Math 437 Homework 2

Xander Naumenko

16/10/23

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 2:

$$4^k - 3^n \equiv -3^n \equiv 1 \mod 4 \implies n = 2l, l \in \mathbb{N}.$$

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 $4k_1 + 3, 4k_2 + 3 \dots, 4k_m + 3$, 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 $(4l_1 + 1)(4l_2 + 1) = 4(4l_1 l_2 + l_1 + l_2) + 1$, 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 $q_0, \dots, q_{k-1}$ 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 $q_n \not| \, l$, 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 $a^2 + b^2$. $\square$