In class questions

1. (10 points) Prove that $\sqrt{12}$ is irrational:
   (a) Using the Fundamental Theorem of Arithmetic.

   **Solution:** If $\sqrt{12}$ is rational then for some positive integers $m$ and $n$, $\sqrt{12} = \frac{m}{n}$. Squaring and clearing fractions gives $m^2 = 12n^2$. We now consider the prime factorization of each side, focusing on the prime $3$. If $m = 2^{a}3^{b}5^{c}7^{d}\cdots$ then $m^2 = 2^{2a}3^{2b}5^{2c}7^{2d}\cdots$. If $n = 2^{e}3^{f}5^{g}7^{h}\cdots$ then $12n^2 = 2^{2e+2f+1}3^{2f+1}5^{2g}7^{2h}\cdots$. Thus, the exponent on $3$ for $m^2$ is an even number ($2b$), but for $12n^2$ it is an odd number ($2f+1$) and this is a contradiction.

   A way to speed up such arguments: There is another piece of notation. We say $p^k || n$ if $p^k | n$ but $p^{k+1} \nmid n$. One reads this $p^k$ exactly divides $n$. This notation only applies to primes, $p$. The way we would use this to prove irrationality, say, for $\sqrt{12}$, we might proceed as follows. Let $3^k || m$ and $3^j || n$. Then $3^{2k} || m^2$, and $3^{2j+1} || 12n^2$. By unique factorization, the exponents on $3$ must be the same, so $2k = 2j + 1$, a contradiction (a number can’t be both even and odd).

   (b) Using an argument by infinite descent.

   **Solution:** If $\sqrt{12}$ is rational then for some positive integer $n$, $n\sqrt{12}$ is an integer. Since $9 < 12 < 16$, $3 < \sqrt{12} < 4$, so $0 < \sqrt{12} - 3 < 1$, and multiplying by $n$ gives $0 < n\sqrt{12} - 3n < n$. Let $m = n\sqrt{12} - 3n$. We have shown that $0 < m < n$. Moreover, since $3n$ and $n\sqrt{12}$ are integers, so is $m$. Thus, $m$ is a smaller positive integer than $n$. But $m\sqrt{12} = 12n - 3n\sqrt{12}$, and this is an integer. This establishes an infinite descent, a contradiction. To be explicit here, the infinite descent is the following: Given any positive integer $n$ for which $n\sqrt{12}$ is an integer, there is a smaller positive integer with that same property (multiplying by $\sqrt{12}$ still gives an integer).

2. (20 points) Some greatest common divisor/diophantine equation questions.
   (a) Find the $\gcd(204, 468)$

   **Solution:**

   $\begin{align*}
   468 &= 2 \times 204 + 60, \\
   204 &= 3 \times 60 + 24, \\
   60 &= 2 \times 24 + 12,
   \end{align*}$

   and $24$ is divisible by $12$ so the greatest common divisor is $12$. 

(b) Use the Euclidean Algorithm to find integers $x, y$ with $\gcd(204, 468) = 204x + 468y$.

**Solution:** Having done one direction in part (a), we backtrack here.

\[
12 = 60 - 2 \times 24 \\
= 60 - 2(204 - 3 \times 60) \\
= 7(468 - 2 \times 204) - 2 \times 204 \\
= 7 \times 60 - 2 \times 204 \\
= 7 \times 468 - 16 \times 204.
\]

That is, $-16 \times 204 + 7 \times 468 = 12$.

(c) Find all integer solutions to $204x + 468y = 600$. In particular, find the solution with the smallest positive $x$-value.

**Solution:** I used the usual approach of multiplying the equation in part (b) by 50 to get $-800 \times 204 + 350 \times 468 = 600$. This means the general solution is $x = -800 + \frac{468}{12}k$, $y = 350 - \frac{204}{12}k$, or $x = -800 + 39k$, $y = 350 - 17k$. Picking $k = 21$ gives $x = 19$, $y = -7$, the solution with the smallest positive $x$-value.

Euler’s method would have gone as follows: $x = \frac{600 - 468y}{204} = 2 - 2y + \frac{192 - 60y}{204}$. Setting $z$ equal to the fraction and clearing denominators gives $60y + 204z = 192$. Solve for $y$, $y = \frac{192 - 204z}{60} = 3 - 3z + \frac{12 - 24z}{60}$. At some point, it just makes sense to divide numerator and denominator by 12. If we do that and set the fraction equal to $w$, we have $2z + 5w = 1$. We could iterate one more time, or just note that $w = 1, z = -2$ is a solution to this. Back substituting, $y = 3 + 6 + 1 = 10$, and $x = 2 - 20 - 2 = -20$. We have the general solution $x = -20 + 39k$, $y = 10 - 17k$, and setting $k = 1$ gives the solution with smallest $x$-value.

(d) One solution to $7x + 10y = 222$ is $x_0 = 66$, $y_0 = -24$. You need not verify this. Find all solutions where $x$ and $y$ are both positive integers.

**Solution:** Having been given one solution, the general solution is $x = 66 - 10k$, $y = -24 + 7k$. For $x$ and $y$ positive, we need $k \leq 6$ for $x$ and $k \geq 4$ for $y$. The $k$-values 4, 5, 6 give solutions $(26, 4), (16, 11), (6, 18)$. 
3. (10 points) Pythagorean triples: It is easy to find primitive Pythagorean triples \((x, y, z)\) with even \(y\). You simply write \(y = 2pq\), and look for ways to factor. For example, if \(y = 80\), then \(pq = 40\). Not all factorizations work, however, we need \(p\) and \(q\) to be relatively prime, so we could pick \(p = 8\), \(q = 5\) but not \(p = 10\), \(q = 4\).

Odd \(x\) is only slightly harder. We write \(x = p^2 - q^2 = (p + q)(p - q)\), and set \(p + q\) equal to one factor and \(p - q\) equal to another. Again, not all factorizations give primitive solutions. When \(x = 45\), the factorizations \(45 \times 1\) and \(9 \times 5\) give primitive solutions, but \(15 \times 3\) does not.

(a) Find a \textbf{primitive} Pythagorean triple \((x, y, z)\) with \(y = 100\).

\[\text{Solution:}\] If we let \(2pq = 100\), then \(pq = 50\). We need one of \(p\), \(q\) to be even, \(p > q\), and \(p\), \(q\) relatively prime. This leads to two possibilities: \(p = 50, q = 1 \rightarrow (2499, 100, 2501)\) or \(p = 25, q = 4 \rightarrow (621, 100, 629)\).

(b) Find a primitive Pythagorean triple \((x, y, z)\) with \(x = 99\).

\[\text{Solution:}\] Simplest is to note that \(p = 10\), \(q = 1\) gives \(x = 99\), so \((99, 20, 101)\) works. If we follow the hint above, we want \(99 = (p + q)(p - q)\), and the possible factorizations of \(99\) are \(99 \times 1, 33 \times 3,\) and \(11 \times 9\) (since \(p + q > p - q\) we list the larger factor first.) \(99 \times 1 \rightarrow p + q = 99, p - q = 1 \rightarrow p = 50, q = 49 \rightarrow (99, 4900, 4901)\), \(33 \times 3\) leads to \(p = 18, q = 15\), not primitive, and \(11 \times 9\) leads to \(p = 10, q = 1\), and the first solution given above.

4. (15 points) (a) Find a \textbf{primitive} solution to \(x^2 + 11y^2 = z^2\) with \(y > 1\).

\[\text{Solution:}\] What I was hoping for: From the homework, we know that \((|p^2 - kq^2|, 2pq, p^2 + kq^2)\) will give solutions to \(x^2 + ky^2 = z^2\). Here, we have \(k = 11\), so \(x = |p^2 - 11q^2|\), \(y = 2pq\), \(z = p^2 + 11q^2\) will give solutions. All we need be care of is that our solutions be primitive. In fact, \(p = 2, q = 1\) will work. It gives \(x = 7, y = 4, z = 15\), the most common solution given. If you don’t like absolute values, \(p = 4, q = 1\) will work (\(p = 3, q = 1\) would give a non-primitive solution). \(p = 4, q = 1\) leads to the solution \(x = 5, y = 8, z = 27\), also given by the class. In fact, with care, we could even have used \(p = 3, q = 1 \rightarrow x = 2, y = 6, z = 20\). This is not primitive, but if we divide by 2, we get \(x = 1, y = 3, z = 10\), which is primitive and still has \(y > 1\). Several people found this solution by inspection, along with the solution \(x = 5, y = 1, z = 6\), which does not satisfy \(y > 1\).
(b) Find a **primitive** solution (with $x, y, z$ positive) to $x^2 + y^2 = z^4$. As a big hint, 

$$(a + bi)^4 = a^4 - 6a^2b^2 + b^4 + i(4a^3b - 4ab^3).$$

**Solution:** As I mentioned in class, a way to do this problem without the hint would be to find a primitive Pythagorean triple $(x, y, z)$ where $z$ is a square. The smallest possibility is $z = 25$, for which $25 = p^2 + q^2$ has primitive solution $(p, q) = (4, 3)$ leading to triple $(7, 24, 25)$. Given this Pythagorean triple, we have that $(7, 24, 5)$ is a solution to the given problem.

If we use the hint instead, then writing $z^4 = x^2 + y^2 = (x + iy)(x - iy)$, if we set $x + iy$ equal to a fourth power, we can generate solutions. So let $x + iy = (a + bi)^4 = a^4 - 6a^2b^2 + b^4 + i(4a^3b - 4ab^3)$. This means $x = a^4 - 6a^2b^2 + b^4$, $y = 4a^3b - 4ab^3$, and $z = a^2 + b^2$. Since $y$ is even, to be primitive, we need $a^2 + b^2$ to be odd, which means one of $a, b$ is even and the other is odd. Also, if $x$ (or $y$) is negative, we can replace it with its absolute value. Picking $a = 2, b = 1$ gives $(7, 24, 5)$, $a = 3, b = 2$ would give $(119, 120, 13)$, and so on.

In class extra credit

5. With regard to problem 4a, find a **primitive** solution to $x^2 + 11y^2 = z^2$ in which $z$ is as close to 1000 as possible (at least within 50 of 1000.) I will give two points for a solution with $|z - 1000| < 50$, two more points if your solution is better than everyone else’s, and two more points if you can prove your $z$ is optimal.

**Solution:** I was disappointed that only one person gave this problem serious attention. That person had a good try, though, so I gave the person 4 points. If we just look for solutions of the form $x = \lfloor p^2 - 11q^2 \rfloor, y = 2pq, z = p^2 + 11q^2$, then we want $z$ near 1000, this means we want $p^2 + 11q^2$ near 1000. The way I searched was that if $11q^2 \leq 1000$ then $q < 9.5$, so I searched based on cases $q = 10, 9, \ldots, 1$, with $q = 9, p = 11$ giving $(770, 198, 1012), q = 9, p = 10$ giving $(791, 180, 991), q = 8, p = 17$ giving $(415, 272, 993)$ and $q = 2, p = 31$ giving $(917, 124, 1005)$ as the closest.

6. (6 points) With regard to problem 3, let $n \geq 2$. Prove or give a counterexample.

(a) There is always a **primitive** a primitive Pythagorean triple of the form $(2n+1, y, z)$.

**Solution:** This is true. If we let $p + q = 2n + 1, p - q = 1$ then we get $p = n + 1, q = n, and since these are two consecutive integers, one is even, the other is odd, and they are relatively prime. This means the give a primitive Pythagorean triple, that triple being $(2n + 1, 2n^2 + 2n, 2n^2 + 2n + 1)$. 
(b) There is always a **primitive** a primitive Pythagorean triple of the form \((x, 2n, z)\).

**Solution:** This is false, as any odd \(n\) will show. For example, if \(n = 3\) then we need \(2pq = 6\), or \(pq = 3\). This has only odd \(p\) and \(q\) as solutions, but we need one of \(p\) and \(q\) to be even for a primitive Pythagorean triple.

---

**Take Home Exam Questions**

1. (10 points) **Hilbert’s Example:** The set \(H = \{1, 5, 9, 13, \ldots, 4k + 1, \ldots\}\) is said to be a multiplicatively closed set because if you multiply any two numbers in the set, you get another number in the set. In any multiplicatively closed set, you can talk about factorization and primes. A **Hilbert prime** is a number \(p > 1\) in \(H\) which is not the product of two smaller numbers in \(H\). For example, the ordinary prime 5 is a Hilbert prime, but so are 9 and 21. A **Hilbert composite** is a number like 25, 45, 65, which is a product of smaller things in \(H\).

   (a) Find the two smallest Hilbert composites in \(H\) which don’t have unique factorization into Hilbert primes.

   **Solution:** The primes in \(H\) come in two varieties: ordinary primes 5, 13, 17, 29, 37, . . . , and odd numbers that are products of ordinary primes of the form \(4k + 3 : 3 \times 3 = 9, 3 \times 7 = 21, 3 \times 11 = 33, 7 \times 7 = 49, \ldots\). For factorization to not be unique, there must be products of this second kind involved. The smallest examples are \(441 = 21 \times 21 = 9 \times 49\) and \(693 = 21 \times 33 = 9 \times 77\).

   (b) Give an example to show that it is possible for a Hilbert prime \(p\) to divide a product \(mn\) of two Hilbert numbers, but not have \(p\) dividing either \(m\) or \(n\).

   **Solution:** Either of the two examples above work here. That is, 9 divides 441 = 21 \times 21 but it does not divide 21. Similarly, 9 divides 693 = 21 \times 33 but it does not divide 21 or 33.

   (c) \(O = \{1, 3, 5, 7, \ldots\}\), the odd numbers, is also multiplicatively closed. Prove that \(O\) DOES have unique factorization. **Strong hint:** Use ordinary unique factorization for the integers to help out.

   **Solution:** The primes in \(O\) are just the ordinary odd primes. Every odd number is an ordinary integer, so it factors uniquely into primes by the Fundamental Theorem. Since the number is odd, 2 will not appear in the factorization, so a factorization of an odd number over the integers is the same as a factorization of an odd number over \(O\), guaranteeing that the factorization is unique.
2. (12 points) To find infinitely many primitive solutions to an equation \( ax^2 + by^2 = cz^2 \), my first step is to find a 1 or 2-variable parameterization, and use (infinitely many) special cases. Consider the equation \( x^2 + 3y^2 = 7z^2 \).

(a) Show that \((2p^2 + 6pq - 6q^2, -p^2 + 4pq + 3q^2, p^2 + 3q^2)\) is a 2-variable parameterization for the equation. Note: I am not asking you to find this, just verify it.

**Solution:** We expand and then factor \((2p^2 + 6pq - 6q^2)^2 + 3(-p^2 + 4pq + 3q^2)^2\).

\[
(2p^2 + 6pq - 6q^2)^2 + 3(-p^2 + 4pq + 3q^2)^2 \\
= 4p^4 + 24p^3q + 12p^2q^2 - 72pq^3 + 36q^4 \\
+ 3p^4 - 24p^3q + 30p^2q^2 + 72p^2q^2 + 27q^4 \\
= 7p^4 + 42p^2q^2 + 63q^4 = 7(p^2 + 3q^2)^2.
\]

(b) Use the parameterization in part (a) to find 5 primitive solutions.

**Solution:** This is just a matter of judiciously picking values for \(p\) and \(q\). I will also point out that we can take the absolute value of \(x\) or \(y\) in the parameterization, as needed.

\[
\begin{array}{|c|c|c|c|}
\hline
p & q & x = |2p^2 + 6pq - 6q^2| & y = |-p^2 + 4pq + 3q^2| & z = p^2 + 3q^2 \\
\hline
1 & 0 & 2 & 1 & 1 \\
1 & 2 & 10 & 19 & 13 \\
2 & 3 & 10 & 47 & 31 \\
4 & 1 & 50 & 3 & 19 \\
4 & 3 & 50 & 59 & 43 \\
2 & 5 & 82 & 111 & 79 \\
4 & 5 & 2 & 139 & 91 \\
5 & 2 & 86 & 27 & 37 \\
5 & 4 & 74 & 103 & 73 \\
\hline
\end{array}
\]

are among the smallest primitive solutions.

(c) Use the parameterization to prove that \(x^2 + 3y^2 = 7z^2\) has infinitely many primitive solutions.

**Solution:** We need conditions on \(p\) and \(q\) so that \(x, y, z\) are relatively prime. Suppose that \(d\) is a common divisor of \(x\) and \(y\), we want conditions on \(p\) and \(q\) to force \(d = 1\). The main trick is that \(x + 2y = 14pq\), so \(d\) must be a divisor of \(14pq\). For a change, let’s set \(p = 1\) this time. Then \(x = |2 + 6q - 6q^2|, y = 3q^2 + 4q - 1, z = 3q^2 + 1\), and we need conditions on \(q\) so that \(d\), a divisor of \(14q\) must be 1. Since \(d\) is a divisor of \(y\), it can’t be a divisor of \(q\) since \(y = 3q^2 + 4q - 1\). If \(q\) is even then \(y\) is odd so \(d\) must be odd. The simplest way to make \(d\) prime to 7 is to let \(q\) be a multiple of 7. This means letting \(q = 14k\)
for any integer \( k \) will product primitive triples. That is, all triples of the form 
\[
x = 1176k^2 - 84k - 2, \quad y = 558k^2 + 52k - 1, \quad z = 558k^2 + 1
\] are primitive.

(d) Order matters in equations like \( ax^2 + by^2 = cz^2 \). Show that \( x^2 + 7y^2 = 3z^2 \) has no solutions other than \( (0, 0, 0) \). Hint: I don’t know any way to do this other than using infinite descent via a prime \( p \), and looking at remainders of squares when divided by \( p \).

**Solution:** We can use the same proof that was used for \( x^2 + y^2 = 3z^2 \). The reason: 7 is 1 more than a multiple of 3. That is, we already know that \( x^2 \) leaves a remainder of 0 or 1 when divided by 3, and \( 7y^2 \) will do the same. The only combination of 0’s and 1’s that’s divisible by 3 is 0 + 0, but \( x^2 + 7y^2 = 3z^2 \) so \( x^2 + 7y^2 \) must be divisible by 3. Thus, given a positive integer solution \((x, y, z)\), \( x = 3x_1, \quad y = 3y_1 \) for some integers \( x_1, y_1 \). Substituting in, \( 9x_1^2 + 63y_1^2 = 3z^2 \), or \( 3(x_1^2 + 7y_1^2) = z^2 \), forcing \( z \) to also be divisible by 3, meaning that \((x/3, y/3, z/3)\) will be a smaller positive solution, giving an infinite descent, for a contradiction.

3. (10 points) The Pythagorean triples \((16, 63, 65)\) and \((33, 56, 65)\) are both primitive and have \( z = 65 \).

(a) Find all values of \( z < 500 \) for which there are exactly two primitive Pythagorean triples.

**Solution:** There are 16 of them: \{65, 85, 145, 185, 205, 221, 265, 305, 325, 365, 377, 425, 445, 481, 485, 493\}.

(b) Make a conjecture as to which \( z \) have this property in general. It might help to factor your \( z \) in part a.

**Solution:** If we factor each of the numbers in the list above, we get \( 5 \times 13, 5 \times 17, 5 \times 29, 5 \times 37, 5 \times 41, 13 \times 17, 5 \times 53, 5 \times 61, 5 \times 5 \times 13, 5 \times 73, 13 \times 29, 5 \times 5 \times 17, 5 \times 89, 13 \times 37, 5 \times 97, 17 \times 29 \). The pattern is that only primes of the form \( p = 4k + 1 \) (one more than a multiple of 4) occur in the list of prime divisors, and in each case there are exactly two distinct such primes. This is probably the best conjecture.

(c) Find a value of \( z \) for which there are at least three primitive Pythagorean triples using \( z \).

**Solution:** One might guess from parts a and b that we need numbers \( z \) which are divisible by three different primes, each of the form \( 4k + 1 \). The smallest
such number is \( z = 5 \times 13 \times 17 = 1105 \), and in fact, this does have more than two primitive triples. In fact, there are four triples with \( z = 1105 \): (1073, 264, 1105), (943, 576, 1105), (817, 744, 1105), (47, 1104, 1105).

4. (8 points) The equation \( x^4 - 8x - 4 = 0 \) has two real solutions. Give a proof by infinite descent that the positive solution is irrational. For consistency sake, call the solution \( \alpha \). All you should need to know about \( \alpha \) is roughly how big it (between which two integers?) and that \( \alpha^4 - 8\alpha - 4 = 0 \) (so \( \alpha^4 = 8\alpha + 4 \)).

Solution: What I had in mind was the following: Since \( 2^4 - 8 \times 2 - 4 < 0 < 3^4 - 8 \times 3 - 4 \), we know \( 2 < \alpha < 3 \). Now suppose that \( \alpha \) is rational. Then there is a positive integer \( n \) for which \( n\alpha \), \( n\alpha^2 \) and \( n\alpha^3 \) are integers. Let \( m = n\alpha - 2n \). From \( 0 < \alpha - 2 < 1 \), we see that \( 0 < m < n \). Since \( 2n \) and \( n\alpha \) are both integers, \( m \) is an integer. Now \( m\alpha = n\alpha^2 - 2n\alpha \) is an integer since \( n\alpha \) and \( n\alpha^2 \) are, \( m\alpha^2 = n\alpha^3 - 2n\alpha^2 \) is an integer because \( n\alpha^3 \) and \( n\alpha^2 \) are, and \( m\alpha^3 = n\alpha^4 - 2n\alpha^3 = n(8\alpha + 4) - 2n\alpha^3 = 6n + 6n\alpha - 2n\alpha^3 \) is also an integer. That is, given a positive integer \( n \) with \( n\alpha \), \( n\alpha^2 \) and \( n\alpha^3 \) all integers, we have constructed a smaller positive integer \( m \) with \( m\alpha \), \( m\alpha^2 \) and \( m\alpha^3 \) integers. This sets up an infinite descent, which is a contradiction.

There is an alternative: Suppose that \( \alpha \) is rational. Then for some positive integers \( m \) and \( n \), \( \alpha = \frac{m}{n} \). This means that \( \left( \frac{m}{n} \right)^4 - 8\frac{m}{n} - 4 = 0 \), or \( m^4 = 8mn^3 + 4n^4 \). Since the right hand side is even, the left hand side must be even as well, meaning that \( m = 2j \) for some positive integer \( j \). Now \( 16j^4 = 16j^3n^3 + 4n^4 \), or \( n^4 = 4j^4 - 4jn^3 \). Since the right hand side of this is even, the left hand side must be as well, so \( n = 2k \) for some positive integer \( k \). But this means that whenever \( \alpha = \frac{m}{n} \) for positive integers \( m \) and \( n \), there must be smaller positive integers \( j \) and \( k \) with \( \alpha = \frac{j}{k} \), and this also gives an infinite descent.

5. (10 points) Here is another way to calculate \( \gcd(m, n) \).

(a) Prove that if \( m \) and \( n \) are both even, then \( \gcd(m, n) = 2 \gcd(m/2, n/2) \).

Solution: In problems like this, usually the approach is to show that each side is at least as big as the other. One way to do this: If \( mx + ny = k \) for integers \( m, x, n, y \), then \( |k| \geq \gcd(m, n) \) because the greatest common divisor of \( m \) and \( n \) divides any combination of \( m \) and \( n \). Let \( \gcd(m, n) = d \). Then for some integers \( x, y \), \( mx + ny = d \). Since \( m \) and \( n \) are both even, \( d \)
must also be even. If we divide by 2, \( \frac{1}{2}mx + \frac{1}{2}ny = \frac{1}{2}d \). This tells us that
\( \frac{1}{2}d \geq \gcd(m/2, n/2) \), or \( d \geq 2 \gcd(m/2, n/2) \). On the other hand, since \( d \) divides both \( m \) and \( n \), \( \frac{1}{2}d \) divides both \( \frac{1}{2}m \) and \( \frac{1}{2}n \), meaning that as a common divisor, \( \frac{1}{2}d \leq \gcd(m/2, n/2) \). Consequently, \( \frac{1}{2} \gcd(m, n) = \frac{1}{2}d = \gcd(m/2, n/2) \), or \( \gcd(m, n) = 2 \gcd(m/2, n/2) \).

(b) Prove that if \( m \) is even and \( n \) is odd, then \( \gcd(m, n) = \gcd(m/2, n) \).

**Solution:** If \( \gcd(m, n) = d \) then for some \( x, y \), \( mx + ny = d \). We can rewrite this \( \frac{1}{2}m(2x) + ny = d \), which shows that \( d \geq \gcd(m/2, n) \). On the other hand, \( d \) is a divisor of \( n \), an odd number, so \( d \) is odd. If \( m = 2k \) then \( d \) is prime to 2 so \( d|2k \) implies \( d \) divides \( k = \frac{1}{2}m \). Thus, \( d \) is a common divisor of \( \frac{1}{2}m \) and \( n \) so \( d \leq \gcd(m/2, n) \). Hence, \( d = \gcd(m, n) = \gcd(m/2, n) \).

(c) Prove that if \( m \) and \( n \) are both odd, then \( \gcd(m, n) = \gcd(m, m - n) \).

**Solution:** This is a special case of a result from class. If \( d = \gcd(m, n) \) then divides both \( m \) and \( n \) so it divides \( m - n \). Consequently, \( d \) is a common divisor of \( m \) and \( m - n \), giving \( \gcd(m, n) \leq \gcd(m, m - n) \). But if \( D = \gcd(m, m - n) \), then \( D \) divides \( m \) and \( m - n \), so \( D \) divides their difference, \( m - (m - n) = n \). Thus, \( D \) is a common divisor of \( m \) and \( n \) showing \( \gcd(m, m - n) \leq \gcd(m, n) \). Thus, the two are equal.

(d) Parts (a), (b), (c) allow one to calculate \( \gcd(m, n) \) using only subtractions and divisions by 2, very fast operations on a computer. Use this method to calculate \( \gcd(10982, 3621) \).

**Solution:** One other result: \( \gcd(m, n) = \gcd(n, m) \), so we can use symmetric versions of (a), (b), (c) above. We have

\[
\gcd(10982, 3621) = \gcd(5491, 3621) = \gcd(5491, 1870) = \gcd(5491, 935)
= \gcd(4556, 935) = \gcd(2278, 935) = \gcd(1139, 935)
= \gcd(204, 935) = \gcd(102, 935) = \gcd(51, 935)
= \gcd(51, 884) = \gcd(51, 442) = \gcd(51, 221) = \gcd(51, 170)
= \gcd(51, 85) = \gcd(51, 34) = \gcd(51, 17) = \gcd(34, 17)
= \gcd(17, 17) = \gcd(17, 0) = 17.
\]

I didn’t say this was short, only fast (on a computer)!
Take Home extra credit

6. (4 points) Prove that the set \( \mathbb{Z}[\sqrt{-3}] \) does not have a division algorithm. In this case, a division algorithm would look like this: given any \( m, n \) in \( \mathbb{Z}[\sqrt{-3}] \) with \( m \neq 0 \), there are elements \( q, r \) in \( \mathbb{Z}[\sqrt{-3}] \) with \( n = qm + r \) and \(|r|^2 < |m|^2\). Here, \(|a + b\sqrt{-3}|^2 = a^2 + 3b^2\).

As a STRONG HINT, \( n = 2, m = 1 + \sqrt{-3} \) will serve as a counterexample.

**Solution:** Following the hint, suppose that we write \( 2 = q(1 + \sqrt{-3}) + r \), with \(|r|^2 < |1 + \sqrt{-3}|^2 = 4 \). If we write \( r = r_1 + r_2\sqrt{-3} \) then we need \( r_1^2 + 3r_2^2 < 4 \). This leads to five cases: \( r \) must be one of the following: 0, 1, \(-1\), \( \sqrt{-3} \), \(-\sqrt{-3} \). Now \( q = \frac{2 - r}{1 + \sqrt{-3}} = \frac{(2 - r)(1 - \sqrt{-3})}{4} \). Plugging in the five values gives \( \frac{1 - \sqrt{-3}}{2}, \frac{1 - \sqrt{-3}}{4}, \frac{3 - 3\sqrt{-3}}{4}, \frac{5 - 3\sqrt{-3}}{4}, \frac{-1 - \sqrt{-3}}{4} \). Since none of these is in \( \mathbb{Z}[\sqrt{-3}] \), no remainder works.

7. (4 points) Prove that the Gaussian integers, \( \mathbb{Z}[i] \), DO have a division algorithm. Hint: Given \( m, n \in \mathbb{Z}[i] \), with \( m \neq 0 \), if \( \frac{n}{m} = x + iy \), pick \( q \) as follows: \( q = a + bi \), with \(|a - x| \leq 1/2 \) and \(|b - y| \leq 1/2 \). Why can you always pick \( a, b \) this way? Why does this show that the resulting \( r \) satisfies \(|r|^2 < |m|^2|\)?

**Solution:** I will just mention that the book gives a proof of this in section 2.2 (pages 35-37). The book goes on to prove that \( \mathbb{Z}[i] \) has unique factorization (pages 37, 38).

8. (4 points) Prove that there are infinitely many Gaussian primes. Find the 10 smallest (in absolute value) Gaussian primes. Here, if \( 5 + 2i \) was one of our primes, we would discount \(-5 - 2i, -2 + 5i, 2 - 5i \) since they only differ from \( 5 + 2i \) by a multiple of a unit (the units are \( \pm 1, \pm i \)).

**Solution:** Can we modify the proof from class for ordinary primes? The proof might go like this: Suppose \( p_1, p_2, \ldots, p_k \) are the only Gaussian primes. Let \( M = p_1p_2 \cdots p_k + 1 \). What are the possibilities for \( M \)? If \( M \) is prime, then we have a contradiction (as we did with \( Z \)). If \( M \) is divisible by a prime, \( q \), then we still get a contradiction because \( q \) can’t be one of the \( p \)'s. The reason for this: If \( q \mid M \) and \( q \) is one of the \( p \)'s, then \( q \mid p_1p_2 \cdots p_k \), but this would force \( q \mid 1 \), but no prime divides 1. Unfortunately, there are other possibilities for \( M \). How do we rule out \( M = 0, 1, -1, i, -i \)? For example, if we had the case \( k = 1 \), and \( p_1 = -1 + i \), then we would have \( M = i \). Of course we know that there is more than just one
prime, so we must use this to show $M$ can’t be 0, 1, -1, i or -i. Here is one way: It turns out that 3 is a prime in $\mathbb{Z}[i]$ so if we take $k$ large enough, 3 will be one of the $p$’s. This means that $M = 3p_1p_2 \cdots p_k + 1$ for some collection of $p$’s, and if $p_1p_2 \cdots p_k = a + bi$ then $M = 3a + 1 + 3bi$, and this can’t be any of the five bad values.

Here is a trickier approach. We know there are infinitely many ordinary primes. Some of these (like 3 or 7) are still prime in $\mathbb{Z}[i]$ some like 13 are not (13 = $(2+3i)(2-3i)$.) But each ordinary prime is either still prime in $\mathbb{Z}[i]$ or it has a Gaussian prime divisor. Can the same Gaussian prime divide two different ordinary primes? The answer is no. Here is one way to see this: If $p$ and $q$ are ordinary primes, then they are relatively prime so for some integers $x$ and $y$, $px + qy = 1$. Now any common (Gaussian) divisor of $p$ and $q$ would have to be a divisor of 1, so it can’t be prime. So each ordinary prime gives us at least one Gaussian prime, and these will all be different. Infinitely many ordinary primes implies infinitely many Gaussian primes.

What are the smallest Gaussian primes? We can proceed as in the second proof, factoring ordinary primes. We have 2 = $(1 + i)(1 - i)$, 3 is prime, 5 = $(2 + i)(2 - i)$, 7 is prime, 11 is prime, 13 = $(3 + 2i)(3 - 2i)$, and so on. Now 1 - i = -i(1 + i), however, the rest are distinct, so the smallest 6 in absolute value are 1 + i, 2 + i, 2 - i, 3, 3 + 2i, 3 - 2i. The next ones are 4 + i, 4 - i, 5 + 2i, 5 - 2i. 7 would have to wait till after 6 + i, 6 - i, 5 + 4i and 5 - 4i.

9. (4 points) Prove by infinite descent that if $p(x) = x^k + a_1x^{k-1} + \cdots + a_k$ is a polynomial with integer coefficients, then the only solutions to $p(x) = 0$ are integers and irrational numbers. That is, if $p(\alpha) = 0$ but $\alpha$ is not an integer, then $\alpha$ is irrational. Hints: If $p(\alpha) = 0$ then $\alpha^k = -a_1\alpha^{k-1} - \cdots - a_k$. If $\alpha$ is not an integer, then $m < \alpha < m + 1$ for some integer $m$.

10. (4 points) The Euclidean algorithm calculates $\text{gcd}(m, n)$ in at most $2\log_2(m)$ steps, where $m$ is the smaller of $m$ and $n$. What can you say about the number of steps the method in problem 5 takes to calculate $\text{gcd}(m, n)$?