

MATHEMATICS 350 FALL 2008 (SHATZ)
Assignment VI, November 17 , 2008. Due December 1, 2008

From “Little Gidding”, the fourth of the “Four Quartets” by T.S. Eliot:

...
What we call the beginning is often the end
And to make an end is to make a beginning.
The end is where we start from ...

...
We shall not cease from exploration
And the end of all our exploring
Will be to arrive where we started
And know the place for the first time.

A PROBLEMS (NOT TO BE HANDED IN).

AI Suppose p is an odd prime, n is a positive integer and a is an integer prime to p . Show that the congruence $x^2 \equiv a \pmod{p^n}$ has a solution if and only if a is a quadratic residue mod p . Show further that, if x is a solution, there are no solutions mod p^n other than x and $-x$.

AII Continue the investigation of the problem above. Take a to be odd and $n > 2$. Show that the congruence $x^2 \equiv a \pmod{2^n}$ has a solution if and only if $a \equiv 1 \pmod{8}$. Find all solutions $\pmod{2^n}$ of $x^2 \equiv a$. Put together these two problems to give a criterion for when the congruence

$$x^2 \equiv a \pmod{m}$$

has a solution where m is any integer and a is prime to m .

AIII Let $x > 1$ be a real number and write $\frac{p_k}{q_k}$ for the k^{th} convergent of its continued fraction expansion. Write $\frac{P_k}{Q_k}$ for the k^{th} convergent of $\frac{1}{x}$. Prove that

$$\frac{P_k}{Q_k} = \frac{q_{k-1}}{p_{k-1}}.$$

B PROBLEMS (TO BE HANDED IN–GROUP WORK).

BI Write ξ for a real irrational number and, as usual, let $\xi = [[a_0, a_1, \dots, a_{n-1}, r_n]]$ be its continued fraction expansion—with r_n being the n^{th} remainder continued fraction. We take d a non-square positive integer and define, inductively for $i \geq 0$, the integers m_i and Q_i by:

$$\begin{aligned}\xi &= \xi_0 = \frac{(m_0 + \sqrt{d})}{Q_0} \\ r_i &= \frac{(m_i + \sqrt{d})}{Q_i} \\ m_{i+1} &= a_i Q_i - m_i \text{ and } Q_{i+1} = \frac{(d - m_{i+1}^2)}{Q_i},\end{aligned}$$

where you must prove the Q_i are integers. When $\xi = \sqrt{d}$, then, of course, $m_0 = 0$ and $Q_0 = 1$, assume this now. Show that for all $n \geq -1$ we have

$$p_n^2 - dq_n^2 = (-1)^{n+1} Q_{n+1}.$$

Now, we know by Lagrange's Theorem that \sqrt{d} has a periodic continued fraction—say ρ is its period length. Prove that $Q_i = 1$ if and only if $\rho|i$ and then prove that if n is even and we set $k = n\rho - 1$, and further if we write $x = p_k$ and $y = q_k$, then x and y satisfy Pell's Equation:

$$x^2 - dy^2 = 1.$$

This gives a prescription for infinitely many solutions (in integers) for Pell's Equation from the continued fraction expansion of \sqrt{d} .

BII Continue the investigation of Problem BI, use the same notation. Choose any positive integer, N , so that $|N| < \sqrt{d}$ and consider Pell's Equation $x^2 - dy^2 = N$. Prove that any positive integer solution of this new equation with $(x, y) = 1$ is exactly of the form $x = p_k$ and $y = q_k$ for some k . Deduce that all positive integer solutions of $x^2 - dy^2 = \pm 1$ are to be found among $x = p_k, y = q_k$ where $\frac{p_k}{q_k}$ is a convergent for \sqrt{d} . Show further if ρ is even, there are no solutions to $x^2 - dy^2 = -1$ and the only positive solutions for $x^2 - dy^2 = 1$ are those found in Problem BI. If ρ is odd, however, then when n is odd the solutions of BI give all positive solutions to $x^2 - dy^2 = -1$ and when n is even we get all positive solutions for $x^2 - dy^2 = 1$ from the method of BI.

BIII a) Consider the complex number $\omega = \frac{(-1+i\sqrt{3})}{2}$ and the collection, $\mathbf{Z}[\omega]$, of all complex numbers of the form $x + y\omega$ in which x, y are integers. This is a domain and its units are $\pm 1, \pm\omega, \pm\omega^2$. Prove that if z is a complex number, there is an element, say q in $\mathbf{Z}[\omega]$, so that $N(z - q) \leq 1/3$. (Here, the $N(\dots)$ stands for an appropriate notion of norm that you must first define.) This will prove that our domain is Euclidean and so has unique factorization.

b) Now take a prime number bigger than 3, say p . Describe exactly when p can be written as $x^2 + xy + y^2$ with integers x, y . Your condition

should be in the form of a congruence involving p and your proof will necessitate using part a) of this problem.

B IV For an odd prime p , determine exactly when -1 will be a *fourth* power mod(p). Your condition or conditions should be a congruence or congruences involving p . For example, we proved that -1 is a square mod(p) if and only if $p \equiv 1 \pmod{4}$.