LINEAR RECURRENCES FOR PELL EQUATIONS

JOHN ROBERTSON

Abstract. We present some theorems on indexes of apparition of primes, prime powers, and composites in the sequence $\{y_n\}$ of solutions to $x^2 - dy^2 = \pm 1$ or ± 4.

1. Introduction

The y_n for consecutive solutions to the Pell equations $x^2 - Dy^2 = \pm 1$, ± 4 satisfy linear recurrence relations. For example, solutions to the equation $x^2 - 2y^2 = \pm 1$ are given in Table 1. Here $y_{n+1} = 2y_n + y_{n-1}$, so, for instance $12 = 2 \cdot 5 + 2$. The linear recurrences satisfied by the y_n for the Pell equations we consider here are given in Table 2.

This article has two main goals:

> Prove the facts about indexes of apparition used in the algorithm in the article "A Fast Algorithm for the Regulator of a Quadratic Order". This algorithm exploits the properties of linear recurrence relations to give a fast algorithm to derive solutions to $x^2 - f^2 dy^2 = \pm 1$, or ± 4, from solutions to $x^2 - dy^2 = \pm 1$ or ± 4.

> Prove that $E \leq 2f$ where E satisfies $\epsilon_1^E = \epsilon_f$, ϵ_1 is the fundamental unit of the ring of integers $\mathcal{O}$ of the quadratic field $\mathbf{Q}(\sqrt{d})$ ($d > 1$ squarefree), and ϵ_f is the fundamental unit of the order of conductor f in $\mathcal{O}$.

Along the way, we present material on linear recurrences related to Pell equations that is of interest in its own right.

Date: February 28, 2009.

Solutions to $x^2 - 2y^2 = \pm 1$

n	x_n	y_n	$x_n^2 - 2y_n^2$
1	1	1	-1
2	3	2	$+1$
3	7	5	-1
4	17	12	$+1$
5	41	29	-1
6	99	70	$+1$
7	239	169	-1
8	577	408	$+1$
9	1393	985	-1
10	3363	2378	$+1$

TABLE 1. $y_{n+1} = 2y_n + y_{n-1}$

Linear Recurrences for Pell Equations

Equation	$x_1^2 - dy_1^2$	a	c	Minimum a
$x^2 - dy^2 = 1$	$+1$	$2x_1$	-1	4
$x^2 - dy^2 = \pm 1$	-1	$2x_1$	$+1$	2
$x^2 - dy^2 = 4$	$+4$	x_1	-1	3
$x^2 - dy^2 = \pm 4$	-4	x_1	$+1$	1

TABLE 2. For the given equation, $y_{n+1} = ay_n + cy_{n-1}$

There is nothing that is essentially new here. Two classic papers that include most of this material are [1] and [6]. Other related classic papers include [4, 5, 7]. Of course, [2] has a lot of this material. Ribenboim [8, Chapter 1] discusses most of this and many more related results. We hope the focus on Pell equations and units in quadratic orders is helpful to readers interested in these topics per se.

2. General Theorems on Linear Recurrences

We consider the recurrences $u_0 = 0$, $u_1 = 1$, $u_{r+1} = au_r + cu_{r-1}$ where $c = 1$ or -1, $a \geq 1$ when $c = 1$, and $a \geq 3$ when $c = -1$. We also use a related sequence $v_0 = 2$, $v_1 = a$, $v_{r+1} = av_r + cv_{r-1}$. Define $\Delta = a^2 + 4c$. For the a and c we are considering, $\Delta \geq 5$. Note that if the sequence $\{y_r\}$ satisfies $y_0 = 0$ and $y_{r+1} = ay_r + cy_{r-1}$ for $r \geq 1$, then $y_r = y_1 u_r$ for all $r \geq 0$.

One characterization of the sequences $\{u_r\}$ and $\{v_r\}$ is in terms of the roots α, β of $x^2 - ax - c$. Let

$$\alpha = \frac{a + \sqrt{a^2 + 4c}}{2} \text{ and } \beta = \frac{a - \sqrt{a^2 + 4c}}{2}.$$

Then

$$\alpha + \beta = a,\ \alpha\beta = -c = \mp 1,\ \alpha - \beta = \sqrt{\Delta},\ (\alpha - \beta)^2 = \Delta, \tag{1}$$

$$u_r = \frac{\alpha^r - \beta^r}{\alpha - \beta}, \tag{2}$$

and

$$v_r = \alpha^r + \beta^r. \tag{3}$$

One relation these two series satisfy is

$$v_r^2 - \Delta u_r^2 = 4(-c)^r. \tag{4}$$

This is easily proved using (2) and (3) or by induction. Using (1), (2), (3), we have that

$$v_r + u_r\sqrt{\Delta} = \frac{1}{2^{r-1}}(v_1 + u_1\sqrt{\Delta})^r = \frac{1}{2^{r-1}}(a + \sqrt{\Delta})^r \tag{5}$$

because each is equal to $2\alpha^r$. In particular, if $m/\nu = s$ is an integer, then

$$v_m + u_m\sqrt{\Delta} = \frac{1}{2^{s-1}}(v_\nu + u_\nu\sqrt{\Delta})^s \tag{6}$$

and so if s is odd then

$$u_m = \frac{1}{2^{s-1}}\left(\binom{s}{1}v_\nu^{s-1}u_\nu + \binom{s}{3}v_\nu^{s-3}u_\nu^3\Delta + \cdots + \binom{s}{s-2}v_\nu^2 u_\nu^{s-2}\Delta^{(s-3)/2} + u_\nu^s\Delta^{(s-1)/2}\right) \tag{7}$$

and if s is even then

$$u_m = \frac{1}{2^{s-1}}\left(\binom{s}{1}v_\nu^{s-1}u_\nu + \binom{s}{3}v_\nu^{s-3}u_\nu^3\Delta + \cdots + \binom{s}{s-3}v_\nu^3 u_\nu^{s-3}\Delta^{(s-4)/2} + \binom{s}{s-1}v_\nu u_\nu^{s-1}\Delta^{(s-2)/2}\right). \tag{8}$$

In particular,

$$u_{2\nu} = v_\nu u_\nu. \tag{9}$$

Another relation between the series $\{u_i\}$ and $\{v_i\}$ is that for $m < n$

$$u_n v_m - u_m v_n = 2(-c)^m u_{n-m}. \tag{10}$$

This is easily proved using equations (2) and (3) and $\alpha\beta = -c$.

Theorem 1. $\gcd(v_r, u_r) \le 2$.

Proof. By (4), if $g = \gcd(v_r, u_r)$ then $g^2|4$, so $g = 1$ or 2. □

Theorem 2. *If $\nu|m$ then $u_\nu|u_m$*

Proof. From (2), we have that

$$\frac{u_m}{u_\nu} = \alpha^{m-\nu} + \alpha^{m-2\nu}\beta^\nu + \alpha^{m-3\nu}\beta^{2\nu} + \cdots + \beta^{m-\nu}.$$

The right hand side is a symmetric polynomial in α and β with integral coefficients, and so is an integer. □

Theorem 3. *If $\nu = \gcd(m, n)$ then $\gcd(u_m, u_n) = u_\nu$.*

Proof. Because $\nu|m$ and $\nu|n$, by Theorem 2 $u_\nu|u_m$ and $u_\nu|u_n$, so $u_\nu|\gcd(u_m, u_n)$. It now suffices to show that $\gcd(u_m, u_n)|u_\nu$.

There are r, $s \ge 0$ so that $rm - sn = \nu$. Then by (10) $|u_{rm}v_{sn} - u_{sn}v_{rm}| = 2u_\nu$. For odd primes p so that $p^t|\gcd(u_m, u_n)$, $p^t|u_\nu$, because $u_m|u_{rm}$ and $u_n|u_{sn}$. It remains to show that if $2^t|\gcd(u_m, u_n)$ then $2^t|u_\nu$.

Suppose that $2^t\|u_\nu$ with $t \ge 2$. Then by (4), $2^1\|v_\nu$. Assume $s = m/\nu$ is odd (one of m/ν or n/ν is odd). Then in (7)

$$2^t\|\frac{1}{2^{s-1}}sv_\nu^{s-1}u_\nu$$

and 2^{t+1} divides the remaining terms. So $2^t\|u_m$. Hence if $2^r|\gcd(u_m, u_n)$ then $r \le t$ and $2^r|u_\nu$.

If $2^1 \| u_\nu$ and a is odd, then $c = 1$, Δ is odd, and $4|v_\nu$, as can be seen by testing a few cases modulo 4. Assume $s = m/\nu$ is odd (again, one of m/ν or n/ν is odd). Then in (7)

$$2^1 \| \frac{1}{2^{s-1}} u_\nu^s \Delta^{(s-1)/2}$$

and 4 divides the remaining terms. So $2^1 \| u_m$.

If $2^1 \| u_\nu$ and a is even, then $a \equiv 2 \pmod 4$, $2 \| v_\nu$, and $8|\Delta$. Then in (7)

$$2^1 \| \frac{1}{2^{s-1}} s v_\nu^{s-1} u_\nu$$

and 4 divides the remaining terms (because $8|\Delta$). So $2^1 \| u_m$.

If u_ν is odd and a is odd, then $3 \nmid \nu$ and assuming $3 \nmid m$, u_m is odd. If u_ν is odd and a is even, then ν is odd and assuming m is odd, u_m is odd. □

Theorem 4. *If $r|u_k$, $r \nmid u_i$ for $1 \le i < k$, and $r|u_m$, then $k|m$.*

Proof. Let $\nu = \gcd(k, m)$. Then $\nu \le k$, $u_\nu \le u_k$, and $u_\nu = \gcd(u_k, u_m)$. As $r|u_k$ and $r|u_m$, we have that $r|u_\nu$. As $r \nmid u_i$ for $i < k$, $u_\nu = u_k$, and so $u_k|u_m$. □

3. Indexes of apparition for odd primes

A fundamental classical theorem is

Theorem 5. *For any odd prime p, $u_p \equiv s \pmod p$ and $p|u_{p-s}$ where $s = \left(\frac{\Delta}{p}\right)$, and $\left(\frac{*}{*}\right)$ is the Legendre symbol.*

These results are cited in [2, pp. 394, 396]. See also [1].

Proof. Expanding (2) using the binomial theorem gives, for r odd,

$$u_r = \frac{1}{2^{r-1}} \left(\binom{r}{1} a^{r-1} + \binom{r}{3} a^{r-3} \Delta + \cdots \right. \\ \left. \binom{r}{r-2} a^2 \Delta^{(r-3)/2} + \binom{r}{r} \Delta^{(r-1)/2} \right), \tag{11}$$

and for r even

$$u_r = \frac{1}{2^{r-1}}\left(\binom{r}{1}a^{r-1} + \binom{r}{3}a^{r-3}\Delta + \cdots \right. \\ \left. \binom{r}{r-3}a^3\Delta^{(r-4)/2} + \binom{r}{r-1}a\Delta^{(r-2)/2}\right). \tag{12}$$

If $p|\Delta$, then by (11), $p|u_p$, because p divides all of the binomial coefficients except the last, and p divides the last term.

If $p \nmid \Delta$, then consider (12) for $r = p+1$. Then p divides all of the binomial coefficients except for $\binom{p+1}{1}$ and $\binom{p+1}{p}$. Thus

$$2^p u_{p+1} \equiv \binom{p+1}{1}a^p + \binom{p+1}{p}a\Delta^{(p-1)/2} \equiv a\left(1 + \left(\frac{\Delta}{p}\right)\right) \pmod{p}.$$

If $\left(\frac{\Delta}{p}\right) = -1$, $p|u_{p+1}$. If $\left(\frac{\Delta}{p}\right) = 1$, then, because $2^p \equiv 2 \pmod{p}$,

$$2u_{p+1} \equiv 2a \pmod{p},$$

and so $u_{p+1} \equiv a \pmod{p}$. By (11), $u_p \equiv 1 \pmod{p}$. Because

$$u_{p+1} = au_p + cu_{p-1},$$

we have $cu_{p-1} \equiv 0 \pmod{p}$, and so $u_{p-1} \equiv 0 \pmod{p}$. □

In fact, by (11), if $p \nmid \Delta$ then

$$u_p \equiv \Delta^{(p-1)/2} \equiv \left(\frac{\Delta}{p}\right) \pmod{p}. \tag{13}$$

We extend the above classical theorem slightly by

Corollary 1.

(a) If $c = 1$ and $(\Delta/p) = 0$, then $p \equiv 1 \pmod 4$, $u_{p-1} \equiv u_{p+1} \pmod p$, and $u_{p-1}^2 \equiv -1 \pmod p$. In particular, $u_{p-1} \not\equiv \pm 1 \pmod p$.

(b) If $c = 1$ and $s = (\Delta/p) = \pm 1$, then $u_{p-1-s} \equiv u_{p+1-s} \equiv s \pmod p$.

(c) If $c = -1$ and $(\Delta/p) = 0$, then $a \equiv \pm 2 \pmod p$. If $a \equiv 2 \pmod p$ then $u_{p-1} \equiv -1 \pmod p$ and $u_{p+1} \equiv 1 \pmod p$.

If $a \equiv -2 \pmod{p}$ *then* $u_{p-1} \equiv 1 \pmod{p}$ *and* $u_{p+1} \equiv -1 \pmod{p}$.

(d) If $c = -1$ *and* $s = (\Delta/p) = \pm 1$, *then* $u_{p-1-s} \equiv -1 \pmod{p}$ *and* $u_{p+1-s} \equiv 1 \pmod{p}$.

To prove this corollary, the following lemma relating u_{k-i} to u_i will be useful

Lemma 1. *If* $u_k \equiv 0 \pmod{m}$ *then*

$$u_{k-i} \equiv (-c)^{i+1} u_{k-1} u_i \pmod{m} \tag{14}$$

for $0 \leq i \leq k$.

Proof. The lemma is true for $i = 0$ because $m | u_k$ and $u_0 = 0$. When $i = 1$,

$$u_{k-1} = (-c)^2 u_{k-1} u_1$$

because $(-c)^2 = u_1 = 1$. Assume it's true for $i - 1$ and i, and we'll show it's true for $i + 1$. We will use the facts that $(-c)^2 = c^2 = 1$. From

$$cu_{r-1} = -au_r + u_{r+1}$$

we have that

$$u_{r-1} = -acu_r + cu_{r+1}. \tag{15}$$

By the inductive hypothesis for i,

$$u_{k-i} \equiv (-c)^{i+1} u_{k-1} u_i \pmod{m}, \tag{16}$$

and by the inductive hypothesis for $i - 1$

$$u_{k-(i-1)} = u_{k-i+1} \equiv (-c)^i u_{k-1} u_{i-1} \pmod{m}. \tag{17}$$

Starting with (15), substituting using (16) and (17), and simplifying, we have

$$\begin{aligned} u_{k-i-1} &= -acu_{k-i} + cu_{k-i+1} \\ &\equiv -ac(-c)^{i+1} u_{k-1} u_i + c(-c)^i u_{k-1} u_{i-1} \\ &= a(-c)^{i+2} u_{k-1} u_i + c(-c)^i u_{k-1} u_{i-1} \\ &= u_{k-1}(-c)^{i+2}(au_i + cu_{i-1}) \end{aligned}$$

$$= u_{k-1}(-c)^{i+2}u_{i+1},$$

where the congruence is modulo m. □

We return to the proof of Corollary 1, beginning with (a). That $p \equiv 1 \pmod 4$ follows from the fact that $p|\Delta = a^2 + 4$. Because

$$u_{p+1} = au_p + u_{p-1}$$

and $p|u_p$, we have $u_{p+1} \equiv u_{p-1} \pmod p$. Applying Lemma 1 with $k = p$ and $i = p - 1$ gives

$$u_1 \equiv (-1)^p u_{p-1}^2 \pmod p$$

so $1 \equiv (-1)u_{p-1}^2 \pmod p$ and $u_{p-1}^2 \equiv -1 \pmod p$.

For (b), $u_{p+1-s} = au_{p-s} + u_{p-1-s}$ and $p|u_{p-s}$ so $u_{p+1-s} \equiv u_{p-1-s} \pmod p$. By (13), $u_p \equiv s \pmod p$. If $s = 1$, then $u_p = u_{p+1-s}$ while if $s = -1$, then $u_p = u_{p-1-s}$.

For (c), $\Delta = a^2 - 4$, so $a^2 - 4 \equiv 0 \pmod p$ and $a \equiv \pm 2 \pmod p$. If $a \equiv 2 \pmod p$, by an easy induction, $u_i \equiv i \pmod p$ for $i \geq 0$, and so $u_{p-1} \equiv -1 \pmod p$ and $u_{p+1} \equiv 1 \pmod p$. If $a \equiv -2 \pmod p$, by induction, $u_i \equiv (-1)^{i+1}i \pmod p$ for $i \geq 0$, and so $u_{p-1} \equiv 1 \pmod p$ and $u_{p+1} \equiv -1 \pmod p$.

For (d), as above, $u_{p-s} \equiv 0 \pmod p$ and $u_p \equiv s \pmod p$. From $u_{p+1-s} = au_{p-s} - u_{p-1-s}$ we get $u_{p+1-s} \equiv -u_{p-1-s} \pmod p$. If $s = 1$, then $u_{p+1-s} = u_p \equiv 1 \pmod p$. If $s = -1$, then $u_{p-1-s} = u_p \equiv -1 \pmod p$. This completes the proof of Corollary 1.

Define $\kappa(m)$ $(= \kappa(m, a, c))$ to be the smallest index i so that $m|u_i$. We will refer to $\kappa(m)$ as the *index of apparition of* m. While Theorem 5 shows that $\kappa(p) \leq p + 1$, this bound is sharpened by the following theorems.

Theorem 6. *Let p be an odd prime and let $s = \left(\frac{\Delta}{p}\right)$. If $s = \pm 1$ and either $c = -1$ or $p \equiv 1 \pmod 4$ then $(p - s)/\kappa(p)$ is an even integer, and in particular, $\kappa(p) \leq (p - s)/2$. If $s = \pm 1$, $c = +1$, and $p \equiv 3 \pmod 4$ then $(p - s)/\kappa(p)$ is an odd integer.*

Proof. By Lemma 1, if $u_k \equiv 0 \pmod p$ and k is even then

$$u_{k/2} \equiv (-c)^{k/2+1}u_{k-1}u_{k/2} \pmod p \tag{18}$$

and so

$$p \mid u_{k/2}\left((-c)^{k/2+1}u_{k-1} - 1\right) \tag{19}$$

Consider now the case where $s = \pm 1$ and $c = -1$. By Theorem 5, $p|u_{p-s}$ and by Corollary 1, for $k = p - s$, $u_{k-1} = -1$. Then, by (19), $p|u_{k/2}(-2)$, and so $p|u_{k/2}$. This implies that $\kappa(p)|k/2$, and so $(p-s)/\kappa(p)$ is even.

Now we look at $s = \pm 1$, $c = 1$, and $p \equiv 1 \pmod 4$. Again, $p|u_{p-s}$, but here, for $k = p - s$, $u_{k-1} = s$. If $s = 1$ then $k/2 + 1 = (p-1)/2 + 1$ is odd and if $s = -1$ then $k/2 + 1 = (p+1)/2 + 1$ is even. In either case

$$(-c)^{k/2+1}u_{k-1} - 1 = (-1)^{k/2+1}s - 1 = -2.$$

So, $p|u_{k/2}(-2)$, and it follows that $p|u_{k/2}$ and $(p-s)/\kappa(p)$ is even.

Now suppose that $s = \pm 1$, $c = 1$, and $p \equiv 3 \pmod 4$. As above, $p|u_{p-s}$, and for $k = p - s$, $u_{k-1} = s$. We have that $(-1)^{k/2+1}s = -1$, so by Lemma 1

$$u_{k/2-1} \equiv (-1)^{k/2+1}su_{k/2+1} \equiv -u_{k/2+1} \pmod p. \tag{20}$$

If $u_{k/2} \equiv 0 \pmod p$ then from $u_{k/2+1} = au_{k/2} + u_{k/2-1}$ we have that $u_{k/2+1} \equiv u_{k/2-1} \pmod p$. In light of (20), $u_{k/2+1} \equiv u_{k/2-1} \equiv 0 \pmod p$, so p divides the three consecutive terms $u_{k/2+1}$, $u_{k/2}$, $u_{k/2-1}$, and p divides all subsequent terms. But, p does not divide u_p, so p cannot divide $u_{k/2}$ and $(p-s)/\kappa(p)$ cannot be even. □

We do not necessarily have $p\|u_{\kappa(p)}$. For example if $a = 8010$ and $c = 1$ then $\kappa(11) = 12$ and $11^4\|u_{12}$. But, we can say a bit more.

Theorem 7. *Let p be an odd prime. If $p|\Delta$ then $\kappa(p) = p$. If $p|\Delta$ and $p > 3$, then $p\|u_p$. If $p > 3$ and $p^r|\Delta$ for $r \geq 1$, then $u_p \equiv p \pmod{p^{r+1}}$. If $3^r|\Delta$ for $r \geq 1$ then $u_3 \equiv 3 \pmod{3^r}$. In particular, if $9|\Delta$ then $3\|u_3$.*

Comment: If $3\|\Delta$ then it can happen that $3^r\|u_3$ for $r > 1$. For example if $a = 244$ and $c = -1$, then $\Delta = 59532 = 2^2 \cdot 3 \cdot 11^2 \cdot 41$ and $3^5\|u_3 = 59535 = 3^5 \cdot 5 \cdot 7^2$.

Proof. That $\kappa(p) = p$ follows from Theorem 5. Consider (11) with $r = p$. Because $\gcd(a, p) = 1$, the term $\binom{p}{1}a^{p-1}$ is divisible by p and not by p^2. If $p > 3$, then each of the remaining terms in the binomial expansion is divisible by p^2, so $p \| u_p$. If $p > 3$ and $p^r | \Delta$, then p^{r+1} divides all terms in the binomial expansion, except the first. So, we have

$$2^{p-1}u_p \equiv pa^{p-1} \pmod{p^{r+1}}.$$

Because $p^r | \Delta$, $a^2 \equiv -4c \pmod{p^r}$, so

$$a^{p-1} \equiv (-c)^{\frac{p-1}{2}}2^{p-1} \pmod{p^{r+1}}.$$

Now, $(-c)^{\frac{p-1}{2}} = 1$ because if $c = 1$ and $p \equiv 3 \pmod 4$ then $p \nmid \Delta$. So, $u_p \equiv p \pmod{p^{r+1}}$.

If $3^r | \Delta$ for $r \geq 1$, then $c = -1$ (because $3 \nmid a^2 + 4$), $a^2 \equiv 4 \pmod{3^r}$ and

$$u_3 = \frac{1}{4}(3a^2 + \Delta).$$

If $r = 1$ then if $a^2 + \Delta/3 \equiv 0 \pmod 3$, $3^t | u_3$ for some $t \geq 2$. If $r > 1$, then $u_3 \equiv 3 \pmod{3^r}$. □

4. Indexes of apparition for powers of odd primes

Theorem 8. *If p is an odd prime and $p^r \| \kappa(p)$ then $\kappa(p^t) = \kappa(p)$ if $t \leq r$ and $\kappa(p^t) = p^{t-r}\kappa(p)$ if $t \geq r$.*

Proof. This follows by induction from the fact that if $p^t \| u_k$ for some $t \geq 1$ then $p^{t+1} \| u_{pk}$, and $p^{t+1} \nmid u_{jk}$ for $1 \leq j < p$, as we now show.

Consider (7) with $s = p$ and $\nu = k$. Then

$$p^{t+1} \left\| \binom{p}{1} v_k^{t-1} u_k \right.$$

and p^{t+2} divides the remaining terms of $2^{p-1}u_{kp}$. Thus $p^{t+1} \| u_{pk}$. If $p^{t+1} | u_{jk}$ for $j < p$ then $p^{t+1} | u_k$ because $k = \gcd(jk, pk)$. But $p^t \| u_k$. □

When $p > 3$ is prime and $p | \Delta$ we can be more specific about $\kappa(p^t)$.

Corollary 2. *If $p > 3$ is prime and $p | \Delta$ then $\kappa(p^t) = p^t$. If $9 | \Delta$ then $\kappa(3^t) = 3^t$.*

Proof. By Theorem 7, $\kappa(p) = p$ and $p \| u_p$. □

5. Indexes of apparition for powers of 2

Theorem 9. *If a is odd and $c = +1$, then $\kappa(2) = 3$, $\kappa(4) = \kappa(8) = 6$, $\kappa(2^t) = 3 \cdot 2^{t-2}$ for $t \geq 2$.*

If a is odd and $c = -1$, then $2^r \| u_3$ for some $r \geq 3$, $\kappa(2^t) = 3$ for $t \leq r$, and $\kappa(2^t) = 3 \cdot 2^{t-r}$ for $t \geq r$.

If a is even, and $2^r \| a$, then $\kappa(2^t) = 2$ for $t \leq r$ and $\kappa(2^t) = 2^{t-r+1}$ for $t \geq r$.

Note that for a even, we have the same rule for $c = +1$ and for $c = -1$. To prove this theorem, we start with a lemma.

Lemma 2. *If $t \geq 2$ and $2^t \| u_r$ then $2^{t+1} \| u_{2r}$.*

Proof. By (9), $u_{2r} = v_r u_r$. If $t \geq 2$ and $2^t \| u_r$ then by (4), $2 \| v_r$, so $2^{t+1} \| u_{2r}$. □

Now we return to the proof of the theorem.

Proof. The most straightforward way to prove statements in the theorem for u_r for particular r is just to run through all the cases modulo 2^t for a suitable t. That said, we'll give proofs for the needed cases.

If a is odd and $c = +1$, then $a^2 \equiv 1 \pmod 8$, so $u_3 = a^2 + 1 \equiv 2 \pmod 8$, $\kappa(2) = 3$, and $\kappa(4) > 3$. From the definition of the series $\{u_r\}$ we have that

$$u_6 = a^5 + 4a^3 + 3a = a(a^4 + 4a^2 + 3)$$

As a is odd, $a^4 \equiv 1 \pmod{16}$, $a^2 \equiv 1$ or $9 \pmod{16}$, $4a^2 \equiv 4 \pmod{16}$, so

$$a^4 + 4a^2 + 3 \equiv 1 + 4 + 3 \equiv 8 \pmod{16}$$

and

$$a(a^4 + 4a^2 + 3) \equiv 8 \pmod{16}.$$

This establishes that $\kappa(4) = \kappa(8) = 6$ and $2^3 \| u_6$. For $t > 3$, Lemma 2 establishes $\kappa(2^t) = 3 \cdot 2^{t-2}$.

If a is odd and $c = -1$, then, as above, $a^2 \equiv 1 \pmod 8$, so $u_3 = a^2 - 1 \equiv 0 \pmod 8$ and $2^r | u_3$ for some $r \geq 3$. By Lemma 2, for $t > r$, $\kappa(2^t) = 3 \cdot 2^{t-r}$.

If a is even then $v_2 = a^2 \pm 2$, so $v_2 \equiv 2 \pmod 4$. As $u_2 = a$, $2|u_2$. Let $2^r \| u_2$ for $r \geq 1$. By (9) $2^{r+1} \| u_4$, and by Lemma 2, $\kappa(2^t) = 2^{t-r+1}$ for $t \geq r$. □

6. Indexes of apparition for arbitrary integers

Proofs of the theorems in this section will use the following facts. First, for $m = \prod_{i=1}^{n} p_i^{\alpha_i}$, where the p_i are distinct primes

$$\kappa(m) = \operatorname{lcm}(\kappa(p_1^{\alpha_1}), \kappa(p_2^{\alpha_2}), \ldots, \kappa(p_n^{\alpha_n})). \tag{21}$$

Second, by Theorems 8 and 9, if p is prime then

$$\frac{\kappa(p^t)}{p^t} \leq \frac{\kappa(p)}{p} \tag{22}$$

Finally, if the h_i are even, then

$$\operatorname{lcm}(h_1, h_2, \ldots, h_n) \left| \frac{1}{2^{n-1}} h_1 h_2 \ldots h_n \right. \tag{23}$$

where the right hand side is an integer.

Theorem 10. *When $c = 1$*

$$\kappa(m) \leq 2m. \tag{24}$$

Equality holds if and only if $m = 6P$, $p|\Delta$ for every prime $p|P$, and $a \equiv 1$ or $5 \pmod 6$.

Proof. Write m as a product of primes

$$m = 2^{\alpha_0} \prod_{i=1}^{n_1} p_i^{\alpha_i} \prod_{j=1}^{n_2} q_j^{\beta_j} \prod_{k=1}^{n_3} r_k^{\gamma_k} \tag{25}$$

where $\kappa(p_i) = p_i + 1$, $\kappa(q_j) = q_j$, and $\kappa(r_k) < r_k$. Then

(26)

$$\frac{\kappa(m)}{m} \le \frac{\operatorname{lcm}(\kappa(2), p_1+1, \ldots, p_{n_1}+1, q_1, \ldots, q_{n_2}, \kappa(r_1), \ldots, \kappa(r_{n_3}))}{2p_1 \ldots p_{n_1} q_1 \ldots q_{n_2} r_1 \ldots r_{n_3}}$$

$$\le \frac{\kappa(2)}{2} \frac{\operatorname{lcm}(p_1+1, p_2+1, \ldots, p_{n_1}+1)}{p_1 p_2 \ldots p_{n_1}} \frac{q_1 q_2 \ldots q_{n_2}}{q_1 q_2 \ldots q_{n_2}} \frac{\kappa(r_1)\kappa(r_2)\cdots\kappa(r_{n_3})}{r_1 r_2 \ldots r_{n_3}}$$

$$\le \frac{\kappa(2)}{2} \frac{\operatorname{lcm}(p_1+1, p_2+1, \ldots, p_{n_1}+1)}{p_1 p_2 \ldots p_{n_1}}$$

$$\le \frac{\kappa(2)}{2} \frac{p_1+1}{p_1} \frac{p_2+1}{2p_2} \cdots \frac{p_{n_1}+1}{2p_{n_1}} \le \frac{\kappa(2)}{2} \frac{p_1+1}{p_1}$$

(where if $\alpha_0 = 0$, drop the obvious terms related to the prime 2). Now, $\kappa(2) \le 3$ and $(p_1+1)/p_1 = 1 + 1/p_1 \le 4/3$, so $\kappa(m)/m \le 2$.

We'll prove the necessity and sufficiency of the remaining conditions in more detail for this theorem than for the similar subsequent theorem.

First we show the necessity. We can have $\kappa(m)/m = 2$ only if $6|m$, $\kappa(2) = 3$, and $\kappa(3) = 4$. If $\kappa(2) = 3$ then a is odd and if $\kappa(3) = 4$ then $3 \nmid a$, so $a \equiv 1$ or $5 \pmod 6$.

Let $2^t 3^s | m$ for some $t, s \ge 1$. If $2^t | m$ for $t \ge 2$ then either $\kappa(2^t) \le 3 \cdot 2^{t-2}$ and $\kappa(2^t)/2^t < 3/2$ or $\kappa(2^t) = 3 \cdot 2^{t-1}$ and $\operatorname{lcm}(\kappa(2^t), \kappa(3^s))/(2^t 3^s) < 2$.If $3^s | m$ for $s \ge 2$ then either $\kappa(3^s) \le 4 \cdot 3^{s-2}$ and $\kappa(3^s)/3^s < 4/3$ or $\kappa(3^s) = 4 \cdot 3^{s-1}$ and $\operatorname{lcm}(\kappa(2^t), \kappa(3^s))/(2^t 3^s) < 2$.

For all primes p so that $p|P$, we need to have $\kappa(p)/p = 1$, so $p|\Delta$.

Now we prove the sufficiency of the conditions. With $a \equiv 1$ or $5 \pmod 6$, $\kappa(2) = 3$ and $\kappa(3) = 4$. For primes p so that $p|\Delta$, $\kappa(p^t) = p^t$. It follows that $\kappa(m)/m = 2$. □

Note that in the Theorem above since a is odd, for any prime p so that $p|\Delta = a^2 + 4$, $p \equiv 1 \pmod 4$.

Theorem 11. *When $c = -1$*

$$\kappa(m) = \frac{3m}{2} \text{ or } \kappa(m) \le m. \tag{27}$$

In the first case

$$\kappa(m) = \frac{3m}{2} \tag{28}$$

if and only if $m = 2P$ *where* P *is odd,* $3 \nmid P$*,* a *is odd, and* $p|\Delta = a^2 - 4$ *for every prime* $p|P$*.*

In the second case, $\kappa(m) = m$ *if and only if* $p|\Delta$ *for every prime* $p > 3$ *so that* $p|m$ *and either* $6|m$*,* $\gcd(m/6, 6) = 1$*, and* $a \equiv 3 \pmod 6$*, or* $6|\Delta$*, if* $4|m$ *then* $a \equiv 2 \pmod 4$*, and if* $9|m$ *then* $a \not\equiv \pm 1 \pmod 9$*.*

Proof. The proof of this theorem is similar to the one above. Because $c = -1$, for any odd prime for which $p \nmid \Delta$, $\kappa(p^t)/p^t \leq (p+1)/2p < 1$. We still have that $\kappa(2) = 3$ if and only if a is odd. □

Many additional characterizations of possible ratios for $\kappa(m)/m$ are possible, as illustrated by the following lemma which gives just two more.

Lemma 3. *If* $3/2 < \kappa(m)/m < 2$ *then* $\kappa(m)/m = 3(p+1)/(2p)$ *for a prime* $p \equiv 7 \pmod{12}$*. If* $c = -1$ *and* $3/4 < \kappa(m)/m < 1$ *then* $\kappa(m)/m = 3(p+1)/(4p)$ *for a prime* $p \equiv 1 \pmod 6$*.*

In particular, $\kappa(m)/m$ cannot take any values between $12/7 \approx 1.714\ldots$ and 2.

7. The sequences $\{y_n\}$ and $\{u_r\}$

Theorem 12. *The sequences* $\{y_n\}$ *satisfy the recurrences given in Table 2.*

Proof. We will prove this when $x_1^2 - dy_1^2 = -4$. The other cases are similar. We have

$$x_1^2 + 2x_1y_1\sqrt{d} + y_1^2 d = 2x_1^2 + 2x_1y_1\sqrt{d} + 4$$

which implies

$$\left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^2 = x_1\left(\frac{x_1 + y_1\sqrt{d}}{2}\right) + 1$$

and so

$$\left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^{n+1} = x_1\left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^n + \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^{n-1}$$

giving

$$\frac{x_{n+1}+y_{n+1}\sqrt{d}}{2} = x_1\left(\frac{x_n+y_n\sqrt{d}}{2}\right)+\frac{x_{n-1}+y_{n-1}\sqrt{d}}{2}$$

from which it follows that

$$x_{n+1} = x_1x_n + x_{n-1} \text{ and } y_{n+1} = x_1y_n + y_{n-1}.$$

□

Lemma 4. *If the sequence $\{y_n\}$ satisfies $y_0 = 0$ and $y_{n+1} = ay_n+cy_{n-1}$ then $y_n = y_1u_n$, where the sequence $\{u_n\}$ satisfies $u_0 = 0$, $u_1 = 1$, and $u_{n+1} = au_n + cu_{n-1}$.*

Lemma 5. *If $x^2-dy^2 = \pm 1$ or ± 4 and $y_n = y_1u_n$ then $dy_1^2 = \Delta$ or 4Δ. In particular, if p is an odd prime and $p \nmid y_1$ or $p|d$, then $\left(\frac{d}{p}\right) = \left(\frac{\Delta}{p}\right)$. Also, if $p|y_1$, then $p|\Delta$.*

Proof. We will do one case; the others are similar. Suppose that $\{y_n\}$ is the sequence of y's that are solutions to $x^2 - dy^2 = \pm 4$ for some d, and that $x_1^2-dy_1^2 = -4$. Then $y_n = y_1u_n$ and $\Delta = a^2+4c = x_1^2+4 = dy_1^2$. In particular, $p|dy_1^2 \iff p|\Delta$, and if $p \nmid y_1$ or $p|d$, then $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right)$. □

8. Indexes of apparition powers of odd primes in the sequence $\{y_n\}$

The issue is what is the smallest j so that $p^t|y_j$ for p an odd prime, $t \geq 1$, and $\{x_n, y_n\}$ the sequence of positive solutions to $x^2 - dy^2 = \pm 1$ or ± 4, with $d > 1$ squarefree. We denote the smallest such j by $\eta(p^t)$, also called the *index of apparition of p^t in the sequence $\{y_j\}$*.

There are three cases to consider: (A) $p|y_1$, (B) $p \nmid y_1$ and $p|d$, and (C) $p \nmid dy_1$.

For (A), if $p^r \| y_1$, then for $s = \max(0, t - r)$, $\eta(p^t) = p^s$. As $p|y_1$, $p^2|\Delta$ so by Corollary 2, $p^s \| u_{p^s}$. Then for $t \geq r$, $p^t \| y_{p^s}$.

For (B) we need to consider $p \neq 3$ and $p = 3$. If $p \neq 3$, $p|d$, and $p \nmid y_1$, then $\eta(p^t) = p^t$. This is because $p|\Delta$ and so by Corollary 2, $p^t \| u_{p^t}$.

If $p = 3$, $3|d$, and $3 \nmid y_1$, and $3^r \| y_3$ (which will happen for some $r \geq 1$), for $s = \max(0, t-r)$, $\eta(3^t) = 3^{s+1}$. By Theorem 7, $\kappa(3) = 3$. That $\eta(3^t) = 3^{s+1}$ then follows from Theorem 8.

For (C), $p \nmid dy_1$, by Lemma 5 and Theorem 6

$$\eta(p) \left| \frac{1}{s}\left(p - \left(\frac{d}{p}\right)\right)\right.$$

where $s = 2$ if $p \equiv 1 \pmod 4$ or $c = -1$ and $s = 1$ if $p \equiv 3 \pmod 4$ and $c = 1$. In the latter case, $\left(p - \left(\frac{d}{p}\right)\right)/\eta(p)$ is odd. If $p^r \| y_{\eta(p)}$ for some $r \geq 1$, then $\eta(p^t)$ is $\eta(p)p^s$ where $s = \max(0, t-r)$. That r need not be 1 can be seen by taking $d = 2285$ and $p = 13$. Then $\eta(13) = 3$ and $13^4 \| y_3 = 285610$.

9. Indexes of apparition for powers of 2 in the sequence $\{y_n\}$

There are several cases to consider when $p = 2$. If $d \equiv 1 \pmod 4$, we consider only solutions to $x^2 - dy^2 = \pm 4$, while if $d \not\equiv 1 \pmod 4$ we consider only solutions to $x^2 - dy^2 = \pm 1$. We let $\{x_1, y_1\}$ denote the minimal positive solution to $x^2 - dy^2 = \pm 4$ or ± 1, as the case might be.

The cases for $p = 2$ are as follows (these all follow from theorems above, or tests mod 32).

(1) If $d \equiv 5 \pmod 8$, and $x_1^2 - dy_1^2 = -4$, then
   (a) If y_1 is odd, then x_1 is odd, $\eta(2) = 3$, $\eta(4) = \eta(8) = 6$, and $\eta(2^t) = 3 \cdot 2^{t-2}$ for $t \geq 3$.
   (b) If y_1 is even, then $y_1 \equiv 2 \pmod 4$, $x_1 \equiv 4 \pmod 8$, $\eta(2) = 1$, $\eta(4) = \eta(8) = 2$, and $\eta(2^t) = 2^{t-2}$ for $t \geq 3$.

(2) If $d \equiv 5 \pmod 8$, and $x_1^2 - dy_1^2 = +4$, then
   (a) If y_1 is odd, then x_1 is odd, as are y_2 and x_2.Let $2^r \| y_3$, where $r \geq 3$. For $t \leq r$, $\eta(2^t) = 3$, and $\eta(2^t) = 3 \cdot 2^{t-r}$ for $t \geq r$.
   (b) If y_1 is even, then $y_1 \equiv 0 \pmod 8$ and $x_1 \equiv 2 \pmod 4$. Let $2^r \| y_1$, where $r \geq 3$. For $t \leq r$, $\eta(2^t) = 1$, and $\eta(2^t) = 2^{t-r}$ for $t \geq r$.

(3) If $d \equiv 1 \pmod 8$ and $x_1^2 - dy_1^2 = -4$, then $2 \| y_1$ and $8 | x_1$. We have $\eta(2) = 1$. Also, $2^r \| y_2$ for some $r \geq 4$. If $1 < t \leq r$ then $\eta(2^t) = 2$. If $t \geq r$ then $\eta(2^t) = 2^{t-r+1}$.
(4) If $d \equiv 1 \pmod 8$ and $x_1^2 - dy_1^2 = +4$ then $2^r \| y_1$ for some $r \geq 3$ and $2 \| x_1$. If $t \leq r$ then $\eta(2^t) = 1$. If $t \geq r$, then $\eta(2^t) = 2^{t-r}$.
(5) If $d \not\equiv 1 \pmod 4$, then
   (a) If y_1 is odd then $2^r \| y_2$ for some $r \geq 1$. For $t \geq 1$, if $t \leq r$ then $\eta(2^t) = 2$, while if $t \geq r$ then $\eta(2^t) = 2^{1+t-r}$.
   (b) If y_1 is even, and $2^r \| y_1$, then for $1 \leq t \leq r$, $\eta(2^t) = 1$, while for $t \geq r$, $\eta(2^t) = 2^{t-r}$.

10. Units in quadratic orders

One of our main goals is to show that if ϵ_1 is the fundamental unit of the ring of integers $\mathcal{O}$ (maximal order) of the real quadratic field $\mathbf{Q}(\sqrt{d})$ for $d > 0$ squarefree, ϵ_f is the fundamental unit of the order of conductor f in $\mathcal{O}$, and $\epsilon_1^E = \epsilon_f$, then $E \leq 2f$ (and some related results). For definitions of terms in the previous sentence, see the article "Computing in Quadratic Orders."

Consider first the case where $d \equiv 1 \pmod 4$. Let $\{x_i, y_i\}$ be the positive solutions to $x^2 - dy^2 = \pm 4$, so $\{x_1, y_1\}$ is the minimal positive solution.The fundamental unit of the maximal order of $\mathbf{Q}(\sqrt{d})$ is

$$\frac{1}{2}(x_1 + y_1\sqrt{d}).$$

The fundamental unit of the order of conductor f is

$$\frac{1}{2}(x_E + y_E\sqrt{d}) = \frac{1}{2}(x_E + \frac{y_E}{f}f\sqrt{d})$$

where E is the smallest index i so that $f | y_i$. Recall that,

$$\frac{x_E + y_E\sqrt{d}}{2} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^E.$$

Now consider the case where $d \not\equiv 1 \pmod 4$. Let $\{x_i, y_i\}$ be the positive solutions to $x^2 - dy^2 = \pm 1$.The fundamental unit of the maximal order of $\mathbf{Q}(\sqrt{d})$ is

$$x_1 + y_1\sqrt{d}.$$

The fundamental unit of the order of conductor f is

$$x_E + y_E\sqrt{d} = x_E + \frac{y_E}{f} f\sqrt{d}$$

where E is the smallest index i so that $f|y_i$. Here,

$$x_E + y_E\sqrt{d} = (x_1 + y_1\sqrt{d})^E.$$

It is then straightforward to apply the above theorems on the sequence $\{y_n\}$ to obtain

Theorem 13. *$E/f \leq 2$. $E/f = 2$ if and only if*

$N(\epsilon_1) = -1$,
$x_1 \equiv 1$ *or* $5 \pmod 6$ *where* $x_1 + y_1\sqrt{d} = 2\epsilon_1$, *and*
$f = 6\prod p_i^{\alpha_i}$ *where* $p_i|d$ *and* $\gcd(p_i, y_1) = 1$.

The above conditions imply that if $E/f = 2$ then $d \equiv 5 \pmod 8$, $\gcd(6, f/6) = 1$, $y_1 \equiv 1$ or $5 \pmod 6$, and $p_i \equiv 1 \pmod 4$.

As an example where $\gcd(d, y_1) > 1$, take $d = 3077$. Then $\epsilon_1 = (943 + 17\sqrt{3077})/2$ and $N(\epsilon_1) = -1$.

If any reader knows a reference in the literature for the fact that $E/f \leq 2$ I would be grateful to hear of it. The only reference that I know is Podsypanin [9, Lemma 1], but the proof given there is wrong. It is my understanding that the results above are well known.

11. Periods

This section discusses period lengths of the sequences $\{u_n \mod m\}$ and $\{y_n \mod m\}$.

Period lengths for $\{u_n \mod m\}$ follow easily from

$u_{\kappa(m)+1} = 1 \implies$ period $= \kappa(m)$,
$u_{\kappa(m)+1} = -1 \implies$ period $= 2\kappa(m)$,
$u_{\kappa(m)+1} \neq \pm 1 \implies u^2_{\kappa(m)+1} \equiv -1 \pmod m$ and
period $= 4\kappa(m)$.

Note that last can only occur when $c = 1$. These are easy consequences of Lemma 1. Write k for $\kappa(m)$. First we have that

$$u_{k-i} \equiv (-c)^{i+1}u_{k-1}u_i \pmod m \implies 1 \equiv u_1 \equiv (-c)^k u^2_{k-1} \pmod m$$
$$\implies u^2_{k-1} \equiv \pm 1 \pmod m.$$

Then , with all congruences modulo m, $u_{k+1} \equiv cu_{k-1}$, so $u_{k+i} \equiv cu_{k-1}u_i$, $u_{2k-1} \equiv cu_{k-1}^2$, $u_{3k-1} \equiv u_{k-1}^3$, $u_{4k-1} \equiv cu_{k-1}^4 \equiv c$, and hence $u_{4k+1} \equiv 1$ (recall $u_k \equiv u_{2k} \equiv u_{3k} \equiv u_{4k} = 0$). Possibilities for periods follow from these.

For $\{y_n \mod m\}$, indexes of apparition and periods are indexes and periods for $\{u_n \mod m/g\}$ where $g = \gcd(y_1, m)$ because

$$m|(y_r - y_s) = \left(\frac{y_1}{g}\right) \cdot g \cdot (u_r - u_s) \iff \frac{m}{g} | \left(\frac{y_1}{g}\right) (u_r - u_s) \iff \frac{m}{g} | (u_r - u_s)$$

and

$$m|y_r = \left(\frac{y_1}{g}\right) \cdot g \cdot u_r \iff \frac{m}{g} | \left(\frac{y_1}{g}\right) u_r \iff \frac{m}{g} | u_r.$$

As an example where the period is $4\kappa(m)$, take $m = 13$, $a = 2$, $c = 1$. Then $\kappa(13) = 7$,

$$u_7 \equiv u_{14} \equiv u_{21} \equiv u_{28} \equiv 0 \pmod{13},$$

$$u_6 \equiv u_8 \equiv 5 \pmod{13},$$

$$u_{13} \equiv u_{15} \equiv 12 \pmod{13},$$

$$u_{20} \equiv u_{22} \equiv 8 \pmod{13}, \text{ and}$$

$$u_{27} \equiv u_{29} \equiv 1 \pmod{13}.$$

Observe that $5^2 \equiv 8^2 \equiv -1 \pmod{13}$, and $12^2 \equiv 1 \pmod{13}$.

12. The sequences $\{x_n\}$

The sequences $\{x_n\}$ satisfy the same recurrences as $\{y_n\}$, that is $x_{r+1} = ax_r + cx_{r-1}$. The sequences $\{x_n\}$ have certain divisibility properties related to those of the sequences $\{y_n\}$, but, because $x_0 \neq 0$, there are some differences. We list a few properties.

If ν is odd, then $x_k | x_{\nu k}$.

$x_k | y_{2k}$.

If $p | y_\nu$ for $p > 2$ prime and ν odd, then $p \nmid x_k$ for any k.

If $p | y_\nu$ for $p > 2$ prime and ν even, and $p \nmid y_i$ for $i < \nu$, then $p | x_{\nu/2}$ and $p \nmid x_i$ for $i < \nu/2$.

13. The generalized Pell equation $x^2 - dy^2 = N$

Each family of solutions $\{x_i, y_i\}$ to the generalized Pell equation $x^2 - dy^2 = N$, $n \neq 0$, ± 1, ± 4, satisfies the recursions

$$x_{r+1} = ax_r - x_{r-1},$$

$$y_{r+1} = ay_r - y_{r-1}$$

where $a = 2t$ and (t, u) is the minimum positive solution to $x^2 - dy^2 = 1$.

As we don't necessarily have $x_i = 0$ or $y_i = 0$ for any i, not all of the above theorems apply to these sequences. But, for example

$$y_i = y_1 u_i - (ay_1 - y_2)u_{i-1}$$

so the period of y_i modulo f is $4f$ or less. One approach to solving $x^2 - f^2 dy^2 = N$ is to solve $x^2 - dy^2 = N$ and, for each family of solutions, look for y so that $f|y$.

14. Where to go from here

Lehmer [5] lists a lot more properties of the sequences considered above, as they relate to Pell equations. Lehmer [6] gives more general results about related recurrence series, aimed mostly at building primality tests.

Please send comments to jpr2718@gmail.com.

15. Appendix 1: A matrix approach to computing $\{u_r\}$

By an easy induction,

$$\begin{pmatrix} a & 1 \\ c & 0 \end{pmatrix}^r = \begin{pmatrix} u_{r+1} & u_r \\ cu_r & cu_{r-1} \end{pmatrix}.$$

This allows "binary exponentiation" methods (see [3, pp. 441-444, 463-465]) of computing u_r, v_r, and so y_r, x_r. We use this method in the next section.

16. Appendix 2: Fast computation of y_k

If k is "small" it is straightforward and reasonably fast to just directly compute y_k. If k is large, we can use a routine analogous to right-to-left binary exponentiation [3, pp. 441-444, 463-465] to compute y_k with a number of steps proportional to $\ln(k)$. If p is odd, the calculations below can be done modulo p to compute y_k modulo p (where division by 2 is called for below, instead multiply by $(p+1)/2$).

Let $\{y_i\}$ satisfy the recurrence relation $y_{r+1} = ay_r + cy_{r-1}$ (so $a = x_1$ or $2x_1$ and $c = \pm 1$). We need two auxiliary sequences (as above), $u_0 = 0$, $u_1 = 1$, $u_{r+1} = au_r + cu_{r-1}$, and $v_0 = 2$, $v_1 = a$, $v_{r+1} = av_r + cv_{r-1}$. Then $y_r = y_1 u_r$. For $\Delta = a^2 + 4c$ we have that $v_r^2 - \Delta u_r^2 = 4(-c)^r$. This gives us the relations

$$u_{r+1} = (u_r v_1 + u_1 v_r)/2,\ v_{r+1} = (v_1 v_r + u_r u_1 \Delta)/2,$$

$$u_{2r} = v_r u_r,\ \text{and}\ v_{2r} = (v_r^2 + \Delta u_r^2)/2.$$

With that background, here's the algorithm to compute u_k. Set $z_1 = 2$, $z_2 = 0$, $w_1 = a$, $w_2 = 1$, and $n = k$. Repeat the following until $n = 0$.

> If n is odd, set $z_1' = (z_1 w_1 + z_2 w_2 \Delta)/2$, $z_2 = (z_1 w_2 + z_2 w_1)/2$, $z_1 = z_1'$. Whether or not n is odd, set $w_1' = (w_1^2 + D w_2^2)/2$, $w_2 = w_1 w_2$, $w_1 = w_1'$. Set $n = \lfloor n/2 \rfloor$.

When $n = 0$, z_2 is u_k.

17. Appendix 3: Index of apparition for prime $p > 2$, $p \nmid dy_1$

In this appendix we discuss a method for finding the index of apparition $\kappa(p)$ of an odd prime p that does not divide dy_1. Then

$$\kappa(p) \mid k = \frac{1}{s}\left(p - \left(\frac{d}{p}\right)\right)$$

where $s = 2$ when $p \equiv 1 \pmod 4$ or $x_1^2 - dy_1^2 > 0$, and $s = 1$ otherwise. Let $k = \prod_{i=1}^n q_i^{\alpha_i}$ be the canonical factorization of k. Then $\kappa(p) = \prod_{i=1}^n q_i^{\beta_i}$ where $0 \le \beta_i \le \alpha_i$ for $1 \le i \le n$. If $j = \prod_{i=1}^n q_i^{\gamma_i}$ where each γ_i equals either β_i or α_i (we really just need $\gamma_i \ge \beta_i$) then $p | y_j$.

Here's a way to determine the β_i one by one. Start with setting $k' = k$. For each q_i in turn, do the following.

Step 1: If $q_i \nmid k'$ go to Step 4 (of course, q_i will divide k' the first time you come to this step for a given q_i).
Step 2: Set $k'' = k'/q_i$.
Step 3: If $q_i | y_{k''}$, set $k' = k''$ and return to Step 1.
Step 4: Go on to the next q_i, if there is one.

When all q_i have been done, $\kappa(p) = k'$.

The method of Appendix 2 can be used to calculate $y_{k''}$ modulo q_i quickly.

This method essentially starts with α_i and keeps subtracting 1 until β_i is found. For large α_i, it would be faster to use a binary search to find β_i.

References

[1] R. D. Carmichael, On the Numerical Factors of the Arithmetic Forms $a^n \pm \beta^n$, *The Annals of Mathematics*, 2nd Ser., Vol. 15, No. 1/4 (1913-1914), 30-48, 49-70.

[2] L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, AMS Chelsea Publishing, Providence, Rhode Island, 1999.

[3] Donald E. Knuth, *The Art of Computer Programming*, Volume 2, *Seminumerical Algorithms*, Second Edition, Addison-Wesley, Reading, Massachusetts, 1981.

[4] Derrick Henry Lehmer, On the Indeterminate Equation $t^2 - p^2Du^2 = 1$, *The Annals of Mathematics*, 2nd Ser., Vol. 27, No. 4. (Jun., 1926), pp. 471-476.

[5] D. H. Lehmer, On the Multiple Solutions of the Pell Equation, *The Annals of Mathematics*, 2nd Ser., Vol. 30, No. 1/4. (1928 - 1929), pp. 66-72.

[6] D. H. Lehmer, An Extended Theory of Lucas' Functions, *The Annals of Mathematics*, 2nd Ser., Vol. 31, No. 3 (July 1930), 419–448.

[7] Edouard Lucas, Théorie des Fonctions Numériques Simplement Périodiques, *American Journal of Mathematics*, Vol. 1, No. 2 (1878), 184-196; Vol. 1, No. 3 (1878), 197-240; Vol. 1, No. 4 (1878), 289-321.

[8] Paulo Ribenboim, *My Numbers, My Friends*, Springer–Verlag, New York, 2000.

[9] E. V. Podsypanin, Length of the period of a quadratic irrational (in Russian), Studies in Number Theory, 5, *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI)* 82 (1979) 95-99, 166; Engl. transl. in *J. Soviet Math.* 18 (1982) 919-923; MR0537024 (80h:12002).

E-mail address: jpr2718@gmail.com