Hardy-Ramanujan Journal
Vol. 6 (1983) 23 — 36

THE GREATEST SQUARE FREE FACTOR OF A BINARY RECURSIVE SEQUENCE

By T. N. SHOREY

§ 1. For any sequence of integers $u_0, u_1, \ldots, u_m, \ldots$ satisfying

$$u_m = r\,u_{m-1} + s\,u_{m-2},\ m = 2, 3, \ldots$$

where r and s are rational integers with $r^2 + 4s \neq 0$, we have

$$(1) \qquad u_m = a\alpha^m + b\beta^m,\ m = 0, 1, 2, \ldots$$

where α and β are roots of the polynomial $X^2 - rX - s$ and

$$(2) \qquad a = \frac{u_0\beta - u_1}{\beta - \alpha},\ b = \frac{u_1 - u_0\alpha}{\beta - \alpha}.$$

The polynomial $X^2 - rX - s$ is called the polynomial associated to the sequence $\{u_m\}$. The sequence $\{u_m\}$ is said to be a non-degenerate binary recursive sequence if a, b, α, β are non-zero and α/β is not a root of unity. For a rational integer x with $|x| > 1$, denote by P(x) the greatest prime factor of x and by Q(x) the greatest square free factor of x. If $p_1, \ldots, p_r$ are all the distinct primes dividing x, then $Q(x) = p_1 \ldots p_r$. For non-zero rational integers x and y, denote by [x, y] and (x, y), respectively, the least common multiple and the greatest common divisor of x and y. Further we define $P(1) = P(-1) = 1$ and

$$P\left(\frac{x}{y}\right) = P\left(\frac{x}{(x, y)}\,\frac{y}{(x, y)}\right) = P\left(\frac{[x, y]}{(x, y)}\right)$$

and

$$Q\left(\frac{x}{y}\right) = Q\left(\frac{[x, y]}{(x, y)}\right)$$

Let $\{u_m\}$ be a non-degenerate binary recursive sequence given by (1). Stewart [4] proved that

$$Q(u_m) > C\left(\frac{m}{((\log m)^2}\right)^{1/d}, m > C',$$

where $d = [Q(\alpha) : Q]$ and $C > 0$, $C' > 0$ are effectively computable numbers depending only on a and b. Observe that d = 1 or 2. Further, if $|\alpha| > |\beta|$, Stewart [4] proved that for any θ with $0 < \theta < 1$,

$$Q(u_m) > m^{\theta}, m > C'',$$

where $C'' > 0$ is an effectively computable number depending only on θ and the sequence $\{u_m\}$. We shall generalise and strengthen this result as follows :

Theorem 1

Let $\{u_m\}$ be a non-degenerate binary recursive sequence. There exist effectively computable numbers $C_1 > 0$ and $C_2 > 0$ depending only on the sequence $\{u_m\}$ such that for every $m > C_1$, we have

$$\log Q(u_m) > C_2 (\log m)^2 (\log \log m)^{-1}.$$

The improvement depends on utilising the fact that the contribution from small primes in u_m is small. Stewart [5] proved theorem 1 for the greatest square free factor of the members of Lucas and Lehmer sequences. Further, for Lucas and Lehmer sequences, Stewart [5] proved that for almost all m

$$\log Q(u_m) > (\log m)^{2+\log 2-\varepsilon}, \varepsilon > 0.$$

Theorem 1 is contained in the following result.

Theorem 2

Let $\{u_m\}$ *be a non-degenerate binary recursive sequence. There exist effectively computable numbers* $C_3>0$ *and* $C_4>0$ *depending only on the sequence* $\{u_m\}$ *such that for every pair* m, n *with* $m > n$, $m > C_3$ *and* $u_n \neq 0$, *we have*

$$\log Q(\Delta'_{m,n}) > C_4 (\log m)^2 (\log\log m)^{-1}$$

where

$$\Delta'_{m,n} = [u_m, u_n] / (u_m, u_n).$$

For a non-degenerate binary recursive sequence $\{u_m\}$, observe that the equation $u_m = 0$ implies that m is bounded by an effectively computable number depending only on the sequence $\{u_m\}$. We apply theorem 2 with the least integer n (n is either 0 or 1) such that $u_n \neq 0$ to obtain theorem 1. For estimates on $P(u_m)$ and $P(\Delta'_{m,n})$, we refer to Stewart [4] and the author [3]. See also the next theorem.

Let $\{u_m\}$ and $\{v_m\}$ be non-degenerate binary recursive sequences whose associated polynomials are identically equal. Denote by α and β the roots of their associated polynomial. Then the sequence $\{u_m\}$ is given by (1) and (2). Further for $m = 0, 1, 2, \ldots$, we have

$$v_m = a_1 \alpha^m + b_1 \beta^m$$

where

$$a_1 = \frac{v_0\beta - v_1}{\beta - \alpha}, \quad b_1 = \frac{v_1 - v_0\alpha}{\beta - \alpha}.$$

For m and n with $u_m v_n \neq 0$, put

$$\Delta_{m,n} = [u_m, v_n] / (u_m, v_n).$$

Then theorem 2 is a particular case of the following result.

Theorem 3

Let $A > 0$ *and* $0 < K < (d+1)^{-1}$ *where* $d = [Q(\alpha) : Q]$ *There exist effectively computable numbers* $C_5 > 0$ *and* $C_6 > 0$ *depending only on* A, K, *the sequences* $\{u_m\}$ *and* $\{v_m\}$ *such that for every pair* m, n *with* $m > n$, $m \geq C_5$, $v_n \neq 0$ *and*

$$(3) \qquad \frac{a\,\alpha^m}{a_1\,\alpha^n} \neq \frac{b\,\beta^m}{b_1\,\beta^n},$$

either

$$\log P(\Delta_{m,n}) \geq (\log m)^A$$

or

$$\sum_{\substack{p \mid \Delta_{m,n} \\ p > m^K}} 1 \geq C_6 \frac{\log m}{\log \log m}$$

where p *runs through primes*

For the proof of theorem 2, we may assume $\log P(\Delta'_{m,n}) < (\log m)^2$. Then we apply theorem 3 with $\{u_m\} = \{v_m\}$, $A = 2$ and $K = \frac{1}{4}$ Observe that (3) is satisfied, since α/β is not a root of unity. Now the assertion of theorem 2 follows immediately.

The proof of theorem 3 depends on the theory of linear forms in logarithms. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers Let K be their splitting field over Q. Put $D = [K:Q]$

We denote by $A_1, \dots, A_n$ upper bounds for the heights of $\alpha_1, \dots, \alpha_n$ respectively, where we assume that $A_j > 3$ for $1 \leq j \leq n$. Write

$$\Omega' = \prod_{j=1}^{n-1} \log A_j \ , \ \Omega = \Omega' \log A_n .$$

The proof of theorem 3 depends on the following theorem of Baker [1] on linear forms in logarithms.

Theorem A .

There exist effectively computable absolute constants $C_7 > 0$ *and* $C_8 > 0$ *such that the inequalities*

$$0 < | \alpha_1^{b_1} \dots \alpha_n^{b_n} - 1 | < \exp\left(-(C_7 n D)^{C_8 n} \Omega \log \Omega' \log B\right)$$

have no solution in rational integers $b_1, \dots, b_n$ *with absolute values at most* B (> 2) .

We shall also need a p-adic analogue, due to van der Poorten [2], of theorem A.

Theorem B.

Let $\wp$ *be a prime ideal of* K *lying above a rational prime p. There exist effectively computable absolute constants* $C_9 > 0$ *and* $C_{10} > 0$ *such that the inequalities*

$$\infty > \mathrm{ord}_{\wp}(\alpha_1^{b_1} \dots \alpha_n^{b_n} - 1) > (C_9 \ nD)^{C_{10} n} \frac{p^D}{\log p} \Omega (\log B)^2$$

have no solution in rational integers $b_1, \dots, b_n$ *with absolute values at most* $B(> 2)$.

§ 2. **Proof of theorem 3.**

Let $A > 0$ and $0 < K < (d+1)^{-1}$. Put

(4) $$\tau = K\,(d+1).$$

Observe that $0 < \tau < 1$. Let $\{u_m\}$ and $\{v_m\}$ be as in theroem 3. There is no loss of generality in assuming that $|\alpha| \geq |\beta|$. Then, since α/β is not a root of unity, we find that $|\alpha| > 1$. For algebraic integer $x \in Q(\alpha)$, denote by $[x]$ the ideal generated by x in the ring of integers of $Q(\alpha)$. There exists a positive rational integer k such that

$$([\alpha^2], [\beta^2]) = [k].$$

Put $\alpha_1 = \alpha^2/k$ and $\beta_1 = \beta^2/k$. Then the ideals $[\alpha_1]$ and $[\beta_1]$ are relatively coprime. For $m = 0,1,2,\ldots$, notice that

$$U_m = k^{-m}u_{2m} = a\alpha_1^m + b\beta_1^m,$$

$$U'_m = k^{-m}u_{2m+1} = a\alpha\alpha_1^m + b\beta\beta_1^m,$$

$$V_m = k^{-m}v_{2m} = a_1\alpha_1^m + b_1\beta_1^m,$$

$$V'_m = k^{-m}v_{2m+1} = a_1\alpha\alpha_1^m + b_1\beta\beta_1^m.$$

Observe that the sequences $\{U_m\}$, $\{U'_m\}$, $\{V_m\}$ and $\{V'_m\}$ are non-degenerate binary recursive sequences. By proving the theorem separately for sequences $\{U_m\}$ and $\{V_m\}$, $\{U_m\}$ and $\{V'_m\}$, $\{U'_m\}$ and $\{V_m\}$, $\{U'_m\}$ and $\{V'_m\}$, there is no loss of generality in assuming that $([\alpha], [\beta]) = [1]$.

Denote by $c_1, c_2, \ldots$ effectively computable positive numbers depending only on A, K, the sequences $\{u_m\}$ and

$\{v_m\}$. We may assume that $m > c_1$ with c_1 sufficiently large. Then, since $\{u_m\}$ is non-degenerate, we see that $u_m \neq 0$. Let $0 < n < m$ satisfy $v_n \neq 0$ and suppose that (3) is valid. We suppose

(5) $\log P(\Delta_{m,n}) < (\log m)^A.$

Let $\pi_1, \ldots, \pi_s$ be all the rational primes satisfying $\pi_i | \Delta_{m,n}$ and $\pi_i > m^K$ for $1 \leq i \leq s$. Let $0 < \varepsilon < 1$. We suppose that

(6) $s < \varepsilon (\log m)(\log\log m)^{-1}.$

We shall arrive at a contradiction for a suitable choice of ε depending only on A, K the sequences $\{u_m\}$ and $\{v_m\}$.

We write

(7) $B_1 = \dfrac{u_m}{(u_m, v_n)}, \quad B_2 = \dfrac{v_n}{(u_m, v_n)},$

$\Lambda = (u_m, v_n).$

When

(8) $\dfrac{u_m}{v_n} = \dfrac{B_1}{B_2}$ and $(B_1, B_2) = 1.$

Further

(9) $\Delta_{m,n} = \pm B_1 B_2.$

For a prime p dividing B_1, we see from (7) that

$$\text{ord}_p (B_1) \leq \text{ord}_p (u_m).$$

Let $\wp$ be a prime ideal in the ring of integers of $Q(\alpha)$ dividing p. Then, since the ideals $[\alpha]$ and $[\beta]$ are relatively prime, either $\wp$ does not divide $[\alpha]$ or $\wp$ does not divide $[\beta]$. For simplicity assume that $\wp$ does not divide $[\alpha]$. Then, by (1), we have

$$\operatorname{ord}_p(u_m) < \operatorname{ord}_{\wp}(u_m)$$

$$< c_2 + \operatorname{ord}_{\wp}\left(- \frac{b}{a}\left(\frac{\beta}{\alpha}\right)^m - 1\right).$$

Now we apply theorem B with $n = 2$, $D = d$, $\alpha_1 = -b/a$, $\alpha_2 = \beta/\alpha$, $b_1 = 1$ and $b_2 = m$ to conclude that

$$\operatorname{ord}_{\wp}\left(- \frac{b}{a}\left(\frac{\beta}{\alpha}\right)^m - 1\right)$$

$$< c_3\, p^d (\log p)^{-1} (\log m)^{+2}.$$

Therefore

$$\operatorname{ord}_p (B_1) < c_4\, p^d (\log p)^{-1} (\log m)^2.$$

This inequality follows similarly when $\wp$ does not divide $[\beta]$. Consequently, by (4),

$$\sum_{\substack{p \mid B_1 \\ p < m^K}} \operatorname{ord}_p (B_1) \log p < c_4\, m^{\tau} (\log m)^2.$$

Similarly

$$\sum_{\substack{p \mid B_2 \\ p < m^K}} \operatorname{ord}_p (B_2) \log p < c_5\, m^{\tau} (\log m)^2.$$

Consequently, by (9), we may write

(10) $$B_1 = B_3\, \pi_1^{x_1} \dots \pi_s^{x_s},\ B_2 = B_4\, \pi_1^{y_1} \dots \pi_s^{y_s}$$

where $x_1, \dots, x_s, y_1, \dots, y_s$ are non-negative integers and $B_3, B_4 \in Z$ with

(11) $$\log \max (|B_3|, |B_4|) < c_6 m^{\tau} (\log m)^2.$$

Further we see from (7) that

$$\log \max (| B_1 | , | B_2 |) < c_7 m$$

which, together with (10), implies that

(12) $$\max (x_1, \ldots, x_s, y_1, \ldots, y_s) < c_8 m$$

with $c_8 > 1$.

We have

(13) $$u_m \quad a_1^{-1} a \alpha^{m-n} v_n$$

$$= - b_1 \beta^n (a_1^{-1} a \alpha^{m-n} - b_1^{-1} b \beta^{m-n})$$

and, by (7) and (1),

(14) $$\Lambda B_1 - a\alpha^m = b \beta^m$$

In view of (3), we see that

(15) $$u_m - a_1^{-1} a \alpha^{m-n} v_n \neq 0.$$

Put

$$T = a_1^{-1} a \alpha^{m-n} v_n u_m^{-1} - 1,$$

$$T_1 = a^{-1} \alpha^{-m} \Lambda B_1 - 1.$$

By (15) and (14), notice that

$$TT_1 \neq 0.$$

Further it follows from (8) and (10) that

$$T_1 = a_1^{-1} \alpha^{-m} \pi_1^{x_1} \cdots \pi_s^{x_s} (B_3 \Lambda) - 1$$

$$\text{and } T = \frac{a}{a_1} \alpha^{m-n} \pi_1^{z_1} \cdots \pi_s^{z_s} \frac{B_4}{B_3} - 1$$

where $z_i = y_i - x_i$ for $1 \leq i \leq s$ Now we split the proof of theorem 3 in two cases.

Case I. $| \alpha | > | \beta |$. Dividing both the sides of (13) by u_m, we have

(16) $0 < |T| < c_9^{-n}, \; c_9 > 1.$

We apply theorem A with

$n = s+3 < \varepsilon (\log m)(\log\log m)^{-1} + 3$ by (6),

$D = d < 2$, $\log A_1 = \log A_2 = c_{10}$, $\log A_3 = \ldots =$

$\log A_{n-1} = (\log m)^A$ by (5), $\log A_n = c_6 m^{\tau} (\log m)^2$ by (11)

and $B = c_8 m$ by (12) to conclude that

(17) $|T| > \exp(-m^{\tau + c_{11}\varepsilon} (\log m)^5).$

We shall choose ε to satisfy

(18) $\varepsilon < (1-\tau)/2 c_{11}.$

Put

$$\tau_1 = (1 + \tau)/2.$$

Then, since $0 < \tau < 1$, we find that $\tau < \tau_1 < 1$.

Combining (16), (17) and (18), we have

$$n < c_{12}\, m^{\tau_1} (\log m)^5 .$$

Then

(19) $\log |\Lambda| < \log |v_n| < c_{13} m^{\tau_1} (\log m)^5 .$

Dividing both the sides of (14) by $a\alpha^m$, we have

(20) $0 < |T_1| < c_{14}^{-m}, \; c_{14} > 1.$

We apply theorem A with $n = s+3 < \varepsilon (\log m)(\log\log m)^{-1} + 3$ by (6), $D = d < 2$, $\log A_1 = \log A_2 = c_{15}$, $\log A_3 = \ldots = \log A_{n-1} = (\log m)^A$ by (5), $\log A_n = 2c_{13} m^{\tau_1} (\log m)^5$ by (19), (11) and $B = c_8 m$ by (12) to conclude that

(21) $$|T_1| > \exp\left(-m^{\tau_1 + c_{16}\varepsilon} (\log m)^8\right).$$

Let

$$\varepsilon = \min\left(\frac{1-\tau}{2c_{11}}, \frac{1-\tau_1}{2c_{16}}, \frac{1}{2}\right)$$

Then (18) is satisfied. Put

$$\tau_2 = (1+\tau_1)/2.$$

Observe that $\tau_1 < \tau_2 < 1$. Now we combine (20) and (21) to conclude that

$$m \leqslant c_{17} m^{\tau_2} (\log m)^8$$

which, since $\tau_2 < 1$, implies that $m \leqslant c_{18}$. But this is not possible if $c_1 > c_{18}$.

Case II

$|\alpha| = |\beta|$. Let τ_1 and τ_2 be defined as in case I. Observe that β is not a unit, since α/β is not a root of unity. Therefore there exists a prime ideal $\wp$ in the ring of integers of $Q(\alpha)$ such that $\wp / [\beta]$. Further, since the ideals $[\alpha]$ and $[\beta]$ are relatively coprime, observe that $\wp$ does not divide $[\alpha]$. Consequently $\text{ord}_{\wp}(u_m) \leqslant c_{19}$. Now, by counting the power of prime ideal $\wp$ on both the sides in (13), we have

$$n \leqslant c_{20} + \text{ord}_{\wp}(u_m) + \text{ord}_{\wp}(T) \leqslant c_{21} + \text{ord}_{\wp}(T).$$

We apply theorem B with $p < c_{22}$ and the same parameters as in case I for obtaining a lower bound for $|\Gamma|$ by theorem A. We obtain

$$\mathrm{ord}_{\wp}(T) < m^{\tau + c_{23}\varepsilon} (\log m)^5 .$$

We shall choose ε to satisfy

$$\varepsilon < \frac{1-\tau}{2\, c_{23}} . \tag{22}$$

Then

$$n < c_{24}\, m^{\tau_1} (\log m)^5$$

which implies that

$$\log |\Lambda| < c_{25}\, m^{\tau_1} (\log m)^5 .$$

Counting the power of prime ideal $\wp$ on both the sides in (14), we obtain

$$m < c_{26} + \mathrm{ord}_{\wp}(T_1).$$

We apply theorem B with $p < c_{22}$, $\log A_n = c_{25}\, m^{\tau_1} (\log m)^5$ and the same parameters as in case I for obtaining a lower bound for $|\Gamma_1|$ by theorem A We obtain

$$\mathrm{ord}_{\wp}(T_1) < m^{\tau_1 + c_{27}\varepsilon} (\log m)^8 .$$

Let $$\varepsilon = \min\left(\frac{1-\tau}{2\, c_{23}}, \frac{1-\tau_1}{2\, c_{27}}, \frac{1}{2} \right)$$

Then (22) is satisfied. We obtain

$$m < c_{28}\, m^{\tau_2} (\log m)^8 .$$

Consequently $m < c_{29}$ which is not possible if $c_1 > c_{29}$. This completes the proof of theorem 3.

Remarks

(i) Let $\{ u_m \}$ be a non-degenerate binary recursive sequence. For every pair m, n with $m > n$, $u_m u_n \neq 0$ and $Q(u_m) = Q(u_n)$, we have

$$m - n > c_{30} (\log m)^2 (\log \log m)^{-1}$$

where $c_{30} > 0$ is an effectively computable number depending only on the sequence $\{ u_m \}$. This follows immediately from theorem 1 and the relation (13) with $a_1 = a$, $b_1 = b$.

(ii) Let $P \geqslant 2$ and denote by S the set of all non-zero integers composed of primes not exceeding P. We can apply the argument of proof of theorem 1 to prove that for every $x \in S$, $y \in S$ with $(x,y) = 1$, $|x| > |y|$ and $\log |x| > e^e$,

$$\log Q(x + y) > c_{31} (\log \log |x|)^2 (\log \log \log |x|)^{-1}$$

where $c_{31} > 0$ is an effectively computable number depending only on P.

References

1. **A. Baker,** *The theory of linear forms in logarithms,* Transcendence theory : Advances and applications, A. Baker and D.W, Masser ed., Academic Press, London and New York 1977.

2. **A. J. van der Poorten,** *Linear forms in logarithms in the p-adic case,* Transcendence theory : Advances and applications, A. Baker and Masser ed., Academic Press, London and New York 1977.

3. **T.N. Shorey,** *Linear forms in members of a binary recursive sequence,* Acta. Arith. (to appear).

4. **C.L. Stewart,** *On divisors of terms of Linear recursive sequences,* Jour. reine angew Math 333 (1982), 12–31.

5. **C.L. Stewart,** *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers III,* Jour. London Math. Soc. (to appear).

School of Mathematics

Tata Institute of Fundamental Research

Homi Bhabha Road

Bombay 400 005

India.