### 18.781 Solutions to Problem Set 9

1. We have

$$
\begin{aligned}
x-\frac{p_{n-1}}{q_{n-1}} & =\frac{x_{n} p_{n-1}+p_{n-2}}{x_{n} q_{n-1}+q_{n-2}}-\frac{p_{n-1}}{q_{n-1}} \\
& =\frac{p_{n-2} q_{n-1}-p_{n-1} q_{n-2}}{q_{n-1}\left(x_{n} q_{n-1}+q_{n-2}\right)} \\
& =\frac{(-1)^{x-1}}{q_{n-1}\left(x_{n} q_{n-1}+q_{n-2}\right)}
\end{aligned}
$$

Now as $n \rightarrow \infty$ we've shown that $q_{n} \rightarrow \infty$. So

$$
\left|x-\frac{p_{n-1}}{q_{n-1}}\right| \rightarrow 0
$$

from above.
2. Using $n+1$ instead of $n$ in Problem 1, we have

$$
\begin{aligned}
\left|q_{n} x-p_{n}\right| & =q_{n}\left|x-\frac{p_{n}}{q_{n}}\right| \\
& =\frac{1}{\left|x_{n+1} q_{n}+q_{n-1}\right|} \\
& =\frac{1}{x_{n+1} q_{n}+q_{n-1}}
\end{aligned}
$$

since $x_{n+1} \geq 1$. We need to show that the RHS is greater than $1 / q_{n+2}$. Now $x_{n+1}<a_{n+1}+1$, so

$$
\begin{aligned}
x_{n+1} q_{n}+q_{n-1} & <\left(a_{n+1}+1\right) q_{n}+q_{n-1} \\
& =a_{n+1} q_{n}+q_{n-1}+q_{n} \\
& =q_{n+1}+q_{n} \\
& \leq a_{n+2} q_{n+1}+q_{n} \\
& =q_{n+2}
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
\left|x-\frac{p_{n+1}}{q_{n+1}}\right| & \leq \frac{1}{q_{n+1} q_{n+2}} \\
& <\frac{\left|x q_{n}-p_{n}\right|}{q_{n+1}} \\
& =\frac{q_{n}}{q_{n+1}}\left|x-\frac{p_{n}}{q_{n}}\right|
\end{aligned}
$$

and since $q_{n+1}=a_{n} q_{n}+q_{n-1}>q_{n}$, we get

$$
\left|x-\frac{p_{n+1}}{q_{n+1}}\right|<\left|x-\frac{p_{n}}{q_{n}}\right| .
$$

3. (a) Proceed by contradiction, assuming that $b<q_{n+1}$ and $|b x-a|<\left|q_{n} x-p_{n}\right|$. As in the hint, we write the vector $(a, b)$ as an integer linear combination of $\left(p_{n}, q_{n}\right)$ and $\left(p_{n+1}, q_{n+1}\right)$. This is possible because the matrix with rows $\left(p_{n}, q_{n}\right)$ and $\left(p_{n+1}, q_{n+1}\right)$ has determinant $(-1)^{n+1}$ and is therefore invertible with the inverse having integer entries. So there are integers $y, z$ such that

$$
\begin{aligned}
& a=y p_{n}+z p_{n+1} \\
& b=y q_{n}+z q_{n+1}
\end{aligned}
$$

First let's make sure that $y$ and $z$ are nonzero. If $y=0$ then $b=z q_{n+1}$, which is impossible since $0<b<q_{n+1}$. If $z=0$ then

$$
|b x-a|=|y|\left|x q_{n}-p_{n}\right| \geq\left|x q_{n}-p_{n}\right|
$$

contradicting the assumption that $|x b-a|<\left|x q_{n}-p_{n}\right|$. So both $y$ and $z$ are nonzero.
Next, we'll show that they have opposite signs. If $z>0$ then

$$
y q_{n}=b-z q_{n+1} \leq b-q_{n+1}<0
$$

so $y<0$, and if $z<0$ then

$$
y q_{n}=b-z q_{n+1}>0
$$

so $y>0$. Finally,

$$
\begin{aligned}
x b-a & =x\left(y q_{n}+z q_{n+1}\right)-\left(y p_{n}+z p_{n+1}\right) \\
& =y\left(x q_{n}-p_{n}\right)+z\left(x q_{n+1}-p_{n+1}\right)
\end{aligned}
$$

Now we showed that $x-p_{n} / q_{n}$ and $x-p_{n+1} / q_{n+1}$ have opposite signs. Since $y$ and $z$ have opposite signs, $y\left(x q_{n}-p_{n}\right)$ and $z\left(x q_{n+1}-p_{n+1}\right)$ have the same sign. So

$$
\begin{aligned}
|b x-a| & =\left|y\left(x q_{n}-p_{n}\right)+z\left(x q_{n+1}-p_{n+1}\right)\right| \\
& =|y|\left|x q_{n}-p_{n}\right|+|z|\left|x q_{n+1}-p_{n+1}\right| \\
& \geq\left|q_{n} x-p_{n}\right|
\end{aligned}
$$

contradiction.
(b) Suppose $1 \leq b \leq q_{n}$. Then $b<q_{n+1}$, so by part (a), $|b x-a| \geq\left|q_{n} x-p_{n}\right|$. Since $1 / b \geq 1 / q_{n}$,

$$
\left|x-\frac{a}{b}\right| \geq\left|x-\frac{p_{n}}{q_{n}}\right|
$$

4. Suppose $a / b$ is not a convergent. As in the hint, choose $n$ such that $q_{n} \leq b<q_{n+1}$. (This is possible since the $q_{i}$ are increasing and go to infinity.) Then

$$
\begin{aligned}
\left|x-\frac{p_{n}}{q_{n}}\right| & =\frac{1}{q_{n}}\left|p_{n} x-q_{n}\right| \\
& \leq \frac{1}{q_{n}}|b x-a| \\
& <\frac{1}{q_{n}} \cdot \frac{b}{2 b^{2}} \\
& =\frac{1}{2 b q_{n}} .
\end{aligned}
$$

Now $\left|a q_{n}-b p_{n}\right| \geq 1$ because by assumption $\frac{a}{b} \neq \frac{p_{n}}{q_{n}}$. Hence,

$$
\begin{aligned}
\frac{1}{b q_{n}} & \leq \frac{\left|a q_{n}-b p_{n}\right|}{b q_{n}} \\
& =\left|\frac{a}{b}-\frac{p_{n}}{q_{n}}\right| \\
& \leq\left|\frac{a}{b}-x\right|+\left|x-\frac{p_{n}}{q_{n}}\right| \\
& <\frac{1}{2 b^{2}}+\frac{1}{2 b q_{n}} .
\end{aligned}
$$

This implies that $\frac{1}{2 b q_{n}}<\frac{1}{2 b^{2}}$, so $b<q_{n}$, contradiction.
5. Problem 4 shows that if $p / q$ satisfies

$$
\begin{equation*}
\left|\phi-\frac{p}{q}\right|<\frac{1}{\kappa q^{2}} \tag{1}
\end{equation*}
$$

then $p / q$ is a convergent to $\phi$, since $\kappa>\sqrt{5}>2$. So it's enough to show that only finitely many convergents $p_{n} / q_{n}$ to $\phi$ can satisfy this bound.
We showed that the $(n-1)$ st convergent to $\phi$ is just $F_{n+1} / F_{n}$. So suppose

$$
\begin{equation*}
\left|\phi-\frac{F_{n+1}}{F_{n}}\right|<\frac{1}{\kappa F_{n}^{2}} \tag{*}
\end{equation*}
$$

Now, we claim that

$$
\lim _{n \rightarrow \infty}\left|\left(\phi-\frac{F_{n+1}}{F_{n}}\right) F_{n}^{2}\right|=\frac{1}{\sqrt{5}}
$$

From this statement it would then follow that for some sufficiently large $N$,

$$
\left|\left(\phi-\frac{F_{n+1}}{F_{n}}\right) F_{n}^{2}\right|>\frac{1}{\kappa}
$$

for all $n>N$. Then the only solutions to $(*)$ occur when $n \leq N$, and thus there are finitely many such convergents.
Now let $\alpha$ and $\beta$ be the roots of $x^{2}-x-1=0$, with $\phi=\alpha>\beta$. Since $F_{n}=\left(\alpha^{n}-\beta^{n}\right) /(\alpha-\beta)$,

$$
\begin{aligned}
\left(\phi-\frac{F_{n+1}}{F_{n}}\right) F_{n}^{2} & =\left(\alpha-\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha^{n}-\beta^{n}}\right) \frac{\left(\alpha^{n}-\beta^{n}\right)^{2}}{(\alpha-\beta)^{2}} \\
& =\left(\frac{\beta^{n}(\beta-\alpha)}{\alpha^{n}-\beta^{n}}\right) \frac{\left(\alpha^{n}-\beta^{n}\right)^{2}}{(\alpha-\beta)^{2}} \\
& =\frac{-\beta^{n}\left(\alpha^{n}-\beta^{n}\right)}{\alpha-\beta} \\
& =-\frac{(\alpha \beta)^{n}-\beta^{2 n}}{\alpha-\beta} \\
& =-\frac{(-1)^{n}-\beta^{2 n}}{\alpha-\beta}
\end{aligned}
$$

We know that $\beta^{2 n} \rightarrow 0$ as $n \rightarrow \infty$ because $|\beta|<1$. It follows that the magnitude of the RHS approaches $1 / \sqrt{5}$, and we are done.
6. (a) Since $i$ is the largest integer such that $q_{i} \leq \sqrt{p}$, we have $\sqrt{p}<q_{i+1}$. So

$$
\left|\frac{p_{i}}{q_{i}}-\frac{u}{p}\right|<\frac{1}{q_{i} q_{i+1}}<\frac{1}{q_{i} \sqrt{p}}
$$

Multiplying by $p q_{i}$, we get the desired bound $\left|p_{i} p-u q_{i}\right|<\sqrt{p}$.
(b) We have $x=q_{i} \leq \sqrt{p}$, and by part (a), $|y|=\left|p_{i} p-u q_{i}\right|<\sqrt{p}$, so $x^{2}+y^{2}<p+p=2 p$. Moreover,

$$
\begin{aligned}
x^{2}+y^{2} & \equiv q_{i}^{2}+u^{2} q_{i}^{2} \\
& \equiv\left(u^{2}+1\right) q_{i}^{2} \\
& \equiv 0 \quad(\bmod p)
\end{aligned}
$$

Clearly, $x^{2}+y^{2}>0$, since $x=q_{i}>0$. The only multiple of $p$ in $(0,2 p)$ is $p$, so we must have $x^{2}+y^{2}=p$.
7. We need to find all $c$ such that $x=(\sqrt{d}+\lfloor\sqrt{d}\rfloor) / c>1$ and its conjugate $x^{\prime}=(-\sqrt{d}+\lfloor\sqrt{d}\rfloor) / c$ lies between 0 and -1 . The second condition is automatic since the numerator is always between 0 and -1 , and $c$ is a positive integer. The first condition holds for all positive integers $c \leq 2\lfloor\sqrt{d}\rfloor$.
8. (a) Consider the fractional part $\{i x\}$ of $i x$ as $i$ ranges from 0 through $N$. Since $x$ is irrational, each $\{i x\}$ is a distinct number in the range $[0,1)$. In fact, we'll want to wrap the interval into a circle. Consider the $N+1$ segments that the circle is broken up into by the $\{i x\}$. Since the total arclength of the segments is 1 , some segment has length no more than $\frac{1}{N+1}$. What this means is that there are two integers $i, j \in\{0,1, \ldots, N\}$ such that for some integer $a$

$$
0<|j x-i x+a| \leq \frac{1}{N+1}
$$

Setting $q=|i-j|<N$ and $p=a$, division by $i-j$ yields

$$
0<\left|x-\frac{p}{q}\right| \leq \frac{1}{q(N+1)}
$$

as desired.
(b) First we pick any $N_{1}$, and find $q_{1} \leq N_{1}$ such that

$$
\left|x-\frac{p_{1}}{q_{1}}\right| \leq \frac{1}{q_{1}\left(N_{1}+1\right)}<\frac{1}{q_{1}^{2}}
$$

Then, since $x$ is irrational, we can pick an $N_{2}$ such that

$$
\frac{1}{N_{2}}<\left|x-\frac{p_{1}}{q_{1}}\right|
$$

Again using part (a), there exists $p_{2} / q_{2}$ with $q_{2} \leq N_{2}$ such that

$$
\left|x-\frac{p_{2}}{q_{2}}\right| \leq \frac{1}{q_{2}\left(N_{2}+1\right)}<\frac{1}{N_{2}}<\left|x-\frac{p_{1}}{q_{1}}\right|
$$

so $p_{1} / q_{1}$ is distinct from $p_{2} / q_{2}$, and as before

$$
\left|x-\frac{p_{2}}{q_{2}}\right| \leq \frac{1}{q_{2}\left(N_{2}+1\right)}<\frac{1}{q_{2}^{2}}
$$

Picking $N_{3}$ with $1 / N_{3}<\left|x-p_{2} / q_{2}\right|$ and continuing this process, we can form an infinite series of distinct $p_{i} / q_{i}$ such that $\left|x-p_{i} / q_{i}\right|<1 / q_{i}^{2}$.
9. (a) We have that $x=m+\frac{1}{x}$. Solving the quadratic equation and taking the positive root, we get

$$
x=\frac{m+\sqrt{m^{2}+4}}{2}
$$

(b) We know that $p_{n}=m p_{n-1}+p_{n-2}$, so the characteristic polynomial is $x^{2}-m x-1=0$. Thus, letting

$$
\alpha=\frac{m+\sqrt{m^{2}+4}}{2}, \beta=\frac{m-\sqrt{m^{2}+4}}{2}
$$

be the roots of the characteristic polynomial, $p_{n}=A \alpha^{n}+B \beta^{n}$. Using the initial conditions $p_{0} / q_{0}=m / 1$ and $p_{1} / q_{1}=\left(m^{2}+1\right) / m$, we can solve the linear system of equations to get

$$
\left\{\begin{array}{l}
A=\frac{\alpha^{2}}{\sqrt{m^{2}+4}} \\
B=\frac{-\beta^{2}}{\sqrt{m^{2}+4}}
\end{array}\right.
$$

So

$$
\begin{aligned}
p_{n} & =\frac{1}{\sqrt{m^{2}+4}}\left(\alpha^{n+2}-\beta^{n+2}\right) \\
& =\frac{\alpha^{n+2}-\beta^{n+2}}{\alpha-\beta} .
\end{aligned}
$$

Similarly, it can be shown that $q_{n}=\left(\alpha^{n+1}-\beta^{n+1}\right) /(\alpha-\beta)$. Therefore,

$$
\frac{p_{n}}{q_{n}}=\frac{\alpha^{n+2}-\beta^{n+2}}{\alpha^{n+1}-\beta^{n+1}} .
$$

10. (a) Suppose we have proven the inequality for $n=2^{k-1}$. Then

$$
\begin{aligned}
\frac{r_{1}+\cdots+r_{2^{k}}}{2^{k}} & =\frac{\left(\frac{r_{1}+\cdots+r_{2^{k-1}}}{2^{k-1}}\right)+\left(\frac{r_{2^{k-1}+1}+\cdots+r_{2^{k}}}{2^{k-1}}\right)}{2} \\
& \geq \frac{\left(r_{1} \cdots r_{2^{k-1}}\right)^{\frac{1}{2^{k-1}}}+\left(r_{2^{k-1}+1} \cdots r_{2^{k}}\right)^{\frac{1}{2^{k-1}}}}{2} \\
& \geq \sqrt{\left(r_{1} \cdots r_{2^{k-1}}\right)^{\frac{1}{2^{k-1}}} \cdot\left(r_{2^{k-1}+1} \cdots r_{2^{k}}\right)^{\frac{1}{2^{k-1}}}} \\
& =\sqrt[2^{k}]{r_{1} \cdots r_{2^{k}}},
\end{aligned}
$$

completing the induction.
(b) Let $2^{k-1}<n \leq 2^{k}$, and append $2^{k}-n$ copies of $r=\frac{r_{1}+\cdots+r_{n}}{n}$. Then the arithmetic mean of $r_{1}, \ldots, r_{n}, r, \ldots, r$ is

$$
\begin{aligned}
\frac{r_{1}+\cdots+r_{n}+\left(2^{k}-n\right) r}{2^{k}} & =\frac{n r+\left(2^{k}-n\right) r}{2^{k}} \\
& =\frac{2^{k} r}{2^{k}} \\
& =r
\end{aligned}
$$

Now part (a) tells us that

$$
r \geq\left(r_{1} \cdots r_{n} \cdot r \cdots r\right)^{1 / 2^{k}}
$$

so

$$
r^{2 k} \geq\left(r_{1} \cdots r_{n}\right) \cdot r^{2^{k}-n}
$$

from which it follows that

$$
r \geq \sqrt[n]{r_{1} \cdots r_{n}}
$$

Equality holds if and only if $r_{1}=r_{2}=\cdots=r_{n}$.
11. We will first define a particular number $x$ (called Liouville's number) which will work for any $c$. Choose exponents $e_{n}=n$ ! and let $q_{n}=10^{e_{n}}$. Note that for all $k, e_{k}<e_{k+1}$, so $q_{k} \mid q_{k+1}$. Now define

$$
x=1+\frac{1}{q_{1}}+\frac{1}{q_{2}}+\frac{1}{q_{3}}+\cdots
$$

which converges because $q_{n} \geq 10^{n}$ and the geometric series $1+1 / 10+1 / 100+\cdots$ converges, and let

$$
\frac{p_{n}}{q_{n}}=1+\frac{1}{q_{1}}+\cdots+\frac{1}{q_{n}}
$$

The denominator is exactly $q_{n}$ because each of $q_{1}, \ldots, q_{n-1}$ must divide $q_{n}$. Now

$$
\begin{aligned}
\left|x-\frac{p_{n}}{q_{n}}\right| & =\left|\frac{1}{q_{n+1}}+\frac{1}{q_{n+2}}+\cdots\right| \\
& =\frac{1}{q_{n+1}}\left|1+\frac{q_{n+1}}{q_{n+2}}+\frac{q_{n+1}}{q_{n+3}}+\cdots\right| \\
& <\frac{1}{q_{n+1}}\left|1+\frac{1}{2}+\frac{1}{4}+\cdots\right| \\
& =\frac{2}{q_{n+1}}
\end{aligned}
$$

So we'll be done if we show that for all large enough $n$,

$$
\frac{2}{q_{n+1}}<\frac{1}{q_{n}^{c}} .
$$

Taking logs base 10 , this is equivalent to saying that

$$
\log _{10} 2+c(n!)<(n+1)!
$$

which is obviously true as soon as $n>c+1$, for instance. Thus, for any $c$, there are infinitely many rational numbers $p / q$ such that

$$
\left|x-\frac{p}{q}\right|<\frac{1}{q^{c}} .
$$

MIT OpenCourseWare
http://ocw.mit.edu

### 18.781 Theory of Numbers

Spring 2012

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.

