SECOND-ORDER LINEAR RECURRENCES OF COMPOSITE NUMBERS

Anatoly S. Izotov

Mining Institute, Novosibirsk, Russia

e-mail: izotov@nskes.ru

(Submitted May 2000-Final Revision July 2001)

In [3], W. Sierpinski proved that there are infinitely many odd integers k (Sierpinski numbers) such that $k2^n+1$ is a composite number for all $n \ge 0$, i.e., he found that the recurrence $u_{n+2} = 3u_{n+1} - 2u_n$, $n \ge 0$, has infinitely many initial values $u_0 = k+1$ and $u_1 = 2k+1$ that give composite u_n for all $n \ge 0$. Analogously, R. L. Graham [1] and D. Knuth [2] found composite integers F_0, F_1, $(F_0, F_1) = 1$ for the Fibonacci-like sequence $\{F_n\}$, $n \ge 0$, $F_{n+2} = F_{n+1} + F_n$ such that F_n are all composite numbers.

In the construction of composite sequences, the authors [1]-[3] used the idea of a covering set, i.e., a set $P = \{p_1, p_2, \ldots, p_h\}$, $h \ge 1$, of prime numbers such that, for each $n \ge 0$, there exists at least one $p \in P$ such that $u_n \equiv 0 \bmod p$.

In this note we give a class of integers $a > 0$, b, $(a, b) = 1$ and find integers u_0, u_1, $(u_0, u_1) = 1$ such that the sequence $\{u_n\}$, $n \ge 0$, $u_{n+2} = au_{n+1} - bu_n$ with initial values u_0, u_1 contain only composite members. For even n, u_n has an algebraic decomposition while, for odd n, u_n has a covering set $P = \{p\}$.

To prove the main theorem, we need the following three lemmas.

Lemma 1: Let integers a, b be such that $\Delta = a^2 - 4b \ne 0$. Let integers v_0, v_1 be initial values for the recurrence $v_{n+2} = av_{n+1} - bv_n$, $n \ge 0$. Then for the sequence $\{u_n\}$, $n \ge 0$, and $u_0 = v_0 w_0$, $u_2 = v_1 w_1$, $u_{n+2} = au_{n+1} - bu_n$, $n \ge 0$, we have

$$u_{2n} = v_n w_n, \tag{1}$$

where

$$w_0 = k(2v_1 - av_0)/d, \;\; w_1 = k(av_1 - 2bv_0)/d, \tag{2}$$

$d = (2v_1 - av_0, \, av_1 - 2bv_0)$, k is an arbitrary integer and $w_{n+2} = aw_{n+1} - bw_n$.

Proof: Let w_0, w_1 be arbitrary integers. We prove that, if $u_{2n} = v_n w_n$, then w_0, w_1 satisfy (2). It is known that the sequence $\{x_n\}$, $n \ge 0$, satisfies the recurrence $x_{n+2} = ax_{n+1} - bx_n$ if and only if $x_n = A\alpha^n + B\beta^n$ for $n \ge 0$, where A, B are constants and α, β are the distinct roots of the characteristic polynomial $z^2 - az + b$, since $\Delta = a^2 - 4b \ne 0$. So we have

$$v_n = A_1\alpha^n + B_1\beta^n, \;\; w_n = A_2\alpha^n + B_2\beta^n,$$

where $\alpha = (a+\Delta)/2$, $\beta = (a-\Delta)/2$, and

$$A_1 = (v_1 - \beta v_0)/(\alpha - \beta), \quad B_1 = (\alpha v_0 - v_1)/(\alpha - \beta),$$
$$A_2 = (w_1 - \beta w_0)/(\alpha - \beta), \quad B_2 = (\alpha w_0 - w_1)/(\alpha - \beta).$$

Furthermore,

$$v_n w_n = (A_1\alpha^n + B_1\beta^n)(A_2\alpha^n + B_2\beta^n) = A_1A_2\alpha^{2n} + (A_1B_2 + A_2B_1)\alpha^n\beta^n + B_1B_2\beta^{2n}.$$

So, if $A_1B_2 + A_2B_1 = 0$, the sequence $\{u_k\}$, $k \ge 0$, $u_k = A_1A_2\alpha^k + B_1B_2\beta^k$ satisfies $u_{k+2} = au_{k+1} - bu_k$ and $u_{2n} = v_n w_n$. Consider

$$0 = A_1B_2 + A_2B_1 = (v_1 - \beta v_0)(\alpha w_0 - w_1)/(\alpha-\beta)^2 + (\alpha v_0 - v_1)(w_1 - \beta w_0)/(\alpha-\beta)^2$$
$$= [(\alpha+\beta)(v_1w_0 + v_0w_1) - 2\alpha\beta v_0w_0 - 2v_1w_1]/(\alpha-\beta)^2.$$

Since $\alpha+\beta = a$, $\alpha\beta = b$, we have $a(v_1w_0 + v_0w_1) - 2bv_0w_0 - 2v_1w_1 = 0$, or

$$(av_1 - 2bv_0)w_0 = (2v_1 - av_0)w_1.$$

If $d = (2v_1 - av_0, av_1 - 2bv_0)$ and k is an arbitrary integer, then we have (2).

Lemma 2: Let $a > 1$, $m > 1$, and b be integers such that $a \equiv 0 \bmod m$ and u_0, u_1 are initial values for the recurrence $u_{n+2} = au_{n+1} - bu_n$, $n \geq 0$. If $u_1 \equiv 0 \bmod m$, then $u_{2n+1} \equiv 0 \bmod m$ for $n \geq 0$.

Proof: Consider the sequence $\{U_n\}$, where $U_0 = 0$, $U_1 = 1$, $U_{n+2} = aU_{n+1} - bU_n$, $n \geq 0$. It is known that $U_{2n} \equiv 0 \bmod a$ for $n \geq 1$. Since $u_{2n+1} = u_1U_{2n+1} - bu_0U_{2n}$ for $n \geq 0$, we have $u_{2n+1} \equiv 0 \bmod m$.

Lemma 3: Let integers $a > 0$ and b be such that $(a, b) = 1$, $\Delta = a^2 - 4b > 0$, and u_0, u_1 be initial values for $u_{n+2} = au_{n+1} - bu_n$, $n \geq 0$, such that $u_0 > 0$, $(b, u_1) = 1$, $(u_0, u_1) = 1$, and $u_1 > au_0/2$. Then $(u_n, u_{n+1}) = 1$ and $u_{n+1} > au_n/2$ for $n > 0$.

Proof: We prove this lemma by induction. We first prove that $(b, u_n) = 1$ for $n > 1$. By the condition of the lemma, $(b, u_1) = 1$. Let $(b, u_i) = 1$ for $1 < i \leq n$. For $i = n+1$, we have $(b, u_{n+1}) = (b, au_n - bu_{n-1}) = (b, au_n) = (b, u_n) = 1$. Since $(u_0, u_1) = 1$, let $(u_i, u_{i+1}) = 1$ for $1 \leq i \leq n$. For $i = n+1$, we have $(u_{n+1}, u_{n+2}) = (u_{n+1}, au_{n+1} + bu_n) = (u_{n+1}, u_n) = 1$. By the statement of Lemma 3, $u_1 > au_0/2$. Assume that $u_i > au_{i-1}/2$ is true for $1 < i \leq n$. Then, for $i = n+1$,

$$u_{n+1} = au_n - bu_{n-1} = au_n/2 + au_n/2 - bu_{n-1}$$
$$> au_n/2 + a(au_{n-1}/2)/2 - bu_{n-1} > au_n/2 + \Delta u_{n-1}/4 > au_{n-1}/2.$$

Thus, the lemma is proved.

We now proceed to prove the main theorem.

Theorem: Let odd $a > 2$ and b be integers such that $(a, b) = 1$ and let $\Delta = a^2 - 4b > 0$. Let p be an odd prime divisor of a such that the Legendre symbol $(b/p) = 1$ and let $t > 0$ be any solution of the congruence $x^2 \equiv b \bmod p$. Let $v_0 > 1$, $(a, v_0) = 1$, and $v_1 = tv_0 + kp$ for some positive k such that $(a, v_1) = (v_0, v_1) = (b, v_1) = 1$, $v_1 > av_0/2$. Let $d = (2v_1 - av_0, av_1 - 2bv_0)$.

Then the sequence $\{u_n\}$ with initial values $u_0 = (2v_0v_1 - av_0^2)/d$, $u_1 = (v_1^2 - bv_0^2)/d$, and $u_{n+2} = au_{n+1} - bu_n$ for $n \geq 0$ is a sequence of composite numbers.

Proof: By Lemma 1, $u_{2n} = v_nw_n$, $n \geq 0$. Here $v_{n+2} = av_{n+1} - bv_n$, $n \geq 0$, for given initial values v_0, v_1, and $w_{n+2} = aw_{n+1} - bw_n$, $n \geq 0$, for initial values $w_0 = (2v_1 - av_0)/d$, $w_1 = (av_1 - 2bv_0)/d$.

We have $u_0 = v_0w_0 = (2v_0v_1 - av_0^2)/d$, $u_2 = v_1w_1 = (av_1^2 - 2bv_0v_1)/d$. Hence,

$$u_1 = (u_2 + bu_0)/a = (av_1^2 - abv_0^2)/ad = (v_1^2 - bv_0^2)/d.$$

Since $t^2 \equiv b \bmod p$, $v_1 = tv_0 + kp$, and $(b, d) = 1$, we have $u_1 \equiv 0 \bmod p$. By Lemma 2, $u_{2m+1} \equiv 0 \bmod p$ for $n > 0$.

Further, $(u_0, u_1) \leq (u_0, au_1) = (u_0, u_2 + bu_0) = (u_0, u_2) = (v_0w_0, v_1w_1)$. Consider

$$(v_0, w_1) < (v_0, dw_1) = (v_0, av_1 - 2bv_0) = (v_0, av_1) = 1.$$

Analogously, $(w_0, v_1) \le (dw_0, v_1) = (2v_1 - v_0, v_1) = 1$. Since $(v_0, v_1) = 1$ and $(w_0, w_1) = 1$, we obtain $(u_0, u_1) = 1$, and by Lemma 3, $(u_n, u_{n+1}) = 1$ for $n \ge 0$.

Finally, consider

$$u_1 - au_0 / 2 = (v_1^2 - bv_0^2)/d - (2av_0v_1 - a^2v_0^2)/2d = (v_1 - av_0/2)^2/d + \Delta v_0^2/4d > 0.$$

By Lemma 3, $u_{n+1} > au_n/2$ for $n > 0$. Thus, the theorem is proved.

On the other hand, it is easy to prove that there are no primes p_0, p_1 such that $p_n = ap_{n-1} - bp_{n-2}$, $a > 0$, $(a, b) = 1$, and $a^2 - 4b > 0$ are primes for all $n > 1$.

Indeed, if $b \equiv 0 \bmod p_1$, then $p_2 = ap_1 - bp_0 \equiv 0 \bmod p_1$. Let $b \not\equiv 0 \bmod p_1$, then there is an $m \le p_1 + 1$ such that $U_m \equiv 0 \bmod p_1$, where $U_0 = 0$, $U_1 = 1$, $U_{n+2} = aU_{n+1} - bU_n$, $n \ge 0$. Since $p_{m+1} = p_1U_{m+1} - bp_0U_m$, we have $p_{m+1} \equiv 0 \bmod p_1$.

It is interesting to find a sequence of primes of maximal length for the Mersenne recurrence $p_{n+2} = 3p_{n+1} - 2p_n$ for $n \ge 0$, where p_0, $p_1 > p_0$ are given primes. The numerical search for small p_0, p_1 gives the sequence of nine primes $\{41, 71, 131, 251, 491, 971, 1931, 3851, 7691\}$. The more exact estimate for length N primes in the Mersenne recurrence uses

$$p_n = p_0M_{n+1} - 2p_{-1}M_n = p_0M_{n+1} - (3p_0 - p_1)M_n, \tag{3}$$

where $M_0 = 0$, $M_1 = 1$, $M_{n+2} = 3M_{n+1} - 2M_n$, $n \ge 0$. p_0, p_1 are given primes and $3p_0 - p_1 \ne 2^t$, $t > 0$. Let $m = \min_{q>2}\{\upsilon(q) : q \mid (3p_0 - p_1)\}$, q is prime, and let $\upsilon(q)$ be the minimal s such that $m_s \equiv 0 \bmod q$. Then by (3), $p_m \equiv 0 \bmod q$ and $N \le m - 1$. N is equal to the upper bound, e.g., for the sequence $\{3467, 6947, 13907, 27827, 55667, 111347, 222707, 445427, 890967\}$. Now, since $p_0 = 3467$, $p_1 = 6947$, and $11 \mid 3454 = 3p_0 - p_1$, we have $m = \upsilon(11) = 10$ and $N = 9$.

REFERENCES

1. R. L. Graham. "A Fibonacci-Like Sequence of Composite Numbers." *Math. Magazine* **37** (1964):322-23.
2. D. Knuth. "A Fibonacci-Like Sequence of Composite Numbers." *Math. Magazine* **63** (1990):21-25.
3. W. Sierpinski. "Sur un Probleme Concernant les Numbres $k2^n + 1$." *Elem. Math.* **15** (1960): 73-74; Corrig. **17** (1962):85.

AMS Classification Number: 11B37

❖❖❖