Dr. Marques Sophie
Office 519

Number theory

Fall Semester 2013

marques@cims.nyu.edu

# Problem Set #10

**Due monday november 25th in Class**

**Exercise 1:** ($\star$) 4 points
Show that if $p \geq 7$ is an odd prime, then

$$(\frac{n}{p}) = (\frac{n+1}{p})$$

for at least one of $n = 2, 4, 5$, or 8.

***Solution:***
*Since* $\left(\frac{n}{p}\right) = \pm 1$, *it is enough to show that* $\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = \left(\frac{n(n+1)}{p}\right) = 1$ *for at least one of these value. That is, we wish to show that one of* $\left(\frac{6}{p}\right)$, $\left(\frac{12}{p}\right)$, *or* $\left(\frac{72}{p}\right)$ *is* 1.
*But* $\left(\frac{6}{p}\right) = \left(\frac{2\times 3}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1$ *when* $\left(\frac{2}{p}\right)$ *and* $\left(\frac{3}{p}\right)$ *have the same sign.*

$$(\frac{12}{p}) = (\frac{2^2 \times 3}{p}) = ((\frac{2}{p}))^2(\frac{3}{p}) = (\frac{3}{p}) = 1$$

*when well,* $\left(\frac{3}{p}\right) = 1$. $\left(\frac{72}{p}\right) = \left(\frac{2^3\times 3^2}{p}\right) = ((\frac{2}{p}))^3((\frac{n}{p}))^2 = \left(\frac{2}{p}\right) = 1$ *when* $\left(\frac{2}{p}\right) = 1$.
*So, if* $\left(\frac{2}{p}\right) = 1$ *then* $\left(\frac{8}{p}\right) = \left(\frac{9}{p}\right)$. *If* $\left(\frac{3}{p}\right) = 1$ *then* $\left(\frac{3}{p}\right) = \left(\frac{4}{p}\right)$. *If neither of these cases occur, then both are* $-1$, *so* $\left(\frac{2}{p}\right) = -1 = \left(\frac{3}{p}\right)$. *So,* $\left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right)$ *for at least one of* $n = 2, 3,$ *or* 8.

**Exercise 2:** ($\star$) 3 points
The prime $p$ for which $x^2 \equiv 13 \ mod \ p$ has solutions.

***Solution:***
*Every integer n is congruent to one of* $-6, -5, ..., 5, 6$ *mod* 13. *By quadratic reciprocity,*

$$(\frac{13}{p})(\frac{p}{13}) = (-1)^{\frac{13-1}{2}\frac{p-1}{2}} = (-1)^{6\frac{p-1}{2}} = 1$$

*so* $\left(\frac{p}{13}\right) = \left(\frac{13}{p}\right)$ *Since we can, in this calculation, work with the residue of p mod* 13, *rather that with p, it suffices to compute Legendre symbols for* $n = -6$ *through* $n = 6$. *Each of these numbers is a product of the numbers* $1, -1, 2, 3$ *and* 5, *so it suffices to compute Legendre symbols for them.*

$$(\frac{1}{13}) = 1$$

$$(\frac{-1}{13}) = (-1)^{\frac{13-1}{2}} = (-1)^6 = 1$$

$$\left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = (-1)^{21} = -1$$

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right)(-1)^{\frac{13-1}{2}\frac{3-1}{2}} = \left(\frac{12+1}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right)(-1)^{\frac{13-1}{2}\frac{5-1}{2}} = \left(\frac{10+3}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right)(-1)^2 = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = (-1) = -1$$

*So*

$$\left(\frac{-6}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = 1 \times (-1) \times 1 = -1$$

$$\left(\frac{-4}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right)^2 = 1 \times 1 = 1$$

$$\left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right) = 1 \times (-1) = -1$$

$$\left(\frac{-5}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{5}{13}\right) = 1 \times (-1) = -1$$

$$\left(\frac{-3}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{3}{13}\right) = 1 \times 1 = 1$$

$$\left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = 1$$

$$\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = (-1) \times 1 = -1$$

*So the primes $p$ for which $x^2 \equiv 13 \bmod p$ has solutions are those that are congruent, mod 13, to $-4$, $-3$, $-1$, 1, 3, or 4. Or, if you prefer those congruent to 1, 3, 4, 9, 10 or 12.*

**Exercise 3: ($\star\star$)** 6 points

Compute the continued fraction expansions of 53/18 and 115/53.

***Solution:***

- $53 = 18 \times 2 + 17$, $18 = 17 \times 1 + 1$ *and* $17 = 1 \times 17 + 0$, *so*

$$\frac{53}{18} = 2 + \frac{17}{18} = 2 + \frac{1}{\frac{18}{17}} = 2 + \frac{1}{1 + \frac{1}{17}} = [2, 1, 17]$$

- $115 = 53 \times 2 + 9$ , $53 = 9 \times 5 + 8$, $9 = 8 \times 1 + 1$, $8 + 1 \times 1 + 0$, *so*

$$\frac{115}{53} = [2, 5, 1, 8]$$

**Exercise 4: ($\star\star\star$)** 3 points

If $x = [a_0, ..., a_n, b]$ and $y = [a_0, ..., a_n, c]$ with $b < c$, then $x < y$ if $n$ is odd and $x > y$ is $n$ is even.

***Solution:***

*By induction; for $n=0$, $x=[a_0,b]=a_0+\frac{1}{b}>a_0+\frac{1}{c}=[a_0,c]=y$, since $b<c$ implies $\frac{1}{b}>\frac{1}{c}$. Inductively, if we assume that whenever $B<C$,*

$$[a_0,...,a_{n-1},B]=[a_0,....,a_{n-1},C]=(-1)^{n-1}P$$

*where $P>0$, then*

$$x=[a_0,...,a_n,b]=[a_0,....,a_n+\frac{1}{b}]$$

*and*

$$y=[a_0,...,a_n,c]=[a_0,....,a_n+\frac{1}{c}]$$

*Set $B=a_n+\frac{1}{c}<a_n+\frac{1}{b}=C$, so*

$$[a_0,...,a_n,c]-[a_0,...,a_n,b]=[a_0,...,a_{n-1},B]-[a_0,...,a_{n-1},C]=(-1)^{n-1}P$$

*So, $[a_0,...,a_n,b]-[a_0,...,a_n,c]=(-1)^nP$ as desired.*
*So by induction, $x<y$ if $n$ is odd, and $x>y$ is $n$ is even. Or, without induction:*
*We know that, for $[a_0,...,a_{n-1}]=\frac{h_{n-1}}{k_{n-1}}$ and $[a_0,...,a_n]=\frac{h_n}{k_n}$ that $x=\frac{h_nb+h_{n-1}}{k_nb+k_{n-1}}$ and $y=\frac{h_nc+h_{n-1}}{k_nc+k_{n-1}}$. If we look at*

$$x-y\frac{h_nb+h_{n-1}}{k_nb+k_{n-1}}-\frac{h_nc+h_{n-1}}{k_nc+k_{n-1}}=\frac{(h_nb+h_{n-1})(k_nc+k_{n-1})-(h_nc+h_{n-1})(k_nb+k_{n-1})}{(k_nb+k_{n-1})(k_nc+k_{n-1})}$$

*since the denominator is positive, this will be positive ($x>y$) or negative $x<y$ depending on the sign of the numerator. But*

$$\begin{aligned} & (h_nb+h_{n-1})(k_nc+k_{n-1})-(h_nc+h_{n-1})(k_nb+k_{n-1}) \\ = & (h_nk_nbc+h_{n-1}k_nc+h_nk_{n-1}b+h_{n-1}k_{n-1})-(h_nk_nbc+h_{n-1}k_nb+h_nk_{n-1}b+h_{n-1}k_{n-1}) \\ = & (h_{n-1}k_n-h_nk_{n-1})(c-b)=(-1)^n(c-b)\end{aligned}$$

*Which, since $c-b>0$, is positive when $n$ is even, negative when $n$ is odd.*

**Exercise 5: ($\star\star\star$)** 3 points
Compute the continued fraction expansion of $\sqrt{17}$ and $\sqrt{19}$, use this to find their first five convergents.

***Solution:***

- $a_0=[\sqrt{17}]=4$, $x_0=sort17-4$, $a_1=[\frac{1}{\sqrt{17}-4}]=[\sqrt{17}+4]=8$, $x_1=(\sqrt{17}+4)-8=\sqrt{17}-4=x_0$, *and then the process will repeat, so* $\sqrt{17}=[4,8,8,8,....]$.
  *Using our formula $h_i=h_{i-1}a_i+h_{i-2}$, $k_i=k_{i-1}a_i+k_{i-2}$, we have*

$$\begin{aligned} \frac{h_0}{k_0} &= \frac{4}{1} \\ \frac{h_1}{k_1} &= \frac{4\times8+1}{1\times8+0}=\frac{33}{8} \\ \frac{h_2}{k_2} &= \frac{33\times8+4}{8\times8+1}=\frac{268}{65} \\ \frac{h_3}{k_3} &= \frac{268\times8+33}{65\times8+8}=\frac{2177}{528} \\ \frac{h_4}{k_4} &= \frac{2177\times8+268}{528\times8+65}=\frac{17684}{4289}\end{aligned}$$

- $4 < \sqrt{19} < 5$, *so,*

$$
\begin{array}{ll}
a_0 = [\sqrt{19}] = 4 & x_0 = \sqrt{19} - 4 \\
a_1 = [\frac{1}{\sqrt{19}-4}] = [\frac{\sqrt{19}+4}{3}] = 2 & x_1 = \frac{\sqrt{19}+4}{3} - 2 = \frac{\sqrt{19}-2}{3} \\
a_2 = [\frac{1}{\sqrt{19}-2}] = [\frac{\sqrt{19}+2}{5}] = 1 & x_2 = \frac{\sqrt{19}+3}{2} - 3 = \frac{\sqrt{19}-3}{2} \\
a_3 = [\frac{2}{\sqrt{19}-3}] = [\frac{\sqrt{19}+3}{5}] = 1 & x_3 = \frac{\sqrt{19}+3}{5} - 1 = \frac{\sqrt{19}-2}{5} \\
a_4 = [\frac{5}{\sqrt{19}-2}] = [\frac{\sqrt{19}+2}{3}] = 2 & x_4 = \frac{\sqrt{19}+2}{3} - 2 = \frac{\sqrt{19}-4}{3} \\
a_5 = [\frac{3}{\sqrt{19}-4}] = [\frac{\sqrt{19}+4}{1}] = 8 & x_5 = \frac{\sqrt{19}+4}{8} - 16 = \frac{\sqrt{19}-4}{1} = x_0
\end{array}
$$

*and then the process will repeat, so*

$$\sqrt{19} = [4, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, ....] = [4, \overline{2, 1, 3, 1, 2, 8}]$$

*Using our formula* $h_i = h_{i-1}a_i + h_{i-2}$, $k_i = k_{i-1}a_i + k_{i-2}$, *we have*

$$
\begin{array}{lcl}
\frac{h_0}{k_0} & = & \frac{4}{1} \\
\frac{h_1}{k_1} & = & \frac{4\times2+1}{1\times2+0} = \frac{9}{2} \\
\frac{h_2}{k_2} & = & \frac{9\times1+4}{2\times1+1} = \frac{13}{3} \\
\frac{h_3}{k_3} & = & \frac{13\times3+9}{3\times3+2} = \frac{48}{11} \\
\frac{h_4}{k_4} & = & \frac{48\times1+13}{11\times1+3} = \frac{61}{14}
\end{array}
$$

1

[1] $(\star)$ = easy , $(\star\star)$= medium, $(\star\star\star)$= challenge