21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

27- Monday November 7, 2011.

Lemma 27.1: If p is an odd prime of the form $4m+1$, then p is the sum of two squares.
Proof: (probably due to EULER) Since -1 is a quadratic residue modulo p, there exists z with $z^2+1=0 \pmod{p}$, i.e. $z^2+1=j\,p$ for some integer j. One considers the integers $z\,x-y$ modulo p, for all the integers x,y satisfying $0 \le x,y < \sqrt{p}$. Since the number of pairs is $(\lfloor\sqrt{p}\rfloor+1)^2 > p$, the pigeon-hole principle implies the existence of two distinct pairs $(x_1,y_1),(x_2,y_2)$ such that $z\,x_1-y_1 = z\,x_2-y_2 \pmod{p}$, i.e. $z\,(x_1-x_2) = y_1-y_2 \pmod{p}$, and taking the squares one finds that $(x_1-x_2)^2+(y_1-y_2)^2$ is a non-zero multiple of p; then $(x_1-x_2)^2+(y_1-y_2)^2 \le 2(\lfloor\sqrt{p}\rfloor)^2 < 2p$, so that $(x_1-x_2)^2+(y_1-y_2)^2 = p$.

Remark 27.2: The argument of FERMAT (who claimed to have proved this result) might have been to start by choosing among all the integer solutions of $a^2+b^2=j\,p$ for an integer j (with a and b not multiples of p) one for which j is minimum. By eventually changing signs, one may assume that both a and b are positive, and one must have $0<a,b<p$, since replacing a or b by the remainder of the division by p would make the value of j smaller; actually, one has $0<a,b<\frac{p}{2}$, since if one had $\frac{p}{2}<a<p$, one could replace a by $p-a$ and make the value of j smaller, hence one has $a^2+b^2<\frac{p^2}{2}$ and $j<\frac{p}{2}$; also, a and b are relatively prime, since if their gcd d was >1, then $\frac{a}{d}$ and $\frac{b}{d}$ would give a smaller value of j.

If there was an odd prime p of the form $4m+1$ which is not the sum of two squares, one would take the smallest, for which j would be >1 and equal to a product of (non necessarily distinct) primes $j=q_1\cdots q_\ell$, with $2\le q_1\le\ldots\le q_\ell\le j<\frac{p}{2}$; since $a^2+b^2=0 \pmod{q_k}$ and a and b are relatively prime, one would deduce that $q_k=2$ or an odd prime of the form $4m+1$ (since it implies that -1 is a quadratic residue modulo q_k), hence q_k would be a sum of two squares (since it is $<p$, supposed to the smallest which cannot be written as a sum of two squares), and one concludes by showing that if $a^2+b^2=k\,q$ and q is prime with $q=\alpha^2+\beta^2$, then $\frac{a^2+b^2}{q}=k$ is the sum of two squares: starting from $k\,q=q_1\cdots q_\ell p$, and repeating this argument for $q_1,\ldots,q_\ell$ then implies that p is the sum of two squares.

If a or b is a multiple of q, then both are multiples of q by the equation, and $\frac{k}{q}=\left(\frac{a}{q}\right)^2+\left(\frac{b}{q}\right)^2$ is a sum of two squares, so that $k=\frac{k}{q}\,q$ is also the sum of two squares by Brahmagupta's identity. If a and b are not multiple of q, then $a^2+b^2=0 \pmod{q}$, and if a' is an inverse of a modulo q, $z=b\,a'$ solves $z^2=-1 \pmod{q}$; similarly, $\alpha^2+\beta^2=0 \pmod{q}$ and if α' is an inverse of α modulo q, $z_1=\beta\,\alpha'$ solves $z_1^2=-1 \pmod{q}$, so that $z_1=\pm z$; after eventually changing β into $-\beta$, one may assume that $z_1=z$, so that one has $b=a\,z \pmod{q}$ and $\beta=\alpha\,z \pmod{q}$, hence $b\,\alpha-a\,\beta=0 \pmod{q}$. Since Brahmagupta's identity gives $(a\,\alpha+b\,\beta)^2+(b\,\alpha-a\,\beta)^2=(a^2+b^2)\,(\alpha^2+\beta^2)=0 \pmod{q}$, one deduces that $a\,\alpha+b\,\beta=0 \pmod{q}$, hence $\left(\frac{a\,\alpha+b\,\beta}{q}\right)^2+\left(\frac{b\,\alpha-a\,\beta}{q}\right)^2=\frac{a^2+b^2}{q}=k$ is a sum of two squares.

Lemma 27.3: An integer $n\in\mathbb{Z}$ is a prime element in $\mathbb{Z}[\sqrt{D}]$ (for $D\in\mathbb{Z}$ not a square) if and only if $n=\pm p$ where p is a prime integer such that D is a quadratic non-residue modulo p.
Proof: One must reject the composite n, so that $n=\pm p$ for a prime integer p; then, $(a+b\sqrt{D})\,(c+d\sqrt{D})$ is a multiple of p if both $a\,c+b\,d\,D$ and $a\,d+b\,c$ are multiple of p, and one wants to know if it implies that a and b are multiple of p or that c and d are multiple of p.

If $D=E^2 \pmod{p}$ for some $E\in\mathbb{Z}$, then $(E+\sqrt{D})\,(E-\sqrt{D})=E^2-D$ is a multiple of p, but neither $E+\sqrt{D}$ nor $E-\sqrt{D}$ are multiple of p, so that one may assume that D is not a quadratic residue modulo p.

If $a\ne 0 \pmod{p}$, then it has an inverse a^{-1} modulo p, and one has $c=-a^{-1}b\,d\,D \pmod{p}$ and then $a\,d=a^{-1}b^2d\,D \pmod{p}$; if $b=0 \pmod{p}$, then both c and d are $=0 \pmod{p}$, so that one considers the case $b\ne 0 \pmod{p}$: one must then have $d=0 \pmod{p}$, since $d\ne 0 \pmod{p}$ implies $a=a^{-1}b^2D \pmod{p}$, so that D is a square modulo p, and $d=0 \pmod{p}$ implies $c=0 \pmod{p}$.

The case $c\ne 0 \pmod{p}$ is similar, and the case $a=c=0 \pmod{p}$ implies $b\,d=0 \pmod{p}$ so that either b or d is a multiple of p.

Remark 27.4: In the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers, an integer $n\in\mathbb{Z}$ is a prime element if and only if $n=\pm p$ where p is an odd prime integer of the form $4n+3$, but there are other prime elements, besides considering the associates, obtained by multiplying by units, which are $\{\pm 1,\pm i\}$.

Remark 27.5: In $\mathbb{Z}[\sqrt{D}]$ with $D < 0$, a unit $a + b\sqrt{D}$ must satisfy $a^2 - D\,b^2 = 1$, so that only ± 1 are units if $D < -1$.

One considers now the case $D > 0$ (not a square), for which the description of units is more elaborate; one recalls that for $r = a + b\sqrt{D}$ one writes $N(r) = a^2 - D\,b^2$, and that a unit of $\mathbb{Z}[\sqrt{D}]$ is a solution of $N(r) = \pm 1$. There always exist (infinitely many) solutions $r \in \mathbb{Z}[\sqrt{D}]$ of $N(r) = +1$, but there are values of D for which there is no solution of $N(r) = -1$: for example, $y^2 - 3x^2 = -1$ has no integer solution, since it would imply $y^2 = 2 \pmod 3$, and 2 is a quadratic non-residue modulo 3. For an integer solution of $N(r) = -1$ to exist, it is necessary that D is not divisible by 4 or by any odd prime of the form $4m + 3$, since -1 is a quadratic non-residue modulo these values, but it is not sufficient, and there are no integer solutions of $N(r) = -1$ for $D = 34$.[1]

It is not difficult for some small positive values of D to find the smallest positive solution of $y^2 - D\,x^2 = +1$: for example $y^2 - 10x^2 = +1$ gives $19^2 = 361 = 10.6^2 + 1$, and the smallest positive solution of $y^2 - 10x^2 = -1$ is $3^2 = 9 = 10.1^2 - 1$, and one has $(3 + \sqrt{10})^2 = 19 + 6\sqrt{10}$; in this example, all the units are of the form $\pm(3 + \sqrt{10})^n$ for some $n \in \mathbb{Z}$, and $(3 + \sqrt{10})^{-1} = -3 + \sqrt{10}$.

However, for some not so big values of D, like 61, trial and error for finding the smallest solution is not a good method.

Remark 27.6: For $D > 0$ not a square, the equation $y^2 - D\,x^2 = +1$ was wrongly called *Pell's equation* by EULER,[2] and it has been suggested that EULER had confused BROUCKNER,[3] who had worked on the equation, with PELL, who had little to do with it. The equation had been studied in India as early as BRAHMAGUPTA, but the first general method was given by BHASKARA (II) in 1150,[4] with some later examples by NARAYANA,[5] although a proof that the algorithm of BHASKARA (II) always terminates in a finite number of steps was only found by LAGRANGE in 1768.

It was FERMAT who issued a challenge concerning this equation in 1657, to FRENICLE,[6] BROUCKNER, and WALLIS,[7] one of them being the case $D = 61$, whose smallest solution ($x = 226\ 153\ 980, y = 1\ 766\ 319\ 049$) had been found by BHASKARA (II). BROUCKNER discovered a method which is essentially the method of continued fractions (for $\sqrt{D}$) which was later developed rigorously by LAGRANGE in 1766; FRENICLE tabulated the (smallest) solutions for $D \le 150$, but he did not publish his results and they were then lost; since BROUCKNER had boasted to be able to solve any example, FRENICLE challenged him with the case $D = 313$, and BROUCKNER sent him the smallest solution ($x = 1\ 819\ 380\ 158\ 564\ 160, y = 32\ 188\ 120\ 829\ 134\ 849$), claiming that it had taken him an hour or two.

Remark 27.7: For showing that there exists a non-trivial integer solution of $y^2 - D\,x^2 = +1$, i.e. with $x \ne 0$, one may use a constructive method based on continued fractions, described further on, but there is also a non-constructive argument which uses a Diophantine approximation result of DIRICHLET, that if θ is irrational, there are infinitely many pairs $a \in \mathbb{Z}, n \in \mathbb{N}^\times$ satisfying $\left|\theta - \frac{a}{n}\right| < \frac{1}{n^2}$.

For proving this result, one notices that for any $\theta \in \mathbb{R} \setminus \mathbb{Q}$ and any $N \in \mathbb{N}^\times$ there exists $a \in \mathbb{Z}$ and $n \in \{1, \ldots, N\}$ with $|n\,\theta - a| < \frac{1}{N+1}$: for $j = 1, \ldots, N$, one considers $a_j \in \mathbb{Z}$ with $\frac{-1}{2} < \varepsilon_j = j\,\theta - a_j < \frac{1}{2}$,

[1] Using the fact that $u = 35 - 6\sqrt{34}$ is a unit of $\mathbb{Z}[\sqrt{34}]$ satisfying $N(u) = 1$, one can deduce that there is no $v = y + x\sqrt{34}$ satisfying $N(v) = -1$: one considers the smallest $x > 0$ and one chooses $y > 0$, and then one observes that $w = u\,v = (35y - 6 \cdot 34\,x) + (35x - 6y)\sqrt{34}$ satisfies $N(w) = -1$, and since $y^2 - 34x^2 = -1$ implies $y < x\sqrt{34}$, so that $6y < 6x\sqrt{34} < 35x$, the value $x' = 35x - 6y$ is positive, and should then be $\ge x$, but it means $6y < 34x$, from which one deduces that $36(34x^2 - 1) < 34^2x^2$, i.e. $68x^2 < 36$, which does not hold for an integer.

[2] John PELL, English mathematician, 1611–1685. Pell's equation is named after him, although he had little to do with it, and it had been studied first by BRAHMAGUPTA.

[3] William BROUCKNER, Irish-born mathematician, 1620–1684. He became the second viscount BROUCKNER of Castles Lyons at the death of his father, who had bought the title. He worked in London, England.

[4] BHASKARA, Indian mathematician and astronomer, 1114–1185. Known as BHASKARA (II) and BHASKARA Acharya (the teacher), his work on differential calculus predates the work of NEWTON by five centuries.

[5] NARAYANA Pandit, Indian mathematician, c. 1340–1400.

[6] Bernard FRENICLE de Bessy, French mathematician, 1605–1675.

[7] John WALLIS, English mathematician, 1616–1703. He held the Savilian chair of geometry at Oxford, England.

the inequalities being strict because θ is irrational, but $\frac{-1}{2}$ and $\frac{1}{2}$ should be identified, as if one imagines the real line wrapped around a circle of perimeter 1, and one looks at $\theta, 2\theta, \ldots, N\,\theta$, which correspond to points $\varepsilon_j, j = 1, \ldots, N$ on the circle; assume by contradiction that all these points satisfy $|\varepsilon_j| \geq \frac{1}{N+1}$, then the N values fall in the remaining part of the circle, which is an interval of length $1 - \frac{2}{N+1} = \frac{N-1}{N+1}$, corresponding to $N-1$ intervals of size $\frac{1}{N+1}$, and one may consider that these intervals are open, since no ε_i can be equal to $\frac{\ell}{N+1}$ for an integer ℓ, since θ is irrational; by the pigeon-hole principle, one of these small open intervals receives ε_j and ε_k for some $j < k$, hence $|(k\,\theta - a_k) - (j\,\theta - a_j)| < \frac{1}{N+1}$, so that one has $|n\,\theta - a| < \frac{1}{N+1}$ for $n = k-j \in \{1, \ldots, N-1\}$ and $a = a_k - a_j \in \mathbb{Z}$, contradicting the hypothesis. Each such pair $(a, n) \in \mathbb{Z} \times \mathbb{N}^\times$ satisfies $\left|\theta - \frac{a}{n}\right| < \frac{1}{n^2}$, and there must be infinitely many distinct pairs, since $|n\,\theta - a|$ cannot be 0, and must tend to 0 as N tends to $+\infty$.

Using $\theta = \sqrt{D}$ (irrational since $D > 0$ is not a square) one has infinitely many pairs (a, n) such that $|n\sqrt{D} - a| < \frac{1}{n}$, and for any such pair, the integer $|a^2 - D\,n^2|$ is $= |a - n\sqrt{D}|\,|a + n\sqrt{D}| < \frac{1}{n}\left(\frac{1}{n} + 2n\sqrt{D}\right) \leq 1 + 2\sqrt{D}$, so that since there are only finitely many integers $m \in \mathbb{Z}$ with $|m| \leq 1 + 2\sqrt{D}$, there exists $m \in \mathbb{Z}$ which can be written as $a^2 - D\,n^2$ for infinitely many distinct pairs (a, n), and one may assume that $a, n \geq 0$ without changing $a^2 - D\,n^2$, and removing at most one pair one may assume that $a, n > 0$. One uses again the pigeon-hole principle by considering classes modulo $|m|$, and one finds two values $\xi, \eta \in \{1, \ldots, |m|\}$ with infinitely many distinct pairs (x, y) of positive integers satisfying $y^2 - D\,x^2 = m$, $x = \xi \pmod{|m|}$, $y = \eta \pmod{|m|}$, and one chooses two distinct pairs (x_1, y_1) and (x_2, y_2) (with $0 < x_1 < x_2$ for example). Since $y_1 y_2 - D\,x_1 x_2 = 0 \pmod{|m|}$ and $y_1 x_2 - y_2 x_1 = 0 \pmod{|m|}$, one defines $Y = \frac{y_1 y_2 - D\,x_1 x_2}{m} \in \mathbb{Z}$ and $X = \frac{y_1 x_2 - y_2 x_1}{m} \in \mathbb{Z}$, and one notices that $m^2(Y^2 - D\,X^2) = (y_1 y_2 - D\,x_1 x_2)^2 - D\,(y_1 x_2 - y_2 x_1)^2 = (y_1^2 - D\,x_1^2)\,(y_2^2 - D\,x_2^2) = m^2$, so that one has $Y^2 - D\,X^2 = 1$, and it remains to notice that it is not a trivial solution with $X = 0$, since it would mean that (x_1, y_1) and (x_2, y_2) are on the same line $y_j = t\,x_j$, which intersects the hyperbola $y^2 - D\,x^2 = m$ at only one point in the positive quadrant.

Remark 27.8: The subject of continued fractions seems to have started with the work of Bombelli and of Cataldi,[8] for extracting square roots,[9] but Archimedes had used the case $d = 3$ for constructing the rational approximation $\frac{1351}{780}$ of $\sqrt{3}$, following Pythagoras who had used the case $d = 2$ for constructing rational approximations of $\sqrt{2}$, much after Baudhayana,[10] who had found the solutions (12,17) and (408,577) of "Pell's equation".

Definition 27.9: For $a_0, a_1, \ldots, a_n \in \mathbb{R}$, all positive except possibly a_0, the *continued fraction* denoted $\langle a_0, a_1, \ldots, a_n\rangle$ is the quantity

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}.$$

If $a_0, \ldots, a_n$ are integers, the continued fraction is called *simple*.

Remark 27.10: Looking for a continued fraction expansion of the rational number $r = \frac{a}{b}$ (with a and b relatively prime) follows closely the Euclidean algorithm for finding the gcd of a and b, and one discovers that there are (exactly) two ways of writing r as a continued fraction, one having the form $\langle a_0, a_1, \ldots, a_n\rangle$ with $a_n > 1$ for some n, and the other being $\langle a_0, a_1, \ldots, a_n - 1, 1\rangle$.

By induction, one then observes that for $k \geq 1$ and any $x \in \mathbb{R}$ one has

$$\langle a_0, a_1, \ldots, a_{k-1}, x\rangle = \frac{x\,p_{k-1} + p_{k-2}}{x\,q_{k-1} + q_{k-2}}$$

[8] Pietro Antonio Cataldi, Italian mathematician, 1548–1626. He worked in Perugia and in Bologna, Italy.

[9] If $a > 0$, then the mapping $f : x \mapsto \frac{1}{2}\left(x + \frac{a}{x}\right)$ has $\sqrt{a}$ as its unique fixed point in $\mathbb{R}_+$, and since $f'(\sqrt{a}) = 0$ the convergence of the iterative method is very fast (quadratic), and basically it is the algorithm used in computers for extracting square roots. Starting with the integer $m = \lfloor\sqrt{a}\rfloor$ (i.e. such that $m^2 \leq a < (m+1)^2$) and applying the algorithm generates a sequence of rationals converging fast to $\sqrt{a}$, but it is different from the one given by the continued fraction expansion of $\sqrt{a}$.

[10] Baudhayana, Indian mathematician, c. 800 BCE.

with

$$p_{-1}=1, q_{-1}=0, p_0=a_0, q_0=1; p_k=a_k p_{k-1}+p_{k-2}, q_k=a_k q_{k-1}+q_{k-2} \text{ for all } k\ge 1,$$

so that $c_k=\langle a_0,a_1,\ldots,a_k\rangle$, which is called the kth *convergent* of the continued fraction $\langle a_0,a_1,\ldots,a_n\rangle$, satisfies

$$c_k=\langle a_0,a_1,\ldots,a_k\rangle=\frac{p_k}{q_k} \text{ for } k\ge 0.$$

By induction, one then shows that

$$p_k q_{k-1}-p_{k-1}q_k=(-1)^{k-1} \text{ for all } k\ge 1,$$

which implies that p_k and q_k are relatively prime, and

$$c_k-c_{k-1}=\frac{(-1)^{k-1}}{q_{k-1}q_k} \text{ for } k\ge 1;$$

similarly, one has $p_k q_{k-2}-p_{k-2}q_k=(-1)^k a_k$ for all $k\ge 1$. One deduces that $c_0<c_2<\cdots<c_3<c_1$.

Lemma 27.11: If $a_0,a_1,\ldots$ is an infinite sequence of integers, all positive except possibly a_0, and $c_n=\langle a_0,a_1,\ldots,a_n\rangle$, then $\ell=\lim_{n\to\infty}c_n$ exists, and is denoted $\langle a_0,a_1,\ldots\rangle$, so that

$$\langle a_0,a_1\ldots\rangle=a_0+\frac{1}{\langle a_1,a_2,\ldots\rangle}.$$

Every irrational ξ is the limit of a unique infinite continued fraction.
Proof: Since the increasing sequence c_{2n} converges to a limit $\le c_1$, the decreasing sequence c_{2n+1} converges to a limit $\ge c_0$, and these limits are equal because $|c_k-c_{k-1}|=\frac{1}{q_{k-1}q_k}$ for $k\ge 1$ and q_k tends to ∞ as $k\to\infty$; actually, since $q_0=1$, $q_1=a_1q_0\ge 1$ and $q_k=a_kq_{k-1}+q_{k-2}\ge q_{k-1}+q_{k-2}$ for all $k\ge 2$, one deduces that

$$q_k\ge F_k \text{ for all } k\ge 0, \text{ where } F_k \text{ is the Fibonacci sequence,}$$

and the Fibonacci sequence grows as ρ^k for the golden ratio $\rho=\frac{1+\sqrt{5}}{2}$.

If an infinite continued fraction has limit ξ, one must have $a_0=\lfloor\xi\rfloor$ (i.e. a_0 is the integer satisfying $a_0\le\xi<a_0+1$), so that $\xi=a_0+\frac{1}{\xi_1}$ with $\xi_1>1$, and one reiterates the process with ξ_1, so that $a_1=\lfloor\xi_1\rfloor$, and so on, showing that $\xi=\langle a_0,a_1,\ldots,a_k,\xi_{k+1}\rangle$, which by Remark 27.10 implies $\xi=\frac{\xi_{k+1}p_k+p_{k-1}}{\xi_{k+1}q_k+q_{k-1}}$, hence

$$\xi-\frac{p_k}{q_k}=\frac{p_{k-1}q_k-p_kq_{k-1}}{q_k(\xi_{k+1}q_k+q_{k-1})}=\frac{(-1)^k}{q_k(\xi_{k+1}q_k+q_{k-1})}, \text{ so that } \left|\xi-\frac{p_k}{q_k}\right|\le\frac{1}{q_kq_{k+1}} \text{ for } k\ge 0,$$

since $\xi_{k+1}q_k+q_{k-1}\ge a_{k+1}q_k+q_{k-1}=q_{k+1}$, and because $q_k\to\infty$ as $k\to\infty$, it shows that $\xi=\langle a_0,a_1,\ldots\rangle$. One has $\langle a_0,a_1\ldots\rangle=a_0+\frac{1}{\langle a_1,a_2,\ldots\rangle}$, and more generally $\xi_k=\langle a_k,a_{k+1},\ldots\rangle$ for all $k\ge 1$.

Definition 27.12: The infinite simple continued fraction $\langle a_0,a_1,\ldots,a_{n-1},\overline{b_0,b_1,\ldots,b_{m-1}}\rangle$ is called *periodic*, and the bar indicates that the sequence $b_0,b_1,\ldots,b_{m-1}$ is repeated indefinitely; if the continued fraction has the form $\langle\overline{b_0,b_1,\ldots,b_{m-1}}\rangle$, it is called *purely periodic*.

Remark 27.13: A purely periodic continued fraction $\xi=\langle\overline{b_0,b_1,\ldots,b_{m-1}}\rangle$ is of the form $\frac{\xi\,p_{m-1}+p_{m-2}}{\xi\,q_{m-1}+q_{m-2}}$, since it can be written as $\langle b_0,b_1,\ldots,b_{m-1},\overline{b_0,b_1,\ldots,b_{m-1}}\rangle$, showing that ξ is a quadratic irrational, i.e. the solution of a quadratic equation $A\,\xi^2+B\,\xi+C=0$ with integer coefficients A,B,C, $A=q_{m-1}\ne 0$, and discriminant $B^2-4A\,C$ positive and not a square (since $B^2-4A\,C=D^2$ gives $\xi=\frac{-B\pm D}{2A}\in\mathbb{Q}$). For example, if $\xi=\langle\overline{1}\rangle$ (i.e. all a_j are equal to 1), then one has $\xi=1+\frac{1}{\xi}$, so that ξ is the positive root of $z^2-z-1=0$, i.e. the golden ratio $\frac{1+\sqrt{5}}{2}$.

More generally, a periodic continued fraction $\eta=\langle a_0,a_1,\ldots,a_{n-1},\overline{b_0,b_1,\ldots,b_{m-1}}\rangle$ is of the form $\frac{\xi\,p_{n-1}+p_{n-2}}{\xi\,q_{n-1}+q_{n-2}}$ for the quadratic irrational $\xi=\langle\overline{b_0,b_1,\ldots,b_{m-1}}\rangle$, hence η is also a quadratic irrational.[11]

[11] Since $\eta=\frac{\xi\,p_{n-1}+p_{n-2}}{\xi\,q_{n-1}+q_{n-2}}$ implies $\xi=\frac{-\eta\,q_{n-2}+p_{n-2}}{\eta\,q_{n-1}-p_{n-1}}$, and $A\,\xi^2+B\,\xi+C=0$ implies $A\,(-\eta\,q_{n-2}+p_{n-2})^2+B\,(-\eta\,q_{n-2}+p_{n-2})\,(\eta\,q_{n-1}-p_{n-1})+C\,(\eta\,q_{n-1}-p_{n-1})^2=0$, hence η is a quadratic irrational.

The converse, that any quadratic irrational has a periodic continued fraction expansion was proved by LAGRANGE (Lemma 27.15), using an algorithm of EULER (Lemma 27.14), essentially the same that BROUCKNER had used (without mentioning continued fractions), and closely related to a "cyclic method" of BHASKARA (II); the characterization of those quadratic irrationals which have a purely periodic continued fraction expansion, implicit in the work of LAGRANGE, was proved in 1828 by GALOIS (Lemma 27.17).

Lemma 27.14: (EULER) A quadratic irrational ξ_0 can be written as $\frac{r_0+\sqrt{d}}{s_0}$, where d is a positive integer which is not a square, and r_0 and s_0 are integers, $s_0 \neq 0$, and $s_0 \mid d - r_0^2$ (and $m \mid n$ means that m divides n).[12] The continued fraction of ξ_0 (which begins with $a_0 = \lfloor \xi_0 \rfloor$) satisfies

$$\xi_k = \frac{r_k + \sqrt{d}}{s_k} \text{ for } k \geq 0,$$

with

$$r_{k+1} = a_k s_k - r_k \text{ with } a_k = \lfloor \xi_k \rfloor, s_{k+1} = \frac{d - r_{k+1}^2}{s_k} \text{ for } k \geq 0,$$

and is such that

$$r_k, s_k \text{ are integers}, s_k \neq 0, s_k \mid d - r_k^2, s_k \mid d - r_{k+1}^2 \text{ for } k \geq 0.$$

Since $\lfloor \sqrt{d} \rfloor \leq \sqrt{d} < \lfloor \sqrt{d} \rfloor + 1$, one has $\lfloor \xi_k \rfloor = \lfloor \frac{r_k+\sqrt{d}}{s_k} \rfloor = \lfloor \frac{r_k+\lfloor \sqrt{d} \rfloor}{s_k} \rfloor$ if $s_k > 0$ (and $= \lfloor \frac{r_k+\lfloor \sqrt{d} \rfloor+1}{s_k} \rfloor$ if $s_k < 0$), so that one needs to compute $\lfloor \sqrt{d} \rfloor$ once, and then the algorithm can be followed using integer arithmetic; a simpler formula is also $s_{k+1} = s_{k-1} + a_k(r_k - r_{k+1})$.[13]
Proof: Since $A\,\xi_0^2 + B\,\xi_0 + C = 0$ for integers A, B, C with $A \neq 0$, one has $\xi_0 = \frac{-B \pm \sqrt{B^2-4A\,C}}{2A}$, and one may choose $d = B^2 - 4A\,C$, $r_0 = \mp B$, $s_0 = \pm 2A$, so that $d - r_0^2 = -4A\,C$ is a multiple of s_0. Then one proceeds by induction on k: r_{k+1} is an integer, equal to $-r_k$ modulo s_k, so that $d - r_{k+1}^2 = d - r_k^2 = 0$ (mod s_k), showing that s_{k+1} is a non-zero integer, which divides $d - r_{k+1}^2$ since the quotient is s_k, and then $\xi_{k+1} = \frac{1}{\xi_k - a_k} = \frac{s_k}{r_k+\sqrt{d}-a_k s_k} = \frac{s_k}{-r_{k+1}+\sqrt{d}} = \frac{s_k(r_{k+1}+\sqrt{d})}{d-r_{k+1}^2} = \frac{r_{k+1}+\sqrt{d}}{s_{k+1}}$.

Lemma 27.15: (LAGRANGE) The continued fraction expansion of any quadratic irrational ξ_0 is periodic.
Proof: One has $\left(\xi_0 - \frac{p_k}{q_k}\right)\left(\overline{\xi_0} - \frac{p_k}{q_k}\right) = \frac{1}{q_k^k(\xi_{k+1}q_k+q_{k+1})\,(\overline{\xi_{k+1}}q_k+q_{k+1})}$, because $\xi_0 - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k(\xi_{k+1}q_k+q_{k+1})}$ (Lemma 27.11), and since $\frac{p_k}{q_k}$ converges to ξ, being alternatively above or below, it eventually falls between ξ_0 and $\overline{\xi_0}$ (which is $\neq \xi_0$), and both sides then being negative one has $\overline{\xi_{k+1}}q_k + q_{k+1} < 0$ for some k, so that $\overline{\xi_{k+1}} < 0$. Since $\xi_{m+1} = \frac{1}{\xi_m - a_m}$, one has $\overline{\xi_{m+1}} = \frac{1}{\overline{\xi_m} - a_m}$, so that $\overline{\xi_m} < 0$ implies $\overline{\xi_{m+1}} < 0$, but also $\overline{\xi_{m+1}} > -1$ since $a_m \geq 1$, hence $-1 < \overline{\xi_n} < 0$ for n large enough. From $1 < \xi_n - \overline{\xi_n} = \frac{2\sqrt{d}}{s_n}$, one deduces that $0 < s_n < 2\sqrt{d}$, and from $\xi_n = \frac{r_n+\sqrt{d}}{s_n}$, one deduces $\frac{r_n^2-d}{s_n^2} = \xi_n\overline{\xi_n} < 0$, so that $-\sqrt{d} < r_n < \sqrt{d}$, but also $r_n > 0$ since $0 < \xi_n + \overline{\xi_n} = \frac{2r_n}{s_n}$. For n large enough, the pair (r_n, s_n) can take at most $2d$ different values, hence there exist $m < n$ with $r_m = r_n$ and $s_m = s_n$, and the recurrence relation of Lemma 27.14 then shows that the continued fraction is periodic.

Definition 27.16: A continued fraction expansion is *reduced* if $\xi_0 > 1$ and $\overline{\xi_0} = \frac{r-\sqrt{d}}{s}$ satisfies $-1 < \overline{\xi_0} < 0$.[14]

Lemma 27.17: (GALOIS) A quadratic irrational $\xi_0 = \frac{r_0+\sqrt{d}}{s_0}$ has a purely periodic continued fraction expansion if and only if it is reduced. If $\xi_0 = \langle \overline{a_0, a_1, \ldots, a_{m-1}} \rangle$, then $\frac{-1}{\overline{\xi_0}} = \langle \overline{a_{m-1}, a_{m-2}, \ldots, a_0} \rangle$.

[12] If $\xi = \frac{a+b\sqrt{d}}{c}$ for integers a, b, c, d, with $c \neq 0$ and d not a square, then one writes it $\frac{R+\sqrt{D}}{S}$ with $R = a\,c$, $D = b^2c^2d$, and $S = c^2$, and one has $S \mid D - R^2$.

[13] From $s_k s_{k+1} = d - r_{k+1}^2$ and $s_{k-1}s_k = d - r_k^2$, one deduces that $s_k(s_{k+1} - s_{k-1}) = r_k^2 - r_{k+1}^2 = (r_k - r_{k+1})\,(r_k + r_{k+1})$, and then one uses $r_k + r_{k+1} = a_k s_k$.

[14] When d_1 is an integer which is not a square, conjugation acts on the field $\mathbb{Q}[\sqrt{d_1}]$ by $\overline{a + b\sqrt{d_1}} = a - b\sqrt{d_1}$, and conjugation is an automorphism of the field $\mathbb{Q}[\sqrt{d_1}]$. If $d_2 = d_1e^2$ for a positive integer e, then $\mathbb{Q}[\sqrt{d_2}]$ is a subfield of $\mathbb{Q}[\sqrt{d_1}]$, and the conjugate of $a + b\sqrt{d_2}$ in $\mathbb{Q}[\sqrt{d_2}]$ coincides with the conjugate of $a + b\,e\sqrt{d_1}$ in $\mathbb{Q}[\sqrt{d_1}]$.

Proof: In the proof of Lemma 27.15 it was shown that if $\overline{\xi_m} < 0$ then ξ_{m+1} is reduced, so that ξ_0 reduced implies ξ_k reduced for all $k \geq 1$ (and this uses the assumption that $\xi_0 > 1$, in order to have $a_0 \geq 1$). By Lemma 27.15, there exists an integer $m \geq 1$ and $j \geq 0$ such that $\xi_j = \xi_{m+j}$, and if $j \geq 1$, one wants to show that it implies $\xi_{j-1} = \xi_{m+j-1}$, so that by repeating the argument it is true for $j = 0$, i.e. one has a purely periodic continued fraction; for proving this, one notices that there is a unique (positive) integer k such that $k + \frac{1}{\xi_j}$ is reduced (so that $\xi_{j-1} = k + \frac{1}{\xi_j} = k + \frac{1}{\xi_{m+j}} = \xi_{m+j-1}$, and $k \geq 1$): indeed, one must have $-1 < k + \frac{1}{\overline{\xi_j}} < 0$, which means $\lfloor \frac{1}{\overline{\xi_j}} \rfloor = -k - 1$.

For the converse, one assumes that $\xi_0 = \langle \overline{a_0, \ldots, a_{m-1}} \rangle$. The case $m = 1$ corresponds to $\xi_0 = a_0 + \frac{1}{\xi_0}$, so that $\xi_0^2 - a_0\xi_0 - 1 = 0$, i.e. $\xi_0 = \frac{a_0+\sqrt{a_0^2+4}}{2} > 1$ and $\overline{\xi_0} = \frac{a_0-\sqrt{a_0^2+4}}{2}$, so that $\xi_0\overline{\xi_0} = -1$. If $m > 1$, one defines $\eta_j = \frac{-1}{\overline{\xi_j}}$ for $j \geq 0$, and one notices that the formula $\xi_j = a_j + \frac{1}{\xi_{j+1}}$ gives $\overline{\xi_j} = a_j + \frac{1}{\overline{\xi_{j+1}}}$, i.e. $\eta_{j+1} = a_j + \frac{1}{\eta_j}$; one deduces that $\eta_0 = \eta_m = \langle a_{m-1}, \eta_{m-1} \rangle = \langle a_{m-1}, a_{m-2}, \eta_{m-2} \rangle = \ldots = \langle a_{m-1}, a_{m-2}, \ldots, a_0, \eta_0 \rangle$, so that $\eta_0 = \langle \overline{a_{m-1}, a_{m-2}, \ldots, a_0} \rangle$, and in particular $\eta_0 > 1$, so that ξ_0 is reduced.

Lemma 27.18: If d is a positive integer which is not a square, the continued fraction expansion of $\sqrt{d}$ has the form $\langle a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0} \rangle$, where $a_0 = \lfloor \sqrt{d} \rfloor$.
Proof: Let $\xi = a_0 + \sqrt{d} > 1$, so that $\overline{\xi} = a_0 - \sqrt{d}$ satisfies $-1 < \overline{\xi} < 0$, i.e. ξ is reduced, hence it has a purely periodic expansion $\langle \overline{2a_0, a_1, a_2, \ldots, a_n} \rangle = \langle 2a_0, a_1, a_2, \ldots, a_n, \overline{2a_0, a_1, a_2, \ldots, a_n} \rangle$ by Lemma 27.17, hence $\sqrt{d} = \langle a_0, \overline{a_1, a_2, \ldots, a_n, 2a_0} \rangle$ after subtracting a_0. By Lemma 27.17, one also has $\frac{-1}{\overline{\xi}} = \langle \overline{a_n, a_{n-1}, \ldots, a_1, 2a_0} \rangle$, and since it is $\frac{1}{\sqrt{d}-a_0}$, one deduces that $\sqrt{d} - a_0 = \langle 0, \overline{a_n, a_{n-1}, \ldots, a_1, 2a_0} \rangle$, hence $\sqrt{d} = \langle a_0, \overline{a_n, a_{n-1}, \ldots, a_1, 2a_0} \rangle$ after adding a_0, so that the sequence $a_1, a_2, \ldots, a_n$ coincides with $a_n, a_{n-1}, \ldots, a_1$, proving the desired symmetry.

Remark 27.19: The preceding proof applies if $\sqrt{d}$ is replaced by $\frac{\sqrt{d}}{s}$ for a positive integer $s < \sqrt{d}$, and a_0 is taken to be $\lfloor \frac{\sqrt{d}}{s} \rfloor$.

Conversely, if $\eta = \langle b_0, \overline{b_1, b_2, \ldots, b_2, b_1, 2b_0} \rangle$, then $\eta = \sqrt{r}$ for a rational $r > 1$: since η is a quadratic irrational, one may write it $\eta = \frac{A+\sqrt{D}}{B}$, and because $\eta = b_0 + \frac{1}{\zeta}$ with $\zeta = \langle \overline{b_1, b_2, \ldots, b_2, b_1, 2b_0} \rangle$, one has $\frac{-1}{\overline{\zeta}} = \langle \overline{2b_0, b_1, b_2, \ldots, b_2, b_1} \rangle = b_0 + \eta$, but $\frac{-1}{\overline{\zeta}} = b_0 - \overline{\eta}$, which implies $\eta + \overline{\eta} = 0$, i.e. $A = 0$, and since $2b_0 > 0$, one has $b_0 \geq 1$, corresponding to $B < \sqrt{D}$.

Lemma 27.20: Let $\frac{p_k}{q_k}$ denote the kth convergent of $\sqrt{d}$, and let r_k and s_k be defined as in Lemma 27.14 (so that $r_0 = 0$ and $s_0 = 1$), then for any $k \geq 0$ one has

$$\frac{p_k + q_k\sqrt{d}}{p_{k-1} + q_{k-1}\sqrt{d}} = \frac{r_{k+1} + \sqrt{d}}{s_k}.$$

Proof: For $k = 0$ one has $r_0 = 0, s_0 = 1, r_1 = a_0 s_0 - r_0 = a_0$, so that the right hand side is $a_0 + \sqrt{d}$; one has $p_{-1} + q_{-1}\sqrt{d} = 1, p_0 + q_0\sqrt{d} = a_0 + \sqrt{d}$, so that the left hand side is also $a_0 + \sqrt{d}$. One proves the result by induction, assuming that the formula is true for k, and one uses the relations $p_{k+1} = a_{k+1}p_k + p_{k-1}$, $q_{k+1} = a_{k+1}q_k + q_{k-1}$, $s_{k+1} = \frac{d-r_{k+1}^2}{s_k}$, $r_{k+2} = a_{k+1}s_{k+1} - r_{k+1}$, so that one has $p_{k+1} + q_{k+1}\sqrt{d} = a_{k+1}(p_k + q_k\sqrt{d}) + p_{k-1} + q_{k-1}\sqrt{d}$, and $\frac{p_{k+1}+q_{k+1}\sqrt{d}}{p_k+q_k\sqrt{d}} = a_{k+1} + \frac{p_{k-1}+q_{k-1}\sqrt{d}}{p_k+q_k\sqrt{d}}$, which is $a_{k+1} + \frac{s_k}{r_{k+1}+\sqrt{d}}$ by the induction hypothesis, i.e. $a_{k+1} + s_k\frac{\sqrt{d}-r_{k+1}}{d-r_{k+1}^2} = a_{k+1} + \frac{\sqrt{d}-r_{k+1}}{s_{k+1}} = \frac{a_{k+1}s_{k+1}-r_{k+1}+\sqrt{d}}{s_{k+1}} = \frac{r_{k+2}+\sqrt{d}}{s_{k+1}}$.

Lemma 27.21: Suppose that the continued fraction expansion of $\sqrt{d}$ has period m, with $\frac{p_k}{q_k}$ denoting the kth convergent of $\sqrt{d}$, and r_k and s_k being defined as in Lemma 27.14 (so that $r_0 = 0$ and $s_0 = 1$); then one has

i) $p_{k-1}^2 - d\,q_{k-1}^2 = (-1)^k s_k$ for all $k \geq 0$,
ii) $s_k > 0$ for all $k \geq 0$,
iii) $s_k = 1$ if and only if $m \mid k$.

Hence $p_{j\,m-1}^2 - d\,q_{j\,m-1}^2 = 1$ for $j = 1, 2, 3, \ldots$ if m is even; if m is odd, one has $p_{j\,m-1}^2 - d\,q_{j\,m-1}^2 = -1$ for $j = 1, 3, 5, \ldots$ and $p_{j\,m-1}^2 - d\,q_{j\,m-1}^2 = 1$ for $j = 2, 4, 6, \ldots$.

Proof: Using Lemma 27.20, one has $\frac{p_k+q_k\sqrt{d}}{p_{k-1}+q_{k-1}\sqrt{d}} = \frac{r_{k+1}+\sqrt{d}}{s_k}$, and taking conjugates $\frac{p_k-q_k\sqrt{d}}{p_{k-1}-q_{k-1}\sqrt{d}} = \frac{r_{k+1}-\sqrt{d}}{s_k}$, so that the product gives $\frac{p_k^2-q_k^2\sqrt{d}}{p_{k-1}^2-q_{k-1}^2\sqrt{d}} = -\frac{d-r_{k+1}^2}{s_k^2} = -\frac{s_{k+1}}{s_k}$, since $d - r_{k+1}^2 = s_k s_{k+1}$; i) then follows from $p_{-1}^2 - d\,q_{-1}^2 = s_0$, which is true, since $p_{-1} = 1$, $q_{-1} = 0$, and $s_0 = 1$.

ii) then follows from the fact that any odd convergent is $> \sqrt{d}$ and any even convergent is $< \sqrt{d}$.

Since $\sqrt{d}$ has the form $\langle a_0, \overline{a_1, \ldots, a_{m-1}, 2a_0}\rangle$, one has $\xi_m = \xi_{2m} = \ldots = \langle\overline{2a_0, a_1, \ldots, a_{m-1}}\rangle = a_0 + \sqrt{d}$ (with $a_0 = \lfloor\sqrt{d}\rfloor$), hence by Lemma 27.14 $r_m = r_{2m} = \ldots = a_0$ and $s_m = s_{2m} = \ldots = 1$. Assume that $s_k = 1$ for some $k \geq 1$; then, since ξ_j has a purely periodic continued fraction expansion for all $j \geq 1$, it is reduced, so that $-1 < \overline{\xi_j} < 0$, and because $\overline{\xi_j} = \frac{r_j-\sqrt{d}}{s_j}$, one deduces that $-1 < r_k - \sqrt{d} < 0$, i.e. $r_k = \lfloor\sqrt{d}\rfloor = a_0$ and $\xi_k = a_0 + \sqrt{d}$, so that k must be a multiple of m by definition of m.

Remark 27.22: There are actually no other positive integer solutions of $y^2 - d\,x^2 = \pm 1$ than those mentioned in Lemma 27.21 (Lemma 27.29), and in particular the condition for an integer solution of $y^2 - d\,x^2 = -1$ to exist is that the continued fraction expansion of $\sqrt{d}$ has an odd period. As mentioned in a previous footnote, since $y^2 = -1 \pmod{d}$ implies that -1 is a quadratic residue modulo any prime divisor of d, it is necessary that d is not a multiple of 4 or of any odd prime number of the form $4m + 3$; however, these conditions are not sufficient, since $34 = 2 \cdot 17$ satisfies these conditions, but $34 = \langle 5, \overline{1, 4, 1, 10}\rangle$, which shows an even period: indeed, $\sqrt{34} = 5 + (\sqrt{34} - 5)$ and $\frac{1}{\sqrt{34}-5} = \frac{\sqrt{34}+5}{9} = 1 + \frac{\sqrt{34}-4}{9}$, $\frac{9}{\sqrt{34}-4} = \frac{\sqrt{34}+4}{2} = 4 + \frac{\sqrt{34}-4}{2}$, $\frac{2}{\sqrt{34}-4} = \frac{\sqrt{34}+4}{9} = 1 + \frac{\sqrt{34}-5}{9}$, $\frac{9}{\sqrt{34}-5} = \sqrt{34} + 5 = 10 + (\sqrt{34} - 5)$.

Lemma 27.23: If p is an odd prime of the form $4m + 1$, and n is an odd integer, then there is an integer solution of $y^2 - p^n x^2 = -1$, so that (by Lemma 27.29) $\sqrt{p^n}$ has a continued fraction expansion with an odd period.
Proof: For $d = p^n$, one considers the smallest positive integer solution (u, v) of $v^2 - d\,u^2 = 1$, and since $d = 1 \pmod{4}$ one has $v^2 - u^2 = 1 \pmod{4}$, which implies that v is odd and u is even, i.e. $v = 2t + 1, u = 2s$, and the equation becomes $t\,(t + 1) = d\,s^2$. Since a prime factor of $t\,(t + 1)$ cannot divide both t and $t + 1$, either $t = d\,a^2, t + 1 = b^2$ with $s = a\,b$, or $t = a^2, t + 1 = d\,b^2$ with $s = a\,b$; in the first case one would deduce that $b^2 - d\,a^2 = 1$, contradicting the fact that one started with the smallest positive integer solution, so that one has the second situation, which implies $a^2 - d\,b^2 = -1$.

Lemma 27.24: (LEGENDRE) If d is a positive integer which is not a square, and is such that $\sqrt{d}$ has a continued fraction expansion with an odd period, then it has a representation $d = a^2 + b^2$ which is primitive, i.e. with a and b relatively prime.
Proof: By Lemma 27.18, $\sqrt{d} = \langle a_0, \overline{a_1, \ldots, a_k, a_k, \ldots, a_1, 2a_0}\rangle$, so that $\xi_{k+1} = \langle\overline{a_k, \ldots, a_1, 2a_0, a_k, \ldots, a_1}\rangle$ is reduced and $\xi_{k+1} = \frac{-1}{\overline{\xi_{k+1}}}$ by Lemma 27.17, hence $\xi_{k+1}\overline{\xi_{k+1}} = -1$, and since $\xi_{k+1} = \frac{r_{k+1}+\sqrt{d}}{s_{k+1}}$ by Lemma 27.14, it means $r_{k+1}^2 + s_{k+1}^2 = 1$.

If a prime p would divide both r_{k+1} and s_{k+1}, it would divide d by the equation, and it would also divide s_k, since one has $d - r_{k+1}^2 = s_k s_{k+1}$ by Lemma 27.14, which implies $s_k = s_{k+1}$. By Lemma 27.21, one has $p_{k-1}^2 - d\,q_{k-1}^2 = (-1)^k s_k$, and $p_k^2 - d\,q_k^2 = (-1)^{k+1} s_{k+1}$, so that p would divide p_{k-1}^2 and p_k^2, i.e. it would divide both p_{k-1} and p_k, contradicting the relation $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ (Remark 27.10).

Remark 27.25: If p is odd prime of the form $4m + 1$, then the continued fraction expansion of $\sqrt{p}$ has an odd period (because Lemma 27.29 asserts that all solutions are given by Lemma 27.21), and the algorithm of Lemma 27.14 starts by defining $r_0 = 0$, $s_0 = 1$, $a_0 = \lfloor\sqrt{p}\rfloor$, and then $r_{k+1} = a_k s_k - r_k$, $s_{k+1} = \frac{p-r_{k+1}^2}{s_k}$, $a_{k+1} = \lfloor\frac{r_{k+1}+\sqrt{p}}{s_{k+1}}\rfloor = \lfloor\frac{r_{k+1}+a_0}{s_{k+1}}\rfloor$, so that $r_1 = a_0$, $s_1 = p - a_0^2$, $a_1 = \lfloor\frac{2a_0}{p-a_0^2}\rfloor$, and then one may use the simpler formula $s_{k+1} = s_{k-1} + a_k(r_k - r_{k+1})$, and a solution is found once one finds an integer j such that $s_j = s_{j+1}$.

Remark 27.26: Continued fractions of $\sqrt{d}$ which have period 1 correspond to $\langle n, \overline{2n}\rangle = \sqrt{n^2 + 1}$ for an integer $n \geq 1$;[15] for values $d < 100$ one finds $\sqrt{2}, \sqrt{5}, \sqrt{10}, \sqrt{17}, \sqrt{26}, \sqrt{37}, \sqrt{50}, \sqrt{65}, \sqrt{82}$.

[15] If $\xi = \langle n, \overline{2n}\rangle$ and $\alpha = \langle\overline{2n}\rangle$, then $\xi = n + \frac{1}{\alpha}$ and $\alpha = 2n + \frac{1}{\alpha}$, or $\alpha^2 - 2n\,\alpha - 1 = 0$, so that $\alpha = n + \sqrt{n^2 + 1}$, $\frac{1}{\alpha} = \frac{n-\sqrt{n^2+1}}{-1}$, and then $\xi = \sqrt{n^2 + 1}$.

Continued fractions of $\sqrt{d}$ which have period 2 correspond to $\langle n, \overline{a, 2n}\rangle = \sqrt{n^2 + \frac{2n}{a}}$ for integers $a, n \geq 1$ with $a \neq 2n$,[16] so that a must divide $2n$ (and $a \neq 2n$), and one obtains the integers $\sqrt{n^2 + b}$ with $b > 1$ dividing $2n$; for values $d < 100$ one finds $\sqrt{3}$, $\sqrt{6}, \sqrt{8}$, $\sqrt{11}, \sqrt{12}, \sqrt{15}$, $\sqrt{18}, \sqrt{20}, \sqrt{24}$, $\sqrt{27}, \sqrt{30}, \sqrt{35}$, $\sqrt{38}, \sqrt{39}, \sqrt{40}, \sqrt{42}, \sqrt{48}$, $\sqrt{51}, \sqrt{56}, \sqrt{63}$, $\sqrt{66}, \sqrt{68}, \sqrt{72}, \sqrt{80}$, $\sqrt{83}, \sqrt{84}, \sqrt{87}, \sqrt{90}, \sqrt{99}$.

For primes $d < 100$, one finds

$$\begin{gathered}
\sqrt{3} = \langle 1, \overline{1, 2}\rangle \\
\sqrt{5} = \langle 2, \overline{4}\rangle \\
\sqrt{7} = \langle 2, \overline{1, 1, 1, 4}\rangle \\
\sqrt{11} = \langle 3, \overline{3, 6}\rangle \\
\sqrt{13} = \langle 3, \overline{1, 1, 1, 1, 6}\rangle \\
\sqrt{17} = \langle 4, \overline{8}\rangle \\
\sqrt{19} = \langle 4, \overline{2, 1, 3, 1, 2, 8}\rangle \\
\sqrt{23} = \langle 4, \overline{1, 3, 1, 8}\rangle
\end{gathered}$$

$$\begin{gathered}
\sqrt{29} = \langle 5, \overline{2, 1, 1, 2, 10}\rangle \\
\sqrt{31} = \langle 5, \overline{1, 1, 3, 5, 3, 1, 1, 10}\rangle \\
\sqrt{37} = \langle 6, \overline{12}\rangle \\
\sqrt{41} = \langle 6, \overline{2, 2, 12}\rangle \\
\sqrt{43} = \langle 6, \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12}\rangle \\
\sqrt{47} = \langle 6, \overline{1, 5, 1, 12}\rangle \\
\sqrt{53} = \langle 7, \overline{3, 1, 1, 3, 14}\rangle \\
\sqrt{59} = \langle 7, \overline{1, 2, 7, 2, 1, 14}\rangle
\end{gathered}$$

$$\begin{gathered}
\sqrt{61} = \langle 7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}\rangle \\
\sqrt{67} = \langle 8, \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}\rangle \\
\sqrt{71} = \langle 8, \overline{2, 2, 1, 7, 1, 2, 2, 16}\rangle \\
\sqrt{73} = \langle 8, \overline{1, 1, 5, 5, 1, 1, 16}\rangle \\
\sqrt{79} = \langle 8, \overline{1, 7, 1, 16}\rangle \\
\sqrt{83} = \langle 9, \overline{9, 18}\rangle \\
\sqrt{89} = \langle 9, \overline{2, 3, 3, 2, 18}\rangle \\
\sqrt{93} = \langle 9, \overline{1, 1, 1, 4, 6, 4, 1, 1, 1, 18}\rangle \\
\sqrt{97} = \langle 9, \overline{1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18}\rangle.
\end{gathered}$$

For composites $d < 100$ which are not squares and have period at least 4, one finds

$$\begin{gathered}
\sqrt{14} = \langle 3, \overline{1, 2, 1, 6}\rangle \\
\sqrt{21} = \langle 4, \overline{1, 1, 2, 1, 1, 8}\rangle \\
\sqrt{22} = \langle 4, \overline{1, 2, 4, 2, 1, 8}\rangle \\
\sqrt{28} = \langle 5, \overline{3, 2, 3, 10}\rangle \\
\sqrt{32} = \langle 5, \overline{1, 1, 1, 10}\rangle \\
\sqrt{33} = \langle 5, \overline{1, 2, 1, 10}\rangle \\
\sqrt{34} = \langle 5, \overline{1, 4, 1, 10}\rangle \\
\sqrt{44} = \langle 6, \overline{1, 1, 1, 2, 1, 1, 1, 12}\rangle \\
\sqrt{45} = \langle 6, \overline{1, 2, 2, 2, 1, 12}\rangle \\
\sqrt{46} = \langle 6, \overline{1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12}\rangle \\
\sqrt{52} = \langle 7, \overline{4, 1, 2, 1, 4, 14}\rangle \\
\sqrt{54} = \langle 7, \overline{2, 1, 6, 1, 2, 14}\rangle \\
\sqrt{55} = \langle 7, \overline{2, 2, 2, 14}\rangle \\
\sqrt{57} = \langle 7, \overline{1, 1, 4, 1, 1, 14}\rangle \\
\sqrt{58} = \langle 7, \overline{1, 1, 1, 1, 1, 1, 14}\rangle \\
\sqrt{60} = \langle 7, \overline{1, 2, 1, 14}\rangle
\end{gathered}$$

$$\begin{gathered}
\sqrt{62} = \langle 7, \overline{1, 6, 1, 14}\rangle \\
\sqrt{69} = \langle 8, \overline{3, 3, 1, 4, 1, 3, 3, 16}\rangle \\
\sqrt{70} = \langle 8, \overline{2, 1, 2, 1, 2, 16}\rangle \\
\sqrt{74} = \langle 8, \overline{1, 1, 1, 1, 16}\rangle \\
\sqrt{75} = \langle 8, \overline{1, 1, 1, 16}\rangle \\
\sqrt{76} = \langle 8, \overline{1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16}\rangle \\
\sqrt{77} = \langle 8, \overline{1, 3, 2, 3, 1, 16}\rangle \\
\sqrt{78} = \langle 8, \overline{1, 4, 1, 16}\rangle \\
\sqrt{85} = \langle 9, \overline{4, 1, 1, 4, 18}\rangle \\
\sqrt{86} = \langle 9, \overline{3, 1, 1, 1, 8, 1, 1, 1, 3, 18}\rangle \\
\sqrt{88} = \langle 9, \overline{2, 1, 1, 1, 2, 18}\rangle \\
\sqrt{91} = \langle 9, \overline{1, 1, 5, 1, 5, 1, 1, 18}\rangle \\
\sqrt{92} = \langle 9, \overline{1, 1, 2, 4, 2, 1, 1, 18}\rangle \\
\sqrt{94} = \langle 9, \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}\rangle \\
\sqrt{95} = \langle 9, \overline{1, 2, 1, 18}\rangle \\
\sqrt{96} = \langle 9, \overline{1, 3, 1, 18}\rangle \\
\sqrt{98} = \langle 9, \overline{1, 8, 1, 18}\rangle.
\end{gathered}$$

Continued fractions of $\sqrt{d}$ which have period 3 correspond to $\langle n, \overline{a, a, 2n}\rangle$ for integers $a, n \geq 1$ with $a \neq 2n$; if $\xi = \langle n, \overline{a, a, 2n}\rangle$ and $\alpha = \langle \overline{a, a, 2n}\rangle$, $\beta = \langle \overline{a, 2n, a}\rangle$, $\gamma = \langle \overline{2n, a, a}\rangle$, then $\xi = n + \frac{1}{\alpha}$, $\alpha = a + \frac{1}{\beta}$, $\beta = a + \frac{1}{\gamma}$, and $\gamma = 2n + \frac{1}{\alpha} = \frac{2n\,\alpha+1}{\alpha}$, so that $\beta = a + \frac{\alpha}{2n\,\alpha+1} = \frac{(2n\,a+1)\,\alpha+a}{2n\,\alpha+1}$, $\alpha = a + \frac{2n\,\alpha+1}{(2n\,a+1)\,\alpha+a}$ or $(2n\,a+1)\,\alpha^2 - 2n\,(a^2+1)\,\alpha - (a^2+1) = 0$, hence $\alpha = \frac{n\,(a^2+1)+\sqrt{n^2(a^2+1)^2+(2n\,a+1)\,(a^2+1)}}{2n\,a+1}$, $\frac{1}{\alpha} = \frac{n\,(a^2+1)-\sqrt{n^2(a^2+1)^2+(2n\,a+1)\,(a^2+1)}}{-(a^2+1)}$, and $\xi = \frac{\sqrt{n^2(a^2+1)^2+(2n\,a+1)\,(a^2+1)}}{a^2+1}$. Period 3 then corresponds to $d = n^2 + \frac{2n\,a+1}{a^2+1}$, with a^2+1 dividing $2n\,a+1$, and $a \neq 2n$, so that a must be even; using $a = 2b$ for $b \geq 1$, one must have $4b^2+1$ dividing $4b\,n+1$ and $n > b$, and since $4b$ is relatively prime with b^2+1 it gives $n = b + (4b^2+1)\,k$ for $k \geq 1$, corresponding to the value $d = (b + (4b^2+1)\,k)^2 + 4b\,k + 1$, the only value below 100 being 41.

Lemma 27.27: For an irrational ξ, suppose integers a and b with b positive have the property that $|b\,\xi - a| < |v\,\xi - u|$ for all integers u, v such that $1 \leq v \leq b$ and $\frac{u}{v} \neq \frac{a}{b}$, then $\frac{a}{b}$ is a convergent of the continued fraction expansion of ξ.

[16] If $\xi = \langle n, \overline{a, 2n}\rangle$ and $\alpha = \langle \overline{a, 2n}\rangle$, $\beta = \langle \overline{2n, a}\rangle$, then $\xi = n + \frac{1}{\alpha}$, $\alpha = a + \frac{1}{\beta}$, and $\beta = 2n + \frac{1}{\alpha} = \frac{2n\,\alpha+1}{\alpha}$, so that $\alpha = a + \frac{\alpha}{2n\,\alpha+1}$ or $2n\,\alpha^2 - 2n\,a\,\alpha - a = 0$, hence $\alpha = \frac{n\,a+\sqrt{n^2a^2+2n\,a}}{2n}$, $\frac{1}{\alpha} = \frac{n\,a-\sqrt{n^2a^2+2n\,a}}{-a}$, and $\xi = \frac{\sqrt{n^2a^2+2n\,a}}{a}$.

Suppose integers c and d with d positive have the property that $|d\,\xi - c| < |q_k\xi - p_k|$ (from the continued fraction expansion of ξ), then $d \geq q_{k+1}$.

Suppose integers c and d with d positive have the property that $\left|\xi - \frac{c}{d}\right| < \left|\xi - \frac{p_k}{q_k}\right|$ for $k \geq 1$, then $d > q_k$.
Proof: Let $c_k = \frac{p_k}{q_k}$ be the kth convergent of ξ. One cannot have $\frac{a}{b} < c_0$, since it implies $|b\,\xi - a| \geq \left|\xi - \frac{a}{b}\right| > |\xi - c_0| = |q_0\xi - p_0|$, because $q_0 = 1$, and this contradicts the hypothesis. By Lemma 27.11 $\left|\xi - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k q_{k+1}}$ for $k \geq 0$, so that $|q_0\xi - p_0| \leq \frac{1}{q_1}$, and one cannot have $\frac{a}{b} > c_1$, since it implies $\left|\xi - \frac{a}{b}\right| > \left|\xi - c_1\right|$, so that after multiplication by b one has $|b\,\xi - a| > \frac{|b\,p_1 - a\,q_1|}{q_1} \geq \frac{1}{q_1}$ (because $b\,p_1 - a\,q_1$ is a non-zero integer), so that $|b\,\xi - a| > |q_0\xi - p_0|$, contradicting the hypothesis. There must exist an integer n such that $\frac{a}{b}$ falls between c_{n-1} and c_{n+1} (which are on the same side of ξ, while c_n is on the other side), and one then assumes that it is not one of them (or the result is proved); it follows that $\left|\frac{a}{b} - c_{n-1}\right| < |c_n - c_{n-1}|$, which after multiplication by $b\,q_n q_{n-1}$ gives $q_n|b\,q_{n-1} - a\,p_{n-1}| < b\,|p_n q_{n-1} - p_{n-1}q_n| = b$ (by Remark 27.10), and since $b\,q_{n-1} - a\,p_{n-1}$ is a non-zero integer it implies that $q_n \leq b$. One also has $\left|\frac{a}{b} - \xi\right| > |c_{n+1} - \xi|$,[17] which implies $|b\,\xi - a| > \frac{|b\,p_{n+1} - a\,q_{n+1}|}{q_{n+1}} \geq \frac{1}{q_{n+1}}$, but since it is $\geq |q_n\xi - p_n|$ (by Lemma 27.11) one obtains a contradiction.

Let b be the smallest positive integer such that there exists an integer a such that $|b\,\xi - a| < |q_k\xi - p_k|$, so that one has $b \leq d$; by the first part, it follows that $\frac{a}{b}$ is a convergent of ξ, i.e. $\frac{a}{b} = \frac{p_m}{q_m}$, and one must have $m \geq k+1$, hence $b \geq q_{k+1}$, because convergents are successively closer to ξ: indeed, one has $\xi - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k(\xi_{k+1}q_k + q_{k-1})}$ by Lemma 27.11, which implies $\left|\xi - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k q_{k+1}}$, and then one notices that $\xi_{k+1}q_k + q_{k-1} < q_k(a_{k+1}+1) + q_{k-1} = q_k + q_{k+1} \leq a_{k+2}q_{k+1} + q_k = q_{k+2}$, so that $|q_k\xi - p_k| = \frac{1}{\xi_{k+1}q_k + q_{k-1}} > \frac{1}{q_{k+2}} \geq |q_{k+1}\xi - p_{k+1}|$, which is a stronger inequality than $\left|\xi - \frac{p_k}{q_k}\right| > \left|\xi - \frac{p_{k+1}}{q_{k+1}}\right|$.

If one had $\left|\xi - \frac{c}{d}\right| < \left|\xi - \frac{p_k}{q_k}\right|$ and $d \leq q_k$, then after multiplying by d one would have $|d\,\xi - c| \leq \frac{d}{q_k}\,|q_k\xi - p_k| \leq |q_k\xi - p_k|$, hence $d \geq q_{k+1}$ by the second part, a contradiction since $q_{k+1} > q_k$ for $k \geq 1$ (but one may have $q_1 = q_0 = 1$).

Lemma 27.28: Suppose p and q are positive integers satisfying $\left|\xi - \frac{p}{q}\right| < \frac{1}{2q^2}$ for an irrational ξ, then $\frac{p}{q}$ is a convergent of the continued fraction expansion of ξ.
Proof: Let u and v be integers, with v positive, and such that $|v\,\xi - u| \leq |q\,\xi - p|$ and $\frac{u}{v} \neq \frac{p}{q}$. By the triangle inequality, $\left|\frac{u}{v} - \frac{p}{q}\right| \leq \left|\frac{u}{v} - \xi\right| + \left|\xi - \frac{p}{q}\right|$, and after multiplying by $q\,v$ and using the fact that $q\,u - p\,v$ is a non-zero integer one deduces that $1 \leq |q\,u - p\,v| \leq q\,|v\,\xi - u| + v\,|q\,\xi - p| \leq (q+v)\,|q\,\xi - p| < \frac{q+v}{2q}$, so that $v > q$. One concludes by applying the first part of Lemma 27.27.[18]

Lemma 27.29: Suppose (p,q) is a positive solution of $p^2 - d\,q^2 = \pm 1$, then $\frac{p}{q}$ is a convergent of the continued fraction expansion of $\sqrt{d}$.
Proof: In order to apply Lemma 27.28, one shows that $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{2q^2}$. Because $|p - q\,\sqrt{d}|\,(p + q\,\sqrt{d}) = 1$, one needs to shows that $p + q\,\sqrt{d} > 2q$, and since $p^2 \geq d\,q^2 - 1 \geq (d-1)\,q^2$, one has $p \geq \sqrt{d-1}\,q$, and $\sqrt{d} + \sqrt{d-1} \geq \sqrt{2} + 1 > 2$ for $d \geq 2$.

[17] Since $c_{n-1}, \frac{a}{b}, c_{n+1}, \xi$ are on this order on the real line (either ascending or descending).

[18] The conclusion $v \geq q$ would be enough for applying Lemma 27.27, and it follows from $\left|\xi - \frac{p}{q}\right| \leq \frac{1}{2q^2}$, but it is equivalent to $\left|\xi - \frac{p}{q}\right| < \frac{1}{2q^2}$ since equality would imply that ξ is rational.