$ can not be a prime, which is our desired result. □

Remark 3.2.1. *From the above theorem, it's quite clear that the progression contains infinitely many composite numbers.*

Theorem 3.2.13. *If all the $n(> 2)$ terms of the arithmetic progression,*

$$p, p + d, p + 2d, \ldots$$

are primes, then $q|d$ where d being the common difference and $q(< n)$ is a prime number.

Proof. Consider a prime $q < n$. In anticipation of a contradiction, assume $q \nmid d$. Again, if possible let us assume that the first q terms of the given progression will leave the same remainders when divided by q. Then $\exists j, k \in \mathbb{Z}$ with $0 \leq j < k \leq q - 1$ or $k - j \leq q - 1$ such that $(p + jd)$ and $(p + kd)$ generates same remainder when divided by q, which further implies $q\big|(k - j)$. But $\gcd(p, q) = 1$ and by Euclid's lemma $q\big|(k - j)$, which is impossible in the light of the inequality $k - j \leq q - 1$. Hence the first q terms of the given progression will leave q different remainder upon division by q. Since they are extended from q integers $0, 1, 2, \ldots, q - 1$, one of them must be zero.This means for some t satisfying $0 \leq t \leq q - 1$, $q|(p + td)$. Hence we conclude, $p + td$ is composite because the inequality $q < n \leq p \leq (p + td)$ holds (for if $p \leq n$, then one of the term of the progression will be $p(1 + d)$). This leads to a contradiction and hence $q\big|d$. □

Remark 3.2.2. *There is a conjecture that there exists arithmetic progression of finite length, consisting of consecutive prime numbers. For instance,* $47, 53, 59$ *and* $251, 257, 263, 269$.

Consider the function $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ defined by $f(n) = n^2 + n + 41$. There was a myth that the image set of the function was only primes. But in 1772, it was proved to be false by Leonhard Euler. Though the myth was true for $n = 0, 1, 2 \ldots, 39$ but fails for $n = 40, 41$. Here

$$f(40) = 40 \cdot 41 + 41 = 41^2, \text{ and}$$
$$f(41) = 41 \cdot 42 + 41 = 41 \cdot 43.$$

Once again $f(42) = 1847$ turns out to be prime. The polynomial $f(n) = (n^2 + n + 41)$ is known as Euler polynomial. It is to be noted that no polynomial of the form $n^2 + n + q$, q being prime, can perform better than Euler polynomial in giving primes for successive values of n.

Theorem 3.2.14. *There exists no non-constant polynomial* $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ *with integral coefficients that generates solely prime numbers for* $n \in \mathbb{Z}^+$.

Proof. To the contrary, assume that such a polynomial f does exists. Set $f(n) = a_k n^k + a_{k-1} n^{k-1} + \ldots + a_2 n^2 + a_1 n + a_0$ where the coefficients $a_i (i = 0, 1, 2 \ldots, k)$ are integers with $a_k \neq 0$. Let $f(n_0) = p$, for some fixed value $n_0 \in \mathbb{Z}^+$. Now, for any $t \in \mathbb{Z}$, consider

$$\begin{aligned} f(n_0 + tp) &= a_k(n_0 + tp)^k + a_{k-1}(n_0 + tp)^{k-1} + \ldots + a_2(n_0 + tp)^2 + a_1(n_0 + tp) + a_0 \\ &= (a_k n^k + a_{k-1} n^{k-1} + \ldots + a_2 n^2 + a_1 n + a_0) + pQ(t) \\ &= f(n_0) + pQ(t) \\ &= p(1 + Q(t)), \end{aligned}$$

$Q(t)$ being a polynomial in t with integral coefficients. This shows $p | f(n_0 + tp)$, which further implies $f(n_0 + tp) = p$ $(t \in \mathbb{Z})$. This leads to a contradiction(Why!).Thus we have established the theorem. □

3.3 Worked out Exercises

Problem 3.3.1. *The lucky numbers are generated by the screening process as follows: Let us begin with the set of positive integers. Starting the process by crossing out every second integer in the list, start the count with the integer* 1. *Other than* 1 *the smallest integer left is* 3, *continuing with the process every third integer left, beginning with the integer* 1. *The next integer left is* 7, *so we cross*

out every seventh integer left. Continuing as above, where at each stage we cross out every κth integer left where κ is the smallest integer left other than one. The integers that remain are the lucky numbers. Prove that the lucky number set is countably infinite.

Solution 3.3.1. *At each stage of the procedure for generating the lucky numbers the smallest number left is κ, say, is designated to be a lucky number and infinitely many primes are left after the deletion of every κ integer left. It follows that there are countably infinite numbers of steps, and at every step a new lucky number is added to the sequence. Hence the proof.*

Problem 3.3.2. *Show that the polynomial $f(x) = x^2 - x + 41$ is prime for all integers x with $0 \leq x \leq 40$. Furthermore, it is composite for $x = 41$.*

Solution 3.3.2. *Hint: Find $f(1), f(2), f(3), \ldots, f(39), f(40)$. But $f(41)$ is composite.*

Problem 3.3.3. *Show that if $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ where the coefficients are integers, then $\exists\, y \in \mathbb{Z}$ such that $g(y)$ is composite.*

Solution 3.3.3. *In anticipation to contradiction, suppose there $\nexists$ any $y \in \mathbb{Z}$ such that $g(y)$ is composite. Let y_0 be a positive integer such that $g(y_0) = p$, a prime. Let κ be any integer such that $g(y_0 + \kappa p) = a_n(y_0 + \kappa p)^n + a_{n-1}(y_0 + \kappa p)^{n-1} + \cdots + a_1(y_0 + \kappa p) + a_0$. By binomial expansion it follows that $g(y_0 + \kappa p) = \sum_{j=0}^{n} a_j x_0^j + Mp$, M being an integer. Now $p|(g(y_0 + Mp) = g(y_0 + \kappa p)$ (Why!). Also $g(y_0 + \kappa p) = p$ (Why!). This contradicts the fact that a polynomial of degree n takes on each value not more than n times. Hence there is an integer y such that $g(y)$ is composite.*

Problem 3.3.4. *Show that no integer of the form $n^3 + 1$ is a prime, other than $2 = 1^3 + 1$.*

Solution 3.3.4. *Note that n must be positive. Otherwise no such integers are prime (Why!). Since $n^3 + 1 = (n+1)(n^2 - n + 1)$, $n^3 + 1$ is not prime unless one of the two factors on the right hand side of the equation is 1 and the other is $n^3 + 1$. But $(n + 1) > 1$ for every positive integer n and the only way for $n + 1 = n^3 + 1$ is when $n = 1$(Verify!). In this case, we have $1^3 + 1 = (1 + 1)(1^2 - 1 + 1) = 2$. Hence 2 is the only prime of this form.*

Problem 3.3.5. *Find all primes that are the difference of the fourth powers of two integers.*

Solution 3.3.5. *Suppose* $n = a^4 - b^4 = (a-b)(a+b)(a^2+b^2)$, *where* $a > b$. *The integer* n *cannot be prime because it is divisible by* $a+b$ *which cannot be* 1 *or* n.

Problem 3.3.6. *Show that if* a *and* n *are positive integers such that* $a^n - 1$ *is prime, then* $a = 2$ *and* n *is prime.*

Solution 3.3.6. *Let* n *be a composite number and* k *be any divisor of* n. *Then* $1 < k < n$ *and* $(a^k - 1)|(a^n - 1)$. *As* $a^n - 1$ *is prime, so* $a^k - 1 = 1$*(Why!). This is true, if* $a = 2$ *and* $k = 1$. *This leads to a contradiction as* $k > 1$. *Thus we have* $a = 2$ *and* n *is prime.*

Problem 3.3.7. *Show that every integer greater than* 11 *is the sum of two composite integers.*

Solution 3.3.7. *Let us assume that* n *be an integer greater than* 11.

Case I n *is even: Then there exists an integer* k *such that* $n = 2k$. *Since* $n > 11$, *therefore* $n \geq 12$ *and thus* $k \geq 6$. *Now* $n - 4 = 2(k-2)$ *with* $k - 2 \geq 4$. *By definition of divisibility, we have* $2|(n-4)$ *and* $(k-2)|(n-4)$. *By definition of compositeness,* $n - 4$ *is composite. Also* $n = (n-4) + 4$. *As* 4 *is composite, therefore* n *is the sum of two composite numbers.*

Case II n *is odd: Then there exists an integer* k *such that* $n = 2k + 1$. *Since* $n > 11$, *therefore* $n \geq 13$ *and thus* $k \geq 6$. *Now* $n - 9 = 2(k-4)$ *with* $k-4 \geq 2$. *By definition of divisibility, we have* $2|(n-9)$ *and* $(k-4)|(n-9)$. *Again by definition of compositeness, we have* $n - 9$ *is composite. Also* $n = (n-9)+9$. *As* 9 *is composite, therefore* n *is the sum of two composite numbers.*

Problem 3.3.8. *If* $p \geq 5$ *is a prime number, show that* $p^2 + 2$ *is composite.*

Solution 3.3.8. *By division algorithm,* $p = 6q + r$ *where* $r = 0, 1, 2, 3, 4, 5$.

Case i: *If* $r = 0$, *then* $p = 6q$ *implies* $6|p$, *a contradiction(Why!). Hence* $r \neq 0$

Case ii: *If* $r = 2$, *then* $p = 6q + 2$ *implies* $2|p$, *a contradiction. Hence* $r \neq 2$

Case iii: *If* $r = 3$, *then* $p = 6q + 3$ *implies* $3|p$, *a contradiction. Hence* $r \neq 3$

Case iv: *If* $r = 4$, *then* $p = 6q + 4$ *implies* $2|p$, *a contradiction. Hence* $r \neq 4$

Thus $r = 1, 5$ *implies* $p = 6q + 1$ *or* $p = 6q + 5$. *Therefore* $3|(p^2 + 2)$ *in either case(Why!). Hence the proof.*

Problem 3.3.9. *If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.*

Solution 3.3.9. *Here p is of the form: $10q + 1, 10q + 3, 10q + 7, 10q + 9$. But $p \neq 10q +$ even since it can factor out 2, so fails to be prime. Now,*

$$(10q + 1)^2 = 100q^2 + 20q + 1 \Rightarrow 10|(p^2 - 1)$$
$$(10q + 3)^2 = 100q^2 + 60q + 9 \Rightarrow 10|(p^2 + 1)$$
$$(10q + 7)^2 = 100q^2 + 140q + 49 \Rightarrow 10|(p^2 + 1)$$
$$(10q + 9)^2 = 100q^2 + 180q + 81 \Rightarrow 10|(p^2 - 1).$$

Problem 3.3.10. *If $n > 1$ is an integer not of the form $6k + 3$, prove that $n^2 + 2^n$ is composite.*

Solution 3.3.10. *Here n is of the form $6q, 6q + 1, 6q + 2, 6q + 4, 6q + 5$.*

Case (i): *When $n = 6q$, then $n^2 + 2^n = 36q^2 + 2^{6q} \Rightarrow 2|(36q^2 + 2^{6q})$ as $q > 0$, hence a composite number.*

Case (ii): *When $n = 6q + 1$, then $n^2 + 2^n = 36q^2 + 12q + 2^{6q+1} + 1 = 36q^2 + 12q+(2+1)(2^{6q} - \cdots + (-1)^{6q}1^{6q})(Why!) \Rightarrow 3|(n^2+2^n)$, hence a composite number.*

Case (iii): *When $n = 6q+2$, then $n^2+2^n = 36q^2+24q+4+2^2 2^{6q} \Rightarrow 2|(n^2+2^n)$, hence a composite number.*

case (iv): *When $n = 6q+4$, then $n^2+2^n = 36q^2+48q+16+2^4 2^{6q} \Rightarrow 2|(n^2+2^n)$, hence a composite number.*

Case (v): *Treated as an exercise.(Hint! Similar to $6q + 1$ as above.)*

Problem 3.3.11. *Prove that a positive integer $a > 1$ is a square if and only if in the prime factorizations of a all the exponents of the primes are even integers.*

Solution 3.3.11. *Let $a > 1$ be square. Then $a = n^2$, for some integer n. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. Therefore $n^2 = p_1^{2k_1} p_2^{2k_2} \cdots p_s^{2k_s}$ shows all exponents are even.*

Conversely, suppose all exponents of $a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ are even. Therefore $k_i = 2m_i$ for some m_i and for every k_i. Therefore $a = p_1^{2m_1} p_2^{2m_2} \cdots p_s^{2m_s} = (p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s})^2$.

Problem 3.3.12. *An integer is said to be square-free if it is not divisible by the square of any integer greater than 1. Prove the following:*

1. *An integer $n > 1$ is square-free if and only if n can be factored into a product of distinct primes.*

2. *Every integer $n > 1$ is the product of a square-free integer and a perfect square.*

Solution 3.3.12. *1. Let $n > 1$ be square free and $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ be the prime factorization of it. Then $k_i \geq 2$ and therefore $p_i^2 | n$, a contradiction to the definition of square free. Therefore $k_i = 1$. Hence $n = p_1 p_2 p_3 \cdots p_s$ with $p_i \neq p_j$. If possible, let n be not a square free and $a^2 | n$. Hence $n = la^2$, for some $l \in \mathbb{Z}$. Let $a = q_1^{k_1} q_2^{k_2} q_3^{k_3} \cdots q_r^{k_r}$. Therefore $p_1 p_2 p_3 \cdots p_s = l q_1^{2k_1} q_2^{2k_2} q_3^{2k_3} \cdots q_r^{2k_r}$ implies $q_j | p_1 p_2 p_3 \cdots p_s$. By virtue of Corollary (3.2.1), $q_j = p_i$ for some $i = 1, 2, 3, \ldots, s$. After factoring out q_j and p_i, we still have $p_1 p_2 p_3 \cdots p_s = l q_1^{2k_1} q_2^{2k_2} q_3^{2k_3} \cdots q_r^{2k_r}$ implies $q_j | p_1 p_2 p_3 \cdots p_s$. But the original factorization $p_1 p_2 p_3 \cdots p_s$ was unique and q_j was factored out. Hence q_j fails to divide the remaining factorization, which shows n to be square free.*

2. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ be the prime factorization of it. If k_i is odd and $k_i > 1$, then $k_i - 1$ is even. Let $a = p_{r_1}^{k_{r_1}} p_{r_2}^{k_{r_2}} \cdots p_{r_m}^{k_{r_m}}, 1 \leq r_i \leq s$ and k_{r_i} is odd with $k_{r_i} \geq 1$. Let $b = p_{r_1} p_{r_2} \cdots p_{r_m}$. Then $a = b p_{r_1}^{k_{r_1}-1} p_{r_2}^{k_{r_2}-1} \cdots p_{r_m}^{k_{r_m}-1}$. Also b is square free(Why!). Since $k_{r_i} - 1$ is even, $p_{r_i}^{k_{r_i}-1} = p_{r_i}^{2l_i}$. Let $c = p_{r_1}^{l_1} p_{r_2}^{l_2} \cdots p_{r_m}^{l_m}$. Then, $a = bc^2$. Finally, suppose $a | n = p_{l_1}^{k_{l_1}} p_{l_2}^{k_{l_2}} \cdots p_{l_j}^{k_{l_j}}$ where all k_{l_j} are even as $a | n$ has factored out all of the odd exponents in the canonical form of n. By previous problem above, $a | n = d^2 \Rightarrow n = bc^2 d^2 = b(cd)^2$, where b is square free.

Problem 3.3.13. *Find all prime numbers that divide* 50!.

Solution 3.3.13. *All primes less than* 50 *will divide* 50! *because each is a term of* 50!. *By the fundamental theorem of Arithmetic, each term k of* 50! *that is non–prime has a unique prime factorization. And each term of the unique factorization of k is smaller than k, so is prime less than* 50. *There is no prime greater than* 50 *represented in this factorization of k. Hence all primes less than* 50 *will divide* 50!.

Problem 3.3.14. *Show that any composite three-digit number must have a prime factor less than or equal to* 31.

Solution 3.3.14. *We know* 999 *is the largest composite three digit number. Now* $\sqrt{999} = 31.6$. *Here* 31 *is prime, so if a is composite, largest prime divisor is less than equal to $\sqrt{a}$. Hence* 31 *is largest possible prime divisor.*

Problem 3.3.15. *Prove that the prime number set is countably infinite using the integer* $N = p! + 1$.

Solution 3.3.15. *Let us assume there are finitely many primes,* p_n *being the largest. Then* $N = p_n! + 1 = 1 \cdot 2 \cdots p_n + 1$. *Now* N *must have a prime divisor* p_k *with* $1 \leq k \leq n$*(Why!). And* $p_k | 1 \cdot 2 \cdots p_n$ *(Why!). Therefore* $p_k | (N - 1 \cdot 2 \cdots p_n) \Rightarrow p_k | 1 \Rightarrow p_k = 1$, *a contradiction.*

Problem 3.3.16. *Any integer* n *can be expressed as* $n = 2^k m$, *where* $k \geq 0$ *and* m *being an odd integer. Verify!*

Solution 3.3.16. *With out any loss of generality, assume* $n > 0$, *for if* $n < 0$ *then* $-n = 2^k m \Rightarrow n = 2^k(-m)$. *Now the following cases will arise:*

Case(i) *If* n *is odd, then* $k = 0$ *and* $m = n$.

Case(ii) *If* n *is even, then* $n = 2k_1, k_1 < n$.

Case(iii) *If* k_1 *is odd, then we are done.*

Case(iv) *If* k_1 *is even, then* $k_1 = 2k_2$ *so* $n = 2^2 k_2$ *where* $k_2 < k_1 < n$.

Continuing as above after i*-th stage we have* $2^i k_i$, *where* $k_i < k_{i-1}$. *This is a finite process and after a certain stage we will reach at* $k_t = 1$ *and there will be no odd integer after* 1. *In that stage,* $n = 2^t k_t = 2^t \cdot 1$. *Thus* n *can be expressed as* $n = 2^k m$, *where* $k \geq 0$ *and* m *being an odd integer.*

Problem 3.3.17. *Prove or Disprove: Every positive integer can be written in the form* $p + a^2$, *where* p *is either a prime or* 1, *and* $a \geq 0$.

Solution 3.3.17. *Hint:* $25 = p + a^2$ *then consider* $a = 1, 2, 3, 4, 5$.

Problem 3.3.18.

1. *Prove: Any prime of the form* $3n+1$ *is also of the form* $6m + 1$.
2. *The only prime of the form* $n^3 - 1$ *is* 7.

Solution 3.3.18.

1. *Here* $p = 3n + 1$ *is prime implies* p *is odd. Then* $p - 1 = 3n$ *is even implies* n *is even. Hence* $n = 2m$, *for integer* m. *Thus* $3n + 1 = 6m + 1$.
2. *Here* $t = n^3 - 1 = (n - 1)(n^2 + n + 1)$. *If* $n = 1$, *then* t *is prime. If* $n = 2, t = 7$. *If* $n > 2$, *then* t *will be a factor of two integers, neither of which is* 1. *Hence for* $n > 2$, t *can't be prime.*

Problem 3.3.19. *Find five primes of the form* $n^2 - 2$.

Solution 3.3.19. *Hint: Consider* $n = 2, 3, 5, 7, 9$.

Problem 3.3.20. *A positive integer* n *is said to be square-full, or powerful, if* $p^2|n$ *for every prime factor* p *of* n. *Prove that if* n *is square-full, then it can be written in the form* $n = a^2b^3$, *with* a *and* b *positive integers.*

Solution 3.3.20. *Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ *be the prime factorization of it. Since* n *is square-full,* $k_i \geq 2$. *Listing first the odd exponents and then the even one, let us assume*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} = q_{m_1}^{k_{m_1}} q_{m_2}^{k_{m_2}} q_{m_3}^{k_{m_3}} \cdots q_{m_s}^{k_{m_s}} q_{n_1}^{k_{n_1}} q_{n_2}^{k_{n_2}} q_{n_3}^{k_{n_3}} \cdots q_{n_t}^{k_{n_t}},$$

where k_{m_i} *are odd(so* $k_{m_s} \geq 3$*) and* k_{n_i} *are even. Therefore for some* v_i, $k_{n_i} = 2v_i$. *Therefore*

$$\begin{aligned} n &= q_{m_1}^{k_{m_1}} q_{m_2}^{k_{m_2}} q_{m_3}^{k_{m_3}} \cdots q_{m_s}^{k_{m_s}} (q_{n_1}^{2v_1} q_{n_2}^{2v_2} q_{n_3}^{2v_3} \cdots q_{n_t}^{2v_t}) \\ &= q_{m_1}^{k_{m_1}} q_{m_2}^{k_{m_2}} q_{m_3}^{k_{m_3}} \cdots q_{m_s}^{k_{m_s}} (q_{n_1}^{v_1} q_{n_2}^{v_2} q_{n_3}^{v_3} \cdots q_{n_t}^{v_t})^2. \\ \text{Hence, } n &= q_{m_1}^{k_{m_1}} q_{m_2}^{k_{m_2}} q_{m_3}^{k_{m_3}} \cdots q_{m_s}^{k_{m_s}} (Y)^2, Y = q_{n_1}^{v_1} q_{n_2}^{v_2} q_{n_3}^{v_3} \cdots q_{n_t}^{v_t}. \end{aligned}$$

Now k_{m_i} *is odd and* ≥ 3 *together implies* $k_{m_i} - 3$ *is even. Thus*

$$n = q_{m_1}^3 q_{m_2}^3 q_{m_3}^3 \cdots q_{m_s}^3 (q_{m_1}^{m_1-3} q_{m_2}^{m_2-3} q_{m_3}^{m_3-3} \cdots q_{m_s}^{m_s-3})(Y)^2.$$

Let $m_i - 3 = 2w_i, q_{m_1} q_{m_2} q_{m_3} \cdots q_{m_s} = b$. *Therefore*

$$n = b^3 (q_{m_1}^{2w_1} q_{m_2}^{2w_2} q_{m_2}^{2w_3} \cdots q_{m_s}^{2w_s})(Y^2).$$

Let $X = q_{m_1}^{w_1} q_{m_2}^{w_2} q_{m_{w_3}}^3 \cdots q_{m_s}^{w_s}$. *Then* $n = b^3X^2Y^2$. *Taking* $a = XY$, *we obtain* $n = a^2b^3$.

Problem 3.3.21. *Given that* $p \nmid n$ *for all primes* $p \leq \sqrt[3]{n}$, *prove that* $n > 1$ *is either a prime or the product of two primes.*

Solution 3.3.21. *Assuming* n *to be composite and taking* $n = p_1 p_2 \cdots p_X$ *with* $X \geq 3$, *we know that*

$$1 < \sqrt[3]{n} < p_i \leq \sqrt{n}.$$

Therefore

$$\begin{aligned} \sqrt[3]{n} \leq p_1 \leq \sqrt{n} \\ \sqrt[3]{n} \leq p_2 \leq \sqrt{n} \\ \sqrt[3]{n} \leq p_3 \leq \sqrt{n}. \end{aligned}$$

Therefore $n = (\sqrt[3]{n})(\sqrt[3]{n})(\sqrt[3]{n}) < p_1 p_1 p_2 p_3 = n \Rightarrow n < n$. *Hence* $X < 3$ *or* $= 2$ *or* $= 1$. *Thus* $n > 1$ *is either a prime*$(X = 1)$ *or the product of two primes*$(X = 2)$.

Problem 3.3.22. *Prove that if $n > 2$, then there exists a prime p satisfying $n < p < n!$.*

Solution 3.3.22. *For $n > 2$,*

$$n < n! - 1 < n!.$$

If $n! - 1$ is prime, we are done. If $n! - 1$ is not prime, taking p to be a prime divisor, we have $p < n! - 1$. Suppose $p \leq n$. Then p is one of the terms in $1, 2, 3, \ldots, n$. So $p|n!$. Therefore $p|n!$ and $p\big|(n! - 1)$ together implies $p\big|\big(n! - (n! - 1)\big) = 1$. Therefore $p > n$ and hence the result.

Problem 3.3.23. *For $n > 1$, show that every prime divisor of $n! + 1$ is an odd integer that is greater than n.*

Solution 3.3.23. *Because $n!$ is even for $n > 1$, therefore $n! + 1$ is odd. Hence $2 \nmid (n! + 1)$, so every prime divisor of $n! + 1$ is odd.*

Suppose every prime divisor p_i of $n!+1$ is less than or equal to n. Since p_i is one of the members of $n!$, therefore $p_i|n!$. Also $p_i|(n!+1) \Rightarrow p_i|(n!+1) - n! = 1$, a contradiction. Thus p_i is greater than n.

Problem 3.3.24. *If a is a positive integer and $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ is an integer.*

Solution 3.3.24. *Let $\sqrt[n]{a} = \dfrac{r}{s}$, where r, s being integers and $\gcd(r, s) = 1$ with $s \neq 0$. Let $r = p_1 p_2 \cdots p_X$, $s = q_1 q_2 \cdots q_Y$. Then $p_i \neq q_j$. Therefore*

$$(q_1 q_2 \cdots q_Y)^n a = (p_1 p_2 \cdots p_X)^n.$$

Therefore $(p_1 p_2 \cdots p_X)^n | a$. Let $a = (p_1 p_2 \cdots p_X)^n t$, for some integer t. Therefore

$$(q_1 q_2 \cdots q_Y)^n (p_1 p_2 \cdots p_X)^n t = (p_1 p_2 \cdots p_X)^n,$$

implies $q_j = 1$ for all j. Thus $s = 1$ and $\dfrac{r}{s} = \sqrt[n]{a}$, an integer.

Problem 3.3.25. *Prove for $n \geq 2$, $\sqrt[n]{n}$ is irrational.*

Solution 3.3.25. *Suppose, $n \geq 2$, $\sqrt[n]{n}$ is rational. Then by Problem 3.3.24, it is an integer. Let $\sqrt[n]{n} = a$. Then $n = a^n$. But $n < 2^n \Rightarrow a^n < 2^n \Rightarrow$ either $a < 2$ or $a = 1$. Therefore $n = 1^n = 1$, a contradiction.*

Problem 3.3.26. *Prove that any odd prime p is of the form $4k + 1$ or $4k + 3$ for any non-negative integer k.*

Solution 3.3.26. *By Division Algorithm, any positive integer can be expressed in the form* $a = bq + r,\ 0 \leq r < b$ *or equivalently written as* $a = 4q + r,\ r = 0, 1, 2, 3$. *Now if;*

$$r = 0, a = 4q = 2(2q),\ \textit{an even integer.}$$
$$r = 1, a = 4q + 1 = 2(2q) + 1,\ \textit{an odd integer.}$$
$$r = 2, a = 4q + 2 = 2(2q) + 2 = 2(2q + 1) = 2m, \textit{an even integer.}$$
$$r = 3, a = 4q = 2(2q) + 3 = 2(2q + 1) + 1 = 2m + 1, \textit{an odd integer.}$$

Hence any odd prime p *is of the form* $4k + 1$ *or* $4k + 3$ *for any non-negative integer* k.

Problem 3.3.27. *If* p *and* $p^2 + 8$ *are both prime numbers, prove that* $p^3 + 4$ *is also prime.*

Solution 3.3.27. *Referring to Problem 3.3.8, if* $p > 3$ *is prime, it is of the form* $(6k + 1)$ *or* $(6k + 5)$. *So for* $p = 6k + 1$ *or* $6k + 5$, *we have* $p^2 + 8 = 36k^2 + 12k + 9$ *or* $p^2 + 8 = 36k^2 + 60k + 33$ *respectively. But* $3 \big| (36k^2 + 12k + 9)$ *and* $3 \big| (36k^2 + 60k + 33)$. *So* $p^2 + 8$ *is not prime, provided* $p > 3$. *By the problem, both* p *and* $p^2 + 8$ *are primes. Thus the only possibility is* $p = 3$, *which yields* $p^2 + 8 = 17$. *Hence* $p^3 + 4 = 31$.

Problem 3.3.28. *Bertrand Conjecture: For any positive integer* z, $\exists$ *a prime* p *satisfying* $z \leq p < 2z$. *Using this proves that for every* $n \geq 2$, $\exists$ *a prime* p *with* $p < n < 2p$.

Solution 3.3.28. ***Case-I:*** n *is odd: Since* $n \geq 2\ \&\ k \geq 1,\ \exists\ k \in \mathbb{Z}$ *such that* $n = 2k + 1$. *Addressing to Bertrand's Conjecture,* $\exists$ *a prime* p *satisfying* $k < p < 2k$. *Now* $p < (p + 1) < (2k + 1) = n \Rightarrow p < n$. *Further* $2k < 2p \Rightarrow (2k+1) \leq 2p \Rightarrow n \leq 2p$. *But* $(2k+1)$ *being odd and* $2p$ *is even, together conclude* $n < 2p$. *Thus* $\exists$ *a prime* p *such that* $p < n < 2p$.

Case-II: n *is even: Since* $k \geq 1,\ \exists\ k \in \mathbb{Z}$ *such that* $n = 2k$ *holds. An appeal to Bertrand's Conjecture yields,* $k < p < 2k = n \Rightarrow p < n$*(*$p$ *being a prime). Therefore* $n = 2k < 2p \Rightarrow n < 2p$. *Thus* $p < n < 2p$.

Problem 3.3.29. *Let* p_n *denote the* n*-th prime number. For* $n \geq 3$, *prove that* $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$.

Solution 3.3.29. *Note that* $p_{n+1} < 2p_n$. *Therefore* $p_{n+3} < 2p_{n+2}$. *So* $p_{n+3}^2 < 4p_{n+2}^2 < 4p_{n+2}(2p_{n+1}) = 8p_{n+2}p_{n+1}$. *Now* $p_5 = 11 \Rightarrow 8p_{n+2}p_{n+1} < p_5 p_{n+2} p_{n+1}$. *Therefore* $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$, *if* $n \geq 5$.

For $n = 4;\ p_7^2 = 289 < p_4 p_5 p_6 = 1001$. *For* $n = 3;\ p_6^2 = 169 < p_3 p_4 p_5 = 385$. *For* $n = 2;\ p_5^2 = 121 < p_2 p_3 p_4 = 105$. *Hence for* $n \geq 3,\ p_{n+3}^2 < p_n p_{n+1} p_{n+2}$.

Problem 3.3.30. *There exist infinitely many primes that do not belong to any pair of twin primes.*

Solution 3.3.30. *Here* $\gcd(5, 21) = 1$. *By Dirichlet's theorem, the series* $5 + 21k$ *for* $k = 1, 2, 3, \ldots$, *contains infinitely many primes. Let* p *be one such prime. Then* $p = 5 + 21k (k \in \mathbb{Z})$ *gives* $p + 2 = 7(1 + 3k)$ *and* $p - 2 = 3(1 + 7k)$. *Thus* $(p + 2)$ *and* $(p - 2)$ *fails to be prime. Hence all the primes contained in* $(5 + 21k)$ *cannot be numbers of twin primes.*

Problem 3.3.31. *Prove that there are infinitely many primes of the form* $6n+5$.

Solution 3.3.31. *To the contrary, assume only a finite number of primes of the form* $(6n + 5)$. *Let this be* $q_1, q_2, \ldots, q_s$. *Consider* $N = 6q_1q_2 \ldots q_s - 1 = 6(q_1q_2 \ldots q_s - 1) + 5$. *Let* $N = r_1r_2 \ldots r_t$ *be its prime factorization. Since* N *is odd,* $r_i \neq 2$ *for each* i, *so each* r_i *can only be of the form* $6n + 1$, $6n + 3$ *or* $6n + 5$. *Since*

$$\begin{aligned}(6n + 1)(6m + 1) &= 36mn + 6m + 6n + 1\\ &= 6(6mn + m + n) + 1\\ &= 6k + 1, \quad \textit{where } k = (6mn + m + n),\end{aligned}$$

this shows the product of two integers of the form $(6n + 1)$ *is of the same form. By similar reasoning, the product of two integers of the form* $(6n + 3)$ *is also so. Furthermore,*

$$\begin{aligned}(6n + 1)(6m + 3) &= 6(6mn + m + 3n) + 3\\ &= 6k' + 3, \quad \textit{where } k' = (6mn + m + 3n).\end{aligned}$$

This implies, the product of two integers of the form $(6n + 1)$ *and* $(6n + 3)$ *is of the form* $(6n + 3)$.

So the only way for N *to be of the form* $(6n + 5)$ *is,* N *must contain at least one factor* r_i *which is of the form* $(6n + 5)$. *But* $\nexists$ *any* q_i *of the form* $6n + 5$. *If such* q_i *exists, then from construction of* N *we get* $N - 6q_1q_2 \ldots q_s = -1$. *Furthermore* $N - 6q_1q_2 \ldots q_s$ *is divisible by a prime of the form* $(6n + 5)$, *which contradicts our assumption(Why!).*

3.4 Exercises:

1. Prove each of the assertions below:
   (a) The only prime of the form $n^3 - 1$is 7.
   (b) The only prime p for which $3p + 1$ is a perfect square is $p = 5$.
   (c) The only prime of the form $n^2 - 4$ is 5.

2. Given that p is a prime and $p|a^n$, prove that $p^n|a^n$.

3. Establish each of the following statements:
   (a) If $n > 4$ is composite, then n divides $(n-1)!$.
   (b) Any integer of the form $8^n + 1$, where $n \geq 1$, is composite.

4. Prove that a positive integer $a > 1$ is a square if and only if in the canonical form of a all the exponents of the primes are even integers.

5. Verify that any integer n can be expressed as $n = 2^k m$, where $k \geq 0$ and m is an odd integer.

6. A positive integer n is called square-full, or powerful, if $p^2|n$ for every prime factor p of n (there are 992 square-full numbers less than $250,000$). If n is square-full, show that it can be written in the form $n = a^2b^3$, with a and b positive integers.

7. Given that $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, show that $n > 1$ is either a prime or the product of two primes.

8. Show that any composite three-digit number must have a prime factor less than or equal to 31.

9. Let q_n be the smallest prime that is strictly greater than $P_n = p_1 p_2 \ldots p_n + 1$. It has been conjectured that the difference $q_n - (p_1 p_2 \ldots p_n)$ is always prime. Confirm this for the first five values of n.

10. Let p_n denotes the n-th prime number and set $d_n = p_{n+1} - p_n$. Find five solutions of the equation $d_n = d_n + 1$.

11. For $n > 3$, show that the integers $n, n+2, n+4$ cannot all be prime.

12. A conjecture of Lagrange (1775) asserts that every odd integer greater than 5 can be written as a sum $p_l + 2p_2$, where p_1, p_2 are both primes. Confirm this for all odd integers through 75.

13. Show that 13 is the largest prime that can divide two successive integers of the form $n_2 + 3$.

14. Determine all twin primes p and $q = p + 2$ for which $pq - 2$ is also prime.

15. Let p_n denote the n-th prime. For $n > 3$, show that $p_n < p_l + p_2 + \ldots + p_{n-l}$.