Math 437 Homework 2

Xander Naumenko

16/10/23

Question 1. Since $1|n\forall n$, we have that $3|n+2 \implies n \equiv 1 \mod 3$. Clearly any prime of the form $3k+1$ works and no other prime does, since for such numbers 1 is the only factor. I claim that primes of that form are the only solution for n.

Proof by contradiction, assume that $n = pa$ where $p < n$ is the smallest prime divisor of n, with $p+2|n+2$ and $a+2|n+2$. If $2|n$ then we have $\frac{n}{2}+2|n+2$, which is impossible since $\frac{n+2}{2} < \frac{n}{2}+2 < n+2$ so $p \neq 2$. Therefore $p \neq 2$. Since $a|n$, there exists an k such that $n+2 = k\left(\frac{n}{p}+2\right) \implies n(p-k) = 2p(k-1) \implies 2|(p-k)$ (since $2 \nmid n$). Also $p > k$ since the right side is positive, so $p-k > 0$. However this implies that $n \leq p(k-1) \leq p(p-2)$. However $n \geq p^2$ since p was supposedly the smallest prime factor of a composite number n, so this chain of inequalities is a contradiction and in fact n is a prime of the form $3k+1$.

Question 2. Consider the equation mod 3:

$$2^m \equiv 1 \mod 3 \implies m = 2k, k \in \mathbb{N}.$$

Now consider the same equation mod 4:

$$4^k - 3^n \equiv -3^n \equiv 3 \mod 4 \implies n = 2l, l \in \mathbb{N}.$$

But then the equation reduces to $4^k - 9^l = (2^k+3^l)(2^k-3^l) = 7$. Since 7 is prime this means that $2^k+3^l = 7$, $2^k - 3^l = 1$. Since 2^k+3^l is clearly increasing in k, l it's trivial to check the possibilities $k = 1, 2, l = 1$ and see that the only solutions correspond to $m = 4, n = 2$. $\square$

Question 3. By theorem 13.4, we know that for a number n, it is expressible as a^2+b^2 if and only if the exponent its prime factors in the form $4l+3$ is even. There are infinitely prime numbers of the form $4l+3$, as if there were finitely many of them $4k_1+3, 4k_2+3\ldots, 4k_m+3$, then we would have that $4(4k_1+3)\cdots(4k_m+3)+3$ isn't divisible by any of them but is of the form $4l+3$. It's prime factors can't be just of the form $4l+1$ as $(4l_1+1)(4l_2+1) = 4(4l_1l_2+l_1+l_2)+1$, so at least on of its prime factors wasn't included on our supposedly complete list, implying there are infinitely many.

Using the fact that there are infinitely many take $q_0, \ldots, q_{k-1}$ to be arbitrary distinct primes of the form $4l+3$. Using the chinese remainder theorem, there exists a unique solution to the following system of equations:

$$\begin{cases} x \equiv 0 & \mod q_0 \\ x \equiv -1 & \mod q_1 \\ \vdots & \\ x \equiv -k+1 & \mod q_{k-1} \end{cases}$$

up to mod $q_1 \cdots q_{k-1}$. Let $m_i = 1$ if $\exp_{q_i}(x+i) \equiv 0 \mod 2$ and $m_i = \exp_{q_i}(x+i)+1$ otherwise. I claim that the following sequence of k integers satisfies the required properties, where n ranges from 0 to $k-1$:

$$x_n = x + n + \prod_{i=0}^{k-1} q_i^{m_i}.$$

Note that the product term does not conflict with the congruence relations found above, since it is a multiple of $q_1 \cdots q_{k-1}$. Consider any individual sequence element x_n. If $\exp_{q_n}(x+n) \equiv 0 \mod 2$, then we can write $x + n = q_n^2 l$ (it can't be that $\exp_{q_n}(x_n) = 0$ since x was the solution to $x \equiv -n \mod q_n$) and $x_n = q_n(q_n l + q_0^{m_0} \cdots q_{k-1}^{m_{k-1}})$. Importantly q_n does not divide the second part of the addition but does the first, so $\exp_{q_n}(x_n) = 1$.

If instead $\exp_{q_n}(x+n) \equiv 1 \mod 2$, then we can write $x + n = q_n^{m_n} l$ for $q_n \nmid l$, and $x_n = q_n^{m_n}(l + q_n q_0^{m_0} \cdots q_{k-1}^{m_{k-1}})$. In reverse from the previous case here the first term is not divisible by l and the second is, so $\exp_{q_n}(x_n) \equiv m_n \equiv 1 \mod 2$. In either case we have that $\exp_{q_n}(x_n) \equiv 1 \mod 2$, so by theorem 13.4 none of the x_n are expressible as $a^2 + b^2$. $\square$

Question 4a. I claim that the limit is equal to 0. Writing $n! = \prod_{i=1}^r p_i^{\alpha_i}$ with $p_1 < p_2 < \ldots < p_r$, using identities proven in class we have that

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

Since $n!|(n+1)!$, each individual term in the product above only increases as n increases. Also since $\alpha_i \geq 1$ and $1 - \frac{1}{p_i} \geq \frac{1}{2}$, each individual term in the product is greater or equal to 1. Thus:

$$\frac{n!}{d(n!)\phi(n!)} \leq \frac{n!}{n! \frac{\exp_2(n!)}{2}} = \frac{2}{\exp_2(n!)} \to 0.$$

Question 4b. This limit is also 0. Applying the ratio test to $x_n = \frac{n!}{2^{d(n!)}}$:

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

Let $n! = \prod_{i=1}^r p_i^{\alpha_i}$, where $p_1 < p_2 < \ldots < p_r$. Then as we showed in class we have $d(n!) = \prod_{i=1}^r (\alpha_i + 1)$. Since $n!|(n+1)!$, if $n+1$ isn't a prime we can represent $d((n+1)!) = \prod_{i=1}^r p_i^{\alpha_i'}$, with $\alpha_i' \geq \alpha_i \forall i$ and strict inequality holding at least once. If $n+1$ is prime, then we have $d((n+1)!) = (n+1)d(n!)$. For $n \geq 2$, $n!$ is even so $p_1 = 2$, and since 2 is the smallest prime, $\alpha_1 \geq \alpha_i \forall i \in \mathbb{N}$. Therefore a lower bound for $d((n+1)!)$ regardless of whether $n+1$ is prime or not is $(\alpha_1 + 2)\prod_{i=2}^r (\alpha_i + 1)$. Applying this:

$$d((n+1)!) - d(n!) \geq \prod_{i=2}^r (\alpha_i + 1) = \#\text{ of odd divisors of } n!.$$

Consider just divisors of $n!$ of the form $3^k 5^l$ which is a subset of all odd divisors of $n!$. Based on the definition of factorial it's true that $\exp_3(n!) \geq \left\lfloor \frac{n}{3} \right\rfloor$ and $\exp_5(n!) \geq \left\lfloor \frac{n}{5} \right\rfloor$. Thus we have

$$\frac{x_{n+1}}{x_n} \leq \frac{n+1}{2^{\left\lfloor \frac{n}{3} \right\rfloor \left\lfloor \frac{n}{5} \right\rfloor}} \to 0.$$

Thus by the ratio test the limit is zero.