Math 437 HW2

marcus lai

October 2023

1. Find all integers $n > 1$ with the property that for each positive divisor d of n, we also have that
$$(d+2)|(n+2) \tag{1}$$

Proof. Let the set of solutions to the question be N (this set is non empty since $7 \in N$). Consider an $n \in N$. Note that since we must have $1|n$, we have that $3|(n+2)$ by (1) and equivalently

$$n \equiv -2 \equiv 1 \mod 3$$

Also note that $\forall a \in \mathbf{N}$, we have $(a+2)|(a+2)$. So prime numbers p such that $p \equiv 1 \mod 3$ are solutions of N since the only two positive divisors are 1 and p (and both satisfy (1)).

Next, I will show that n cannot be a composite number.

First, I will show $2 \nmid n$ by contradiction. Suppose $2|n$. Then $n = 2k \implies k = \frac{n}{2} > 0$ is a positive divisor of n. So by (1), $(k+2)|n+2 \iff l(k+2) = n+2$ for $l \in \mathbf{Z}$. In particular, since $k+2 > 0$, $n+2 > 0$, $l \in \mathbf{N}$. Now, note that $l \neq 1$ since $k+2 = \frac{n}{2} + 2 \neq n+2$ since $n \neq 0$. However, if $l \geq 2$, we have that $l(k+2) \geq 2(k+2) = n+4 > n+2$. So no solution to l exists (**contradiction**).

Now, suppose n is a composite number. Then $\exists d_1, d_2 \in \mathbf{N}$ such that $n = d_1 d_2$ for $d_1 \neq n, d_2 \neq 1$ (without loss of generality assume $d_1 \geq d_2$). From above, we know that $2 \nmid n$, so d_1, d_2 are **odd**. Then by (1), we have:

$$(d_1+2)|(d_1d_2+2) \iff (d_1+2)|(d_1(d_2-1)+d_1+2) \iff (d_1+2)|(d_1(d_2-1))$$

<u>Claim: consecutive odd integers are coprime</u>

Let o an odd integer. Then $o = 2k+1$ for some $k \in \mathbf{Z}$ and $o+2 = 2k+3$. Suppose o and $o+2$ are not coprime. Then $\exists c \in \mathbf{N}$ and $c|o$ and $c|o+2$. So $c|o-(o+2) \implies c|2$. Then $c = 1$ or 2. Since o is odd, $2 \nmid o$ so $c = 1$ as desired.

By our claim, we know that d_1 and $d_1 + 2$ are coprime. Thus by theorem in class:
$$(d_1+2)|(d_1(d_2-1)) \iff (d_1+2)|(d_2-1)$$

Since $d_2 \neq 1$ by assumption, we obtain a **contradiction** since we have $d_1 \geq d_2 \implies d_1 + 2 > d_2 - 1 > 0$ but $(d_1 + 2) | (d_2 - 1)$.

Thus n cannot be composite, so n is any prime number such that $n \equiv 1 \mod 3$. $\square$

2. Suppose there exist integers m, n positive integers such that

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

Taking (1) mod 3 gives:

$$2^m \equiv 7 \equiv 1 \mod 3$$

Suppose that m is odd ($m = 2k + 1, k \in \mathbf{Z}$). Since $4 \equiv 1 \mod 3$:

$$2^m \equiv 4^k \cdot 2 \equiv 1^k \cdot 2 \equiv 2 \mod 3$$

So m is not odd. Check m can be even ($m = 2k, k \in \mathbf{Z}$):

$$2^m \equiv 4^k \equiv 1^k \equiv 1 \mod 3$$

as desired. Along with (1), this gives us:

$$2^{2k} - 3^n = 7 \tag{2}$$

Taking (2) mod 4 gives:

$$-3^n \equiv 7 \mod 4 \iff -3^n \equiv -1 \mod 4 \iff 3^n \equiv 1 \mod 4$$

Suppose that n is odd ($n = 2j + 1, j \in \mathbf{Z}$). Since $9 \equiv 1 \mod 4$:

$$3^m \equiv 9^j \cdot 3 \equiv 1^j \cdot 3 \equiv 3 \mod 4$$

So m is not odd. Check n can be even ($n = 2j, j \in \mathbf{Z}$):

$$3^m \equiv 9^j \equiv 1^j \equiv 1 \mod 4$$

as desired. So overall:

$$2^{2k} - 3^{2j} = 7 \iff (2^k - 3^j)(2^k + 3^j) = 7$$

So we have $(2^k + 3^j)|7$. Note that $j < 2$ and $k < 3$ (otherwise $(2^k + 3^j) > 7$ which yields a **contradiction** by theorem from class since $7 \in \mathbf{N}$ and $(2^k + 3^j)|7$). Note m, n are positive integers so $k = \frac{m}{2} > 0$ and $j = \frac{n}{2} > 0$. So check solutions for $j = \{1\}, k = \{1, 2\}$ using (1):

$$2^{2\cdot 1} - 3^{2\cdot 1} = -5 \neq 7$$

$$2^{2\cdot 2} - 3^{2\cdot 1} = 7$$

Thus, the only solution is $m = 4, n = 2$.

3. Let $k \in \mathbf{N}$. I want to show that there exist k consecutive positive integers with the property that no integer from this set is of the form $a^2 + b^2$ for some $a, b \in \mathbf{Z}$.

Proof. Claim: There are infinite primes of form $4k+3$:

Suppose there are a finite number of primes of form $4k+3$, denoted $P_1, P_2, ..., P_a$ for $a \in \mathbf{N}$. Then consider the number $n = 4P_1P_2...P_a - 1$ (note 3 is one such prime so $n \geq 11$). Note from class, we've shown every integer greater than 1 can be prime factorized. Note next that n is odd so it's prime divisors must be of form $4k+1$ or $4k+3$. By construction of n, it can't have a factor of form $4k+3$ since none of $P_1, P_2, ..., P_a$ divide n. Thus, n must only have prime factors of form $4k+1$. Prime factoring n thus gives:

$$n = (4k_1 + 1)(4k_2 + 1)...(4k_j + 1)$$

where each k_i for $i \in \{1, 2, ..., j\}$ is an integer (not necessarily distinct). By taking the equation mod 4:

$$n = (4k_1 + 1)(4k_2 + 1)...(4k_j + 1) \equiv 1 \cdot 1 \cdot ... \cdot 1 \equiv 1 \mod 4$$

This is a contradiction since $n = 4P_1P_2...P_a - 1 \equiv -1 \mod 4$.

Now, I will find an integer n such that $n+1, n+2, ..., n+k$ are not of the form $a^2 + b^2$. Denote the set of primes of form $4k+3$ as S and enumerate: $S = \{3, 7, 11, 19, ...\} = \{p_1, p_2, ...\}$. Now, construct k equations of congruence like so:

$$x + 1 \equiv s_1 \mod s_1^2 \iff x \equiv s_1 - 1 \mod s_1^2$$

$$x + 2 \equiv s_2 \mod s_2^2 \iff x \equiv s_2 - 2 \mod s_2^2$$

$$...$$

$$x + k \equiv s_k \mod s_k^2 \iff x \equiv s_k - k \mod s_k^2$$

Note that clearly $s_1^2, s_2^2, ..., s_k^2$ are pairwise coprime. So by CRT, we can find a unique solution x_0 for x such that $0 < x_0 \leq s_1^2 s_2^2 ... s_k^2$. Pick $n = x_0$. Then by **Proposition 5.3 (1)**, we have that

$$n + 1 \equiv s_1 \mod s_1^2 \implies n + 1 \equiv s_1 \equiv 0 \mod s_1$$

$$n + 2 \equiv s_2 \mod s_2^2 \implies n + 2 \equiv s_2 \equiv 0 \mod s_2$$

$$...$$

$$n + k \equiv s_k \mod s_k^2 \implies n + k \equiv s_k \equiv 0 \mod s_k$$

So each $n+i$ for $i \in \{1, 2, ..., k\}$ is divisible by s_i but not divisible by s_i^2. So $\exp_{s_i}(n+i) = 1$. Recall that s_i has form $4k+3$, so there exists a prime divisor of form $4k+3$ in the prime factorization of each $n+i$ with an odd exponent. Therefore by **Theorem 13.4**, we have that none of $n+1, n+2, ..., n+k$ can be represented by some a^2+b^2 for $a, b \in \mathbf{Z}$ as desired.

$\square$

4. (a) I want to evaluate

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

Proof. First, note that $\forall n \in \mathbf{N}, n! > 0$, $d(n!) > 0$, $\phi(n!) > 0$. Thus, the limit is lower bounded by 0. Next, $\forall n \in \mathbf{N}, n \geq 2$, prime factorize n into $\prod_{i=1}^{k_n} p_{(n,i)}^{r_{(n,i)}}$. for $p_{(n,i)}$ distinct primes for fixed n and $r_{(n,i)}, k_n \in \mathbf{N}$.

Note that for $i, j \in \{1, 2, ..., k_n\}$ such that $i \neq j$, $p_{(n,i)}^{r_{(n,i)}}$ and $p_{(n,j)}^{r_{(n,j)}}$ are coprime. So we obtain:

$$\lim_{n\to\infty} \frac{\prod_{i=1}^{k_n} p_{(n,i)}^{r_{(n,i)}}}{d(\prod_{i=1}^{k_n} p_{(n,i)}^{r_{(n,i)}})\cdot\phi(\prod_{i=1}^{k_n} p_{(n,i)}^{r_{(n,i)}})} = \lim_{n\to\infty} \frac{\prod_{i=1}^{k_n} p_{(n,i)}^{r_{(n,i)}}}{\prod_{i=1}^{k_n} d(p_{(n,i)}^{r_{(n,i)}})\cdot\prod_{i=1}^{k_n} \phi(p_{(n,i)}^{r_{(n,i)}})}$$

$$= \lim_{n\to\infty} \frac{\prod_{i=1}^{k_n} p_{(n,j)}^{r_{(n,j)}}}{\prod_{i=1}^{k_n} r_{(n,i)}\cdot\prod_{i=1}^{k_n} p_{(n,j)}^{r_{(n,j)}}(1-\frac{1}{p_{(n,j)}})} = \frac{1}{\prod_{i=1}^{k_n} r_{(n,i)}\cdot(1-\frac{1}{p_{(n,j)}})}$$

Since the smallest possible prime is 2:

$$\frac{1}{\prod_{i=1}^{k_n} r_{(n,i)}\cdot(1-\frac{1}{p_{(n,j)}})} \leq \frac{1}{\prod_{i=1}^{k_n} r_{(n,i)}\cdot(1/2)} = \frac{2}{\prod_{i=1}^{k_n} r_{(n,i)}}$$

<u>Claim: $\lim_{n\to\infty}\prod_{i=1}^{k_n} r_{(n,i)} = \infty$</u>

Define the sequence $(a_n) = \prod_{i=1}^{k_n} r_{(n,i)}$ (begin indexing at $n = 2$ since we cannot prime factorize 1). First, I will show that a_n is non-decreasing. Consider $a_{(n+1)}$ and a_n. Then:

$$n! = \prod_{i=1}^{k_n} p_{(n,i)}^{r_{(n,i)}}$$

$$(n+1)! = \prod_{i=1}^{k_{n+1}} p_{(n+1,i)}^{r_{(n+1,i)}}$$

$$(n+1)! = (n+1)\prod_{i=1}^{k_n} p_{(n,i)}^{r_{(n,i)}}$$

Since $n+1 > 1$, we can prime factorize $n+1 = \prod_{i=1}^{j} p_i^{r_i}$ for p_i distinct primes and $j, r_i \in \mathbf{N}$. So:

$$(n+1)! = \prod_{i=1}^{j} p_i^{r_i} \prod_{i=1}^{k_n} p_{(n,i)}^{r_{(n,i)}}$$

Notice we are simply multiply more primes, so each $r_{(n,i)}$ is not reduced. Also note that prime factorization is unique. Thus the product of the powers of primes $(n+1)!$ must be greater or equal to that of $n!$:

$$\prod_{i=1}^{k_{n+1}} r_{(n+1,i)} \geq \prod_{i=1}^{k_n} r_{(n,i)}$$

In particular,

$$a_{(n+1)} \geq a_n$$

So a_n is non-decreasing. Using this, I will show by formal definition that a_n diverges to infinity. Let some real $M > 0$. Then choose $N = 2^M \in \mathbf{N}$. Then $a_N = M$. Further, since a_n is non-decreasing, I get that for all positive integer $n > N$, $a_n \geq M$. Since M is arbitrary, this process works $\forall M > 0$. So by definition, $\lim_{n\to\infty}(a_n) = +\infty$ and thus

$$\lim_{n\to\infty} \prod_{i=1}^{k_n} r_{(n,i)} = +\infty$$

as desired. So in all:

$$0 = \lim_{n\to\infty} 0 \leq \lim_{n\to\infty} \frac{n!}{d(n!) \cdot \phi(n!)} \leq \lim_{n\to\infty} \frac{2}{\prod_{i=1}^{k_n} r_{(n,i)}} = \lim_{n\to\infty} \frac{2}{+\infty} = 0$$

Thus:

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

by Squeeze Theorem. □

(b) I want to evaluate

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

Proof. Perform the ratio test for sequences:

$$\lim_{n\to\infty} \left|\frac{(n+1)!}{2^{d((n+1)!)}} \Big/ \frac{n!}{2^{d(n!)}}\right| = \lim_{n\to\infty} \left|\frac{n+1}{2^{d((n+1)!)-d(n!)}}\right|$$

First, note that since $n! | (n+1)!$, all positive divisors of $n!$ divides $(n+1)!$ as well. To show this, let d be a positive divisor of $n!$. Then $d|n! \implies \exists k \in \mathbf{Z} : dk = n! \implies dk(n+1) = (n+1)! \implies d|(n+1)!$ as desired. Next, I will construct n positive divisors of $d((n+1)!)$ that do not divide $d(n!)$ by performing the following process for $k \in \{1, 2, ..., n\}$:

Process for each k: Consider $n! = n \cdot n-1 \cdot ... \cdot 2 \cdot 1$. Construct a positive integer c_k by replacing k by $(n+1)$ in $n!$. Then $c_k = (n+1) \cdot n \cdot ... \cdot k+1 \cdot k-1 \cdot ... \cdot 2 \cdot 1$. Then note that c_k is a positive divisor of $(n+1)!$ since $(n+1)! = c_k \cdot k$. Further, since $n+1 > k$, we have $c_k > n!$ which implies $c_k \not| n!$ since $n! \in \mathbf{N}$ (by theorem in class). Finally, note that each c_k is distinct because we are replacing a different divisor of $n!$.

In all, we have $d((n+1)!) - d(n!) \geq n$ since every positive divisor of $n!$ is a positive divisor of $(n+1)!$ and we were able to construct n distinct, positive divisors (each c_k) of $(n+1)!$ that do not divide $n!$.

Thus:

$$\lim_{n\to\infty} |\frac{n+1}{2^{d((n+1)!)-d(n!)}}| \leq \lim_{n\to\infty} |\frac{n+1}{2^n}| = \lim_{n\to\infty} \frac{n+1}{2^n} = 0$$

Since exponential functions grow much faster than linear functions (can also apply l'Hopital). This implies:

$$\lim_{n\to\infty} |\frac{(n+1)!}{2^{d((n+1)!)}} / \frac{n!}{2^{d(n!)}}| = 0$$

by Sequeeze Theorem (since absolute values are lower bounded by 0). Then:

$$\lim_{n\to\infty} |\frac{(n+1)!}{2^{d((n+1)!)}} / \frac{n!}{2^{d(n!)}}| < 1$$

Therefore by the ratio test,

$$\lim_{n\to\infty} \frac{n!}{2^{d(n!)}} = 0$$

$\square$