# 1 Problem 1

*Find all integers $n > 1$ with the property that for each positive divisor $d$ of $n$, we also have that*

$$(d+2) \mid (n+2)$$

*Solution.* We first show no even integers satisfy our property. If $n$ is even, there exists some $k \in \mathbb{N}$ such that $2k = n$, so $k \mid n$. Furthermore, $n+2$ is even as well, so $\frac{n+2}{2}$ is an integer, specifically $\frac{n+2}{2} = \frac{n}{2} + 1 = k+1$. So $2(k+1) = n+2 \implies k+1 \mid n+2$. Furthermore, $k+1$ must be the greatest possible divisor of $n+2$ that is not equal to $n+2$, since if a divisor $d$ was greater than $k+1$, there is some integer $1 < m < 2$ where $dm = n+2$, but no such integer $m$ exists. But $k+2 > k+1$, and $k+2 = \frac{n}{2} + 2 \neq n+2$ when $n > 1$, so $k+2 \nmid n+2$. So there exists a divisor of $n$ such that two more than it is not a divisor of $n+2$.

Now, we consider odd composite integers $n$. Then there exists an integers $1 < d, q < n$ (not necessarily distinct) such that $qd = n$ (so $d \mid n$). Without loss of generality, let $d \geq q$. Then $n+2 = qd+2$. Note that both $q$ and $d$ must be odd, otherwise $n$ would be divisible by 2 and would be even, which would be against our assumption. We can write $n+2 = qd+2+2q-2q = q(d+2) - 2(q-1)$, so

$$(n+2)/(d+2) = q - 2(q-1)/(d+2)$$

But since $d \geq q$, $d+2 > q-1$ so $d+2 \nmid q-1$. Furthermore, $q-1$ is even so $2(q-1)$ is even, but $d+2$ is odd, so $d+2 \nmid 2(q-1)$, so $2(q-1)/(d+2)$ is not an integer, thus our term on the right is not an integer. But then $d+2 \nmid n+2$. Thus odd composite integers do not satisfy our property either.

Finally, consider the only remaining possibility, when $n$ is an odd prime number. The only such divisors of this is $n$ and 1. $n+2 \mid n+2$ trivially. If and only if $1+2 = 3 \nmid n+2$, we have our desired property then. So if $n$ is prime and of the form $n = 3j-2$ for some $j \in \mathbb{N}$, then $n$ must satisfiy our property. We have shown that no other such $n$ can satisfy our property, thus this is all the possible solutions. $\square$

## 2 Problem 2

*Find all positive integers $m$ and $n$ such that*

$$2^m - 3^n = 7$$

*Solution.* We can rearrange our equation to get

$$2^m = 7 + 3^n \tag{1}$$

Obviously, any $m$ that satisfies the above equation will also satisfy $2^m = 2 \cdot 2^{m-1} \equiv 7 \pmod 3$ (since $3 \mid 3^n$ for any $n$). That is to say, the set of solutions $M_1$ to equation (1) (elements in $M_1$ are of the form $2^m$) is a subset of the set of solutions $M_2$ to our subsequent relation, $M_1 \subset M_2$. If $X$ is the set of solutions $x \in \mathbb{Z}$ to $2x \equiv 7 \pmod 3$, then clearly $M_2 \subset X$.

Recall proposition 7.2 (B) from the course notes: if $a, b, m \in \mathbb{Z}$ with $m \neq 0$ and $d = gcd(a, m)$, then if $d \mid b$, the congruence equation $ax \equiv b \pmod m$ has exactly $d$ solutions. Since 2 and 3 are coprime, we have that $d = 1$, so $d \mid 7$, thus $2x \equiv 7 \pmod 3$ has exactly one solution. Thus, $X$ has exactly one element. Therefore, since $M_1 \subset X$, equation (1) has at most one solution.

We can verify that there does exist such a solution, namely when $m = 4$ and $n = 2$, then we have $2^4 - 3^2 = 16 - 9 = 7$. □

# 3 Problem 3

*Let $k \in \mathbb{N}$. Show that there exists $k$ consecutive positive integers with the property that no integer from this set is of the form $a^2 + b^2$ for some $a, b \in \mathbb{Z}$.*

*Solution.* Let $k \in \mathbb{N}$ be arbitrary. Let $m$ be the product of the squares of the first $k$ primes $q$ of the form $q = 4j + 3$ (for some $j \in \mathbb{N}$), i.e. $m = \prod_{i=1}^{k} q_i^2$.

Note that we can always $k$-many $q_i$. To prove this, for the sake of contradiction, assume there are only $r < k$ many such primes of this form, $q_1, q_2, \ldots, q_r$ (where $q_1 < q_2 < \cdots < q_r$). Note that $n = 4q_1q_2 \cdots q_r - 1$ is of the form $4j + 3$, but $n > q_r$, so by assumption, $n$ cannot be prime, so is composite. Further, note that none of the $q_i$ and 2 divide $n$, thus all the primes in the prime factor decomposition of $n$ is of the form $4j + 1$, thus $n \equiv 1 \pmod 4$ which is a contradiction. Thus $n$ is a prime greater than $q_r$ and $n = 4j - 1$. We can do this indefinitely to get $k$ many primes of the form $4j + 3$.

Now, consider the system

$$\begin{aligned} x &\equiv q_1 - 1 \pmod{q_1^2} \\ x &\equiv q_2 - 2 \pmod{q_2^2} \\ &\vdots \\ x &\equiv q_k - k \pmod{q_k^2} \end{aligned}$$

By the Chinese Remainder Theorem, there exists a unique solution to the system modulo $m$, which we'll call $x_0$. Then, let $x_i = x_0 + i$ for $1 \leq i \leq k$. Note that $x_i = q_i + nq_i^2$, thus $q_i \mid x_i$ but $q_i^2 \nmid x_i$ (and so $q_i^s \nmid x_i$ for all $s \geq 2$). Thus, there are $k$ consecutive integers $x_1, x_2, \ldots, x_k$ whose prime number decomposition that contain a prime of the form $4j+3$ with exponent 1. But by Theorem 13.4 from the notes, for all $a, b \in \mathbb{Z}$, $a^2 + b^2 \neq x_i$ for all $1 \leq i \leq k$, since the exponent of $q_i$ is $\gamma_i = 1$, which is not even. $\square$

# 4 Problem 4

*As always, for each positive integer $m$, we have that $d(m)$ is the number of the positive divisors of $m$; also, we let $\phi(m)$ be the corresponding value of the Euler $\phi$-function. Then compute the following limits:*

$$\lim_{n\to\infty} \frac{n!}{d(n!)\phi(n!)}$$

$$\lim_{n\to\infty} \frac{n!}{2^{d(n!)}}$$

*Solution.*
**Limit 1:** Note that the prime factor decomposition of $n!$ contains every prime that came before it, since if $p$ is prime and $p < n$, $p \mid n!$ by definition of factorial. Thus, if we enumerate the primes in order (ie. $p_1 = 2$, $p_2 = 3$, etc.), let $p_r$ be the greatest prime less than or equal to $n$. Then we can write $n! = \prod_{i=1}^r p_i^{\alpha_i}$ thus

$$\frac{n!}{d(n!)\phi(n!)} = \prod_{i=1}^r \frac{p_i^{\alpha_i}}{d(p_i^{\alpha_i})\phi(p_i^{\alpha_i})} = \prod_{i=1}^r \frac{p_i^{\alpha_i}}{(\alpha_i+1)p_i^{\alpha_i-1}(p_i-1)} = \prod_{i=1}^r \frac{p_i}{(\alpha_i+1)(p_i-1)}$$

Note that if $n$ is an integer such that $n > 3$, we have $3n - 2n > 3 \implies 3(n-1) > 2n \implies \frac{n}{n-1} < \frac{3}{2}$. Thus for $i \geq 3$, $p_i \geq 5$, and since $\alpha_i \geq 1$, we have

$$\frac{p_i}{(\alpha_i+1)(p_i-1)} \leq \frac{p_i}{2(p_i-1)} < \frac{3}{4}$$

for all $i \geq 3$.

If $\pi(n)$ denotes the prime counting function (the number of prime numbers less than $n$), we have that

$$\frac{n!}{d(n!)\phi(n!)} \leq \frac{p_1}{(\alpha_1+1)(p_1-1)} \frac{p_2}{(\alpha_2+1)(p_2-1)} \left(\frac{3}{4}\right)^{r-2} = \frac{p_1}{(\alpha_1+1)(p_1-1)} \frac{p_1}{(\alpha_1+1)(p_1-1)} \left(\frac{3}{4}\right)^{\pi(n)-2}$$

But since there are infinitly many primes, $\pi(n)$ approaches infinity as $n$ does, thus $\left(\frac{3}{4}\right)^{\pi(n)-2} \to 0$ as $n \to \infty$. But since $\frac{n!}{d(n!)\phi(n!)}$ is bounded below by zero, by squeeze theorem, we have that

$$\lim_{n\to\infty} \frac{n!}{d(n!)\phi(n!)} = 0$$

as well.

**Limit 2:** Let $a_n = \frac{n!}{2^{d(n!)}}$. Then

$$\frac{a_{n+1}}{a_n} = \frac{(n+1)!/2^{d((n+1)!)}}{n!2^{d(n!)}} = (n+1)/2^{d(n!)-d((n+1)!)}$$

Thus, it is sufficient to show that $2^{d((n+1)!)-d(n!)} > 2n+2$ for sufficiently large $n$, because then $(n+1)/2^{d((n+1)!)-d(n!)} < (n+1)/(2n+2) = \frac{1}{2}$, so $a_n < C\left(\frac{1}{2}\right)^n$ (where $C$ is a constant). Since $C\left(\frac{1}{2}\right)^n \to 0$ as $n \to \infty$, and $a_n > 0$ for all $n$, by squeeze theorem, we would have $\lim_{n\to\infty} a_n = 0$.

We show first show that $d((n+1)!) - d(n!) \geq 2^{\pi(n)-1}$ (where $\pi(n)$ is number of primes $\leq n$). To see this, let $n! = \prod_{i=1}^{\pi(n)} p_i^{\alpha_i}$ be the unique prime factorization of $n!$, where $p_i$ is the $i$th prime number (e.g. $p_1 = 2$). We deal with two case: when $n+1$ is prime, and when it is composite. First, let $n+1$ be prime. Then $(n+1)! = p_{\pi(n)+1}\prod_{i=1}^{\pi(n)} p_i^{\alpha_i}$. Then let $\beta_i \in \{0,1\}$, we have that $p_{\pi(n)+1}\prod_{i=1}^{\pi(n)} p_i^{\beta_i} \mid p_{\pi(n)+1} = n+1 \mid (n+1)!$, but since $p_{n+1} \nmid n!$, we have $p_{\pi(n)+1}\prod_{i=1}^{\pi(n)} p_i^{\beta_i} \nmid n!$. There are a total of two possibilities for $\pi(n)$ many $\beta_i$, thus there are $2^{\pi(n)}$ ways to choose the $\beta_i$, so there are at least $2^{\pi(n)}$ many divisors of $(n+1)!$ but not of $n!$. Thus

$$d((n+1)!) - d(n!) \geq 2^{\pi(n)} \geq 2^{\pi(n)-1}$$

which proves the $n+1$ is prime case. Now let $n+1$ be composite. Then we have the unique prime factorization $(n+1)! = \prod_{i=1}^{\pi(n)} p_i^{\beta_i}$ where there is at least one $i$ such that $\gamma_i > \alpha_i$ (by unique factorization). Denote this $\gamma_i$ by $\gamma_j$ (and $p_j$). Then using $\beta_i \in \{0,1\}, i \neq j$ as before, let

$$m = p_j^{\gamma_j} \prod_{\substack{i=1 \\ i \neq j}}^{\pi(n)} p_i^{\beta_i}$$

Similar to before, we have $m \mid (n+1)!$, but $m \nmid n!$ since $p_j^{\gamma_j} \nmid n!$. There are $\pi(n)-1$ ways to choose the $\beta_i$ (similar to the prime case), so there are at least $2^{\pi(n)-1}$ many divisors of $(n+1)!$ but not of $n!$. Thus

$$d((n+1)!) - d(n!) \geq 2^{\pi(n)-1}$$

Thus, we have that $2^{d((n+1)!)-d(n!)} \geq 2^{2^{\pi(n)-1}}$.

Note that for all $k \in \mathbb{N}$ such that $k \geq 5$, $2^{k-1} > 2k+2$ (since $2^{5-1} > 2 \cdot 5 + 2$, and the exponential grows faster than linear thereafter). Since $\pi(n) \geq 5$ when $n \geq 11$, we have $2^{2^{\pi(n)-1}} > 2^{2\pi(n)+2}$ when $n \geq 11$.

Finally, we show that $2^{2\pi(n)} > n$. Consider all $m \in \mathbb{N}$ such that $m \leq n$. We can rewrite a unique prime factorization $m = p_1^{\eta_1} p_2^{\eta_2} \cdots p_{\pi(n)}^{\eta_{\pi(n)}}$ where $\eta_i$ may be 0. By the division algorithm, we have $\eta_i = 2q_i + r_i$ where $r_i \in \{0,1\}$ and $r_i, q_i$ are unique. Thus we can uniquely write $m = u^2 p_1^{r_1} \cdots p_{\pi(n)}^{r_{\pi(n)}}$ where $u \in \mathbb{N}$ such that $u = p_1^{q_1} \cdots p_{\pi(n)}^{q_{\pi(n)}}$. See that $u \leq \sqrt{m}$. We use the notation $\mathbb{N}_j = \{i \colon i \in \mathbb{N}, i \leq j\}$. Now define a map

$$\phi \colon \mathbb{N}_n \to \mathbb{N}_{\lfloor \sqrt{n} \rfloor} \times \mathcal{P}(\{p_i \colon i \in \mathbb{N}_{\pi(n)}\})$$

with $m \mapsto (u, \{p_i \colon i \in \mathbb{N}_{\pi(n)}, r_i = 1\}$. By uniqueness, this map is injective. Thus we have that $|\mathbb{N}_n| \leq |\mathbb{N}_{\lfloor \sqrt{n} \rfloor}||\mathcal{P}(\{p_i \colon i \in \mathbb{N}_{\pi(n)}\})|$, i.e. $n \leq 2^{\pi(n)}\sqrt{n}$. We want to show the strict inequality. We now deal with when $n$ is a perfect square, and when $n$ is not. If $n$ is not a perfect square, we have that

$$n \leq \lfloor \sqrt{n} \rfloor 2^{\pi(n)} < 2^{\pi(n)} \sqrt{n}$$

Now let $n$ be a perfect square. Note the pre-image of $(\sqrt{n}, \{p_i \colon i \in \mathbb{N}_{\pi(n)}, r_i = 1\}$ is the $m$ of the form $m = np_1 p_2 \cdots p_{\pi(n)}$, but then $m > n$, which is a contradiction. But then the pre-image is empty, thus $n \neq 2^{\pi(n)}\sqrt{n}$ giving us the strict inequality. Thus, regardless of $n$, we have $n \neq 2^{\pi(n)}\sqrt{n}$, and squaring both sides (both are positive) gives us $2^{2\pi(n)} > n$.

Finally, we have that

$$2^{d((n+1)!)-d(n!)} > 2^{2\pi(n)+2} > 2 \cdot 2^{2\pi(n)} + 2 > 2n + 2$$

for $n \geq 11$, as desired. Thus we have shown the desired limit as observed before. □