Fields Institute Communications
Volume **00**, 0000

Jeepers, Creepers, ... †

Roger D. Patterson
Department of Mathematics,
Macquarie University, Sydney, NSW 2109, Australia
`rogerp@ics.mq.edu.au (Roger Patterson)`

Alfred J. van der Poorten
ceNTRe for Number Theory Research,
1 Bimbil Place, Killara, NSW 2071, Australia
`alf@math.mq.edu.au (Alf van der Poorten)`

Dedicated to Hugh Cowie Williams on his 60th Birthday
and, with our thanks for asking some fine questions,
to Irving Kaplansky

Abstract. We provide a brief introductory report on our study, jointly with Hugh Williams, of polynomially parametrised families of quadratic number fields with explicitly computable regulator and, seemingly therefore, relatively small regulator. Notwithstanding that, our subject in fact is hyperelliptic curves with torsion divisor of relatively high order.

Several years ago, Irving Kaplansky [10] told three Canadian number theorists about his investigation of the length $\ell p(\sqrt{D_n})$ of the period of the continued fraction expansion of the square root $\sqrt{D_n}$ of families of discriminants

$$D_n = D_n(a, b, c; x) = ax^{2n} + bx^n + c\,; \tag{1}$$

here x, a, b, c are given integers and $n = 0,\ 1,\ 2,\ 3,\ \dots$.

Typically, $\ell p(\sqrt{D_n})$ leaps upwards with n at frantic rate. On the other hand, one does notice occasional triples a, b, c so that, for some (or all) congruence classes x modulo some appropriate modulus, $\ell p(\sqrt{D_n})$ is constant.

There are also triples for which $\ell p(\sqrt{D_n})$ increases only slowly, indeed linearly in n. Naturally, Kap called those triples *creepers*, thus distinguishing them from the generic *leapers* and the seemingly dull *sleepers*.

If only because of that fine terminology, the matter clearly warranted study. Specifically, Kaplansky had mooted the possibility that all creepers were known,

† From the song "Jeepers, creepers... where'd ya get them peepers, ... " by Al Donohue, and Johnny Mercer (recorded by Louis Armstrong, 1938). Note also the 2001 film 'Jeepers Creepers'.

2000 *Mathematics Subject Classification.* Primary 11J70, 11A65, 11J68.
Key words and phrases. discriminant, continued fraction, function field, unit.
This work was supported in part by an ARC IREX grant.

having already been described in work of Williams [30]. We soon saw that's not so; there are sequences of polynomially parametrised discriminants quite different in shape from (1) that "creep". Not all creepers are *kreepers*.

It seems, at any rate experimentally, that there are no triples a, b, c with integers x so that the period lengths $\ell p(D_n)$ increase calmly, yet more excitably than linearly. Apparently, there are no *jeepers*.

ASIDE: Of course period length, while fun, is not of great importance. What is significant is the "weighted length" — weighted by the partial quotients — of the continued fraction expansion, to wit the regulator of the number field. The point thus is that we know no polynomially parametrised sequences of discriminants so that the regulators increase calmly, yet faster than $O(n^2)$.

Were it not that we wished to dedicate this report to Hugh Williams reaching three score years, we would here be Hugh's co-authors. Mind you, Hugh might well not have chosen to be a co-author of this eccentric introduction to the subject.

Roger Patterson's work has been variously supervised by Alf van der Poorten in Sydney and Hugh Williams in Manitoba (and, later, in Calgary). The collaboration between the Sydney and Canadian groups was partially supported by an Australian Research Council International Research Exchange Grant, and by the NSERC.

A Warning. Throughout, we switch from numerical example $D_n(x)$, where D_n is some polynomial with degree depending on n, and x is a rational integer, to function field example $Y^2 = D_n(X)$. Tacitly, we suppose the base field to be the rationals $\mathbb{Q}$, but many of our remarks are more general; nonetheless, contrary to common usage, when we say "function field" we rarely include *congruence* function field, to wit, with some finite base field.

1 A Brief History

Presumably, "finding" creepers is a matter of detailing appropriate parametrised sequences of discriminants D_n. Such studies go back at least to Nyberg's sequence [18] given by $D_n = (x^n + x - 1)^2 + 4x^n$ and to the experimental rediscovery by Daniel Shanks of a particular case $S_n = (2^n + 1)^2 + 4 \cdot 2^n$. In subsequent years one finds a sequence of ever more complicated constructions of Yamamoto [33], Hendy [9], Bernstein [3], Williams [30], Lévesque and Rhin [14], Lévesque [13], Azuhata [2], Halter-Koch [8], Mollin and Williams [17] and [16], and of Williams [31]; the remarks of van der Poorten [20] attempt to provide a uniform analysis of these examples.

The cited studies vary in their emphasis. Some explicitly display what we now choose to call kreepers. In those cases one can obtain the detailed continued fraction expansion and therefore the fundamental unit. For example, Shanks [28] notices that the triples $1, 6, 1$, and $1, 6, 25$, both with $x = 2$, are kreepers. Other studies above provide sequences for which the period length provably grows faster than linearly; however, that these cases are leapers and not jeepers is no more than a compelling experimental observation. We shall explain why one might feel confident they are not jeepers.

More precisely, all the cited cases are examples of

$$\begin{aligned} D_n(x) &= \bigl(qrx^n + (mx^k - l)/q)\bigr)^2 + 4lrx^n \\ &= \bigl(qrx^n - (mx^k - l)/q)\bigr)^2 + 4mrx^{n+k} . \end{aligned} \tag{2}$$

Here, without loss of generality*, $\gcd(n,k)=1$. The sequences $\bigl(D_n(x)\bigr)$ sleep or kreep if $qr\bigm|(mx^k-l)$ and l, m, and x satisfy certain conditions, including that x is so chosen that also both $l\bigm|D_n(x)$ and $m\bigm|D_n(x)$. If not, the sequences are apparently generic; experimentally, they leap.

If, indeed, (2) provides all kreepers then in (1) necessarily

$$a=q^2r^2\,,\quad b=2r(mx^k+l)\quad\text{and}\quad c=(mx^k-l)^2/q^2\,;$$

in particular, both a and c are squares. Suppose that the conditions to kreep are satisfied. We also note that while the length $\ell p(\sqrt{D_n})$ of the expansion of $\sqrt{D_n}$ is to vary linearly with n, the logarithm of the fundamental unit of the quadratic number field $\mathbb{Q}(\sqrt{D_n})$, thus the regulator of the field, is in these cases of size $O(n^2)$.

Conversely, we can show that (2) provides all kreepers if we presume that in (1) both a and c are squares and that each quadratic number field $\mathbb{Q}(\sqrt{D_n})$ contains a principal ideal of norm x^g, for some positive integer g.

2 Sleepers

Sleep is all important. Fortunately, the issues are well understood because of work of Andrzej Schinzel [27] some forty years ago.

Schinzel asks about the period lengths $\ell p\bigl(\sqrt{F(x)}\bigr)$ for polynomials $F(X)$, taking positive integer values, not squares, for all sufficiently large integers x. He proves that if $\ell p\bigl(\sqrt{F(x)}\bigr)$ is bounded then certainly F is of even degree $2g+2$ and its leading coefficient is a square. More — with $\mathcal{C}:Y^2=F(X)$ — the function field $\mathbb{Q}(X,Y)$ of $\mathcal{C}$ must have a nontrivial unit $a(X)+b(X)Y$. It is out of the ordinary for a function field of positive genus and defined over an infinite base field to have non-trivial units, so we say such fields are *exceptional*.

Schinzel shows that $\limsup_{x\to\infty}\ell p\bigl(\sqrt{F(x)}\bigr)$ is finite if and only if $\mathbb{Q}(X,Y)$ contains a non-trivial unit $a(X)+b(X)Y$ of norm 1 so that the polynomials a and b both have coefficients in $\mathbb{Z}$. We call this *Schinzel's condition* and then say that $F(X)$ is a *sleeper*.

The function field $\mathbb{Q}(X,Y)$ being exceptional is equivalent to the continued fraction expansion of $Y=\sqrt{F(X)}$ being periodic (by Berry [4] and related remarks, if a quadratic irrational $Y(X)$ has polynomial trace then the quasi-periodicity of its continued fraction expansion entails its periodicity). Schinzel's condition in effect guarantees that the periods of the numerical expansions of $\sqrt{F(x)}$, for sufficiently large integers x, have a "pattern" obviously corresponding to the period of $\sqrt{F(X)}$.

If $\mathcal{C}$ is of genus zero its function field always has a unit. For details of the Schinzel condition in this case see page 8.

All our examples of creep arise from torturing some curve $Y^2=D(X)$ whose function field is exceptional; note examples of such maltreatment in §5 on page 9.

3 Jeepers, Creepers, ...

We follow Kaplansky in thinking of *creepers* as sequences $\bigl(D_n(X)\bigr)$ of polynomials of degree increasing linearly in n and having the feature that there are integers x so that the period lengths $\ell p\bigl(\sqrt{D_n(x)}\bigr)$ "increase gently, forming one or more arithmetic progressions when sorted into residue classes; there may be a waiting period before the arithmetic progressions begin" [10]. Strictly speaking, one might

*If not, work with $x^{\gcd(n,k)}$ in place of x.

better speak of certain sequences of curves $(\mathcal{C}_n)$, where $\mathcal{C}_n : Y_n^2 = D_n(X)$. However, our remarks underemphasise creep as such in favour of giving weight to being able explicitly to determine units of the quadratic fields $\mathbb{Q}\big(Y_n(x)\big)$; surprisingly, perhaps, that seems to coincide with creep.

All examples known to us provide regulators of size $O(n^2)$, both where relevant in the function field case, and for specialisations X to appropriate integers x.

3.1 Kreepers. In particular we read Kaplansky to be concerned with creepers

$$aX^{2n} + bX^n + c \tag{1'}$$

of quadratic shape with coefficients a, b, c independent of n; here, at least one of the coefficients must be a rational function properly depending on X; otherwise $(1')$ is a sleeper.

However, in practice it seems that all kreepers are of the shape (3) below. That leads us — we hope Kap does not object too strongly — to describe any creeper of the "shape" (3) as a *kreeper*.

Mind you, if the parameters q, r, l, and m in (3) are allowed to depend on n then, at first glance at any rate, one might be able to concoct "kreepers" with period lengths increasing somewhat faster with n than proper creep allows. Nonetheless, the regulators would remain of size $O(n^2)$.

3.2 Jeepers! It happens to happen that all the examples we have noticed, both of sequences of function fields with nontrivial units†, and of creepers, have regulator of size $O\big(n^2\big)$. We refer to a putative sequence of discriminants with regulator growing calmly, but at greater rate, as a *jeeper*.

3.3 Leapers. We join Kaplansky in referring to a polynomially parametrised sequence (D_n) of discriminants with period lengths $\ell p(\sqrt{D_n})$, and with regulator of the orders $\mathbb{Z}[\sqrt{D_n(x)}]$ behaving "typically", as a *leaper*. Heuristics entail the majority of such regulators being of size $O(\exp n)$.

Our suggestion, that the sequences of discriminants here considered either sleep, creep, or leap, is based on no more than heuristics and experiment.

ASIDE: The paper [21] introduces sequences of discriminants displaying, well, creep, but producing regulators just of size $O(n)$. Those discriminants are not "polynomially parametrised". Given the wager provoking [21], we long ago dismissed these sequences of discriminants as "merely *beepers*"

4 Ideal Multiplication

Now consider the sequence of polynomials

$$\begin{aligned} D_n(X) &= \big(qrX^n + (mX^k - l)/q)\big)^2 + 4lrX^n \\ &= \big(qrX^n - (mX^k - l)/q)\big)^2 + 4mrX^{n+k} \end{aligned} \tag{3}$$

obtained from the numbers D_n by replacing all explicit and implicit occurrences of the integer x by X; note here that the parameters q, r, l and m may be functions of x. Set $S = qrX^n + (mX^k - l)/q$ and $S' = qrX^n - (mX^k - l)/q$ and write $Y^2 = D_n(X)$. Plainly, the $\mathbb{Z}$-modules $\mathfrak{a} = \langle 4lrX^n, Y + S\rangle$ and $\mathfrak{a}' = \big\langle 4mrX^{n+k}, Y + S'\big\rangle$ are principal ideals of the order $\mathbb{Q}[X, Y]$. First, we write as if all of q, r, l and m

†We readily resisted a momentary urge to name the relevant polynomials "peepers".

are units of $\mathbb{Q}[X]$, in particular as if $4lrX^n$ is a common divisor of $4mrX^{n+k}$ and of $2qrX^n$. Then it makes sense to allege that $\mathfrak{b} := \mathfrak{a}\mathfrak{a}' = \langle (m/l)X^k, Y+S' \rangle$. So

$$\mathfrak{b}^j = \langle (m^j/l^j)X^{kj}, Y+S' \rangle \quad \text{for } j = 0,\, 1,\, \ldots,\, n_1 = \lfloor n/k \rfloor ,$$

and, by taking $\mathfrak{a}\mathfrak{b} = \langle 4mrX^{n-k}, Y+S \rangle$,

$$\mathfrak{a}\mathfrak{b}^j = \langle 4(m^j/l^{j-1})rX^{jk-n}, Y+S' \rangle ; \quad \text{for } j = n_1+1,\, n_1+2,\, \ldots,\, n_2 = \lfloor 2n/k \rfloor ;$$

and so on. In general, where $\hat{\imath} = 0$ if i is even, and $\hat{\imath} = 1$ if i is odd, we have

$$\mathfrak{a}^i\mathfrak{b}^j = \langle 4(m^j/l^{j-i})r^{\hat{\imath}}X^{jk-in}, Y+S' \rangle ; \quad \text{for } j = n_i+1,\, \ldots,\, n_{i+1} = \lfloor (i+1)n/k \rfloor .$$

For $i = k-1$, take j only up to $n_k - 1$ and then multiply by $\mathfrak{a}\mathfrak{b}$. Specifically, we see that

$$\mathfrak{a}^k\mathfrak{b}^n = \left\langle 4(m^n/l^{n-k})r^{\hat{k}}, Y+S' \right\rangle , \tag{4}$$

showing that the order $\mathbb{Q}[X,Y]$ contains a non-trivial unit.

The quantity $(Y+S)^{n+k}(Y+S')^n$ has norm $4^{2n+k}l^{n+k}m^nr^{2n+k}X^{2n(n+k)}$, so since not both n and k can be even we had better consider

$$U_n = (Y+S)^{2(n+k)}(Y+S')^{2n}/4^{(2n+k)}l^{n+k}m^nr^{2n+k}X^{2n(n+k)} .$$

Of course it is implicit in the ideal multiplications above that $X^n \big| (Y+S)(Y+S')$, and that $X^{n+k} \big| (Y+S)^2(Y+S')$, and so on, so U is indeed a unit of $\mathbb{Q}[X,Y]$. Just so, the condition $r \big| (mx^k - l)/q$ is all of $r \big| S$, $r \big| S'$, and $r \big| Y^2$. It follows that if $m \big| S'$, and if also $l \big| S$, and if there is no inappropriate duplication of factors (see §§4.5 on page 8), then U also is integral at all divisors of m and of l.

Finally, we specialise X back to a suitable integer x. One now acknowledges, given a discriminant $D = D_n(x)$, one ought to expand either $\omega = \sqrt{D}/2$ if $4 \big| D$, or $\omega = (1+\sqrt{D})/2$ if $D \equiv 1 \pmod 4$. Accordingly, let $t = \omega + \overline{\omega}$, and set $s = (S-t)/2$, $s' = (S'-t)/2$. Then

$$u_n = (\omega+s)^{2(n+k)}(\omega+s')^{2n}/l^{n+k}m^nr^{2n+k}x^{2n(n+k)} \tag{5}$$

is a unit of the quadratic order $\mathbb{Z}[\omega]$. By the construction, it is the fundamental unit unless $l = m = 1$ and k is even, or $l = m = r = 1$, in which cases it is the square of the fundamental unit.

Examples. One might wonder whether the possibility that some of q, r, l and m be functions of x is spurious. It is not, though for any fixed x one can of course always write a kreeper with q, r, l, and m in $\mathbb{Z}$. With $\omega_n = (\sqrt{D_n}+1)/2$ if x is even and $\sqrt{D_n}/2$ if x is odd, and

$$D_n(x) = \big((x-1)x^{2n+1} + x^n - 1\big)^2 + 4(x-1)x^{2n+1}, \tag{6}$$

one finds $\ell p(\omega_n) = 5m+2$ if $n = 2m$ is even, and $\ell p(\omega_n) = 5n+3$ if n is odd. Note that here "n" has been replaced by $2n+1$ and is always odd, and $k = n$.

A less transparent such example is given by

$$D_n(y) = \big(y^{2b+2} + (y^2+1)y^b - 1\big)^2 + 4y^b , \tag{7}$$

where in fact $r = y^b + 1$, $l = -1$, $m = q = 1$, $x^k = y^b$, $x^n = y^{b+2}$.

4.1 Composition. Multiplication of ideals $\mathfrak{c} = \langle Q, \omega + P \rangle$, $\mathfrak{c}' = \langle Q', \omega + P' \rangle$ presented as $\mathbb{Z}$-modules is just composition [23] of the corresponding quadratic forms, and yields a product $G \langle q, \omega + p \rangle$. Here $G = \gcd(Q, Q', P + P' + t)$, where $t = \omega + \overline{\omega}$, $q = QQ'/G^2$, and $(p - P)(p - P') \equiv (\omega + p)(\overline{\omega} + p) \pmod{QQ'/G}$; the last condition entails both $p \equiv P \pmod{Q/G}$ and $p \equiv P' \pmod{Q'/G}$. We must note that an ideal multiplication $\mathfrak{c} \cdot \mathfrak{c}'$ yields not $\mathfrak{c}\mathfrak{c}'$, but $G\mathfrak{c}\mathfrak{c}'$, where G is the common factor actually removed in the ideal multiplication.

Finding the relevant G for the product $\mathfrak{a}^{2(n+k)}\mathfrak{a}'^{2n} = \mathfrak{a}^{2k}\mathfrak{b}^{2n}$ is a matter of accumulating the factors G used in the steps detailed above. For example, each construction of $\mathfrak{b}$ produces $G = 4lrX^n$. The k multiplications by $\mathfrak{a}$ together produce $G = 2^{k-1}r^{\lceil (k-1)/2 \rceil}X^{kn}$.

Thus the relevant G for $\mathfrak{a}^{2(n+k)}\mathfrak{a}'^{2n}$ is $(2^{k-1}r^{\lceil (k-1)/2 \rceil}X^{nk})^2 \cdot (4lrX^n)^{2n}$, and so the unit U_n is

$$(Y + S)^{2(n+k)}(Y + S')^{2n}/G \cdot 4(m^n/l^{n-k})r^{\hat{k}}, \tag{8}$$

precisely as we guessed above.

4.2 Formal Continued Fraction Expansion. We all know that a continued fraction expansion $\alpha = [\, a_0 \,, a_1 \,, \ldots \,, a_h \,, \alpha_{h+1} \,]$ is defined inductively by

$$[\, a_0 \,, a_1 \,, \ldots \,, a_h \,, \alpha_{h+1} \,] = a_0 + 1/[\, a_1 \,, \ldots \,, a_h \,, \alpha_{h+1} \,] \quad \text{and} \quad [\quad] = \infty\,; \tag{9}$$

and that induction on the number of matrices readily shows that the products

$$\begin{pmatrix} a_0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 0 & 1 \end{pmatrix}\cdots\begin{pmatrix} a_h & 1 \\ 0 & 1 \end{pmatrix} =: \begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix} \tag{10}$$

entail $[\, a_0 \,, a_1 \,, a_2 \,, \ldots \,, a_h \,] = x_h/y_h$, displaying a useful correspondence between certain matrix products and continued fraction expansions. A matrix inversion now leads one to notice that

$$\alpha_{h+1} = -\frac{y_{h-1}\alpha - x_{h-1}}{y_h\alpha - x_h},$$

from which it follows that

$$\alpha_1\alpha_2\cdots\alpha_{h+1} = (-1)^h(x_h - y_h\alpha)^{-1}\,. \tag{11}$$

In particular, the expansion of an irrational quadratic integer $\omega = \omega_0$ is given by a sequence of lines, of which the h-th is

$$\omega_h := (\omega + P_h)/Q_h = a_h - (\overline{\omega} + P_{h+1})/Q_h\,. \tag{line h}$$

Here, the next *complete quotient* ω_{h+1} of course is the reciprocal of the preceding *remainder* $-(\overline{\omega} + P_{h+1})/Q_h$. Plainly

$$P_h + P_{h+1} + (\omega + \overline{\omega}\,) = a_hQ_h \text{ and } \omega\overline{\omega} + (\omega + \overline{\omega})P_{h+1} + P_{h+1}^2 = -Q_hQ_{h+1}\,. \tag{12}$$

It thus follows from (11), by taking norms, that

$$(x_h - y_h\omega)(x_h - y_h\overline{\omega}) = (-1)^{h+1}Q_{h+1}\,. \tag{13}$$

All these, and many similar well known remarks are formal identities in the variables α and a_0, a_1, a_2, ... *They do not rely on the rules, if any, whereby the partial quotients have been selected.* Many classical results are considerably simplified if they allow for a "more sympathetic" notion of partial quotient than the usual "admissible" partial quotient. Our ideal multiplication relies on the principle just enunciated.

4.3 "Numberising" a Function Field Expansion. In particular, it is quite straightforward sequentially to cleanse an expansion from its nonintegral partial quotients; negative partial quotients are even less of an issue [22, §3, page 362].

Hilfsatz *Set* $a/c = [\,a_0\,,\,w\,]$ *where* $a_0 = \lfloor a/c \rfloor$, *and* $w := a_1\,,\,\ldots\,,\,a_h$. *Then*

$$a/c + \gamma = [\,a_0\,,\,w\,,\,(-1)^h/c^2\gamma - d/c\,] \quad \textit{where } ad \equiv (-1)^{h+1} \mod c\,.$$

Proof By the matrix correspondence we should study

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} (-1)^h/c^2\gamma - d/c & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} (-1)^h a/c^2\gamma - ad/c + b & a \\ (-1)^h/c\gamma & c \end{pmatrix};$$

and so

$$\big((-1)^h a/c^2\gamma - ad/c + b\big)/\big((-1)^h/c\gamma\big) = a/c - (-1)^h\gamma(ad - bc) = a/c + \gamma\,,$$

because $ad - bc = (-1)^{h+1}$. □

This is essentially Mendès France's "Folding Lemma" [15], [24]. Note that one may choose admissible integers b, d, and hence the word w, in two ways so as to make $n = |w|$ odd, or even, at will. One applies the Hilfsatz to the general kreeper (2) commencing as follows.

Set $2\alpha = Y + S$, or $\alpha =: (\omega + s)$; similarly $2\alpha' = Y + S'$, or $\alpha' =: (\omega + s')$. It seems helpful to write $\beta = \overline{\alpha}$ and $\beta' = \overline{\alpha}'$. We note here that $\alpha\beta = -lrx^n$, and $\alpha'\beta' = -mrx^n$. Then the expansion of ω commences

$$\omega = [\,s\,,\,\alpha/lrx^n\,] = [\,s\,,\,q/l - \beta'/lrx^n\,] = [\,s\,,\,a_0(q/l)\,,\,w(q/l)\,,\,\ldots\,]$$

with next complete quotient

$$-lrx^n/l^2\beta' - d/l = (\alpha' - dmx^k)/lmx^k = (qrx^n - dmx^k)/lmx^k - \beta/lmx^k\,.$$

However, $l\big|(qrx^n - dmx^k)$ because $l\big|S$. Thus, here the fraction "a/c" has no l in its denominator; rather, $c = m$. Hence, by the Hilfsatz, we next have the expansion of $\big((qrx^{n-k} - dm)/l\big)/m$, followed by a complete quotient . . . and, well (on the wise advice of the referee) so on . . . . The main thing is that one "rediscovers" the conditions for creep precisely as those necessary to produce the miracles essential to continue happily.

4.4 The Number of Partial Quotients. Had we shown more example steps in the expansion of (2) we could have seen pretty well all that goes on. In summary, $2n$ applications of the Hilfsatz provide a complete quotient without an x in its denominator; compare the n ideal multiplications on page 4.

Moreover, each application of the Hilfsatz, such as those above, yields the expansion of some rational. The lengths of those expansions depends on n at most by way of x^n modulo m, l, and qr. Plainly there are congruence classes of integers x for which $\ell p(\omega)$ increases linearly with n. The whole thing is no more than a mildly complicated generalisation of the example $D_n(x) = (x^n + x - 1) + 4x^n$; $\omega_n = (\sqrt{D}_n + 1)/2$:

$$\omega_n = [\,\tfrac12(x^n + x)\,,\,\overline{1\,,\,x^{n-1}\,,\,x\,,\,x^{n-2}\,,\,x^2\,,\,\ldots\,,\,x\,,\,x^{n-1}\,,\,1\,,\,x^n + x - 1}\,] =$$

$$[\,\tfrac12(x^n + x + 2)\,,\,\overline{-x^{n-1} - 1\,,\,-x\,,\,-x^{n-2}\,,\,-x^2\,,\,\ldots\,,\,-x\,,\,-x^{n-1} - 1\,,\,x^n + x + 1}\,].$$

Here, we see that $\ell p(\omega_n) = 2n + 1$ when $q = r = m = l = 1$. However, the function field expansion of $\sqrt{D_n(X)}$ has period length $2n - 1$ because constant partial quotients are now inadmissible. Nyberg [18] almost knew it all.

4.5 Inappropriate Duplication of Factors. Mind you, it's not quite as straightforward as our summary may suggest. For example, we do not check that the various "a/c" are in lowest terms; they will not be if certain pairs of the parameters x, q, r, l, and m have common factors. We remove this problem by factoring appropriate squares out of D. A cost is that the parameters become rationals, complicating one's description of the expansion[‡], though not in fact the expansion itself.

Example. Take $q=2$, $r=509$, $x=1319011$, $m=3^2\cdot 11$, $l=5^2\cdot 7$, and restrict n to $n\equiv 4 \pmod{30}$. Here l, and m, divide $D_n(x)$ but $l\nmid S$, $m\nmid S'$. We do get kreep, but very messily: $15\ell p(\omega_n)=862n-478$. If $n\equiv 9$, or $21 \pmod{30}$, we get respectively $3\ell p(\omega_n)=392n-168$, or $3\ell p(\omega_n)=392n-144$.

If, however, we start from discriminant $D_n'=D_n/3^2\cdot 5^2$ then we get $\ell p(\omega_n')=16n-6$ for all n; but we are left to multiply the continued fraction expansion by 15. The annoying surprise is that D_n' yields a more simple period than does D_n.

Multiplying the continued fraction expansion of ω by f becomes a matter of finding the units of the order $\mathbb{Z}[f\omega]$ instead of the fundamental unit u of $\mathbb{Z}[\omega]$. Happily, there is a suitable power $\psi(f)$ of u so that $u^{\psi(f)}$ is a unit in $\mathbb{Z}[f\omega]$; a description of ψ is given at [32, p327].

Raney [26] explains how one multiplies a continued fraction expansion by an integer. We suggest that, for x^n fixed modulo f, the incantation "finite state transducer" suffices to prove that if the sequence (ω_n) creeps, then so does $(f\omega_n)$.

In the function field case, however, even if the order $\mathbb{Q}[X,Y]$ contains non-trivial units, the occurrence of such units in some other order $\mathbb{Q}[X,f(X)Y]$ remains happenstance and cannot be guaranteed as in the number field case.

4.6 Numberising the Quadratic Case. Set $Y^2=a^2X^2+2bX+c$, with $\Delta=b^2-a^2c\neq 0$. Then $Y=[\,aX+b/a\,,\overline{2a(a^2X+b)/(b^2-a^2c)\,,\,2(aX+b/a)}\,]$ displays the function field continued fraction expansion of $Y(X)$. Now presume that a, b, c are rational integers, and let x be a positive integer large enough so that $y=Y(x)$ is positive and not a square. Our remarks suppose we are in the "general case" (for example, that a and b have no common factor). The numerical continued fraction expansion begins $y=[\,ax+b/a+(y-ax-b/a)\,]$. By the Hilfsatz, this yields a continued fraction expansion of the rational $ax+b/a$ with next complete quotient

$$(-1)^{n+1}\big((ay+a^2x+b)/a\Delta-d/a\big)\quad\text{where } bd\equiv 1 \pmod{a},\ 0<d<a.$$

For convenience of exposition we choose n odd. Thus we have

$$\big(2(a^2x+b)-d\Delta\big)/a\Delta+\big(ay-(a^2x+b)\big)/a\Delta$$

waiting to be helped by the Hilfsatz. Suppose first that $\Delta\big|2(a^2x+b)$ so that the true denominator is just a divisor of a; suppose it is a. Then our next partial quotients are the expansion of $\big(2(a^2x+b)-d\Delta\big)/a\Delta$ and, again having taken n odd, the next complete quotient is $(y+ax+b/a)-d'/a$ where $\big(2(a^2x+b)-d\Delta\big)d'\equiv\Delta \pmod{a\Delta}$.

For example,

$$y=\sqrt{9x^2+16x+7}=3x+8/3+\big(y-(3x+8/3)\big)$$

[‡] One has to wave one's arms noticeably more excitedly.

so, note that $\Delta = 1$ always implies that $b^2 \equiv 1$, hence $d \equiv b \pmod{a}$,

$$y = [\,3x+2\,,\,1\,,\,1\,,\,1\,,\,y+3x+8/3-2/3\,]$$
$$= [\,3x+2\,,\,1\,,\,1\,,\,1\,,\,y+3x+2\,] = [\,3x+2\,,\,\overline{1\,,\,1\,,\,1\,,\,2(3x+2)}\,].$$

In fact, one can check that if $\gcd(a, 2b, c) = 1$ then, given $\Delta \big| 2(a^2x+b)$, always $d' \equiv b$, so that at most two applications of the Hilfsatz yield the period.

If, however, $\Delta \not| \, 2(a^2x+b)$ then the process explodes unpleasantly and, of course unless one specifies the generic integer x, the numberised expansion is not periodic. The bottom line is Schinzel's result [27, I].

Theorem (Schinzel) *Set $\Delta = b^2 - a^2c$. The quadratic $a^2X^2 + 2bX + c$ is a sleeper if and only if $\Delta \big| 2\gcd(a^2, b)$.*

5 Hyperelliptic Curves

On the one hand, ideal multiplication is composition, and such composition allows one to jump through a continued fraction expansion in multiple steps [29, 12]. On the other hand, composition is well known, see [5] and [11] for explanations for the innocent, to be addition on the Jacobian of the curve $\mathcal{C} : Y^2 = D(X)$. A very explicit illustration of this phenomenon is given by Adams and Razar [1], reminding one that periodicity is equivalent to the divisor at infinity being a torsion divisor. So a curve $\mathcal{C}$ has a nontrivial unit in its function field if and only if the divisor at infinity on $\mathrm{Jac}(\mathcal{C})$ is torsion of order the degree of the fundamental unit, thus the regulator, of the quadratic order $\mathbb{Q}[X, Y]$. For example, the kreepers of §4 provide a family $Y_n^2 = D_n(X)$ of curves which, when q, r, l, and m are constants, have torsion divisor at infinity of order n^2.

Accordingly we studied the "torsion literature" with a view to finding new examples of creepers. Patterson had an immediate success with Elkies' curve [7]

$$\mathcal{C} : Y^2 = X^6 + 4X^4 + 10X^3 + 4X^2 - 4X + 1 \tag{14}$$

which has regulator 39. Indeed, $\mathcal{C}$ achieves that feat because $Y^2 = S_i^2 + 4R_i$ with

$$\begin{aligned} S_1 &= (X^3+2X+5) & A_1 &= -6(X+1) \\ S_2 &= (X^3+2X+1) & A_2 &= -2X(X-1)(X+1) \\ S_3 &= (X^3-4X-1)^2 & A_3 &= 3(X-1)(X+1)^2 \\ S_4 &= (X^3-2X-3) & A_4 &= 2(X-1)(X+1)^3\,, \end{aligned}$$

and $X(X-1)(X+1)\big|(S_2+S_3)$; $X+1\big|(S_1+S_2)$; $(X+1)^2\big|(S_3+S_4)$.

Now set $Y_n^2 = D_n(X) := X^{2n} + 4X^{n+1} + 10X^n + 4X^2 - 4X + 1$. Remarkably, with $x = 3$ one finds, if $n \equiv 0 \pmod 4$, that

$$\ell p\big(\sqrt{D_n(3)}\big) = 22(n-1).$$

Note that we have a kreeper ($x = 3$, $m = r = q = k = 1$, $l = 8$, $x^4 \equiv 1 \mod l$). Conversely, while the existence of the four expressions $Y^2 = S_i^2 + 4R_i$ providing "nice composition" is no more than a happy accident, their detection by Elkies is with intent. It is precisely such "accidents" that yield hyperelliptic curves with fairly high torsion. Just so then, one might well expect to find creepers in like manner.

All elliptic curves over $\mathbb{Q}$ with nontrivial torsion are known, see [25] and its references. Moreover, Patterson [19] has shown they may be rediscovered by the methods of Elkies, Flynn, Leprévost *et al*, see [6] for references. These methods appear inexorably to produce creepers, mostly kreepers, as described above. Indeed, we first realised that the "constants" q, r, l, m could of course depend on x because Flynn's example $Y^2=\big(A^{(g)}(X)\big)^2-tX^g(X-1)^g$, [6, p. 87], boils down to

$$Y^2=((X-1)X^g+(X-1))^2+4(X-1)X^g \quad g=1,\ 2,\ \dots,$$

displaying a family of hyperelliptic curves of genus g and torsion order $2g^2+2g+1$.

As example, [25], the elliptic curves with torsion 5 are given by

$$Y^2=\big(X^2-(t^2-6t+1)\big)^2+32t\big(X-(t-1)\big),$$

$t\in\mathbb{Q}\setminus\{0\}$. The replacement, $X\leftarrow X^n$ and a choice of t so as to yield a "helpful collection" of equations $Y^2=S_i^2+4R_i$, can lead to

$$(X-1)^2Y_n^2=\big((X-1)X^{2n}-X^{n+1}-1\big)^2-4X^n(X^n-1)\,. \tag{15}$$

We have here sidestepped an interesting trap for young players. In the number field case it would not have been critical to divide by $(x-1)^2$. In the function field case, however, the continuing presence of a "redundant" factor can be so damaging as to destroy periodicity of the continued fraction expansion. Indeed, the order $\mathbb{Q}[X,(X-1)Y_n]$ has a nontrivial unit only for $n=1$, 2, and 3. But (15) is more interesting than just that. Surprisingly, $\ell p(Y_n)=6$, and is independent of n. So (15) is an instance, probably the first ever noticed, of a nontrivial sequence of function field sleepers.

The tricks used above are not special to the previous example. Just so, from [25] one sees that its elliptic curves with torsion 7 become

$$Y^2=\big(X^2+(t^2-t-1)X+t^2(t-1)\big)^2+4t^2(t-1)X \tag{16}$$

after a helpful translation and dilation. Again, replacing X by X^n and selecting t so as to arrange that ideals "compose nicely" suffices for creep. The only viable selection of t as function of X turns out to be $t=X^m$ with $m\big|n$. Also, for example, $X=t=2$ does not yield a kreeper, but leads to the creeper

$$D_n=(2^2\,2^{2n}+2^n+1)^2+4\cdot 2^n\,,$$

with $\ell p(\omega_n)=7n-13$ if n is even, while $\ell p(\omega_n)=2(7n-13)$ if n is odd. The very similar creeper arising from the torsion 5 case,

$$D=(2\cdot 2^{2n}+2^n+1)^2+4\cdot 2^n,$$

has $\ell p(\omega_n)=4n+1$ if n is even, and $\ell p(\omega_n)=8n+2$ if n is odd.

Taking $t=X$ in (16), above, gives a curve $Y^2=S_i^2+4T_i$ where

$$\begin{aligned}
S_1&=X^{2n+2}+(X^2-X-1)X^n+(X-1) &\qquad T_1&=(X-1)X^n\\
S_2&=X^{2n+2}+(X^2-X-1)X^n-(X-1) &\qquad T_2&=(X-1)X^{n+1}J_n\\
S_3&=X^{2n+2}+(X^2-3X+1)X^n-(X-1) &\qquad T_3&=(X-1)X^nJ_n^2
\end{aligned}$$

with $J_n=X^{n+1}+X-1$. The three principal ideals $\mathfrak{a}_i=\langle T_i\,,\omega+(S_i-t)/2\rangle$ suffice to find a principal ideal of norm X^g. It seems congenial to look at $\mathfrak{a}_1\mathfrak{a}_2$, then $\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$, next $\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3\mathfrak{a}_2$. Whatever, this case is interesting because it appears to rely on three, not two, ideals to generate a unit. Because $J_n\not\big| D_n$ this example cannot be a kreeper. In this example $\ell p(Y_n)=12n$ and the regulator $R(Y_n)$ of the order $\mathbb{Q}[X,Y_n]$ is $7n^2+9n+3$. When we numberise we find $\ell p(\omega_n)=14n+2$.

The families of elliptic curves with torsion 10, respectively 12 never satisfy the Schinzel condition [25, p. 400]. It is therefore no surprise that the family with torsion 10 appear to give rise only to two "isolated" creepers

$$(2^{2n+3} - 5 \cdot 2^n + 3)^2 - 12 \cdot 2^n \quad \text{and} \quad \bigl(3^{2n+3} - 31 \cdot 3^n + 10\bigr)^2 + 40 \cdot 3^n\,.$$

6 Concluding Remarks

The information we report is a selection from more extensive but still sporadic data collected by Patterson. That "experimental" data lends support to the suggestion that families of hyperelliptic curves with genus g increasing in arithmetic progression have a divisor at infinity of torsion order at most $O(g^2)$. Conversely, since there was already a suggestion to this effect ambient in the torsion literature, one may take that as justifying our implied assertion that there are no jeepers — see their "definition" on page 4.

Of course our data has only little to say about the maximum torsion one might expect to find on a hyperelliptic curve of genus g. All our examples may well be atypical in that many of their partial quotients are of degree greater than one whereas generically — and that includes our algebraic functions — all but the zero-th partial quotient of a power series in $\mathbb{Q}((X^{-1}))$ should be expected to be of degree one; see [22] for a discussion. Mind you, periodicity is itself atypical in that it is equivalent to the occurrence of a later partial quotient of degree $g+1$. Elkies [7] suggests that the continued fraction expansion of the square root of a sextic has at most five partial quotients of degree 2, unless it is periodic — in which case there is one example with six such partial quotients, to wit $\mathcal{C}$ of (14) on page 9.

Concluding Aside: The thesis [19], and papers with Hugh Williams, will eventually flesh out the remarks made in the preceding pages.

References

[1] William W. Adams and Michael J. Razar, 'Multiples of points on elliptic curves and continued fractions', *Proc. London Math. Soc.* **41** (1980), 481–498.

[2] T. Azuhata, 'On the fundamental units and the class numbers of real quadratic fields II', *Tokyo J. Math.* **10** (1987), 259–270

[3] L. Bernstein, 'Fundamental units and cycles in the period of real quadratic number fields II', *Pacific J. Math.* **63** (1976), 63–78.

[4] T. G. Berry, 'On periodicity of continued fractions in hyperelliptic function fields', *Arch. Math.* **55** (1990), 259–266.

[5] D.G. Cantor, 'Computing in the Jacobian of a hyperelliptic curve', *Math. Comp.* **48**.177 (1987), 95–101.

[6] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, 230. Cambridge University Press, Cambridge, 1996. xiv+219 pp.

[7] Noam Elkies, e-mail, January, 2001. See the item "genus-2 Jacobians with rational torsion points of high order" at http://www.math.harvard.edu/~elkies/compnt.html.

[8] F. Halter-Koch, 'Einige periodische Kettenbruchentwicklungen und Grundeinheiten', *Abh. Math. Sem. Univ. Hamburg* **59** (1989), 157–169; and 'Reel-quadratischer Zahlkörper mit grosser Grundeinheit', *ibid.*, 171–181

[9] M. D. Hendy, 'Applications of a continued fraction algorithm to some class number problems', *Math. Comp.* **28** (1974), 267–277.

[10] Irving Kaplansky, 'A memo on creepers', letter to R. A. Mollin, H. C. Williams, and K. S. Williams, 23 November, 1998.

[11] Kristin E. Lauter, 'The equivalence of the geometric and algebraic group laws for Jacobians of genus 2 curves', to appear in Proceedings of the conferences in memory of Ruth Michler, AMS *Contemporary Mathematics* Series.

[12] H. W. Lenstra Jr., 'On the calculation of regulators and class numbers of quadratic fields', in J. V. Armitage ed., '*Journées Arithmétiques 1980*' LMS Lecture Notes **56**, Cambridge 1982, 123–151.

[13] C. Lévesque, 'Continued fraction expansions and fundamental units', *J. Math. Phys. Sci.* **22** (1988), 11–14.

[14] C. Lévesque and G. Rhin, 'A few classes of periodic continued fractions', *Utilitas Math.* **30** (1986), 79–107.

[15] Michel Mendès France, 'Sur les fractions continues limitées', *Acta Arith.* **23** (1973), 207–215.

[16] R. A. Mollin and H. C. Williams, 'Consecutive powers in continued fractions', *Acta Arith.* **51** (1992), 233–264

[17] R. A. Mollin and H. C. Williams, 'On the period length of some special continued fractions', *Séminaire de Théorie des Nombres de Bordeaux* **4**.1 (1992), 19–42.

[18] M. Nyberg, 'Culminating and almost culminating continued fractions', *Norks. Mat. Tidskr.* **31** (1949), 95–99.

[19] Roger D. Patterson, PhD Thesis, Macquarie University, Sydney, 2003.

[20] A. J. van der Poorten, 'Explicit formulas for units in certain quadratic number fields', in *Algorithmic Number Theory* (1st Algorithmic Number Theory Symposium — Cornell University, May 6–9, 1994), Lecture Notes in Computer Science 887, Springer-Verlag 1994, 194–208.

[21] ———, 'Beer and continued fractions with periodic period', in *Number Theory : Fifth Conference of the Canadian Number Theory Association*, K. S. Williams and R. Gupta eds., CRM Proceedings and Lecture Notes (Centre de Recherches Mathématiques, Montreal) **19** (1999), 309–314.

[22] ———, 'Formal power series and their continued fraction expansion', in Joe Buhler ed., *Algorithmic Number Theory* (Proc. Third International Symposium, ANTS-III, Portland, Oregon, June 1998), Springer Lecture Notes in Computer Science **1423** (1998), 358–371.

[23] Alfred J. van der Poorten, 'A note on NUCOMP', *Math. Comp.*, **72**.244 (2003), 1935–1946.

[24] ———, 'Symmetry and Folding' (dedicated to Michel Mendès France on his 65th birthday), *Jour. Théorie des Nombres de Bordeaux*, **14**.2 (2002), 603–611.

[25] Alfred J. van der Poorten and Xuan Chuong Tran, 'Periodic continued fractions in elliptic function fields', in Claus Fieker and David R. Kohel eds, *Algorithmic Number Theory* (Proc. Fifth International Symposium, ANTS-V, Sydney, NSW, Australia July 2002), Springer Lecture Notes in Computer Science 2369 (2002), 390–404.

[26] G. N. Raney, 'On continued fractions and finite automata', *Math. Ann.* **206** (1973), 265–283.

[27] A. Schinzel, 'On some problems of the arithmetical theory of continued fractions', *Acta Arith.* **6** (1961), 393–413; and 'II' *ibid.* (1962), 287–298.

[28] D. Shanks, 'On Gauss's class number problems', *Math. Comp.* **23** (1969), 151–163.

[29] D. Shanks, 'Class number, a theory of factorization, and genera', in *Proc. Symp. Pure Math.* **20** (1969 Institute on Number Theory), Amer. Math. Soc., Providence 1971, 415–440; and 'The infrastructure of a real quadratic field and its applications', *Proc. Number Theory Conference, Boulder, 1972*.

[30] H. C. Williams, 'A note on the period length of the continued fraction expansion of certain $\sqrt{D}$', *Utilitas Math.* **28** (1985), 201–209.

[31] H. C. Williams, 'Some generalizations of the S_n sequence of Shanks', *Acta Arith.*, **69**.3 (1995), 199–215.

[32] H. C. Williams, 'Solving the Pell equation', in *Number theory for the millennium III*, edited by Bennett, M.A.; Berndt, B.C.; Boston, N.; Diamond, H.G.; Hildebrand, A.J.; and Philipp, W.; Proceedings of the millennial conference on number theory, Urbana-Champaign, IL, USA, May 21–26, 2000. (English) Natick, MA: A K Peters. (2002), 397–435 = *Surveys in Number Theory*, same details, 325–363.

[33] Y. Yamomoto, 'Real quadratic number fields with large fundamental units', *Osaka J. Math.* **8** (1971), 261–270.