Homework Set Eight

Due Thursday, June 23.

Question 1. Use Tonelli's algorithm to find the two solutions of the congruence

$$x^2 \equiv 8 \pmod{41}.$$

Question 2. Given $n \in \mathbb{Z}$, show that $n = a^2 - b^2$ for some $(a, b) \in \mathbb{Z}^2$ if and only if $n \not\equiv 2 \pmod 4$.

Question 3.

(a) Find all ways to write 1002375 as the sum of two squares.

(b) Find all ways to write 1184625 as the sum of two squares.

Question 4. Assume that p is an odd prime and $\left(\frac{-1}{p}\right) = 1$. In practice, for small primes p it is most efficient to simply test whether or not $p - a^2$ is a square for all $1 \leq a \leq \sqrt{p}$ in search of pairs such that $p = a^2 + b^2$. However, for large primes, the following algorithm proves to be superior.

Algorithm: Given a prime p as above,

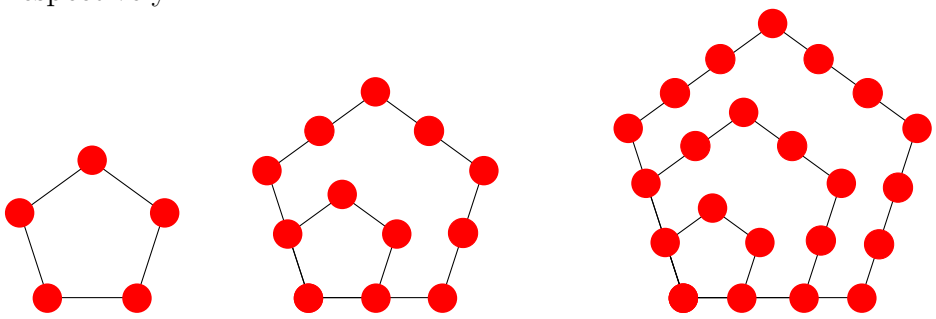
(i) find a solution n to the congruence $n^2 \equiv -1 \pmod p$, and

(ii) use the Euclidean algorithm in $\mathbb{Z}[i]$ to find $\gcd(n + i, p)$.

(a) Let p and n be as in the algorithm above. Suppose $\gcd(n + i, p) = a + ib$. Show that $p = a^2 + b^2$.

(b) Perform Steps (i) and (ii) above for $p = 41$. In the process, find n and $a + bi$.

Question 5. Consider the values $P(0) = 0$, $P(1) = 1$, $P(2) = 5$, $P(3) = 12$, and $P(4) = 22$. These are the first 5 *pentagonal numbers* which are the total sum of nodes representing unit lengths of n many nested pentagons (and $P(0)$ is simply defined to be 0). For example, the values $P(2)$, $P(3)$, and $P(4)$ are the sum of nodes in the following diagrams, respectively.



(a) Find a recursive formula for the pentagonal numbers. That is, express $P(n)$ as sum involving n and expressions $P(k)$ for $k \leq n - 1$.

(b) Find a closed formula for $P(n)$. That is, find an expression for $P(n)$ dependent only on n. Be sure to derive the formula or otherwise prove that it is correct.