1. Prove that the number 123456782 cannot be represented as $a^2 + 3b^2$ for any integers a and b. (*Hint: Consider the remainder* mod 3).

Solution: First, note that $123456782 \equiv 2 \mod 3$. How did we find out? Of course, you can just try to find out what the remainder of this number mod 3 is using a calculator: try subtracting 0, 1 or 2 and dividing by 3. However, a much better way is by using Problem 5(a) from Workshop 3: this number is congruent to the sum of its digits mod 3 (make sure you understand why Problem 5(a) from the Workshop implies this; that problem says something about congruence mod 9). We have: $123456782 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 2 \mod 3$, and you do not even have to evaluate this sum, since we only care about its remainder mod 3, so you can right away eliminate everything that's divisible by 3, so $1 + 2$ disappears, 3 disappears, 6 disappears, $4 + 5$ disappears, 7 gets replaced by 1, and 8 gets replaced by 2, and finally you get 2 (make sure you understand this calculation!).

Next, observe that for any integers a, b, $a^2 + 3b^2 \equiv a^2 \mod 3$ (Why?).

Finally, let us prove a lemma: if a is an integer, then a^2 can be congruent to 1 or 0 mod 3. Proof of this lemma is by cases: the possibilities are, $a \equiv 0 \mod 3$, $a \equiv 1 \mod 3$, $a \equiv 2 \mod 3$. In the first case, $a^2 \equiv 0^2 = 0 \mod 3$, in the second case $a^2 \equiv 1^1 = 1 \mod 3$; in the third case, $a^2 \equiv 2^2 \equiv 1 \mod 3$, and the lemma is proved.

Now we can complete the proof of our original statement by contradiction. Suppose there existed a, b such that $123456782 = a^2 + 3b^2$. Then we would have: $123456782 \equiv a^2 \mod 3$, but by the Lemma, a^2 can be congruent only to 0 or 1 mod 3,and our number is congruent to 2 mod 3, and we arrive at a contradiction.

2. (a) Prove that there are infinitely many primes p such that $p \equiv 3 \mod 4$. *Hint: try to proceed the same way as in Euclid's proof of the statement that there are infinitely many prime numbers; but instead of making the number* $N = p_1, \ldots p_n + 1$, *make a number* N *that is definitely congruent to* 3 *modulo* 4 *(and that still differs by* 1 *from a number that is divisible by all of* $p_1, \ldots p_k$*).*

   (b) Could this proof have worked for the primes congruent to 1 modulo 4?

Solution: Suppose, to the contrary, there were only finitely many prime numbers of the form $4k + 3$. Let us denote them by $p_1, \ldots, p_n$. Let $N = 4p_1 \ldots p_n - 1$. If N is prime, we get a contradiction, since N is bigger than all the p_i, $i = 1, \ldots, n$, and therefore N is not one of these numbers, on the other hand, $N \equiv 3 \mod 4$, and thus N would be a prime number of the form $4k + 3$ that is not on our list. Then N has to be a product of prime numbers, by the Fundamental Theorem of Arithmetic (which we have not yet proved, but we agreed we can use). Note that $p_i | (N + 1)$, so p_i cannot divide N, for all $i = 1, \ldots, n$. Note also that N is odd, so 2 is not on the list of prime factors of N; all the prime numbers that are not equal to 2 are odd, so they have to be either congruent to 1 or 3 mod 4. Then all the prime factors of N have to be congruent to 1 mod 4, since we are assuming that the numbers p_i are *all* the prime numbers that are congruent to 3 mod 4, and none of them can be among

the factors of N. Then we get that N is a product of several factors, each congruent to 1 mod 4. But then N itself has to be congruent to 1 mod 4 (since we know that we can multiply congruences) – a contradiction.

Part (b). Note that if we tried to make a similar proof for the fact that there are infinitely many primes congruent to 1 mod 4, it would not work: if we made some number N, and tried to prove that all its factors cannot be congruent to 3 mod 4, we would not be able to do that, because the product of two numbers congruent to 3 mod 4 is a number that is congruent to 1 mod 4 (so all we would get is that there has to be an even number of factors of the form $4k+3$, and we would not be able to obtain a contradiction with our assumption this way).

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

Solution: It is 6. Indeed, note that the last digit is the remainder of a number mod 10. We have: $2016 \equiv 6 \mod 10$, wo $2016^{2016} \equiv 6^{2016} \mod 10$ by the properties of congruence proved in class. Then: $6^2 \equiv 6 \mod 10$, then

$$6^{2016} = (6^2)^{1008} \equiv 6^{1008} \equiv 6^{504} \equiv 6^{252} \equiv 6^{126} \equiv 6^{63} \mod 10.$$

Now, using the same idea, $6^{63} = 6 \cdot 6^{62} \equiv 6 \cdot 6^{31} \equiv 36 \cdot 6^{30} \equiv 6 \cdot 6^{15} \mod 10$, and so on – you can keep reducing the power until you just get 6 itself.

4. Prove that there do not exist integers a, b and c such that

$$12345678910111213 = a^2 + 25b^2 + 5c^2.$$

Solution: The key to this question is to consider congruence mod 5. Since 5 and 25 are divisible by 5, the right-hand side is congruent to $a^2 \mod 5$. The left-hand side is congruent to its last digit mod 5, which is 3.

Now we can do proof by contradiction: suppose such a, b, c exist. Then we would have that $a^2 \equiv 3 \mod 5$. The Lemma below shows that this is a contradiction.

Lemma. If a is an integer, then a^2 is congruent to 0, 1, or 4 mod 5.

Proof. Proof of Lemma: By cases.

Case 1: $a \equiv 0 \mod 5$. Then $a^2 \equiv 0^2 = 0 \mod 5$.

Case 2: $a \equiv 1 \mod 5$. Then $a^2 \equiv 1^2 = 1 \mod 5$.

Case 3: $a \equiv 2 \mod 5$. Then $a^2 \equiv 2^2 = 4 \mod 5$.

Case 4: $a \equiv 3 \mod 5$. Then $a^2 \equiv 3^2 \equiv 4 \mod 5$.

Case 5: $a \equiv 4 \mod 5$. Then $a^2 \equiv 4^2 \equiv 1 \mod 5$. □

5. Suppose that the following three statements are true:

   1. Rainbows are colourful.
   2. If it isn't sparkly, then it must be extravagant.
   3. Colourful things are never extravagant.

   What can you conclude about rainbows?

Solution:

Combining statements 1 and 3 we see that since rainbows are colourful and colourful things are never extravagant we must have that rainbows are never extravagant. Reinterpreting statement 2 by its contrapositive we learn that if something is not extravagant then it must be sparkly. Therefore, rainbows are also sparkly!

6. Consider the statement (implication):

   If Bill takes Sam to the concert, then Sam will take Bill to dinner.

   Which of the following implies that this statement is true:

   (a) Sam takes Bill to dinner only if Bill takes Sam to the concert.
   (b) Either Bill doesn't take Sam to the concert or Sam takes Bill to dinner.
   (c) Bill takes Sam to the concert.
   (d) Bill takes Sam to the concert and Sam takes Bill to dinner.
   (e) Bill takes Sam to the concert and Sam doesn't take Bill to dinner.
   (f) The concert is canceled.
   (g) Sam doesn't attend the concert.

Solution: Let P be the statement "Bill takes Sam to the concert", and Q be the statement "Sam takes Bill to dinner". Then the original statement is the implication $P \Rightarrow Q$. Now we need to analyze which statements on the list imply that this implication is true.

We will write "Yes" when the statement in question implies that $P \Rightarrow Q$ is true, and "No" otherwise.

(a) Sam takes Bill to dinner only if Bill takes Sam to the concert.

This is saying P is *required* for Q, which is, $\sim P \Rightarrow \sim Q$, which is the contrapositive of $Q \Rightarrow P$ (and thus logically equivalent to $Q \Rightarrow P$), which is the *converse* of our statement and implies nothing about it. (That is, even if Sam is determined not to take Bill to dinner unless Bill takes him to the concert, this says nothing about whether Bill will actually take Sam to the concert). So here the answer is "No".

(b) Either Bill doesn't take Sam to the concert or Sam takes Bill to dinner.

This is saying, $\sim P \vee Q$, which is equivalent to $P \Rightarrow Q$, so the answer is "Yes".

(c) Bill takes Sam to the concert.

This just says P is true without saying anything about Q, so this says nothing about whether the implication $P \Rightarrow Q$ is true, and so the answer is "No".

(d) Bill takes Sam to the concert and Sam takes Bill to dinner.

This says, P is True and Q is True, which makes the implication True, so the answer is "Yes".

(e) Bill takes Sam to the concert and Sam doesn't take Bill to dinner.

This says, P is True and Q is False, which makes the implication False, so the answer is "No".

(f) The concert is canceled.

This says P is False; regardless of Q then, the implication is True, so the answer is"Yes".

(g) Sam doesn't attend the concert. Same as above: this says P is False; regardless of Q then, the implication is True, so the answer is"Yes".

7. Consider the statement: *The fish are biting and there are no bugs, or the fish are not biting and there are bugs, or it is winter.* Write out the negation of the above in English. You should simplify your answer as much as possible, being sure of course that it is logically equivalent to the negation. Justify your answer.

Solution: P: the fish are biting; B: there are bugs; W: it is winter.
So we want $\neg\Big((P\wedge\neg B)\vee(\neg P\wedge B)\vee W\Big)$. Using a double application of De Morgan's laws this is logically equivalent to

$$\begin{aligned}&(\neg(P\wedge\neg B))\wedge(\neg(\neg P\wedge B))\wedge\neg W\\ &\equiv((\neg P)\vee B)\wedge(P\vee(\neg B))\wedge\neg W. \qquad (1)\end{aligned}$$

This answer is not bad but one can simplify further using the distributive laws. A double application of the distributive laws given in the text (we did this version in class in Sec. 201) shows that

$$(R\vee S)\wedge(T\vee U)\equiv(R\wedge T)\vee(R\wedge U)\vee(S\wedge T)\vee(S\wedge U).$$

Use this in (4), noting that $P\wedge\neg P$ and $B\wedge\neg B$ are always F to see that (4) is

logically equivalent to

$$\Big(F \vee (\neg P \wedge \neg B) \vee (B \wedge P) \vee F\Big) \wedge (\neg W)$$
$$\equiv \Big((\neg P \wedge \neg B) \vee (B \wedge P)\Big) \wedge (\neg W)$$
$$\equiv (\neg P \wedge \neg B \wedge \neg W) \vee (P \wedge B \wedge \neg W).$$

This reads: the fish are not biting and there are no bugs and it is not winter, or the fish are biting and there are bugs and it is not winter.

8. Let $P(x)$ and $Q(x)$ be open sentences where the domain of the variable x is a set S. Which of the following implies that $\sim P(x) \Rightarrow Q(x)$ is false for some $x \in S$?

   (a) $P(x) \wedge Q(x)$ is false for all $x \in S$.

   (b) $P(x)$ is true for all $x \in S$.

   (c) $Q(x)$ is true for all $x \in S$.

   (d) $P(x) \vee Q(x)$ is false for all $x \in S$.

Solution: First, let R be the statement "$\sim P(x) \Rightarrow Q(x)$ is false for some $x \in S$". We need to simplify R before we can proceed. First, recall that $P \Rightarrow Q \equiv \ \sim P \vee Q$; then $\sim P \Rightarrow Q \equiv \ P \vee Q$. Note that R says:

$$\exists x \in S \text{ s.t. } \ \sim (\sim P(x) \Rightarrow Q(x)).$$

The statement R contains the negation of an implication, and replacing it by its equivalent as discussed above, we get they R is logically equivalent to:

$$\exists x \in S \text{ s.t. } \ \sim (P(x) \vee Q(x)) \ \equiv \ \exists x \in S \text{ s.t. } (\sim P(x)) \wedge (\sim Q(x)).$$

Now, we are asked which of the listed statements imply R. We get:

(a) "$P(x) \wedge Q(x)$ is false for all $x \in S$."

This says: $\forall x \in S \ \sim (P(x) \wedge Q(x))$, which is equivalent to $\forall x \in S (\sim P(x)) \vee (\sim Q(x))$, which does not imply R.

To see this, we just need to give a counterexample: an example of open sentences $P(x)$ and $Q(x)$ and a set S such that "$\forall x \in S (\sim P(x)) \vee (\sim Q(x))$" is True, but "$\exists x \in S$ s.t. $(\sim P(x)) \wedge (\sim Q(x))$" is False. Consider, for example, $S = \{1, 2, 3\}$, and $P(x) : x \neq 1$, $Q(x) : x \notin \{2, 3\}$. Then for all $x \in S$, $(\sim P(x)) \vee (\sim Q(x))$ says that $x = 1$ or $x \in \{2, 3\}$, which is true. At the same time, $(\sim P(x)) \wedge (\sim Q(x))$ says $x = 1$ and $x \in \{2, 3\}$, which is false for all x.

(b) $P(x)$ is true for all $x \in S$.

This says, $\forall x \in S\ P(x)$. This actually makes R false, so it does not imply R (it implies $\sim R$, in fact).

(c) $Q(x)$ is true for all $x \in S$. This also implies $\sim R$, so does not imply R.

(d) $P(x) \vee Q(x)$ is false for all $x \in S$. This says: "$\forall x \in S, \sim (P(x) \vee Q(x))$", which is logically equivalent to "$\forall x \in S$ s.t. $(\sim P(x)) \wedge (\sim Q(x))$", which, in particular, implies that $\exists x \in S$ s.t. $(\sim P(x)) \wedge (\sim Q(x))$, so this statement does imply R.

9. Suppose you have the following information about the population of the planet QE220:

   - Among the inhabitants of QE220 who can watch TV, not all have antennae on their head.
   - The inhabitants of QE220 that are green and do not have antennae, cannot watch TV.

   Does it follow that not all the inhabitants of QE220 that can watch TV are green? Justify your answer.
   Hint. Start by writing down the statement you are asked about.

Solution: Let Q be the universal set – the set of all inhabitants of QE220. Let A be the set of those who have antennae, let G be the set of those who are green, and let TV be the set of those who can watch TV. The the question is asking, is it true that $TV - G$ is not empty?

We are given: $TV - A \neq \varnothing$, and $(G - A) \cap TV = \varnothing$. Let $b \in TV - A$ – such an element b exists by the first condition. (In words, this says that there is an alien on QE220 who can watch TV but has no antenna. Let us call him Billy.) We claim that Billy cannot be green. Indeed, by the second statement, since Billy can watch TV, he has to either not be green, or have an antenna. But we know that he does not have an antenna, so he has to be not green. So the set of QE220-iers who can watch TV but are not green contains Billy, and thus this set is not empty.

This is how some mathematicians might write the same solution: (Check for yourself that these solutions are in fact equivalent solutions, just stated differently). Let Q be the set of inhabitants of QE220. Introduce the following open statements: $G(x) : x$ is green; $A(x) : x$ has antennae; $TV(x) : x$ can watch TV.
The statement we are asked about is:

$$\sim (\forall x \in Q\ TV(x) \Rightarrow G(x)). \tag{2}$$

We claim this is true. To prove this we can show the logically equivalent (recall $\sim (P \Rightarrow Q) \equiv P \wedge \sim Q$):

$$\exists x \in Q\, s.t.\ TV(x) \wedge \sim G(x). \tag{3}$$

The second given bit of information is that

$$\forall x \in Q\ G(x) \wedge \sim A(x) \Rightarrow\ \sim TV(x),$$

or equivalently (using the contrapositive),

$$\forall x \in Q\ TV(x) \Rightarrow\ \sim G(x) \vee A(x). \tag{4}$$

So lets prove the existence of an inhabitant who can watch TV and is not green, as is required in (3). By the first bit of given information there is an $x_0 \in Q$ who can watch TV and does not have an antenna. By (4), either x_0 is not green or has an antenna. The latter is impossible by our choice of x_0, so x_0 cannot be green. Therefore x_0 is the required inhabitant who can watch TV and is not green. We have verified (3) and are done. □