ON PRIME CHAINS

DOUGLAS S. STONES

Abstract. Let \( b \) be an odd integer such that \( b \equiv \pm 1 \pmod{8} \) and let \( q \) be a prime with primitive root 2 such that \( q \) does not divide \( b \). We show that if \( (p_k)_{k=0}^{q-2} \) is a sequence of odd primes such that \( p_k = 2p_{k-1} + b \) for all \( 1 \leq k \leq q - 2 \), then either (a) \( q \) divides \( p_0 + b \), (b) \( p_0 = q \) or (c) \( p_1 = q \).

For integers \( a, b \) with \( a \geq 1 \), a sequence of primes \( (p_k)_{k=0}^{\lambda-1} \) such that \( p_k = ap_{k-1} + b \) for all \( 1 \leq k \leq \lambda - 1 \) is called a prime chain of length \( \lambda \) based on the pair \( (a, b) \). This follows the terminology of Lehmer [7]. The value of \( p_k \) is given by

\[
p_k = a^k p_0 + b \frac{(a^k - 1)}{(a - 1)}
\]

for all \( 0 \leq k \leq \lambda - 1 \).

For prime chains based on the pair \( (2, +1) \), Cunningham [2, p. 241] listed three prime chains of length 6 and identified some congruences satisfied by the primes within prime chains of length at least 4. Prime chains based on the pair \( (2, +1) \) are now called Cunningham chains of the first kind, which we will call \( C_{+1} \) chains, for short. Prime chains based on the pair \( (2, -1) \) are called Cunningham chains of the second kind, which we will call \( C_{-1} \) chains.

We begin with the following theorem which has ramifications on the maximum length of a prime chain; it is a simple corollary of Fermat’s Little Theorem. A proof is also given by L"oh [9]. Moser [10] once posed Theorem 1, with \( a, b, p_0 \geq 1 \), as an exercise, for which he received fourteen supposedly correct proofs.

**Theorem 1.** Let \( (p_k)_{k \geq 0} \) be an infinite sequence for which \( p_k = ap_{k-1} + b \) for all \( k \geq 1 \). Then the set \( \{p_k\}_{k \geq 0} \) is either finite or contains a composite number.

There are some choices of \( (p_0, a, b) \) that are uninteresting. For example, if \( b = -(a - 1)p_0 \), then the prime chain is \( (p_0, p_0, \ldots) \). In fact, if \( p_i = p_j \) for any distinct \( i, j \) then \( \{p_k\}_{k=0}^{\infty} \) will be periodic, with period dividing \( |p_i - p_j| \). Also if \( \gcd(a, b) > 1 \) then the sequence could only possibly be of length 1, since \( \gcd(a, b) \) divides \( ap_0 + b \).

In this article we will therefore assume that \( (p_k)_{k=0}^{\infty} \) is a strictly increasing sequence. Theorem 1 implies that no choice of \( (p_0, a, b) \) will give rise to a prime chain of infinite length. However, this raises the question, how long can a prime chain be? Green and Tao [5] proved that, for all \( \lambda \geq 1 \), there exists a prime chain of length \( \lambda \) based on the pair \( (1, b) \) for some \( b \). Lehmer [7] remarked that Dickson’s Conjecture [3], should it be true, would imply that there are infinitely many prime chains of length \( \lambda \) based on the pair \( (a, b) \), with the exception of some inappropriate pairs \( (a, b) \).
Discussions about searching for Cunningham chains were given by Lehmer [7], Guy [8, Sec. A7], Loh [9] and Forbes [4]. Tables of Cunningham chains are currently being maintained by Wikipedia [12] and Caldwell [1].

In this article, we will frequently deal with primes, denoted either $p$ or $q$, that have a primitive root $a$. We therefore introduce the following terminology for brevity. If $a$ is a primitive root modulo $q$ then we will write $a \triangle q$ and if $q$ is prime and $a \triangle q$, we will call $q$ an $a\triangle$-prime.

We begin with the following theorem, which slightly improves [7, Thm 1].

**Theorem 2.** Let $q$ be an $a\triangle$-prime such that $q$ does not divide $b$. Suppose $(p_k)_{k=0}^{q-2}$ is a prime chain based on the pair $(a, b)$. Then $q$ divides $p_0(a-1)+b$ or $q=p_k$ for some $0 \leq k \leq q-2$.

**Proof.** To begin, note that $a \not\equiv 0, 1 \pmod{q}$ since $a \triangle q$. Suppose $q$ does not divide $p_0(a-1)+b$. Let $S = \{p_k\}_{k=1}^{q-2}$ and let $S_q = \{p_k \pmod{q}\}_{k=1}^{q-2}$. If $p_i \equiv p_j \pmod{q}$ then

$$a^i p_0 + b \frac{(a^i - 1)}{(a - 1)} \equiv a^j p_0 + b \frac{(a^j - 1)}{(a - 1)} \pmod{q}$$

by (1) and so

$$\frac{a^i}{a - 1} (p_0(a-1)+b) \equiv \frac{a^j}{a - 1} (p_0(a-1)+b) \pmod{q}$$

since $a \not\equiv 1 \pmod{q}$. Since $q$ does not divide $p_0(a-1)+b$ we find $a^i \equiv a^j \pmod{q}$ implying that $i \equiv j \pmod{q-1}$, since $a \triangle q$. Therefore $|S_q| = q - 1$.

If $-b/(a-1) \pmod{q}$ is an element of $S_q$ then for some $i$,

$$a^i p_0 + b \frac{(a^i - 1)}{(a - 1)} \equiv \frac{-b}{a - 1} \pmod{q}$$

by (1), implying that $p_0 \equiv -b/(a-1) \pmod{q}$ contradicting our initial assumption. Hence $S_q = \{0, 1, 2, \ldots, q-1\} \setminus \{-b/(a-1)\}$. Since $q$ does not divide $b$, we find that $0 \in S_q$ and therefore $q$ divides an element of $S$. But since $S$ contains only primes, therefore $q \in S$. □

To show that Theorem 2 is the “best possible” in at least one case, we identify the prime chain $(7, 11, 23, 59, 167, 491)$ of length $\lambda = q-1 = 6$ based on $(a, b) = (3, -10)$. Here $-b/(a-1) = -10/2 = 5 \pmod{7}$ while $p_0 \equiv 0 \pmod{7}$. This raises the question, when can there exist a prime chain of length $q-1$, for $q$, $a$ and $b$ satisfying the conditions of Theorem 2 while $p_0 \not\equiv -b/(a-1) \pmod{q}$? In the next section, we will find that prime chains of this form, when $b \equiv \pm 1 \pmod{8}$, are exceptional, which includes Cunningham chains of both kinds.

Cunningham [2] p. 241] claimed that a $C_{+1}$ chain $(p_k)_{k=0}^{\lambda-1}$ of length $\lambda \geq 4$ must have (a) each $p_k \equiv -1 \pmod{3}$ and (b) each $p_k \equiv -1 \pmod{5}$. However, condition (b) is incorrect for the prime chain $(2, 5, 11, 23, 47)$. In Theorem 3 we will prove that there are no counter-examples to Cunningham’s condition (b) when $p_0 > 5$. Lehmer [7] stated that $C_{+1}$ chains $(p_i)_{i=0}^{\lambda-1}$ of length $\lambda \geq 10$ have $p_0 \equiv -1 \pmod{2 \cdot 3 \cdot 5 \cdot 11}$. Loh [9] showed that $C_{-1}$ chains $(p_i)_{i=0}^{\lambda-1}$ of length $\lambda \geq 12$ have $p_0 \equiv 1 \pmod{2 \cdot 3 \cdot 5 \cdot 11 \cdot 13}$. In Corollary 1 we will generalise this list of results to prime chains based on $(2, b)$ for all odd integers $b \equiv \pm 1 \pmod{8}$.

For any odd prime $s$ let $o_s(2)$ denote the multiplicative order of $2$ modulo $s$. Let $\mathbb{N} = \{1, 2, \ldots\}$. We make use of the following Legendre symbol identities, which
can be found in many elementary number theory texts, for example [3]. For odd prime \( q \)

\[
(2) \quad \left( \frac{2}{q} \right) = \begin{cases} 
1 & \text{if } q \equiv \pm 1 \pmod{8} \\
-1 & \text{if } q \equiv \pm 3 \pmod{8}
\end{cases} \quad \text{and} \quad \left( \frac{a}{q} \right) \equiv a^{\frac{q-1}{2}} \pmod{q}.
\]

We are now ready to state and prove the main theorem.

**Theorem 3.** Let \( b \) be an odd integer such that \( b \equiv \pm 1 \pmod{8} \) and let \( q \) be a \( 2\Delta \)-prime that does not divide \( b \). Suppose \( (p_{k})_{k=0}^{q-2} \) is a prime chain based on the pair \((2, b)\). Then either (a) \( q \) divides \( p_{0} + b \), (b) \( p_{0} = q \), (c) \( p_{1} = q \) or (d) \( p_{0} = 2 \).

**Proof.** Suppose \( p_{0} \) is an odd prime and is of the form \( p_{0} = 2m - b \) for some integer \( m \). So \( p_{k} = 2^{k+1}m - b \) for all \( 0 \leq k \leq q - 2 \) by [14]. If \( q \) does not divide \( p_{0} + b \), then Theorem [2] implies that \( q = p_{k} = 2^{k+1}m - b \) for some \( 0 \leq k \leq q - 2 \). If \( q = 2^{k+1}m - b \) where \( k \geq 3 \), then

\[
1 = \left( \frac{2}{q} \right) \equiv 2^{\frac{q-1}{2}} \pmod{q}
\]

by (2) since \( b \equiv \pm 1 \pmod{8} \). However, this contradicts that \( 2 \Delta q \). Hence \( q = p_{0} \) or \( q = p_{1} \).

We can now deduce the following corollary, for which we make use of the fact that contiguous subsequences of prime chains are themselves prime chains to find a large divisor for \( p_{0} - 1 \). Let \( \lambda \in \mathbb{N} \).

**Corollary 1.** Let \( (p_{k})_{k=0}^{q-1} \) be a prime chain based on \((2, b)\) for an odd integer \( b \equiv \pm 1 \pmod{8} \). Let

\[
Q = \{q \leq \lambda + 1 : q \text{ is a prime and } 2 \nmid q \} \cup \{2\} \setminus \{p_{0}, p_{1}\}.
\]

If \( p_{0} \geq 3 \), then \( p_{k} + b \) is divisible by every \( q \in Q \) for all \( 0 \leq k \leq \lambda - 1 \).

**Proof.** We know that 2 divides each \( p_{k} + b \) since both \( p_{k} \) and \( b \) are odd. So let \( q \in Q \setminus \{2\} \). If \( p_{0} \equiv -b \pmod{q} \) then \( q \) divides \( p_{k} + 1 \) for all \( 0 \leq k \leq \lambda - 1 \) since \( 2 \times (-b) + b \equiv 0 \pmod{q} \). Observe that \( (p_{i})_{i=0}^{q-2} \) is a prime chain of length \( q - 1 \) for all \( q \in Q \). The result therefore follows from Theorem [3]. \( \square \)

The \( 2\Delta \)-primes are given by Sloane’s [11] A001122 as 3, 5, 11, 13, 19, 29, 37, 53, and so on. It would also be of interest to know if an analogue of Corollary [1] holds for other non-trivial values of \((a, b)\). The techniques in this article use the Legendre symbol identity (2) which requires \( a = 2 \) and \( b \equiv \pm 1 \pmod{8} \), so they are not easily extended to encompass other pairs \((a, b)\).

Corollary [2] does not hold when \( p_{0} = 2 \). For example, \((2, 5, 11, 23, 47)\) is a prime chain based on \((2, 1)\). In fact, the subsequences \((2, 5, 11, 23)\) and \((5, 11, 23, 47)\) also illustrate why we need to exclude \( p_{0} \) and \( p_{1} \) from \( Q \) in Corollary [1].

Finally, the author would like to thank Hans Lausch for valuable feedback.

**References**

1. Chris Caldwell, [http://primes.utm.edu/glossary/xpage/CunninghamChain.html](http://primes.utm.edu/glossary/xpage/CunninghamChain.html)
2. Allan Cunningham, *On hyper-even numbers and on Fermat’s numbers*, Proc. London Math. Soc. (2) 5 (1907), 237–274.
3. L. E. Dickson, *A new extension of Dirichlet’s theorem on prime numbers*, Messenger of Math. 33 (1904), 155–161.
4. Tony Forbes, *Prime clusters and Cunningham chains*, Math. Comp. 68 (1999), no. 228, 1739–1747.
5. Ben Green and Terence Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. 2 (2008), no. 167, 481–547.
6. Richard K. Guy, *Unsolved problems in number theory*, 3rd ed., Springer, 2004.
7. D. H. Lehmer, *On certain chains of primes*, Proc. London Math. Soc. (3) 14A (1965), 183–186.
8. William J. LeVeque, *Fundamentals of number theory*, Dover, 1996.
9. Günter Löh, *Long chains of nearly doubled primes*, Math. Comp. 53 (1989), no. 188, 751–759.
10. Leo Moser et al., E988, Amer. Math. Monthly 5 (1952), no. 59, 331.
11. Neil James Alexander Sloane, *The on-line encyclopedia of integer sequences*, [http://www.research.att.com/~njas/sequences/](http://www.research.att.com/~njas/sequences/)
12. Wikipedia, [http://en.wikipedia.org/wiki/Cunningham_chain](http://en.wikipedia.org/wiki/Cunningham_chain)

School of Mathematical Sciences, Monash University, VIC 3800 Australia

E-mail address: douglas.stones@sci.monash.edu.au