Factoring Generalized Repunits

JOHN H. JAROMA

Abstract. Twenty-five years ago, W. M. Snyder extended the notion of a repunit R_n to one in which for some positive integer b, $R_n(b)$ has a b-adic expansion consisting of only ones. He then applied algebraic number theory in order to determine the pairs of integers under which $R_n(b)$ has a prime divisor congruent to 1 modulo n. In this paper, we show how Snyder's theorem follows from existing theory pertaining to the Lucas sequences.

1. Introduction

A *repunit* R_n is any integer written in decimal form as a string of 1's. The numbers 1, 11, 111, 1111, 11111, etc., are examples of repunits. In [7], S. Yates alludes to a letter dated June, 1970 that he received from A. H. Beiler in which Beiler claims to have invented the term years earlier. An interesting characteristic regarding repunits is the apparent scarcity of primes among them. Letting R_n denote the nth repunit, only R_2, R_{19}, R_{23}, R_{317}, and R_{1031} have thus far been identified as prime. In fact, they are the only repunit primes for $n \leq 16000$. Although it is necessary for n to be prime in order for R_n to be prime, this is not a sufficient condition as $R_5 = 11111 = 41 \cdot 271$ is composite.

In [6], W. M. Snyder extended the notion of a repunit to one in which for some integer $b > 1$, $R_n(b)$ has a b-adic expansion consisting of only ones. In other words, $R_n(b) = \Sigma_{i=0}^{n-1} b^i = (b^n - 1)/(b - 1)$, where $n > 0$. Examples of these "generalized repunits" include the Mersenne numbers, $M_n = 2^n - 1 = 1 + 2^1 + 2^2 + \ldots + 2^{n-1}$, for $n \geq 2$. Snyder's admitted objective was to apply algebraic number theory in cyclotomic fields in order to determine the pairs of integers n and b under which $R_n(b)$ has a prime divisor congruent to 1 modulo n. To this purpose, Snyder demonstrated the following proposition.

Theorem 1 (Snyder)**.** *$R_n(b)$ has a prime divisor congruent to* 1 (mod *n*) *if and only if $n \neq 2$, or $n = 2$ and $b \neq 2^e - 1$, for all integers e greater than* 1*.*

In this paper, we illustrate how Theorem 1 may be derived from the existing theory of the Lucas sequences, upon which, we then introduce a primality test for base-10 repunits.

2. The Lucas Sequences

Let P and Q be any pair of relatively prime integers. We define the *Lucas* and *companion Lucas sequences*, respectively, as

$$U_{n+2}(P,Q) = PU_{n+1} - QU_n,\ U_0 = 0,\ U_1 = 1,\ n \in \{0, 1, \ldots\} \quad (1)$$

$$V_{n+2}(P,Q) = PV_{n+1} - QV_n,\ V_0 = 2,\ U_1 = P,\ n \in \{0, 1, \ldots\}. \quad (2)$$

Now, (1) and (2) are linear, and hence, solvable. Letting $D = P^2 - 4Q$ be the discriminant of $X^2 - PX + Q = 0$, the roots of the said characteristic equation are $\theta = (P + \sqrt{D})/2$ and $\phi = (P - \sqrt{D})/2$. Thus, the Lucas and companion Lucas sequences are given explicitly by

$$\begin{aligned} U_n(P,Q) &= \frac{\theta^n - \phi^n}{\theta - \phi}, \qquad n \in \{0, 1, \ldots\} \\ V_n(P,Q) &= \theta^n + \phi^n, \qquad n \in \{0, 1, \ldots\}. \end{aligned} \quad (3)$$

The *rank of apparition* of a prime is the index of the first term in the sequence with nonnegative index in which N occurs as a divisor. We let $\omega(p)$ denote the rank of apparition of p in $\{U_n\}$ and $\lambda(p)$ the corresponding rank of apparition of p in $\{V_n\}$. Also, we say that p is a *primitive* prime factor of the term in which it has rank of apparition. The next lemma contains results that are found in [5].

Lemma 1. *Let p be an odd prime.*

(1) *If $p \nmid P$, $p \nmid Q$, and $p \mid D$, then $p \mid U_k$ exactly when $p \mid k$.*
(2) *If $p \nmid PQD$, then $p \mid U_{p-(D/p)}$, where (D/p) denotes the Legendre symbol.*
(3) *$p \mid U_n$ if and only if $n = k\omega$, for some positive integer k.*

3. Generalized Repunits by the Lucas Sequences

Now, we show that for any base $b > 1$, $\{R_n(b)\}$ is a Lucas sequence.

Theorem 2. *Let b be any integer > 1. Then,*

$$U_n(b+1, b) = (b^n - 1)/(b-1).$$

Proof. Let $P = b + 1$ and $Q = b$. Since b and $b+1$ are relatively prime, then by (3),

$$U_n = \frac{\left(\frac{P+\sqrt{D}}{2}\right)^n - \left(\frac{P-\sqrt{D}}{2}\right)^n}{\left(\frac{P+\sqrt{D}}{2}\right) - \left(\frac{P-\sqrt{D}}{2}\right)} = \frac{\left(\frac{b+1+(b-1)}{2}\right)^n - \left(\frac{b+1-(b-1)}{2}\right)^n}{b-1} = \frac{b^n - 1}{b-1}.$$

□

4. An Elementary Proof of Theorem 1

In this section, we shall demonstrate Snyder's Theorem 1 by first establishing that every term of the Lucas sequence $\{R_n(b)\} = \{U_n(b+1, b)\}$ has a primitive prime factor. The latter result rests upon Carmichael's generalization of K. Zsigmondy's theorem for numbers of the form $a^n \pm b^n$ to the family of Lucas sequences [3]. We also point out that Zsigmondy's result given in [8] is an extension of a theorem of A. S. Bang, who in 1886, proved the special case $b = 1$ [1]. A further discussion of these results is found in [5]. The following is Carmichael's result, which will lead us to Lemma 3.

Lemma 2 (Carmichael)**.** *Let $\{U_n(P, Q)\}$ be a Lucas sequence and $D = P^2 - 4Q$.*

(1) *Let $D > 0$. Then, for all $n \neq 1, 2, 6$, U_n has a primitive prime factor, unless $n = 12$, $P = \pm 1$, and $Q = -1$.*

(2) *Let D be a square. Then, for all n, U_n has a primitive prime factor unless $n = 6$, $P = \pm 3$, and $Q = 2$.*

Lemma 3. *Every term of $\{R_n(b)\}$ $=\{U_n(b+1, b)\}$, with the exception of $b = 2$ and $n = 6$ has a primitive prime factor.*

Proof. Since $P = b+1$, $Q = b$, and $D = P^2 - 4Q = (b+1)^2 - 4b = (b-1)^2$, it follows by Lemma 2 that $R_n(b)$ has a primitive prime factor unless $b = 2$ and $n = 6$. □

Remark. If n is odd, say $2k+1$ $(k \geq 1)$, then

$$R_n = b^{2k} + b^{2k-1} + \ldots + b + 1$$

is odd. On the other hand, if n is even, say $2k$ $(k \geq 2)$, then

$$\begin{aligned} R_n &= (b^{2k}-1)/(b-1) = [(b^k+1)(b^k-1)]/(b-1) \\ &= (b^k+1)(b^{k-1}+b^{k-2}+\ldots+1). \end{aligned}$$

Hence, for $k \geq 2$, we have $b^k+1 \neq 2^\alpha$ for all integral values of α. Thus, if $n \geq 3$ then there exists at least one odd prime factor of R_n regardless of the parity of n. It is also without loss of generality we assume that $b=2$ and $n=6$ do not simultaneously hold for otherwise, $R_6(2)=63$ has the prime factor 7 congruent to $1 \pmod 6$. Under this stipulation, it then follows that every term of $\{R_n\}$ has a primitive prime factor. Moreover, for generalized repunits, we further extend the reach of Lemma 3 to include the existence of an odd primitive prime factor. This is so, because if $k=2$ then $2 \mid R_4$. Hence, if b is odd then $R_2=b+1$ and $\omega(2)=2$ and if b is even then the odd factor b^2+1 necessarily contains an odd prime factor that divides neither $R_2=b+1$ nor $R_3=(b+1)^2-b$.

We now give our alternative demonstration of Theorem 1.

Proof of Theorem 1. Let's assume that either $n \neq 2$, or $n=2$ and $b \neq 2^e-1$ is not true for all integers $e>1$. Then, $n=2$ and $b=2^e-1$ for some $e>1$. Therefore, $R_2(b)=R_2(2^e-1)=2^e$, which has no prime divisors congruent to $1 \pmod 2$. To prove necessity, we may assume that $n>1$. Otherwise, every prime is trivially congruent to $1 \pmod 1$.

Case 1: Let $n=2$. Then, $R_n=R_2=b+1$. Hence, if $b=2^e-1$ then $R_n=2^e$, which does not have a prime factor congruent to 1 $(\text{mod } n)$.

Now, assume that $n \geq 3$. By the previous remark, we let p be an odd primitive prime factor of R_n. In turn, this implies that $\omega(p)=n$.

Case 2: Let $p \nmid PQD$. Since $D=P^2-4Q=(b-1)^2$, it follows that $(D/p)=1$. So, by the second statement of Lemma 1, $p \mid U_{p-1}$, from which it follows from the third conclusion of the same lemma that $\omega(p) \mid p-1$. Therefore, $\omega(p)k=p-1$, for some integer k. In other words, $p=\omega(p)k+1$.

Case 3: Let $p \mid P=b+1$. Then, $U_2=b+1$ and $\omega(p)=2$, which is impossible, as p is a primitive prime factor of R_n $(n \geq 3)$.

Case 4: Let $p \mid Q=b$. But this implies that $p \mid R_n=b^{n-1}+b^{n-2}+\ldots+b+1$, which is also impossible, as $p \neq 1$.

Case 5: Let $p \nmid PQ$ and $p \mid D = P^2 - 4Q$. By (1) of Lemma 1, $p \mid R_n$ exactly when $p \mid n$. As $R_{n+1} > R_n$ and $R_3 = P^2 - Q$, it then follows that $\omega(p) < 3$, which under our assumptions cannot happen. □

5. Testing the Primality of Base-10 Repunits

A corollary to Fermat's Little Theorem tells us that for any integer a, $a^n \equiv a \pmod{n}$ if n is a prime. Thus, if we can identify an integer a for which this congruence does not hold, then we may conclude that n is composite. For example, by taking $a = 3$ and $n = 8$, we see that $3^8 \equiv 1 \pmod{8}$. This proves that 8 is composite. So, Fermat's Theorem is a way to determine if a number n is composite without having to first extract a factor. Nonetheless, for large values of n the number of computations involved is prohibitively large.

A method that is sometimes used for making an educated guess as to the prime or composite character of an integer n is the *Miller–Rabin test*. The idea of this algorithm is to write $n = 2^h m + 1$, where m is odd. Then, for a particular base $a : 1 < a < n - 1$, we consider the sequence of terms $a^m, a^{2m}, a^{4m}, \ldots, a^{2^h m} = a^{n-1}$ modulo n. The number n is said to "pass the test" if the first occurrence of 1 is either the first term or -1 precedes it. An odd prime will pass this test for all bases. To help us decide if n is prime or composite, we may randomly select k integers, say, a_i, $1 \leq i \leq k$. If n fails the Miller–Rabin test for any one of these bases, we immediately conclude that n is composite. On the other hand, if n passes the test for all a_i, then n is dubbed a *probable prime*. Although we can never be certain that n is prime after conducting the Miller–Rabin test, the probability of a composite number surviving k applications of the algorithm is at most $(1/4)^k$ [2]. In 1999, Harvey Dubner announced that R_{49081} is a probable repunit prime [4] and in 2000, Lew Baxter added R_{86453} to the short list.

We now arrive at our final objective—to construct a definitive Lucas-type test for deciding the primality of any base-10 repunit. To this purpose, we introduce the Legendre symbols $\sigma = (P^2/p)$, $\epsilon = (D/p)$, and $\tau = (Q/p)$. The following lemmas will be alluded to and may be found in [5].

Lemma 4. *The gcd(U_n, V_n) is* 1 *or* 2.

Lemma 5. *Suppose that ω is odd. Then, $V_n(\sqrt{R}, Q)$ is not divisible by p for any value of n. If n is even, say $2k$, then $V_{(2n+1)k}(\sqrt{R}, Q)$ is divisible by p for every n but no other term of the sequence contains p as a factor.*

Lemma 6. $U_{(p-\sigma\epsilon)/2}(P, Q) \equiv 0 \pmod{p}$ *if and only if* $\sigma = \tau$.

Lemma 7. *If $N \pm 1$ is the rank of apparition of N then N is prime.*

Base-10 repunits are generated by the Lucas sequence $\{U_n(11, 10)\}$. Thus, celebrated properties of the Lucas sequences such as the necessity of the index being prime in order for U_n to be prime, $U_m \mid U_n$ if $m \mid n$, and if $d \mid U_m$ and $d \mid U_n$ then $d \mid U_{m+n}$ are also attributable to base-10 repunits. Furthermore, we point out that $10 \mid R_n - 1$. This enables us to state and prove the following necessary and sufficient condition for the primality of an arbitrary R_n, bearing in mind that R_n is prime only if n is prime. We remark that although there are infinitely many Lucas sequences that can be used for this purpose, we have opted to use the Fibonacci numbers $\{U_n(1, -1)\}$.

Theorem 3. *Let p be any prime and $2 \cdot 5p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of R_{p-1}. Let $R_p \nmid \prod_{i=1}^{k} U_{(10p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k})/p_i}(1, -1)$. Then, R_p is prime if and only if $R_p \mid V_{5p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}}(1, -1)$.*

Proof. ($\Rightarrow$) Assume that R_p is prime. Since $P = 1$ and $Q = -1$, we have $\sigma = \left(P^2/R_p\right) = (1/R_p) = 1$ and $\tau = (Q/R_p) = ((-1)/R_p) \equiv (-1)^{((10^p-10)/9)/2} \equiv (-1)^{(5(10^{p-1}-1))/9} \pmod{R_p} = -1$. By Gauss's Reciprocity Law, $(5/R_p)(R_p/5) = (-1)^{R_p-1} = 1$. Hence, $(5/R_p) = (R_p/5)$. Hence, $\epsilon = (D/R_p) = (5/R_p) = (R_p/5) \equiv R_p^2 \pmod{5} = 1$. Furthermore, since $D = 1$, it follows from the second part of Lemma 1 that $U_{10p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \equiv 0 \pmod{R_p}$. However, as $\sigma \neq \tau$, by Lemma 6, $R_p \nmid U_{5p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$. Thus, $\omega(R_p)$ is either equal to $10p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ or must divide exactly one of $U_{(10p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k})/p_i}$. But, by hypothesis, the latter is impossible. Therefore, $\omega(R_p) = 10p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, and by Lemma 4, $R_p \mid V_{5p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$.
($\Leftarrow$) We now suppose that $R_p \mid V_{5p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$. By the identity $U_{2n} = U_n V_n$ and Lemma 5, we have $R_p \mid U_{10p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$ but $R_p \nmid U_{5p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$. As $R_p \nmid \prod_{i=1}^{k} U_{(10p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k})/p_i}$, it follows that $\omega(R_p) = 10p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Therefore, by Lemma 7, R_p is prime. □

In conclusion, it may be argued that the factorization of R_{p-1} is difficult to obtain due to the large size of the number. Indeed, this is true. Nevertheless, if we are able to factor $p-1$, then it follows from the theory of Lucas that $R_k \mid R_{p-1}$, for all factors k of $p-1$.

References

[1] A. S. Bang, Taltheoretiske undersogelser, *Tidskrift f. Math.*, 4th and 5th Ser. (1886), 130–137, 70–80.

[2] D. M. Burton, *Elementary Number Theory*, 5th ed., McGraw Hill, New York, 2002.

[3] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. Math.* **15**, (1913–1914), 30–70.

[4] H. Dubner, Repunit R49081 is a probable prime, *Math. Comp.* **71** 238 (2002) 833–835.

[5] P. Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1996.

[6] W. M. Snyder, Factoring repunits, *Amer. Math. Monthly* **89** (1982), 462–466.

[7] S. Yates, *Repunits and repetends*, Boynton Beach: Star Publishing Co., 1982.

[8] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsch. f. Math.* **3** (1892), 265–284.

John H. Jaroma,
Department of Mathematical Sciences,
Loyola College in Maryland,
Baltimore, MD 21210, USA
jhjaroma@loyola.edu

Received on 9 September 2006 and in revised form on 21 June 2007.