Remark without proof. An infinite simple continued fraction has a repeating block if and only if it is a quadratic irrational of the form $\frac{a + b\sqrt{d}}{c}$ for integers $a, b, c, d$, where $d$ is a non-square.

Remark without proof. The continued fraction of $\sqrt{d}$ with $d$ a non-square integer has a very interesting structure. For example it always has the form $x = [a, \ldots, 2a]$ after which the block repeats. The stuff between the $a$ and $2a$ also has very interesting symmetries.

Remark without proof. Almost nothing is known about the continued fraction expansions of other real numbers. For example the convergents of $\sqrt{2}$ are not known. Though for example $\sqrt{2} = [1, 2, 2, 2, \ldots]$ and so the partial quotients are all bounded, a similar result is not known for $\sqrt{3}$.

There is one interesting number whose continued fraction is known:

$$e = [2, 1, 2, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$$

**Theorem 8.** There are only finitely many rational numbers $\frac{p}{q}$ such that $r - \frac{p}{q} < \frac{1}{q^2}$ for any rational number $r > 0$.

Proof Suppose that $r = \frac{a}{b} > 0$ and

$$|r - \frac{p}{q}| = \left| \frac{a}{b} - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Multiply by $bq$ to get

$$|aq - bp| > \frac{|b|}{|q|}.$$

If $|q| \geq |b|$, then $\frac{|b|}{|q|} \leq 1$, and so

$$|aq - bp| < 1.$$

But $|aq - bp|$ is a non-negative integer and so it must be 0.

Hence $aq = bp$ and

$$\frac{p}{q} = \frac{a}{b} = r.$$
Hence there is only one rational number \( \frac{p}{q} \) with \( |q| \geq |b| \) which satisfies the inequality \( \left| \frac{a}{b} - \frac{p}{q} \right| < \frac{1}{q^2} \), namely \( \frac{a}{b} \) itself.

This leaves only finitely many possibilities for \( q \).

For each of those finitely many possibilities for \( q \) we have \( |aq - bp| < \frac{|b|}{|q|} \) and so

\[
aq - \frac{|b|}{|q|} < bp < aq + \frac{|b|}{|q|}.
\]

Hence \( bp \) lies in a finite interval \( (aq - \frac{|b|}{|q|}, aq + \frac{|b|}{|q|}) \) of length \( 2\frac{|b|}{|q|} \). Any such interval has only finitely many integer multiples of an integer \( p \) so there are only finitely many choices of \( p \) for those finitely many values of \( q \). Hence there are only finitely many rational \( \frac{p}{q} \) which satisfy the condition.

Remark. If we have \( r = \frac{a}{b} > 0 \), with of course \( a > 0, b > 0 \), then there are never any negative rationals \( \frac{p}{q} \) such that \( |r - \frac{p}{q}| < \frac{1}{q^2} \) and so it is never necessary to check the negative values of \( q \) above. For if \( \left| \frac{a}{b} - \frac{p}{q} \right| < \frac{1}{q^2} \), then multiplying by \( |bq| \) we have

\[
|aq - bp| < \frac{|b|}{|q|}.
\]

If \( \frac{p}{q} < 0 \), with \( q < 0 \), and \( p > 0 \), then \( |q| = -q \) and

\[
\frac{|b|}{|q|} > |aq - bp| = |-a|q| - bp| = a|q| + bp \geq b,
\]

because \( a, p, q \) are integers \( \geq 1 \). This is a contradiction.

We will only ever need to check positive approximations in applications of this theorem.

This completes the proof.

This proof will become clearer from an example.

There are only finitely many rationals \( \frac{p}{q} \) such that \( \left| \frac{4}{7} - \frac{p}{q} \right| < \frac{1}{q^2} \).

For if \( \left| \frac{4}{7} - \frac{p}{q} \right| < \frac{1}{q^2} \), then multiplying by \( 7q \) we have

\[
|4q - 7p| < \frac{7}{|q|}.
\]

If \( |q| \geq 7 \), then \( \frac{7}{|q|} \leq 1 \) and so \( |4q - 7p| < 1 \).
Since $|4q - 7p|$ is a non-negative integer less than 1, it must be zero. Hence $|4q - 7p| = 0$ and $\frac{p}{q} = \frac{4}{7}$.

Suppose $q = 6$. Then we have $|4.6 - 7p| < \frac{7}{6}$ and so $7p$ is a multiple of 7 in the interval $(24 - \frac{7}{6}, 24 + \frac{7}{6})$. There are no multiples of 7 in this interval and so no rational with the property with denominator 6.

Suppose $q = 5$. Then we have $|4.5 - 7p| < \frac{7}{5}$ and so $7p$ is a multiple of 7 in the interval $(20 - \frac{7}{5}, 20 + \frac{7}{5})$. There is only one integer multiple of 7 in that interval, namely, 21, and so $p = 3$ in this case. There is one rational in the interval and so only one rational $\frac{3}{5}$ with the property with denominator 5.

Suppose $q = 4$. Then we have $|4.4 - 7p| < \frac{7}{4}$ and so $7p$ is a multiple of 7 in the interval $(16 - \frac{7}{4}, 16 + \frac{7}{4})$. There is no integer multiple of 7 in that interval and so no rational in the interval.

Suppose $q = 3$. Then we have $|4.3 - 7p| < \frac{7}{3}$ and so $7p$ is a multiple of 7 in the interval $(12 - \frac{7}{3}, 12 + \frac{7}{3})$. There is only one integer multiple of 7 in that interval, namely, 14, and so $p = 2$ in this case. There is one rational in the interval and so only one rational $\frac{2}{3}$ with the property with denominator 3.

Suppose $q = 2$. Then we have $|8 - 7p| < \frac{7}{2}$ and so $7p$ is a multiple of 7 in the interval $(8 - \frac{7}{2}, 8 + \frac{7}{2})$. There is only one integer multiple of 7 in that interval, namely, 7, and so $p = 1$, in this case. There is one rational in the interval and so only one rational $\frac{1}{2}$ with the property with denominator 2.

Suppose $q = 1$. Then we have $|4 - 7p| < \frac{7}{1}$ and so $7p$ is a multiple of 7 in the interval $(4 - \frac{7}{1}, 4 + \frac{7}{1}) = (-3, 11)$. There are two integer multiples of 7 in that interval, namely, 0 and 1, and so 0 and $p = 1$ in this case. There are two rationals in the interval with the property, namely, 0 and 1.

If $q < 0$ and $p < 0$ then $\frac{p}{q} > 0$ and we obviously get the same collection of rationals in this case.

If $q < 0$ and $p > 0$ then $\frac{p}{q} < 0$ and so $\frac{1}{q^2} > \frac{|p|}{q^2} > \frac{|p - 4|}{7} > \frac{4}{7}$.

Hence $|q| = 1$ and $q = -1$ and $\frac{p}{q}$ is an integer. But then

$$\frac{1}{q^2} > \frac{|4 - p|}{q} \geq 1 + \frac{4}{7} = \frac{11}{7}.$$

This is a contradiction..

As we have shown it is never necessary to check values of $q$ which are negative.

I want us to do arithmetic in a number of different algebras and so at this time I want us to consider a quite different ring.
**Definition:** The polynomial ring $\mathbb{Z}_p[x]$ is the set of all polynomials $a_0 + a_1x + \ldots + a_nx^n$ for any $n \geq 0$, where $a_i \in \mathbb{Z}_p$, for some prime $p$ and $x$ is the unknown! Just a placeholder..

We define addition and multiplication in the usual way. I’m sure you know how to calculate with polynomials in $\mathbb{Z}_p[x]$.

Please remind yourself of how to divide two polynomials to get a quotient and remainder of degree smaller than the degree of the divisor. So we have a Division Algorithm in $\mathbb{Z}_p[x]$. In fact this algorithm works for polynomials in $\mathbb{F}[x]$ for any field $\mathbb{F}$. We won’t bother giving a formal proof of this. You know how to divide one polynomial by another with rational, real or complex coefficients. You will also be able to do it for polynomials with coefficients in $\mathbb{Z}_p$. When later we need to do it for other fields, it will be no effort either.