Math 445

Take-home Exam (Exam 2) Solutions

1. If $p \equiv 1 \pmod 4$, p is prime, and $a^2 + b^2 = p$ with $a > 0$ and odd, then $\left(\frac{a}{p}\right) = 1$.

   Since p is prime, $\left(\frac{a}{p}\right)$ can be treated as either a Legendre or Jacobi symbol. We treat it as a Jacobi symbol, since $\left(\frac{p}{a}\right)$ makes sense as a Jacobi symbol (a is odd), and then we know that $\left(\frac{a}{p}\right)\left(\frac{p}{a}\right) = (-1)^{\frac{p-1}{2}\frac{a-1}{2}} = 1$, since $p = 4k+1$ for some k, so $\frac{p-1}{2} = 2k$ is even. So $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)$.

   But if $a = a_1 \cdots a_k$ is the prime factorization of a, then $\left(\frac{p}{a}\right) = \left(\frac{p}{a_1}\right) \cdots \left(\frac{p}{a_k}\right)$. But since $a^2 + b^2 = p$, $b^2 = p - a^2 = p + a_i(-a \cdot a_1 \cdots a_{i-1}a_{i+1} \cdots a_k) \equiv p \pmod{a_i}$, so $\left(\frac{p}{a_i}\right) = 1$ for every i, so $\left(\frac{p}{a}\right) = 1$, so $\left(\frac{a}{p}\right) = 1$, as desired.

2. If $x = [a_0, a_1, \ldots, a_n, \ldots] > 1$, then $\frac{1}{x} = [0, a_0, a_1, \ldots, a_n, \ldots]$. We can then describe the convergents $\frac{H_n}{K_n}$ of $\frac{1}{x}$ in terms of the convergents $\frac{h_n}{k_n}$ of x .

   If we write $1/x = [b_0, b_1, \ldots]$, then since $x > 1$, $0 < 1/x < 1$, so $b_0 = \lfloor 1/x \rfloor = 0$. In fact, $1/x = 0 + 1/x = [0, x]$. So $b_1 = \lfloor x \rfloor = a_0$, and if we write $x_0 = x - a_0$, then $x = [a_0 + x_0]$ and $1/x = [0, a_0 + x_0]$. Assume, inductively, that $b_n = a_{n-1}$ and if $x = [a_0, \ldots, a_{n-1}, a_n + x_n]$ then $1/x = [0, a_0, \ldots, a_{n-1}, a_n + x_n]$. Then writing $1/x_n = \lfloor 1/x_n \rfloor + x_{n+1} = a_{n+1} + x_{n+1}$, we have $x = [a_0, \ldots, a_{n-1}, a_n + x_n] = [a_0, \ldots, a_n, 1/x_n] = [a_0, \ldots, a_n, a_{n+1} + x_{n+1}]$ and $1/x = [0, a_0, \ldots, a_{n-1}, a_n + x_n] = [0, a_0, \ldots, a_n, 1/x_n] = [0, a_0, \ldots, a_n, a_{n+1} + x_{n+1}]$, so $b_{n+1} = a_n$. So, by induction, we have $b_0 = 0$ and $b_{i+1} = a_i$ for every $i \geq 1$, so $1/x = [0, a_0, a_1, \ldots]$.

   [[Or the short proof! $[0, a_0, a_1, \ldots] = 0 + \frac{1}{[a_0, a_1, \ldots]} = \frac{1}{x}$, since $x = [a_0, a_1, \ldots]$!]]

   From this, we can compute, for $\frac{1}{x}$, $\frac{H_{-1}}{K_{-1}} = \frac{1}{0}$, $\frac{H_0}{K_0} = \frac{0}{1} = \frac{k_{-1}}{h_{-1}}$, $\frac{H_1}{K_1} = \frac{1}{a_0} = \frac{k_0}{h_0}$, and if we assume, by induction, that $\frac{H_j}{K_j} = \frac{k_{j-1}}{h_{j-1}}$ for every $j < n$, then $\frac{H_n}{K_n} = \frac{H_{n-1}b_n + H_{n-2}}{K_{n-1}b_n + K_{n-2}} = \frac{k_{n-2}a_{n-1} + k_{n-3}}{h_{n-2}a_{n-1} + h_{n-3}} = \frac{k_{n-1}}{h_{n-1}}$. So, by induction, we have $\frac{H_n}{K_n} = \frac{k_{n-1}}{h_{n-1}}$ for all $n \geq 0$.

3. The equation $x^2 = 2 + 41y$, $x, y \in \mathbb{Z}$ has a solution, but the equation $x^2 = 2 + 41y^2$, $x, y \in \mathbb{Z}$ has no solution.

   $x^2 = 2 + 41y$ has a solution $x, y \in \mathbb{Z} \Leftrightarrow x^2 \equiv 2 \pmod{41}$ has a solution $x \in \mathbb{Z} \Leftrightarrow \left(\frac{2}{41}\right) = 1$. But $\left(\frac{2}{41}\right) = (-1)^{\frac{41^2-1}{8}} = (-1)^{1680/8} = (-1)^{210} = 1$, so $x^2 = 2 + 41y$ has a solution $x, y \in \mathbb{Z}$, as desired.

On the other hand , $x^2 = 2 + 41y^2$ has a solution $x, y \in \mathbb{Z} \Leftrightarrow x^2 - 41y^2 = 2$ has a solution. But since $|2| = 2 < \sqrt{41}$ is not a square, $x^2 - 41y^2 = 2 \Leftrightarrow h_i^2 - 41k_i^2 = 2$ for some convergent h_i/k_i of $\sqrt{41}$. But we can compute, for $\sqrt{41} = [a_0, a_1, \ldots]$:

$6 < \sqrt{41} < 7$, so $a_0 = 6$, $x_0 = \sqrt{41} - 6$; $\zeta_1 = \dfrac{\sqrt{41}+6}{5}$, $a_1 = 2$, $x_1 = \dfrac{\sqrt{41}-4}{5}$; $\zeta_2 = \dfrac{\sqrt{41}+4}{5}$, $a_2 = 2$, $x_2 = \dfrac{\sqrt{41}-6}{5}$; $\zeta_3 = \dfrac{\sqrt{41}+6}{1}$, $a_3 = 12$, $x_3 = \dfrac{\sqrt{41}-6}{1}$, and the process repeats. In particular, the set of possible values of $h_i^2 - 41k_i^2$, starting from $i = -1$, are 1, -5, 5, -1, 5, -5, 1, and then they repeat (from the first -5) . So the only non-square values of $x^2 - 41y^2 = N$, with $|N| < \sqrt{41}$, are $-5, -1, 1, 5$. Since 2 is not in this list, $x^2 - 41y^2 = 2$ has no solutions with $x, y \in \mathbb{Z}$.

4. If $n \equiv 3 \pmod 4$, then the length of the periodic part of the continued fraction of $\sqrt{n}$ is *even.*

   We know from previous work that, if p is prime, then $x^2 \equiv -1 \pmod p$ has a solution $\Leftrightarrow$ $p \equiv 1 \pmod 4$. Since $n \equiv 3 \pmod 4$, at least one of it's prime factors p is $\equiv 3 \pmod 4$. So $x^2 \equiv -1 \pmod n$ has no solutions, since if $n | x^2 + 1$ then $p | x^2 + 1$. In particular, $x^2 - ny^2 = -1$ has no solutions. In particular, this means that for every convergent of $\sqrt{n}$, $h_i^2 - nk_i^2 \neq -1$. But if the length of the periodic part of the continued fraction expansion of $\sqrt{n}$ is odd, $\sqrt{n} = [a_0, \overline{a_1, \ldots, a_{m-1}, 2a_0}]$, i.e., m is <u>odd</u>, then $h_{m-1}^2 - nk_{m-1}^2 = (-1)^{m-2}(1) = -1$. Since this is impossible, m, the length of the period, must be even.

5. A solution to the equation $x^2 - 29y^2 = 7$, $x, y \in \mathbb{Z}$, with $x \geq 1000$ and $y \geq 1000$:

   By inspection, we find that $6^2 - 29(1)^2 = 36 - 29 = 7$. To find larger solutions, we first find a solution to $x^2 - 29y^2 = 1$. We compute:

   $5 < \sqrt{29} < 6$, so $a_0 = 5$, $x_0 = \sqrt{29} - 5$; $\zeta_1 = \dfrac{\sqrt{29}+5}{4}$, $a_1 = 2$, $x_1 = \dfrac{\sqrt{29}-3}{4}$; $\zeta_2 = \dfrac{\sqrt{29}+3}{5}$, $a_2 = 1$, $x_2 = \dfrac{\sqrt{29}-2}{5}$; $\zeta_3 = \dfrac{\sqrt{29}+2}{5}$, $a_3 = 1$, $x_3 = \dfrac{\sqrt{29}-3}{5}$; $\zeta_4 = \dfrac{\sqrt{29}+3}{4}$, $a_4 = 2$, $x_4 = \dfrac{\sqrt{29}-5}{4}$; $\zeta_5 = \dfrac{\sqrt{29}+5}{1}$, $a_5 = 10$, $x_5 = \dfrac{\sqrt{29}-5}{1}$.
   So $q_5 = 1$, so $h_4^2 - 29k_4^2 = (-1)^3 q_5 = -1$. Computing convergents, $h_0 = 5, h_1 = 2 \cdot 5 + 1 = 11, h_2 = 1 \cdot 11 + 5 = 16, h_3 = 1 \cdot 16 + 11 = 27, h_4 = 2 \cdot 27 + 16 = 70$, and $k_0 = 1, k_1 = 2 \cdot 1 + 0 = 2, k_2 = 1 \cdot 2 + 1 = 3, k_3 = 1 \cdot 3 + 2 = 5, k_4 = 2 \cdot 5 + 3 = 13$.
   So $70^2 - 29 \cdot 13^2 = -1$, so computing $(70 + 13\sqrt{29})^2 = 4900 + 70 \cdot 26\sqrt{29} + 169 \cdot 29 = 4900 + 4901 + 1820\sqrt{29} = 9801 + 1820\sqrt{29}$, we have $9801^2 - 29 \cdot 1820^2 = 1$. Then, finally, $(6 + \sqrt{29})(9801 + 1820\sqrt{29}) = 6 \cdot 9801 + 1820 \cdot 29 + 9801\sqrt{29} + 6 \cdot 1820\sqrt{29} = 58806 + 52780 + 9801\sqrt{29} + 10920\sqrt{29} = 111586 + 20721\sqrt{29}$. So $111586^2 - 29 \cdot 20721^2 = 7$.

   If we want an even bigger example, $(9801 + 1820\sqrt{29})^2 = 192119201 + 35675640\sqrt{29}$, and $(192119201 + 35675640\sqrt{29})(6 + \sqrt{29}) = 2187308766 + 406173041\sqrt{29}$, so $2187308766^2 - 29 \cdot 406173041^2 = 7$, as well. If we want smaller values, we can use $(6 - \sqrt{29})(9801 + 1820\sqrt{29}) = 6026 + 1119\sqrt{29}$, so $(6026, 1119)$ also works.