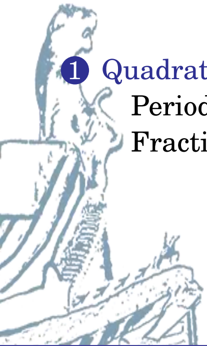
Sums of Two Squares,Sum of Four Squares

Chao Qin

School of Mathematical Sciences

June 6, 2024

Sums of Two Squares,Sum of Four Squares

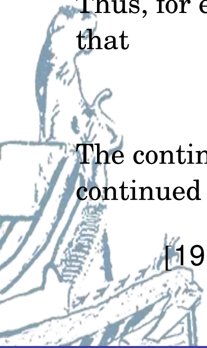


1. Quadratic Irrationals
   - Periodic Continued Fractions
   - Continued Fractions of Algebraic Numbers of Higher Degree
2. Recognizing Rational Numbers
3. Sums of Two Squares

Quadratic Irrationals

Definition (Quadratic Irrational)

A quadratic irrational is a real number $\alpha \in \mathbf{R}$ that is irrational and satisfies a quadratic polynomial with coefficients in $\mathbf{Q}$.

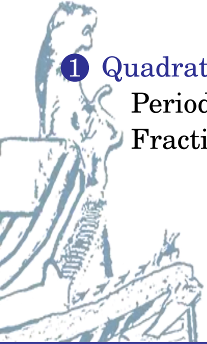


Thus, for example, $(1+\sqrt{5})/2$ is a quadratic irrational. Recall that

$$\frac{1+\sqrt{5}}{2} = [1, 1, 1, \ldots].$$

The continued fraction of $\sqrt{2}$ is $[1, 2, 2, 2, 2, 2, \ldots]$, and the continued fraction of $\sqrt{389}$ is

$$[19, 1, 2, 1, 1, 1, 1, 2, 1, 38, 1, 2, 1, 1, 1, 1, 2, 1, 38, \ldots].$$



1. Quadratic Irrationals
   - Periodic Continued Fractions
   - Continued Fractions of Algebraic Numbers of Higher Degree
2. Recognizing Rational Numbers
3. Sums of Two Squares

Periodic Continued Fractions

Definition (Periodic Continued Fraction)

A *periodic continued fraction* is a continued fraction $[a_0, a_1, \ldots, a_n, \ldots]$ such that

$$a_n = a_{n+h}$$

for some fixed positive integer h and all sufficiently large n. We call the minimal such h the *period of the continued fraction*.

Periodic Continued Fractions

Example

Consider the periodic continued fraction $[1,2,1,2,\ldots] = [\overline{1,2}]$. What does it converge to? We have

$$[\overline{1,2}] = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cdots}}}},$$

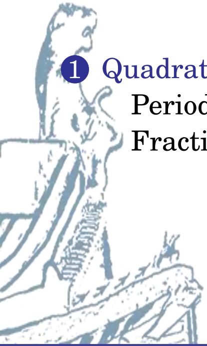
Periodic Continued Fractions

so if $\alpha = [\overline{1,2}]$ then

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{\alpha}} = 1 + \frac{1}{\frac{2\alpha+1}{\alpha}} = 1 + \frac{\alpha}{2\alpha+1} = \frac{3\alpha+1}{2\alpha+1}$$

Thus $2\alpha^2 - 2\alpha - 1 = 0$, so

$$\alpha = \frac{1+\sqrt{3}}{2}.$$



1. Quadratic Irrationals
   - Periodic Continued Fractions
   - Continued Fractions of Algebraic Numbers of Higher Degree
2. Recognizing Rational Numbers
3. Sums of Two Squares

Continued Fractions of Algebraic Numbers of Higher Degree

Definition (Algebraic Number)

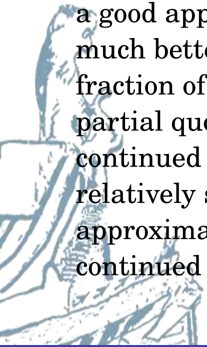
An algebraic number is a root of a polynomial $f \in \mathbf{Q}[x]$.

Sums of Two Squares,Sum of Four Squares

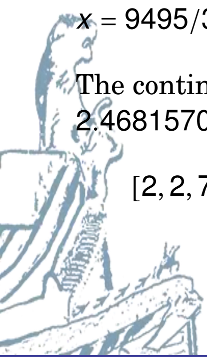
1. Quadratic Irrationals
   - Periodic Continued Fractions
   - Continued Fractions of Algebraic Numbers of Higher Degree
2. Recognizing Rational Numbers
3. Sums of Two Squares

Recognizing Rational Number

Suppose that somehow you can compute approximations to some rational number, and want to figure what the rational number probably is. Computing the approximation to high enough precision to find a period in the decimal expansion is not a good approach, because the period can be huge (see below). A much better approach is to compute the simple continued fraction of the approximation, and truncate it before a large partial quotient a_n, then compute the value of the truncated continued fraction. This results in a rational number that has a relatively small numerator and denominator, and is close to the approximation of the rational number, since the tail end of the continued fraction is at most $1/a_n$.



Recognizing Rational Number



We begin with a contrived example, which illustrates how to recognize a rational number. Let

$x = 9495/3847 = 2.46815700545879906420587470756433584611385$

The continued fraction of the truncation 2.4681570054587990064 is

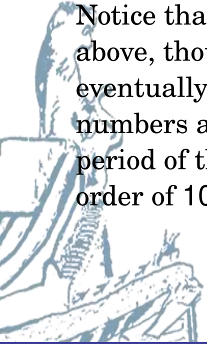
$$[2, 2, 7, 2, 1, 5, 1, 1, 1, 1, 1, 1, 328210621945, 2, 1, 1, 1, \ldots]$$

Recognizing Rational Number

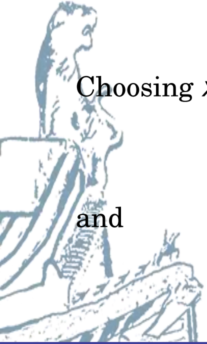
We have

$$[2, 2, 7, 2, 1, 5, 1, 1, 1, 1, 1, 1] = \frac{9495}{3847}.$$

Notice that no repetition is evident in the digits of x given above, though we know that the decimal expansion of x must be eventually periodic, since all decimal expansions of rational numbers are eventually periodic. In fact, the length of the period of the decimal expansion of $1/3847$ is 3846, which is the order of 10 modulo 3847



Recognizing Rational Number



For example, suppose $f = 3847x^2 - 14808904x + 36527265$. To apply Newton's method, let x_0 be a guess for a root of f. Iterate using the recurrence

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Choosing $x_0 = 0$, approximations of the first two iterates are

$$x_1 = 2.466574501394566404103909378,$$

and

$$x_2 = 2.468157004807401923043166846.$$

Recognizing Rational Number

The continued fraction of the approximations x_1 and x_2 are

$$[2, 2, 6, 1, 47, 2, 1, 4, 3, 1, 5, 8, 2, 3]$$

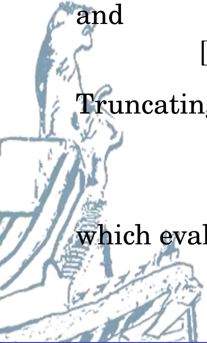
and

$$[2, 2, 7, 2, 1, 5, 1, 1, 1, 1, 1, 1, 103, 8, 1, 2, 3, \ldots].$$

Truncating the continued fraction of x_2 before 103 gives

$$[2, 2, 7, 2, 1, 5, 1, 1, 1, 1, 1, 1],$$

which evaluates to $9495/3847$, which is a rational root of f.



Sums of Two Squares,Sum of Four Squares

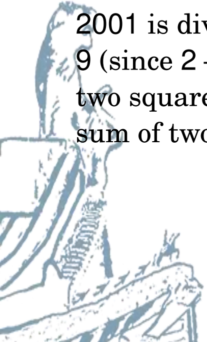
1. Quadratic Irrationals
   - Periodic Continued Fractions
   - Continued Fractions of Algebraic Numbers of Higher Degree
2. Recognizing Rational Numbers
3. Sums of Two Squares

Sums of Two Squares

Theorem

A positive integer n *is a sum of two squares if and only if all prime factors of* $p \mid n$ *such that* $p \equiv 3 \pmod 4$ *have even exponent in the prime factorization of* n.

Sums of Two Squares



We first consider some examples. Notice that $5 = 1^2 + 2^2$ is a sum of two squares, but 7 is not a sum of two squares. Since 2001 is divisible by 3 (because $2 + 1$ is divisible by 3), but not by 9 (since $2 + 1$ is not), Theorem implies that 2001 is not a sum of two squares. The theorem also implies that $2 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 13$ is a sum of two squares.

Sums of Two Squares

Definition (Primitive)

A representation $n = x^2 + y^2$ is *primitive* if x and y are coprime.

Sums of Two Squares

Lemma

If n is divisible by a prime $p \equiv 3 \pmod 4$, then n has no primitive representations.

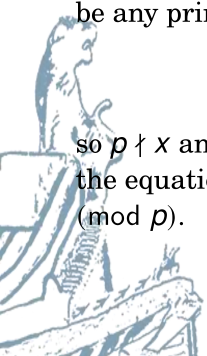
Sums of Two Squares

Proof.

Suppose n has a primitive representation, $n = x^2 + y^2$, and let p be any prime factor of n. Then

$$p \mid x^2 + y^2 \quad \text{and} \quad \gcd(x, y) = 1,$$

so $p \nmid x$ and $p \nmid y$. Since $\mathbf{Z}/p\mathbf{Z}$ is a field, we may divide by y^2 in the equation $x^2 + y^2 \equiv 0 \pmod{p}$ to see that $(x/y)^2 \equiv -1 \pmod{p}$. □

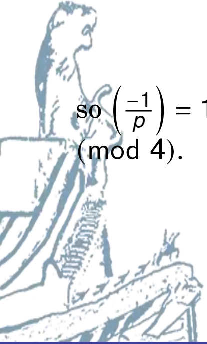


Sums of Two Squares

Thus the Legendre symbol $\left(\frac{-1}{p}\right)$ equals $+1$. However, by Proposition,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

so $\left(\frac{-1}{p}\right) = 1$ if and only if $(p-1)/2$ is even, which is to say $p \equiv 1 \pmod 4$.



Sums of Two Squares

Lemma

If $x \in \mathbf{R}$ *and* $n \in \mathbf{N}$*, then there is a fraction* $\dfrac{a}{b}$ *in lowest terms such that* $0 < b \leq n$ *and*

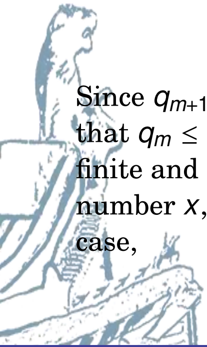
$$\left|x - \frac{a}{b}\right| \leq \frac{1}{b(n+1)}.$$

Sums of Two Squares

Proof.

Consider the continued fraction $[a_0, a_1, \ldots]$ of x. for each m

$$\left| x - \frac{p_m}{q_m} \right| < \frac{1}{q_m \cdot q_{m+1}}.$$



Since $q_{m+1} \geq q_m + 1$ and $q_0 = 1$, either there exists an m such that $q_m \leq n < q_{m+1}$, or the continued fraction expansion of x is finite and n is larger than the denominator of the rational number x, in which case we take $\frac{a}{b} = x$ and are done. In the first case, □

Sums of Two Squares

$$\left|x - \frac{p_m}{q_m}\right| < \frac{1}{q_m \cdot q_{m+1}} \le \frac{1}{q_m \cdot (n+1)},$$

so $\frac{a}{b} = \frac{p_m}{q_m}$ satisfies the conclusion of the lemma.