Even more continued fractions for Pell's Equation. Introduction to Quadratic Reciprocity

October 19, 2012

1 Reading Assignment:

- Again Davenport: *All* of Chapter IV.
- Read closely sections 1,2 of Chapter 5 of [**I-R**]; and look over the entire chapter.

2 Homework due October 25:

1. [**I-R**] Page 63, Exercises 11,14-16;
2. Page 64, Exercises 18-21
3. Page 65 Exercise 38.

3 For General Practice, but don't hand in:

[**I-R**] Page 64, Exercise 22.

4 For General Culture, but don't hand in:

[**I-R**] Page 64, Exercises 25-28.

5 Recall: Purely periodic continued fractions

If

$$a_0, a_1, a_2, \ldots a_{n-1}, a_0, a_1, a_2, \ldots a_{n-1}, \ldots$$

are the terms of a continued fraction, we'll say that it is **purely periodic** and denote it

$$\overline{a_0,\ a_1,\ a_2,\ \ldots\ a_{n-1}}$$

and say that it has **period** n.

Theorem 1 ** Let D be a natural number, not a perfect square. Then $\sqrt{D} + \lfloor\sqrt{D}\rfloor$ has a purely periodic continued fraction expansion.*

So,

$$\sqrt{D} = \lfloor\sqrt{D}\rfloor;\ \overline{a_1,\ a_2,\ \ldots\ a_{n-1},\ 2\lfloor\sqrt{D}\rfloor}.$$

Or, more readably:

$$\sqrt{D} \ = \ \frac{1}{a_0+}\frac{1}{a_1+}\cdots\frac{1}{a_{n-1}+}\frac{1}{2a_0+}\frac{1}{a_1+}\cdots\frac{1}{a_{n-1}+}\frac{1}{2a_0+}\cdots,$$

with $a_0 = \lfloor\sqrt{D}\rfloor$.

6 Recall: Reduced quadratic numbers

By a *real quadratic number* I'll mean an algebraic number that is real, irrational, and is a root of a quadratic polynomial with rational coefficients. More precisely, we can ask that it be a root of a polynomial $aX^2 + bX + c$, with $0 \neq a$ and $a, b, c \in \mathbf{Z}$. So α can be expressed as:

$$(*) \quad \alpha = \frac{A + \sqrt{D}}{B}$$

for $A, B, D \in \mathbf{Z}$—with $D > 0$, and not a perfect square. (Here $D = b^2 - 4ac$. And $(A^2 - D)/B = 2c \in \mathbf{Z}$. So

(**) B divides $A^2 - D$. Let $E \in Z$ be such that

$$B \cdot E = A^2 - D.$$

If α is a quadratic number, denote by α' its (algebraic) conjugate. Let's define the **companion** of α to be the real quadratic number

$$\beta := \frac{-1}{\alpha'}.$$

Note that (sappy as it may sound) companionship is a symmetric relationship.

Also:

If α satisfies (*), then

$$(*) \quad \beta = \frac{A + \sqrt{D}}{-E}$$

Let α and β be (real quadratic number) companions. Say that α is **reduced** if $\alpha > 1$ and $\beta > 1$. The latter requirement is equivalent to the bounds: $-1 < \alpha' < 0$. By the symmetry of the conditions in the definition of "reduced," α is reduced if and only if β is reduced.

Moreover, if α is reduced we get that

- $\alpha + \alpha' > 0$ (so A and B have the same sign)
- $\alpha - \alpha' > 1$ (so $0 < B$; hence A is positive as well)
- $\alpha' < 0$ (so $0 \leq A \leq \sqrt{D}$)
- $\alpha > 1$ (so $0 \leq B \leq 2\sqrt{D}$)

Note: $\sqrt{D} + \lfloor \sqrt{D} \rfloor$ *is* reduced. Let $\mathcal{R}(D)$ denote the set of *reduced real quadratic numbers expressible as bf (*) above.*

Proposition 1 *The set $\mathcal{R}(D)$ is finite, and is closed under passing to companions, and to the continued fraction iteration*

$$\alpha \mapsto \alpha_1 \mapsto \alpha_2 \mapsto \dots$$

Let's play with a single 'move forward' in the continued fraction expansion of α.

$$\alpha_n = a_n + 1/\alpha_{n+1}$$

So

$$\alpha'_n = a_n + 1/\alpha'_{n+1}$$

and

$$-\beta_n = \frac{1}{a_n - 1/\beta_{n+1}}$$

or

$$\beta_{n+1} = a_n + 1/\beta_n.$$

Proposition 2 *Keep to the above notation, where α_n is the n-th continued fraction iteration of α, and a_n is the n-th term in the continued fraction expansion. Let $\beta_n := -1/\alpha'_n$ be the companion of α_n. Then β is the n-th continued fraction iteration of β:*

$$\beta_{n+1} = a_n + \frac{1}{a_{n-1} + \frac{1}{\ldots + \frac{1}{\beta}}}$$

Extend to 'minus infinity trick'!

Corollary 2 *Reduced real quadratic numbers are purely periodic.*

7 Recall Quadratic residues

Now let us go back to studying congruence modulo a prime p (and assume that $p > 2$). An integer a is a *quadratic residue* or *quadratic nonresidue* mod p according as the equation

$$x^2 \equiv a \bmod p$$

has a solution or not. Of course, if a is divisible by p there is indeed a solution, namely $x = 0$, but the fun is when a is not divisible by p, i.e., represents a class in $\mathbf{F}_p^*$ (and half of these classes are residues, half nonresidues).

The Legendre symbol is a way of keeping track of this trichotomy: that symbol $\binom{a}{p}$ is defined to be zero if a is divisible by p, $+1$ if a is a quadratic residue, and -1 if a is a nonresidue.

Just to make sure you're on track, check that you see that this symbol is multiplicative, i.e.,

$$\binom{a}{p}\binom{b}{p} = \binom{ab}{p},$$

and also remember that that the symbol $\binom{a}{p}$ is dependent *only* on the integer a modulo p, and is insensitive to multiplying the "a" by any square not divisible by p. Recall that we know:

$$\binom{-1}{p} = (-1)^{\frac{p-1}{2}},$$

it is $+1$ if $p \equiv 1 \bmod 4$ and -1 if $p \equiv -1 \bmod 4$. BUT, in this case we know more: we have an explicit formula for *the square root of minus one mod p* when it exists.

There are other ways of dewcribing, in effect, the same (Legendre) symbol, e.g.:

- $$\binom{a}{p} = a^{\frac{p-1}{2}}.$$

- Here's another; and–I confess—when I first learned this I thought it was frivolous, but soon came to see that it wasn't: $\left(\frac{a}{p}\right)$ is one less than the number of solutions in $\mathbf{F}_p^*$ to the equation $x^2 \equiv a \bmod p$.

- Here's a third way–due to Gauss (see the lemma on page 52) (Define: *least residue.*) If a is prime to p form the $\frac{p-1}{2}$ distinct congruence classes mod p:

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a.$$

Now pass to the "least residues of these $\frac{p-1}{2}$ classes. So we have a collection of $\frac{p-1}{2}$ integers, some positive, some negative. Let μ be the number of positive ones, and ν the number of negative ones, so

$$\mu + \nu = \frac{p-1}{2}.$$

Proposition 3 (Gauss's Lemma)

$$\left(\frac{a}{p}\right) = (-1)^{\nu},$$

I.e., if there's an odd number of negative least residues in the set

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

then

$$\left(\frac{a}{p}\right) = -1;$$

and if not, then

$$\left(\frac{a}{p}\right) = +1.$$

8 For which (odd) primes p is the number $a = 2$ a quadratic residue?

Answer: if the smallest integer larger than or equal to $\frac{p-1}{4}$ is even. If that smallest integer is odd, then 2 is a nonresidue mod p. Give a proof of this, as follows from Gauss's Lemma. Give alternate formulations of this: If p is congruent to 1 or 7 mod 8, then 2 is a quadratic residue mod p; otherwise not. Is 2 a quadratic residue modulo 691? For fun, when is one twin prime a residue modulo the other twin prime?

9 Quadratic Reciprocity

Statement for odd primes $p \neq q$.

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Unpackage this. Compute with it.

If either p or q is congruent to 1 mod 4, then

$$\left(\frac{p}{q}\right) \;=\; \left(\frac{q}{p}\right).$$

If both are congruent to -1 mod 4, then

$$\left(\frac{p}{q}\right) \;=\; -\left(\frac{q}{p}\right).$$

Proof(s) later!

10 Compute

$$\left(\frac{4001}{691}\right) \;=\; \left(\frac{4001-6\times 691}{691}\right) \;=\; \left(\frac{4001-4146}{691}\right) \;=$$

$$=\; \left(\frac{-145}{691}\right) \;=\; \left(\frac{(-1)\cdot 5\cdot 29}{691}\right) \;=\; \left(\frac{-1}{691}\right)\cdot\left(\frac{5}{691}\right)\cdot\left(\frac{29}{691}\right) \;=$$

$$=\; (-1)\cdot\left(\frac{691}{5}\right)\cdot\left(\frac{691}{29}\right) \;=\; (-1)\cdot(+1)\left(\frac{691-23\times 29}{29}\right) \;=\; (-1)\cdot(+1)\left(\frac{691-667}{29}\right) \;=$$

$$=\; (-1)\cdot\left(\frac{4\cdot 2\cdot 3}{29}\right) \;==\; (-1)\cdot\left(\frac{2}{29}\right)\cdot\left(\frac{3}{29}\right) \;==\; (-1)\cdot(-1)\cdot(-1) \;=\; -1.$$