Math 845. Final Exam

(1) Definitions/Theorem statements
   (a) State **Fermat's little theorem**.

   (b) Define the **order** of an element in a group.

   (c) State **Euler's criterion**.

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

(2) Computations.

(a) Compute the inverse of $[311]_{3141}$.

(b) On the real elliptic curve $\overline{E}$ given by the equation $y^2 = x^3 + 12x + 9$ with group operation $\star$, compute $(0, 3) \star (0, 3)$.

(c) Determine whether 67 is a square modulo 221. Note that 67 and 221 are prime. If any step in your calculation has a congruence condition as a hypothesis, be sure to indicate it.

(d) Find the first two convergents (*after* $C_0 = \frac{5}{1}$) in the continued fraction expansion of $\sqrt{29}$ and use a result from class to bound $|C_2 - \sqrt{29}|$.

(e) One integer solution of the equation $x^2 - 30y^2 = 1$ is given by $(x, y) = (11, 2)$. Find two other pairs of positive integers (x, y) that are solutions of the given equation.

(f) Solve $x^{187} \equiv 103 \pmod{319}$. Note that $319 = 11 \cdot 29$.

(g) Find the square roots of 1 in $\mathbb{Z}_{319}$. Recall from above that $319 = 11 \cdot 29$; you can also use that $8 \cdot 11 - 3 \cdot 29 = 1$.

(3) Proofs. Select **three** of the problems in this part. If you write in more than three answer areas, be sure to make clear which three you would like to be graded.

(a) Let $\gcd(a, 101) = 1$. Show that a has a fourth root modulo 101 if and only if $a^{25} \equiv 1 \pmod{101}$.

(b) Consider the equation $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{Z}$ are integers with $4a^3 \neq 27b^2$ (this is the technical condition on coefficients for an elliptic curve). Suppose that there are exactly 15 pairs of rational numbers (x, y) are solutions to this equation. Prove that this curve does *not* have any rational inflection points.

(c) Modify Euclid's argument to show that there are infinitely many primes p such that $p \equiv 1 \pmod 4$.

(d) Consider the group $\mathbb{Z}_{52}^{\times}$.

(i) Show that there is no element of order 51 in $\mathbb{Z}_{52}^{\times}$.

(ii) Show that[1] there is no element of order 24 in $\mathbb{Z}_{52}^{\times}$.

[1]Hint: Use CRT and show $x^{12} \equiv 1 \ldots$

(e) Show that the equation $x^2 + 2x + y^2 = 4202$ has no integer solutions x, y.

Bonus: On the first week of class, we considered some examples of Pythagorean triples where the lengths of the legs were nearly equal. Let's say that a right triangle with integer side lengths is **almost isoceles** if the lengths of its two legs differ by one; for example, the triangle with lengths $3, 4, 5$ and the triangle with lengths $20, 21, 29$ are almost isoceles.

Find a formula/expression for the side lengths (a, b, c) of all almost isoceles integer right triangles, and use it to find the next three smallest such triangles.