Continued fractions: closeness of the approximations

Throughout this section, we suppose that θ is irrational, so that the continued fraction process does not terminate.

(a) $|q_n\theta - p_n|$ decreases as n increases.

Proof $\theta = \frac{p_n\theta_{n+1}+p_{n-1}}{q_n\theta_{n+1}+q_{n-1}}$, hence, using 1.5(a),

$$\begin{aligned}
|q_n\theta - p_n| &= |\frac{q_np_n\theta_{n+1} + q_np_{n-1} - p_nq_n\theta_{n+1} - p_nq_{n-1}}{q_n\theta_{n+1} + q_{n-1}}| \\
&= \frac{1}{q_n\theta_{n+1} + q_{n-1}} \\
&< \frac{1}{q_n + q_{n-1}} \\
&= \frac{1}{(a_n + 1)q_{n-1} + q_{n-2}} \\
&< \frac{1}{q_{n-1}\theta_n + q_{n-2}} \\
&= |q_{n-1}\theta - p_{n-1}|.
\end{aligned}$$

(b) The convergents give successively closer approximations to θ.

Proof This is a weaker statement than (a).

(c)

$$\frac{1}{(a_{n+1} + 2)q_n^2} < |\theta - \frac{p_n}{q_n}| < \frac{1}{a_{n+1}q_n^2} \leq \frac{1}{q_n^2}.$$

Proof $a_{n+1}q_n^2 < q_n^2\theta_{n+1} + q_nq_{n-1} < (a_{n+1}+2)q_n^2$. Now use $|\theta - p_n/q_n| = 1/(q_n^2\theta_{n+1} + q_nq_{n-1})$, as in the proof of (a).

(d) If p and q are integers with $0 < q < q_{n+1}$, then $|q\theta - p| \geq |q_n\theta - p_n|$. (In this sense, continued fraction approximations are "best possible".)

Proof From 1.5(a), we can find integers u, v such that

$$\begin{aligned} p &= up_n + vp_{n+1}, \\ q &= uq_n + vq_{n+1}. \end{aligned}$$

Thus $u \neq 0$ $(0 < q < q_{n+1})$. If $v \neq 0$, then u and v cannot both be negative $(0 < q)$ nor both positive $(q < q_{n+1})$, so they have opposite signs. Since $q_n\theta - p_n$ and $q_{n+1}\theta - p_{n+1}$ also have opposite signs, we have

$$|q\theta - p| = |u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})| \geq |q_n\theta - p_n|,$$

as required.

(e) If p, q are positive integers with $|\theta - p/q| < 1/(2q^2)$, then p/q is a convergent to θ.

Proof Take n such that $q_n \leq q < q_{n+1}$ (one can clearly do this if θ is irrational; as an exercise, check the rational case). Then

$$\begin{aligned} |p/q - p_n/q_n| &\leq |\theta - p/q| + |\theta - p_n/q_n| \\ &= q^{-1}|q\theta - p| + q_n^{-1}|q_n\theta - p_n| \\ &\leq (1/q + 1/q_n)|q\theta - p| \quad \text{by (d)} \\ &< (2/q_n).(1/2q) \\ &= 1/qq_n. \end{aligned}$$

Hence $|p/q - p_n/q_n| = 0$.

Thus we see that all continued fraction approximations are "good", and that all "sufficiently good" rational approximations arise via the continued fraction process.

Continued fractions: quadratic irrationals

The partial quotients of θ are ultimately periodic if and only if θ is a quadratic irrational. (For a proof see any of the standard texts.) Moreover, the continued fraction expansion of $\sqrt{n}$ can be computed using only integer arithmetic,

and relatively low precision.

Example
$\lfloor\sqrt{19}\rfloor = 4$

$\sqrt{19} = 4 + (\sqrt{19} - 4)$

$\frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{19-16} = \frac{\sqrt{19}+4}{3}$

$\lfloor\frac{\sqrt{19}+4}{3}\rfloor = \lfloor\frac{4+4}{3}\rfloor$
(Exercise: $\lfloor\frac{a+b}{c}\rfloor = \lfloor\frac{\lfloor a\rfloor+b}{c}\rfloor$ for any positive integers b, c.)

$\frac{\sqrt{19}+4}{3} = 2 + \frac{\sqrt{19}-2}{3}$

$\frac{3}{\sqrt{19}-2} = \frac{3(\sqrt{19}+2)}{15} = \frac{\sqrt{19}+2}{5}$
(Exercise: the denominator always divides the norm of the numerator, which keeps the numbers small.)

The Legendre symbol

If n is an integer with $n \geq 2$, then $(\mathbb{Z}/n\mathbb{Z})^*$ denotes the multiplicative group of those residue classes of integers mod n which are relatively prime to n. The order of this group is $\phi(n)$, where ϕ is **Euler's totient function**.

Let p be prime, greater than 2. Then $\phi(p) = p - 1$. Moreover $(\mathbb{Z}/p\mathbb{Z})^*$ is then cyclic. The subset of invertible squares mod p is a subgroup of order $(p-1)/2$. Indeed if g is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, then the squares are precisely the even powers of g, and the non-squares are the odd powers of g.

If b is an integer, and p is an odd prime, then the **Legendre symbol**, $(\frac{b}{p})$, is defined by

$$\begin{aligned}(\tfrac{b}{p}) &= 0 \text{ if } p \text{ divides } b;\\ (\tfrac{b}{p}) &= 1 \text{ if } b \text{ is a non-zero square mod } p;\\ (\tfrac{b}{p}) &= - \text{ if } b \text{ is a not a square mod } p.\end{aligned}$$

If $(\frac{b}{p}) = 1$, then b is called a **quadratic residue** mod p; if $(\frac{b}{p}) = -1$, then b is called a **quadratic non-residue** mod p.

The Legendre symbol $(\frac{b}{p})$ can be computed in $O(p)$ operations in $(\mathbb{Z}/p\mathbb{Z})^*$, simply by testing whether $a^2 = b \pmod p$ for $a = 1, 2, \ldots, p-1$. We can do much better by using **Euler's criterion**:

$$(\tfrac{b}{p}) = b^{(p-1)/2} (\text{mod } p).$$

This is trivial if p divides b. Otherwise note that $g^r = 1 (\text{mod } p)$ if and only if $p-1$ divides r, and deduce that $b^{(p-1)/2} = 1 (\text{mod } p)$ if and only if b is an even power of g, and so, equivalently, if and only if b is a non-zero square mod p. If b is not a square mod p then $b^{(p-1)/2}$ is a non-trivial square-root of 1(mod p), and so must be -1. Using the modular exponentiation algorithm of §1.3 we can compute $(\frac{b}{p})$ via Euler's criterion in $O(\log p)$ operations in $(\mathbb{Z}/p\mathbb{Z})^*$.

The Jacobi symbol

If n is composite, then the structure of $(\mathbb{Z}/n\mathbb{Z})^*$ is more complicated than when n is prime. The group is usually not cyclic. In general, far fewer than half the elements are squares. We shall extend the Legendre symbol $(\frac{b}{n})$ to include odd composite n, when $(\frac{b}{n})$ is called the **Jacobi symbol**. It will still be true that $(\frac{b}{n}) = 1$ for all b which are squares mod n (and relatively prime to n) but $(\frac{b}{n})$ will equal 1 for some non-squares also. Indeed $(\frac{b}{n})$ will equal 1 for exactly half the elements of $(\mathbb{Z}/n\mathbb{Z})^*$.

If $n = \prod_i p_i^{e_i}$, where the p_i are distinct odd primes, we define the Jacobi symbol by

$$(\tfrac{b}{n}) = \prod_i (\tfrac{b}{p_i})^{e_i}$$

(with $(\frac{b}{1}) = 1$), where the expression on the right is a product of Legendre symbols.

The Jacobi symbol satisfies the following properties (where m, n are odd positive integers, and a, b are arbitrary integers).

(a) $(\frac{b}{n}) = (\frac{b \bmod n}{n})$;

(b) $(\frac{b}{mn}) = (\frac{b}{m})(\frac{b}{n})$;

(c) $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$;

(d) $(\frac{-1}{n}) = (-1)^{(n-1)/2}$;

(e) $(\frac{2}{n}) = (-1)^{(n^2-1)/8}$;

(f) $(\frac{m}{n}) = (\frac{n}{m})(-1)^{(m-1)(n-1)/4}$.

All of these follow readily from properties of the Legendre symbol. For the Legendre symbol, formula (f) is the celebrated law of **quadratic reciprocity**, first proved by Gauss. We take these properties on trust, and use them to remark that the Jacobi symbol $(\frac{b}{n})$ can be computed in $O(\log n)$ operations on $\mathbb{Z}/n\mathbb{Z}$ without needing to know the prime factorization of n. Indeed by (a) we can suppose that $0 \leq b < n$, and then we can use (c) and (e) to remove any factors of 2 from b, to reduce to the case in which b and n are positive odd integers; then (f) reduces the computation to that of $(\frac{n}{b})$. One may check that after two such reductions the value of "n" is at least halved. Thus after $O(\log n)$ reductions we will be left with either $(\frac{1}{n})$ or $(\frac{0}{n})$, which have values 1 and 0 respectively. The reader will observe that this process is somewhat similar to the "binary gcd algorithm".

Square-roots modulo a prime

We start with a particularly simple special case. If $p = 3 \pmod 4$ we may write $p = 2s + 1$ with s odd. Then $x = b^{(s+1)/2}$ will be a square root of $b \bmod p$ whenever b is a quadratic residue of p. To see this we note that $b^s = b^{(p-1)/2} = 1 \pmod p$, by Euler's criterion, so that

$$x^2 = b^{s+1} = b \pmod p.$$

In general we have to work a bit harder. Suppose again that we are trying to find a square-root of $b \pmod p$, where b is a quadratic residue of p. Assume we have an integer z which is a quadratic non-residue modulo p. (It is not quite obvious, but in fact the above algorithm for $p = 3 \pmod 4$ corresponds to taking $z = -1$.) Write $p - 1 = 2^r s$, where s is odd, and set

$$y = z^s \pmod p.$$

Then run the following procedure.

Step 1. Initialize by setting $w = b^{(s+1)/2} \pmod p$ and $n = r$.

Step 2. Check whether $w^2 = b \pmod p$, and if so set $x = w$ and stop.

Step 3. Compute $(w^2 b^{-1})^{2^{t-1}}$ modulo p for $t = n-1, n-2, \ldots$ until one reaches a value which is -1 modulo p.

Step 4. Set $w_0 = wy^{2^{r-t-1}} \pmod p$.

Step 5. Replace w by w_0 and n by $n - 1$, and return to Step 2.

Of course the parameter n plays no role in the algorithm — it is just a convenience for the proof. To check that this works we will show that we always have $(w^2 b^{-1})^{2^{n-1}} = 1 \pmod p$ at Step 2. In particular, if we ever get down to $n = 1$ we will have $w^2 = b \pmod p$. We prove this claim by induction. It is certainly true at the outset, when $w = b^{(s+1)/2} \pmod p$ and $n = r$, since we then have

$$(w^2b^{-1})^{2^{n-1}} = (b^s)^{2^{r-1}} = b^{(p-1)/2} = 1 \pmod{p},$$

by Euler's criterion. Then, provided that $(w^2b^{-1})^{2^{n-1}} = 1 \pmod{p}$ at Step 2, when we compute the value in Step 3 for $t = n-1$ we will have $n \geq 2$ and

$$\{(w^2b^{-1})^{2^{t-1}}\}^2 = (w^2b^{-1})^{2^{n-1}} = 1 \pmod{p},$$

so that

$$(w^2b^{-1})^{2^{t-1}} = \pm 1 \pmod{p}.$$

Thus either $t = n-1$ is satisfactory or $(w^2b^{-1})^{2^{n-2}} = 1 \pmod{p}$. In this latter case we must have $n \geq 3$, and we can repeat the argument. Hence, provided that $(w^2b^{-1})^{2^{n-1}} = 1 \pmod{p}$ at Step 2, there will always be a satisfactory value of t in Step 3. We can never reach the stage at which the decreasing sequence of exponents produces $(w^2b^{-1})^{2^0} = 1 \pmod{p}$, since this is equivalent to the stopping condition $w^2 = b \pmod{p}$ in Step 2.

To complete the proof of the claim it is now enough to check that

$$(w_0^2b^{-1})^{2^{n-2}} = 1 \pmod{p}$$

at Step 4. We will in fact show that

$$(w_0^2b^{-1})^{2^{t-1}} = 1 \pmod{p},$$

which is sufficient, since $t \leq n-1$. However

$$(w_0^2b^{-1})^{2^{t-1}} = (w^2b^{-1}y^{2^{r-t}})^{2^{t-1}} = (w^2b^{-1})^{2^{t-1}}y^{2^{r-1}} \pmod{p}.$$

We arranged in Step 3 that $(w^2b^{-1})^{2^{t-1}} = -1 \pmod{p}$. Thus it is enough to observe that

$$y^{2^{r-1}} = z^{2^{r-1}s} = z^{(p-1)/2} = -1 \pmod{p}$$

by Euler's criterion, since z was assumed to be a quadratic non-residue.

There remains the problem of finding a quadratic non-residue z of p. This is easy in practice, since one can choose z at random and have a 50% chance that $(\frac{z}{p}) = -1$. Thus the expected number of trials before finding a suitable z is 2. This produces a **probabilistic algorithm**. However to give a **deterministic algorithm**, which is guaranteed to succeed without any random choices, is another matter entirely.