Math 445/845. Exam #2

(1) Definitions/Theorem statements

(a) Define the **norm function** on $\mathbb{Z}[\sqrt{D}]$ for some positive integer D that is not a square.

> The norm function on $\mathbb{Z}[\sqrt{D}]$ is the function $N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$ given by $N(a + b\sqrt{D}) = a^2 - b^2 D$.

(b) Define a **triangular number**.

> A triangular number is a natural number that counts the number of dots in a triangular array with base k for some k.

(c) State **Lagrange's theorem** (about elements of groups).

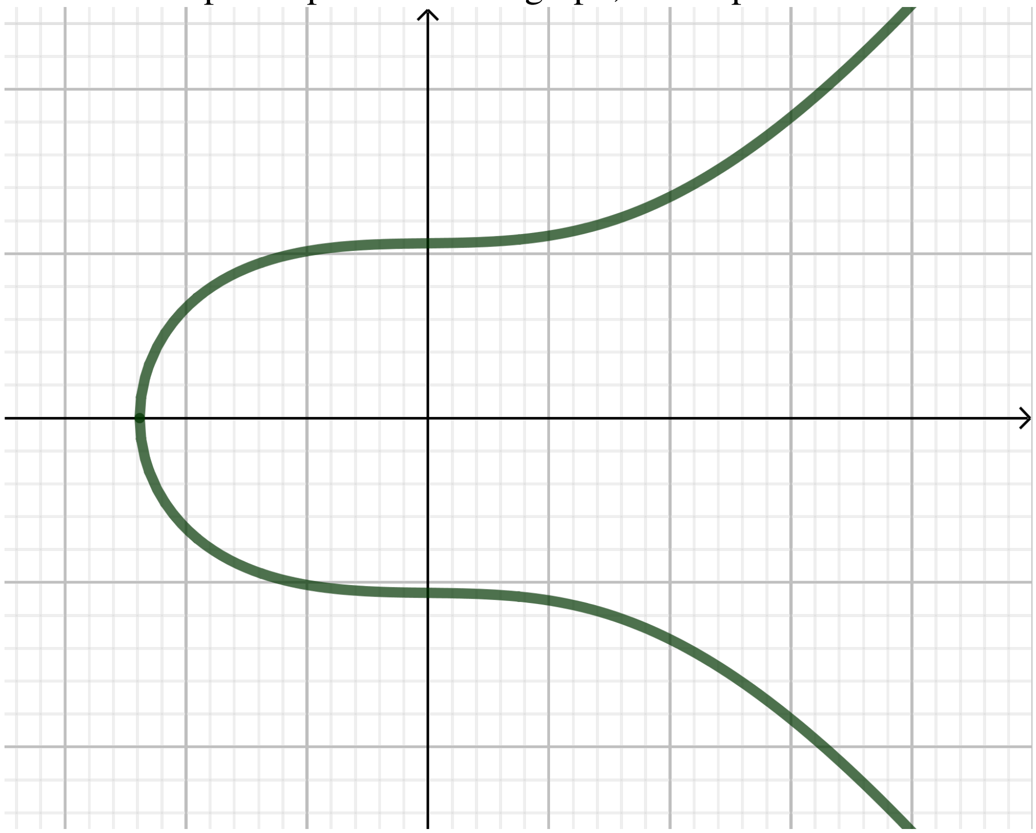
> If G is a finite group, the order of an element of G divides the cardinality of G.

(d) State the **Dirichlet approximation theorem**.

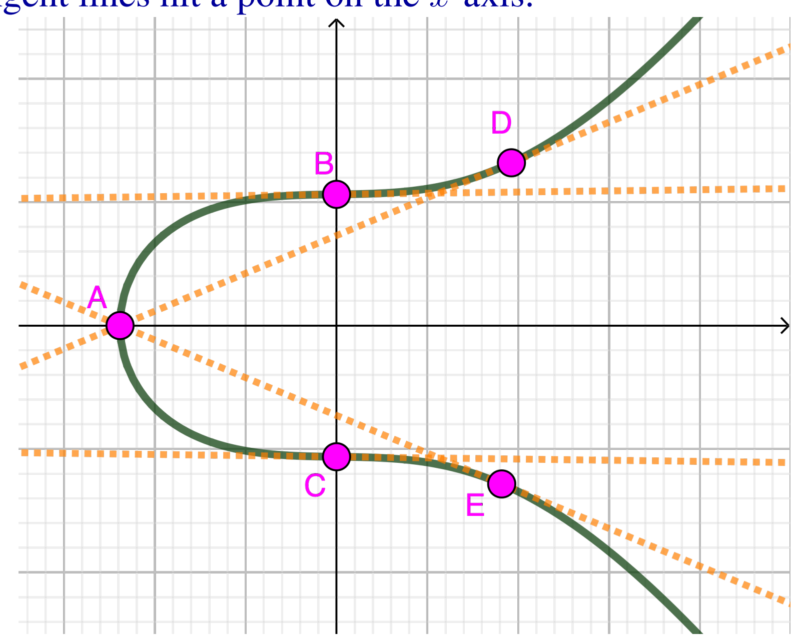
> For any irrational number α, there are infinitely many rational numbers $\frac{p_k}{q_k}$ such that $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2}$.

(2) Computations.

(a) The picture below is part of the graph of an elliptic curve. Mark all points of order *at most* four in the depicted portion of the graph, and explain each.



The point A has order 2 since it has a vertical tangent line. The points B and C have order 3 because they are inflection points. The points D and E have order 4 since their tangent lines hit a point on the x-axis.



(b) (i) Compute the first two partial quotients (*after* the integer part) in the continued fraction of $\sqrt{11}$.

We compute

$$\sqrt{11} = 3 + (\sqrt{11} - 3) = 3 + \frac{1}{(\sqrt{11}-3)^{-1}} = 3 + \frac{1}{\left(\frac{\sqrt{11}+3}{2}\right)} = 3 + \frac{1}{3 + \frac{\sqrt{11}-3}{2}}$$

$$= 3 + \frac{1}{3 + \frac{1}{\left(\frac{2}{\sqrt{11}-3}\right)}} = 3 + \frac{1}{3 + \frac{1}{\left(\frac{2(\sqrt{11}+3)}{2}\right)}} = 3 + \frac{1}{3 + \frac{1}{6 + \ddots}}$$

(ii) Use your calculation from part (a) to give a rational approximation of $\sqrt{11}$. Using results from this class (and not using the decimal expansion from a calculator), what can you say about the accuracy of your approximation?

We get the convergent $3 + \frac{1}{3+\frac{1}{6}} = \frac{63}{19}$. We know that $|\sqrt{11} - \frac{63}{19}| < \frac{1}{19^2}$.

(c) Give an expression for the general[1] integer solution of $x^2 - 11y^2 = 1$.

By trial and error (or using the convergents of $\sqrt{11}$), we can find the first solution $(10, 3)$. Then we know that every solution is given as $(\pm x_k, \pm y_k)$ for $k \geq 0$, where $x_k + y_k\sqrt{11} = (10 + 3\sqrt{11})^k$.

[1] To find *one* solution, you can either use the general technique or trial and error.

(d) The equation $y^2 = x^3 + 44x + 25$ defines an elliptic curve. Two rational solutions to the equation are $(0, 5)$ and $(2, 11)$. Their reflections over the x-axis are also solutions. Find another rational solution besides these four.

The line between $(0, 5)$ and $(2, 11)$ is given by the equation $y = 3x + 5$. Substituting, we get

$$\begin{aligned}(3x + 5)^2 &= x^3 + 44x + 25 \\ x^3 - 9x^2 + 14x &= 0 \\ x(x - 2)(x - 7) &= 0\end{aligned}$$

The roots $x = 0, x = 2$ are accounted for, so $x = 7$ yields the third point on the curve. We then get $(7, 26)$ as another point on the curve.

(3) Proofs.

(a) Consider the equation

$$x^2 - Dy^2 = 2 \tag{†}$$

where D is some positive integer that is not a perfect square.

(i) Show that if the equation (†) has an integer solution $(x, y) = (a_0, b_0)$, then the equation (†) has infinitely many integer solutions $(x, y) = (a_k, b_k)$.

Observe that $N(a + b\sqrt{k}) = 2$ if and only if (a, b) is a solution to (†). We have show that there are infinitely many solutions (c_k, d_k) to Pell's equation $x^2 + Dy^2 = 1$. Note that a solution (c_k, d_k) to Pell's equation has $N(c_k + d_k\sqrt{D}) = 1$. Then if we define (a_k, b_k) by the rule $a_k + b_k\sqrt{D} = (a_0 + b_0\sqrt{D})(c_k + d_k\sqrt{D})$, we have $N(a_k + b_k\sqrt{D}) = N(a_0 + b_0\sqrt{D})N(c_k + d_k\sqrt{D}) = 2 \cdot 1 = 2$, so (a_k, b_k) is a solution. These are distinct since $(a_k, b_k) \neq (a_j, b_j)$ implies $a_k + b_k\sqrt{D} = a_j + b_j\sqrt{D}$ implies $c_k + d_k\sqrt{D} = c_j + d_j\sqrt{D}$, which implies $(c_k, d_k) = (c_j, d_j)$.

(ii) Show that for $D = 83$, the equation (†) has no solution.

Suppose that (a, b) is a solution. Then $a^2 = 83b^2 + 2$. Going modulo 83, we have $a^2 \equiv 2 \pmod{83}$. But $\left(\frac{2}{83}\right) = -1$ by quadratic reciprocity, so no such a exists. This contradicts the existence of a solution.

(b) Let $\overline{E}_p$ be an elliptic curve over $\mathbb{Z}_p$ given by the equation $y^2 = x^3 + [a]x + [b]$, where $p \geq 5$ is a prime. Suppose that $[c] \in \mathbb{Z}_p$ is a root of the polynomial $x^3+[a]x+[b] = 0$.

(i) Find[2] a point of order 2 in $\overline{E}_p$.

Consider the point $P = ([c], [0])$. This is on the curve, by construction. To compute the tangent line at P, we take $2y\frac{dy}{dx} = 3x^2 + [a]$; since $y = [0]$, this is a line of vertical slope, so $2P = \infty$. This is then our point of order 2.

(ii) Use part (i) and the group structure to show that the equation $y^2 = x^3 + [a]x + [b]$ has an odd number of solutions in $\mathbb{Z}_p \times \mathbb{Z}_p$.

Since there is a point of order 2, we know that $\overline{E}_5$ has an even number of element by Lagrange's Theorem. Since $\overline{E}_5 = E_5 \cup \{\infty\}$, where E_5 is the solution set tot he equation, E_5 has an odd number of elements.

[2]You can use any characterization of points of order 2 that we have encountered in this class.

Bonus: Show that for $\varphi = \dfrac{1+\sqrt{5}}{2}$, there do *not* exist infinitely many rational numbers $\dfrac{p}{q}$ such that $\left|\varphi - \dfrac{p}{q}\right| < \dfrac{1}{q^3}$.

Note first that for $q > 2$, we have $q^3 > 2q^2$, so $\left|\varphi - \frac{p}{q}\right| < \frac{1}{q^3}$ implies $\left|\varphi - \frac{p}{q}\right| < \frac{1}{2q^2}$, and we know that this implies that $\frac{p}{q} = \frac{p_k}{q_k}$ for some convergent $C_k = \frac{p_k}{q_k}$ (by a Theorem saying that good approximations are convergents). For $q \leq 2$, we can see that $\frac{1}{1}$ and $\frac{2}{1}$ are the only numbers that work, so it suffices to show that at most finitely many convergents satisfies the hypotheses.

From the continued fraction expansion $\varphi = [1; 1, 1, 1, 1, 1, \ldots]$ that we computed in class, we see that $C_k = \frac{f_{k+1}}{f_k}$ for the Fibonacci numbers f_k. We know that $C_{2n} < C_{2n+2} < \varphi < C_{2n+1} < C_{2n-1}$ for all n, so it suffices to show that $|C_{k+2} - C_k| > \frac{1}{f_k^3}$ for large enough k. After simplifying, the left hand side is $\frac{|f_{k+2}f_k - f_{k+1}^2|}{f_k f_{k+2}}$.

We claim that $f_{k+2}f_k - f_{k+1}^2 = (-1)^k$ for all k. We show the claim by induction on k. For $k = 0$, we get $1 \cdot 2 - 1^1 = 1$. For the induction step, assuming the equality holds for k, we have

$$\begin{aligned} f_{k+3}f_{k+1} - f_{k+2}^2 &= (f_{k+2} + f_{k+1})f_{k+1} - (f_1 + f_0)^2 = f_{k+2}f_{k+1} - 2f_{k+1}f_k - f_k^2 \\ &= f_{k+1}^2 + f_k f_{k+1} - 2f_{k+1}f_k - f_k^2 = f_{k+1}^2 - f_{k+1}f_k - f_k^2 \\ &= f_{k+1}^2 - f_k f_{k+2} = -(-1)^k = (-1)^{k+1}, \end{aligned}$$

completing the proof of the claim. Thus, $|C_{k+2} - C_k| = \frac{1}{f_k f_{k+2}}$.

Now

$$f_{k+2} = f_{k+1} + f_k = 2f_k + f_{k-1} \leq 3f_k,$$

so $\frac{1}{f_k^3} < \frac{1}{3f_k^2} \leq \frac{1}{f_k f_{k+2}} = |C_{k+2} - C_k|$ for $f_k > 3$. This completes the proof.