MATH 220 — Assignment 6

Stephanie Knill
54882113
Due: February 25, 2016

Question 1

Proposition: $\sqrt{6}$ is irrational.

Proof. Assume that $\sqrt{6}$ is rational. Then there exists natural numbers a and b such that

$$\sqrt{6} = \frac{a}{b}$$

Then by the axiom of natural numbers, we can take a pair (a, b) with smallest b (i.e. a and b have no common factors). So we have

$$\begin{aligned} \sqrt{6} \cdot b &= a \\ 6b^2 &= a^2 \\ 2(3b^2) &= a^2 \end{aligned}$$

This means that a^2 is even if and only if a is even (proof done in class). Since a is even, then there exist a natural number k such that $a = 2k$. Substituting this back gives us

$$\begin{aligned} 6b^2 &= (2k)^2 \\ 6b^2 &= 4k^2 \\ 3b^2 &= 2k^2 \end{aligned}$$

Here, $3b^2$ is even. By the properties of congruence, b^2 is also even. Since b^2 is even, then b is even. However, a and b have no common factors. If a is even, then b must be odd. Since b cannot be both even and odd, we have arrived at a contradiction. Thus our initial assumption is false and $\sqrt{6}$ is irrational. ■

Question 2

Proposition: $\sqrt{2} + \sqrt{3}$ is irrational.

Proof. Assume that $\sqrt{2} + \sqrt{3}$ is rational. Then there exists natural numbers a and b such that

$$\sqrt{2} + \sqrt{3} = \frac{a}{b}$$

Performing algebraic manipulation yields

$$\begin{aligned}
(\sqrt{2} + \sqrt{3})b &= a \\
(2 + \sqrt{6} + 3)b^2 &= a^2 \\
\sqrt{6}b + 5b^2 &= a^2 \\
\sqrt{6} &= \frac{a^2 - 5b^2}{b^2} \\
&= \frac{a^2}{b^2} - 5
\end{aligned}$$

From Question 1, we know that $\sqrt{6}$ is irrational. However, $\frac{a^2}{b^2} - 5$ is rational, thereby giving us a contradiction. Thus our initial assumption is false and $\sqrt{2} + \sqrt{3}$ is irrational. ■

Question 3

Proposition: If a, b both odd, then $a^2 + b^2$ cannot be a perfect square.

Proof. Assume that $a^2 + b^2$ is a perfect square. Then there exists an integer c such that

$$a^2 + b^2 = c^2$$

Let us partition the value of c^2 into two cases: c^2 is even and c^2 is odd.

Case 1: c^2 is even.

Since c^2 is even, then c is also even. Then there exists an integer k such that

$$\begin{aligned}
a^2 + b^2 &= (2k)^2 \\
&= 4k^2 \\
&= 2k^2 + 2k^2
\end{aligned}$$

Here we have that $a^2 = b^2 = 2k^2$. Since a^2 and b^2 are both even, then a and b are both even.

Case 2: c^2 is odd.

Since c^2 is odd, then c is also odd. Then there exists an integer q such that

$$\begin{aligned} a^2 + b^2 &= (2q+1)^2 \\ &= (4q^2) + (4q+1) \end{aligned}$$

Without loss of generality, let $a^2 = 4q^2 = 2(2q^2)$ and $b^2 = 4q + 1 = 2(2q) + 1$. Since a^2 is even, then a is even. Similarly, since b^2 is odd, then b is odd. Thus we have that either 1) a is even and b is odd, or 2) a is odd and b is even.

Combining both cases, we have that for all values of c^2, a or b is even. In other words, a and b are both *not* odd, giving us the necessary contradiction. ■

Question 4

Proposition: The number 123456782 cannot be represented as $a^2 + 3b^2$ for any integers a and b.

Proof. Assume that 123456782 can be represented as $a^2 + 3b^2$ for any integers a and b. Using long division, we find that

$$\begin{aligned} 123456782 &= a^2 + 3b^2 \\ &= 2 + 3 \cdot (41152260) \end{aligned}$$

which gives us $a^2 = 2$ and $b^2 = 4115226$. However, $a = \sqrt{2}$ which contradicts our assumption that a belongs to the set of integers. Thus our initial assumption is false, thereby proving that the number 123456782 cannot be represented as $a^2 + 3b^2$ for any integers a and b. ■

Question 5

(a) **Conjecture:** There are infinitely many primes p such that $p \equiv 3 \bmod 4$.

Proof. Assume there is a finite number of primes p such that $p \equiv 3 \bmod 4$. We will denote this set by $P' = \{p \mid p \text{ is prime and } p \equiv 3 \pmod 4\}$, which is a proper subset of the finite set of all primes $P = \{p \mid p \text{ is prime}\}$. Let $q = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ be the product of all primes that are congruent to 3 modulo 4. Consider

$$\begin{aligned} N &= 4q - 1 \\ N &= 4(q-1) + 3 \\ N - 3 &= 4(q-1) \end{aligned}$$

Then $4 \mid N - 3$ and $N \equiv 3 \bmod 4$. By the Fundamental Theorem of Arithmetic, N can be factored as a product of prime numbers. By Lemma, there exists such a prime factor k that is congruent to 3 (mod 4). Since $k \mid N$, then by our in class Lemma $k \nmid N + 1 = 4q$. So k is not in the set of all primes P, which contradicts our initial assumption. Thus there are infinitely many primes p such that $p \equiv 3 \bmod 4$. ∎

Lemma N has a prime factor congruent to 3 (mod 4).

Assume that N has no prime factors congruent to 3 (mod 4). Then all prime factors must be of the form $4m$, $4m + 1$, or $4m + 2$. However, since we are only looking for prime factors and 2 cannot be a factor (since N is odd) then we cannot be of the form $4m$ or $4m + 2$. Since all prime factors must be of the form $4m + 1$, let us express this in terms of congruence, where $p_i \equiv 1 \pmod 4$ and $p_j \equiv 1 \pmod 4$:

$$\begin{aligned} p_i \cdot p_j &\equiv 1 \cdot 1 \pmod 4 \\ &\equiv 1 \pmod 4 \end{aligned}$$

However, this contradicts the fact that N is congruent to 3 (mod 4). Thus, N has a prime factor congruent to 3 (mod 4).

(b) To prove that there are infinitely many primes congruent to 1 modulo 4, we would instead consider $N = 4q + 1$. However, when we arrive at our Lemma, the proof will break down as N does not have to have a prime factor congruent to 1 (mod 4).

Question 6

Find the last digit of the number 2016^{2016}.

Breaking the number 2016 into its prime factors allows us to re-express it as

$$2016 = 2^5 \cdot 3^2 \cdot 7 = 2^3 \cdot (2 \cdot 3) \cdot (2 \cdot 3 \cdot 7) = 2^3 \cdot 6 \cdot 42$$

Similarly, 2016^{2016} can be expressed as

$$2016^{2016} = (2^3 \cdot 6 \cdot 42)^{2016} = (2^3)^{2016} \cdot (6)^{2016} \cdot (42)^{2016}$$

To find the last digit, let us find the congruence of each product to modulo 10. Using the power of 2 method, $(2^3)^{2016}$ can be reduced to

$$\begin{aligned}
(2^3)^{2016} &\equiv (2^5)^{1209} \cdot 2^3 \equiv 2^{1209} \cdot 2^3 \pmod{10} \\
&\equiv 2^{1212} \equiv (2^5)^{242} \cdot 2^2 \equiv 2^{242} \cdot 2^2 \pmod{10} \\
&\equiv 2^{244} \equiv (2^5)^{48} \cdot 2^4 \equiv 2^{48} \cdot 2^4 \pmod{10} \\
&\equiv 2^{52} \equiv (2^5)^{10} \cdot 2^2 \equiv 2^{10} \cdot 2^2 \pmod{10} \\
&\equiv 2^{12} \equiv (2^5)^2 \cdot 2^2 \equiv 2^2 \cdot 2^2 \pmod{10} \\
&\equiv 2^4 \pmod{10} \\
&\equiv 16 \pmod{10} \\
&\equiv 6 \pmod{10}
\end{aligned}$$

Using the power of 6 method, we can reduce $(6)^{2016}$ to

$$6^{2016} \equiv 6 \pmod{10}$$

Again using the power of 2 method, we have that

$$\begin{aligned}
(42)^{2016} &\equiv 2^{2016} \pmod{10} \\
&\equiv (2^5)^{403} \cdot 2^1 \equiv 2^{403} \cdot 2^1 \pmod{10} \\
&\equiv 2^{404} \equiv (2^5)^{80} \cdot 2^4 \equiv 2^{80} \cdot 2^4 \pmod{10} \\
&\equiv 2^{84} \equiv (2^5)^{16} \cdot 2^4 \equiv 2^{16} \cdot 2^4 \pmod{10} \\
&\equiv 2^{20} \equiv (2^5)^4 \pmod{10} \\
&\equiv 2^4 \pmod{10} \\
&\equiv 6 \pmod{10}
\end{aligned}$$

Combining we have

$$\begin{aligned} 2016^{2016} = (2^3)^{2016} \cdot (6)^{2016} \cdot (42)^{2016} &\equiv 6 \cdot 6 \cdot 6 \pmod{10} \\ &\equiv 6^3 \pmod{10} \\ &\equiv 6 \pmod{10} \end{aligned}$$

Thus the last digit of 2016^{2016} is 6.

Question 7

(a) If x and y are both irrational, then $x + y$ is irrational.

Proof. Since $\sqrt{2} - \sqrt{2} = 0$, which is a rational sum, then $x = \sqrt{2}$ and $y = -\sqrt{2}$ is a counterexample. ■

(b) If x and y are both irrational, then xy is irrational.

Proof. Since $\sqrt{2} \cdot \sqrt{2} = 2$, which is a rational product, then $x = y = \sqrt{2}$ is a counterexample. ■

(c) If x is rational and y is irrational, then xy is irrational.

Proof. Since $0 \cdot y = 0$, which is a rational product, then $x = 0$ and y any irrational number is a counterexample. ■

(d) If $x \neq 0$ is rational and y is irrational, then xy is irrational.

Proof. Assume, to the contrary, that there exists a rational x and an irrational y whose product xy is rational. Then there exists integers a, b, c, d where $b, c, d \neq 0$, such that $xy = \frac{a}{b}$ and $x = \frac{c}{d}$. This implies that

$$\begin{aligned} xy &= \frac{a}{b} \\ \frac{c}{d} \cdot y &= \frac{a}{b} \\ y &= \frac{ad}{bc} \end{aligned}$$

Since ad and bc are integers and $bc \neq 0$, it follows that y is rational, which is a contradiction. ■

(e) If $a, b \in \mathbb{Q}$ and $ab \neq 0$, then $a\sqrt{3} + b\sqrt{2}$ is irrational.

Proof. Assume, to the contrary, that we have rational numbers a and b where $ab \neq 0$ and $a\sqrt{3} + b\sqrt{2}$ is rational. Then there exists rational integers c and d such that

$$a\sqrt{3} + b\sqrt{2} = \frac{c}{d}$$

Squaring both sides and simplifying gives us

$$\begin{aligned}
3a^2 + 2ab\sqrt{6} + 2b^2 &= \frac{c^2}{d^2} \\
2ab\sqrt{6} &= \frac{c^2}{d^2} - 3a^2 - 2b^2 \\
2ab\sqrt{6} &= \frac{c^2 - 3a^2d^2 - 2b^2d^2}{d^2} \\
\sqrt{6} &= \frac{c^2 - 3a^2d^2 - 2b^2d^2}{2abd^2}
\end{aligned}$$

Since $c^2 - 3a^2d^2 - 2b^2d^2$ and $2abd^2$ are integers and $ab \neq 0$, it follows that $\sqrt{6}$ is rational. However, we know by Question 1 that $\sqrt{6}$ is irrational, thus giving us the necessary contradiction. ■