HOMEWORK ASSIGNMENT # 8
DUE, Friday, December 5

Collaboration: On the homework sets, collaboration is not only allowed but encouraged. However, you must write up and understand your own individual homework solutions, and you may not share written solutions. If you learn how to solve a problem by talking to a classmate, CA, or looking it up in a book, you should cite the source in your homework write-up, just as you would reference your sources in a literature or history class.
Show all your working, and write up your solutions as neatly as possible.

1. **More imaginary quadratic fields of class number** 1.
   (a) (1 point) Prove that x^2+x+41 is prime for all $x = 0, 1, \ldots 38, 39$, and that $163 + x^2$ is four times a prime for $x = 1, 3, 5, \ldots, 77, 79$.
   (b) (3 points) Show that the only reduced binary quadratic form of discriminant -163 is
   $$x^2 + xy + 41y^2.$$
   (c) (1 point) Prove that all ideals of the ring $\mathbb{Z}[(1+\sqrt{-163})/2]$ are principal.
   (d) (3 points) Let $p \equiv -1 \mod 4$ be prime. Suppose that the polynomial $x^2+x+\frac{p+1}{4}$ is prime for all $x = 0, 1, \ldots \frac{p+1}{4} - 2$. Prove that
   $$x^2 + xy + \frac{p+1}{4}y^2$$
   is the only reduced binary quadratic form of discriminant $-p$ and that all ideals of the ring $\mathbb{Z}[(1+\sqrt{-p})/2]$ are principal.
   (e) (3 points) Suppose that $x^2 + x + \frac{p+1}{4}$ is composite for some $x = m$ with $0 \leq m \leq \frac{p+1}{4} - 2$. Prove that $m^2 + m + \frac{p+1}{4}$ has an odd prime factor q with $q < \frac{p+1}{4}$. Moreover, prove for this prime factor q that
   $$\left(\frac{-p}{q}\right) = 1.$$
   (f) (1 point) Using results from last week's homework, conclude that $R = \mathbb{Z}[(1 + \sqrt{-p})]/2$ is a principal ideal domain if and only if the polynomial
   $$x^2 + x + \frac{p+1}{4}$$
   is prime for all $x = 0, 1 \ldots, \frac{p+1}{4} - 2$.
   (g) (1 point) Evaluate $e^{\pi\sqrt{163}}$ to an accuracy of 10^{-10}.
2. (7 points) Prove that the class group of $\mathbb{Z}[\sqrt{-21}]$ has order 4. What is the group structure?