1. Let E be the set of all positive even numbers: $E = \{2, 4, 6, 8, 10, \ldots\}$. We can define divisibility in E: we say n is divisible by k if there is some q in E for which $n = kq$. For example, 40 is divisible by 10 since $40 = 10 \cdot 4$. However, 30 is not divisible by 10 in E. We say p is a prime in E if p has no divisors. For example, 2 and 30 are primes in E.

   (a) Find all primes in E with $p \leq 50$.

   Solution: I could just as easily have asked for all primes in E. The primes in E are all the numbers not divisible by 4. That is, all numbers which are twice an odd number. The reason, if $n = km$, with k and m in E, then both k and m are even, so their product is divisible by 4. The list of primes to 50: 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50.

   (b) Give an example to show that E does not have unique factorization.

   Solution: The smallest example is $36 = 2 \times 18$ and $36 = 6 \times 6$, so 36 does not factor uniquely into primes. More generally, one can take any (ordinary) integer with at least two odd prime divisors and get an example. For example, from $15 = 3 \times 5$ we can derive $60 = 2 \times 30$ and $60 = 6 \times 10$.

2. Prove that $\sqrt{5}$ is irrational:

   (a) using the Fundamental Theorem of Arithmetic

   Solution: If $\sqrt{3}$ were rational, then there would be positive integers m and n with $\sqrt{5} = \dfrac{m}{n}$ so $m^2 = 5n^2$. We compare the prime factorizations of each side, looking specifically at the prime 5. If m is exactly divisible by 5^a, then m^2 is divisible by exactly 5^{2a}. If n is exactly divisible by 5^b then $5n^2$ is exactly divisible by 5^{2b+1}. Thus, the power of 5 dividing m^2 is even, but the power of 5 dividing $5n^2$ is odd. Since these are supposed to be the same positive integer, this contradicts the Fundamental Theorem.

   (b) using a proof by Infinite Descent.

   Solution: If $\sqrt{5}$ is rational, then there is some positive integer, n, for which $n\sqrt{5}$ is an integer. For a proof by infinite descent, we need to construct a positive integer m satisfying $m < n$ for which $m\sqrt{5}$ is an integer. Such an m is given by $m = n\sqrt{5} - 2n$. To check, since $2 < \sqrt{5} < 3$, $2n < n\sqrt{5} < 3n$, so $0 < n\sqrt{5} - 2n < n$, or $0 < m < n$. The first inequality shows that m is positive. Next, $m\sqrt{5} = (n\sqrt{5} - 2n)\sqrt{5} = 5n - n\sqrt{5}$, and since $n\sqrt{5}$ is an integer, so is $m\sqrt{5}$. By infinite descent, there can be no such n, so $\sqrt{5}$ is irrational.

3. Prove that $\sqrt{500}$ is irrational:

   (a) using the Fundamental Theorem of Arithmetic

   Solution: First factor 500: $500 = 2^2 3^3$. It will be the prime 5 that causes a problem. If $\sqrt{500}$ were rational, then there would be positive integers m and n with $\sqrt{500} = \frac{m}{n}$ so $m^2 = 500n^2$. If m is exactly divisible by 5^a, then m^2 is divisible by exactly 5^{2a}. If n is exactly divisible by 5^b then $500n^2$ is exactly divisible by 5^{2b+3}. Thus, the power of 5 dividing m^2 is even, but the power of 5 dividing $500n^2$ is odd. Since these are supposed to be the same positive integer, this contradicts the Fundamental Theorem.

   (b) using a proof by Infinite Descent.

   Solution: If $\sqrt{500}$ is rational, then for some positive integer, n, $n\sqrt{500}$ will be an integer. Again, we need a positive integer m with $m < n$, $m\sqrt{500}$ an integer. We use $m = n\sqrt{500} - 22n$, where 22 was picked because $\lfloor\sqrt{500}\rfloor = 22$. Since $22 < \sqrt{500} < 23$, $0 < \sqrt{500} - 22 < 1$, so $0 < m < n$. Next, $m\sqrt{500} = (n\sqrt{500} - 22n)\sqrt{500} = 500n - 22n\sqrt{500}$, and this is an integer since both $500n$ and $22n\sqrt{500}$ are integers. Thus, m is a smaller positive integer with n's property, so by infinite descent, no such n can exist.

4. Prove that $\sqrt[3]{2}$ is irrational:

   (a) using the Fundamental Theorem of Arithmetic

   Solution: If $\sqrt[3]{2}$ were rational, then there would be positive integers m and n with $\sqrt[3]{2} = \frac{m}{n}$ so $m^3 = 2n^3$. If m is exactly divisible by 2^a, then m^3 is divisible by exactly 2^{3a}. If n is exactly divisible by 2^b then $2n^3$ is exactly divisible by 2^{3b+1}. Thus, the power of 2 dividing m^3 is divisible by 3, but the power of 2 dividing $2n^3$ is not divisible by 3. Since these are supposed to be the same positive integer, this contradicts the Fundamental Theorem.

   (b) using a proof by Infinite Descent.

   Solution: Suppose that $\sqrt[3]{2}$ is rational. Then there is a positive integer, n, for which $n\sqrt[3]{2}$ and $n\sqrt[3]{4}$ are both integers ($(\sqrt[3]{2})^2$ being $\sqrt[3]{4}$). Since $1 < \sqrt[3]{2} < 2$, define $m = n\sqrt[3]{2} - n = n(\sqrt[3]{2} - 1)$. Then $0 < \sqrt[3]{2} - 1 < 1 \to 0 < m < n$. Also, by construction, m is an integer. Thus, m is a positive integer strictly smaller than n. We must check that m has **both** n's properties. We have $m\sqrt[3]{2} = n\sqrt[3]{4} - n\sqrt[3]{2}$ is an integer since $n\sqrt[3]{4}$ and $n\sqrt[3]{2}$ both are, and $m\sqrt[3]{4} = 2n - n\sqrt[3]{4}$ is also an integer. Thus, m DOES have n's properties, setting up an infinite descent, which proves no such n can exist.

5. Prove that $\log_{10} 2$ is irrational. Hint: If $\log_{10} 2$ is rational, then there would be positive integers m and n for which $\log_{10} 2 = \frac{m}{n}$. Clear fractions, exponentiate, and use unique factorization to get a contradiction.

> **Solution:** Following the hint, if $\log_{10} 2$ were rational, then there would be positive integers m and n for which $\log_{10} 2 = \frac{m}{n}$, or $n \log_{10} 2 = m$. Exponentiating gives $10^m = 10^{n \log_{10} 2} = 2^n$. This means that $2^n = 2^m 5^m$, so by unique factorization, $m = n$ and $m = 0$, so $m = n = 0$. However, this is not possible since n is the denominator of a rational number.

6. In general $ax^2 + by^2 = cz^2$ has either infinitely many **primitive** solutions or no solutions other than (0, 0, 0).

   (a) Show that $x^2 + 2y^2 = 3z^2$ has infinitely many primitive solutions. You don't have to find them all, but make sure your argument is ok. I used

$$(x + y\sqrt{-2})(x - y\sqrt{-2}) = (1 + \sqrt{-2})(1 - \sqrt{-2})z^2.$$

> **Solution:** Using the idea above, we can write $z^2 = \dfrac{x + y\sqrt{-2}}{1 + \sqrt{-2}} \dfrac{x - y\sqrt{-2}}{1 - \sqrt{-2}}$, and look for solutions in which each factor is a square. If we write
>
> $$\frac{x + y\sqrt{-2}}{1 + \sqrt{-2}} = (p + q\sqrt{-2})^2 = p^2 - 2q^2 + 2pq\sqrt{-2}, \quad \text{then}$$
>
> $$x+y\sqrt{-2} = (1+\sqrt{-2})(p^2-2q^2+2pq\sqrt{-2}) = p^2-2q^2-4pq+(p^2-2q^2+2pq)\sqrt{-2},$$
>
> so if we are careful we should be able to let $x = p^2-4pq-2q^2,\ y = p^2+2pq-2q^2$. We don't need all solutions so it probably does not hurt to set $q = 1$, giving $x = p^2 - 4p - 2,\ y = p^2 + 2p - 2$. A calculation gives $z = p^2 + 2$. What is left is to show that there are infinitely many values of p for which these three are linearly independent.
>
> What I do now is to let d be a common divisor of x, y, z, and see what I can do to force $d = 1$. If d is a divisor of x, y, z, then it is a divisor of any combination of them. Let's use $z = p^2 + 2$ to get rid of the p^2 terms in x and y: $z-x = 4p+4$, $y-z = 2p-4$. Next, eliminate p from these: $(z-x)-2(y-z) = 12$. This means any common divisor of x, y, z must also be a divisor of 12. If we pick p so x, y, z are not divisible by either 2 or 3, then this will force $d = 1$. We eliminate 2 by making z odd, which we can do by making p odd. To ensure z, say, is not divisible by 3, we pick p so that p^2+2 is not divisible by 3. This is the case p is

divisible by 3. So one solution might be $(x, y, z) = (|p^2-4p-p|, p^2+2p-2, p^2+2)$ where p is odd and divisible by 3. There are lots of other possibilities.

This is overkill, but to get an actual family, we could say $p = 6k+3$. In this case, p is odd and divisible by 3. The result: $(36k^2+12k-5,\ 36k^2+48k+13,\ 36k^2+36k+11)$ will be a primitive triple satisfying $x^2+2y^2 = 3z^2$ for all positive integers k. As a check, the very first one like this is (43, 97, 83), and $43^2 + 2 \times 97^2 = 1849 + 2 \times 9409 = 20667 = 3 \times 6889 = 3 \times 83^2$.

(b) Show that $x^2 + 3y^2 = 2z^2$ has no solutions other than (0, 0, 0).

Solution: One proof here is similar to a proof I gave in the notes and in class: Since 3 divides $3y^2$ it must be that 3 divides $2z^2 - x^2$. Now a square divided by 3 leaves a remainder of 0 or 1, so $2z^2 = 3q_1 + r_1$ where r_1 is 0 or 2 and $x^2 = 3q_2 + r_2$ where r_2 is 0 or 1. This means $2z^2 - x^2 = 3(q_1 - q_2) + (r_1 - r_2)$, and $r_1 - r_2$ must be divisible by 3. The only combination that works is for r_1 and r_2 to both be 0, so x and z must each be divisible by 3. Writing $x = 3x_1$, $z = 3z_1$, we have $3y^2 = 2z^2 - x^2 = 9(2z_1^2 - x_1^2)$ so $y^2 = 3(2z_1^2 - x_1^2)$ forcing y to be divisible by 3 as well. Writing $y = 3y_1$, we get $9x_1^2 + 27y_1^2 = 18z_1^2$, or $x_1^2 + 3y_1^2 = 2z_1^2$. Thus, if (x, y, z) is a solution to $x^2 + 3y^2 = 2z^2$, then x, y, and z are all divisible by 3, and $(x/3, y/3, z/3)$ gives a smaller triple. This gives an infinite descent, proving no (x, y, z) exist except (0, 0, 0).

(c) To which category does $x^2 + y^2 = 7z^2$ belong?

Solution: The only integer solution to $x^2 + y^2 = 7z^2$ is (0, 0, 0). To see this, calculate the remainders when a square is divided by 7. Writing $n = 7k+r$, $n^2 = 49k^2+14kr+r^2 = 7(7k^2+2kr)+r^2$. This means the remainder when n^2 is divided by 7 is the same as the remainder when r^2 is divided by 7. These remainders are 0, 1, 4, 2, 2, 4, 1, for $r = 0, 1, 2, 3, 4, 5, 6$, respectively. If $x^2 + y^2 = 7z^2$ then $x^2 + y^2$ must be divisible by 7. But the only combination of remainders which is divisible by 7 is 0 and 0, so we need both x and y to be divisible by 7. This means $x^2 + y^2$ is divisible by 7^2 so z must also be divisible by 7. Again, it is an easy check that if (x, y, z) satisfies $x^2 + y^2 = 7z^2$ then so does $(x/7, y/7, z/7)$, setting up an infinite descent if there is a nonzero solution.

For extra credit:

7. With regard to problem 6, determine (with proof) which category each of the following are in.

   (a) $x^2 + 2y^2 = 5z^2$

   Solution: If $n = 5k+r$ then $n^2 = 5(5k^2+2kr)+r^2$, so n^2 and r^2 have the same remainder when divided by 5. Checking $r = 0, 1, 2, 3, 4$ gives possible remainders of 0, 1, 4, 4, 1. This means that if we divide $x^2 + 2y^2$ by 5, the remainder will be the same as the remainder of 0, 1 or 4 added to 0, 2 or 3. The 9 sums are 0, 1, 4, 2, 3, 6, 3, 4, 7. This shows that the only way to get a remainder of 0 for x^2+2y^2 is if both x and y are divisible by 5, which would force z to be divisible by 7. This would allow for an infinite descent so this equation has no positive integer solutions.

   (b) $2x^2 + 3y^2 = 7z^2$

   Solution: There are no positive solutions, with divisibility by 3 as the trick: When $2x^2$ is divided by 3, the possible remainders are 0 and 2 When $7z^2$ is divided by 3, the possible remainders are 0 and 1. But the remainder has to be the same on both sides, which means x and z must both be divisible by 3, which will force y to also be divisible by 3. We can now give an infinite descent proof that no positive solutions exist.

8. Prove the statement in problem 6 for equations of the form $x^2 + y^2 = kz^2$. That is, for equations of this form, prove that there are either no solutions, or infinitely many primitive solutions. As a hint, what you need is the following: if there is even one nonzero solution, then there should be infinitely many primitive ones. You don't have to find a formula for a solution to know one exists. The geometric approach is quite powerful here.

Solution: If there is even a single solution (a, b, c) to $x^2 + y^2 = kz^2$ then there is a rational point $\left(\frac{a}{c}, \frac{b}{c}\right)$ on the circle $x^2 + y^2 = k$. Given this point, we can find all lines through this point with rational slope, and they must intersect the circle in another rational point. The reason for this: the line will have the form $y = mx + j$ where m and j are rational, so $x^2 + (mx+j)^2 = k$ will give a quadratic with rational coefficients. Since this has one rational solution, $x = \frac{a}{c}$, the other solution must be rational as well.

This means that the circle has infinitely many rational points, and in particular, infinitely many in the first quadrant. Each rational point (x, y) converts to a triple (a, b, c) by letting c be the least common denominator of x and y, and $a = cx,\ b = cy$. If necessary, divide by any common factors so that (a, b, c) is primitive. We have one last question: Can two different points on the circle convert to the same primitive solution? The answer is no: If (a, b, c) and (d, e, f) are primitive solutions to $x^2 + y^2 = kz^2$ then the corresponding points on the circle are $\left(\frac{a}{c}, \frac{b}{c}\right)$ and $\left(\frac{d}{f}, \frac{e}{f}\right)$. But using the Fundamental Theorem, since a, c are relatively prime and d, f are relatively prime, the only way $\frac{a}{c} = \frac{d}{f}$ is if $a = d$ and $c = f$. From this, it follows that $b = e$, giving the same primitive triple.

9. I'd love to have an easy example like problem 5, but for a trig function instead. Can you find an example where unique factorization easily shows **sin (some angle)** is irrational?