Arithmetic Properties for a Certain Family of Knot Diagrams

Darrin D. Frey
Department of Science and Math
Cedarville University
Cedarville, OH 45314
freyd@cedarville.edu

and

James A. Sellers
Department of Mathematics
The Pennsylvania State University
University Park, PA 16802
sellersj@math.psu.edu

October 22, 2003

Abstract

In this note, we consider arithmetic properties of the function

$$K(n) = \frac{(2n)!(2n+2)!}{(n-1)!(n+1)!^2(n+2)!}$$

which counts the number of two–legged knot diagrams with one self–intersection and $n-1$ tangencies. This function recently arose in a paper by Jacobsen and Zinn–Justin on the enumeration of knots via a transfer matrix approach. Using elementary number theoretic techniques, we prove various results concerning $K(n)$, including the following:

- $K(n)$ is never odd,
- $K(n)$ is never a quadratic residue modulo 3, and
- $K(n)$ is never a quadratic residue modulo 5.

1 Background

In their recent work [2], Jacobsen and Zinn–Justin consider the problem of enumerating certain families of alternating knots. Much of their work involves asymptotics and computational enumeration, but in some cases they give closed formulas for certain types of knot diagrams. In particular, Jacobsen and Zinn–Justin note that the number of two–legged knot diagrams with one self–intersection and $n-1$ tangencies is given by

$$K(n) = \frac{(2n)!(2n+2)!}{(n-1)!(n+1)!^2(n+2)!}. \tag{1}$$

In this note, our goal is to prove some arithmetic properties for this function $K(n)$. We do so by considering the computation of $K(n)$ in light of the following lemma:

Lemma 1.1. *The number of factors of a prime p in $N!$, denoted $ord_p(N!)$, is equal to*

$$\sum_{k\geq 1} \left\lfloor \frac{N}{p^k} \right\rfloor.$$

For a proof of Lemma 1.1, see for example [3, Theorem 2.29].
Such an approach has been used by the authors in another setting [1]. We begin by defining

$$c_{p,k}(n) = \left\lfloor \frac{2n}{p^k} \right\rfloor + \left\lfloor \frac{2n+2}{p^k} \right\rfloor - \left\lfloor \frac{n-1}{p^k} \right\rfloor - 2\left\lfloor \frac{n+1}{p^k} \right\rfloor - \left\lfloor \frac{n+2}{p^k} \right\rfloor,$$

and then introduce the increment

$$\begin{aligned} c_{p,k}(n+1) - c_{p,k}(n) \quad &= \quad \left(\left\lfloor \frac{2n+4}{p^k} \right\rfloor - \left\lfloor \frac{2n}{p^k} \right\rfloor \right) + \left(\left\lfloor \frac{n-1}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor \right) \\ &\quad + \left(2\left\lfloor \frac{n+1}{p^k} \right\rfloor - \left\lfloor \frac{n+2}{p^k} \right\rfloor - \left\lfloor \frac{n+3}{p^k} \right\rfloor \right) \end{aligned}$$

of $c_{p,k}(n)$. Note that the increment is periodic with period p^k. We then find a closed form formula for $c_{p,k}(n)$. Thanks to Lemma 1.1, we can use this closed formula for $c_{p,k}(n)$ to calculate $ord_p(K(n))$ given that

$$ord_p(K(n)) = \sum_{k\geq 1} c_{p,k}(n).$$

This will then allow us to prove a number of arithmetic properties of $K(n)$.

We now turn our attention to the increment mentioned above.

Proposition 1.2. *If $p^k \geq 7, 0 \leq n < p^k$ then*

$$c_{p,k}(n+1) - c_{p,k}(n) = \begin{cases} -1 & \textit{if} \quad n = 0, p^k - 3, p^k - 2 \\ 1 & \textit{if} \quad n = \left\lfloor \dfrac{p^k - 3}{2} \right\rfloor, \left\lfloor \dfrac{p^k - 1}{2} \right\rfloor, p^k - 1 \\ 0 & \textit{otherwise.} \end{cases} \tag{2}$$

Note that since the number of 1's is equal to the number of -1's, $c_{p,k}(n)$ is periodic with period p^k.

Hence, we have

Proposition 1.3. *If $p^k \geq 7, 0 \leq n < p^k$ then,*

$$c_{p,k}(n) = \begin{cases} 0 & \textit{if} \quad 1 \leq n \leq \left\lfloor \dfrac{p^k - 1}{2} \right\rfloor - 1 \ \textit{or} \ n = p^k - 1 \\ 1 & \textit{if} \quad n = 0, \left\lfloor \dfrac{p^k - 1}{2} \right\rfloor, p^k - 2 \\ 2 & \textit{if} \quad \left\lfloor \dfrac{p^k - 1}{2} \right\rfloor + 1 \leq n \leq p^k - 3. \end{cases} \tag{3}$$

Finally, we note a few special cases of $c_{p,k}(n)$.

Proposition 1.4. *If $p^k \leq 5, 0 \leq n < p^k$, then we have the following:*

$$\begin{array}{llll} c_{2,1}(0) = 1 & c_{2,2}(0) = 1 & c_{3,1}(0) = 1 & c_{5,1}(0) = 1 \\ c_{2,1}(1) = 0 & c_{2,2}(1) = 1 & c_{3,1}(1) = 0 & c_{5,1}(1) = 0 \\ & c_{2,2}(2) = 1 & c_{3,1}(2) = 0 & c_{5,1}(2) = 1 \\ & c_{2,2}(3) = 0 & & c_{5,1}(3) = 1 \\ & & & c_{5,1}(4) = 0 \end{array}$$

Moreover, $c_{2,1}(n), c_{2,2}(n), c_{3,1}(n)$ and $c_{5,1}(n)$ are periodic with period 2, 4, 3 and 5 respectively.

2 Arithmetic Properties of $K(n)$

In many of the proofs that follow, we will consider the base p representation of n (where p is some prime) and note that the base p expression of the least nonnegative residue of n mod p^k is simply the base p expression of n with all but the rightmost k digits truncated.

We also need the following definition:

Definition 2.1. *Let m be an integer. We define $f_p(m) = \dfrac{m}{p^{ord_p(m)}}$.*

Note that $f_p(m)$ is multiplicative.

Finally, we note that, for $K(n) \not\equiv 0 \pmod{p}$, we have

$$K(n) = \frac{(2n)!^2}{(n-1)!^2(n+1)!^2} \cdot \frac{(2n+1)\cdot 2}{n(n+2)}$$
$$\equiv f_p\left(\binom{2n}{n+1}\right)^2 \frac{f_p\left((2n+1)\right)\cdot f_p\left(2\right)}{f_p\left(n\right) f_p\left((n+2)\right)} \pmod{p} \tag{4}$$

We now consider certain arithmetic properties of $K(n)$. We begin with a parity result for $K(n)$.

2.1 $K(n) \pmod{2}$

Theorem 2.2. *For all $n \in \mathbb{N}$, $K(n)$ is even.*

Proof. Note that the base 2 representation of n contains at least one 1 (unless $n = 0$). Let k be the least number required so that the rightmost k digits contain exactly one 0. If $k = 1$ or $k = 2$, then by Proposition 1.4, either $c_{2,1}(n) = 1$ or $c_{2,2}(n) = 1$ so $ord_2(K(n)) \geq 1$. Otherwise, $n \equiv 2^{k-1} - 1 \pmod{2^k}$, which, by Proposition 1.3, implies that $c_{2,k}(n) = 1$ and therefore implies that $ord_2(K(n)) \geq 1$. □

We can actually refine our parity result with the following:

Theorem 2.3. *$ord_2(K(n)) = 1$ if and only if $n = 2^k - 1$ for some $k \in \mathbb{N}$.*

Proof. Suppose $n = 2^k - 1$ for some $k \in \mathbb{N}$. Then the base 2 representation of n is a string of k 1's. Thus, by Propositions 1.3 and 1.4, $c_{2,r}(n) = 0$ for $r \leq k$, $c_{2,k+1}(n) = 1$ since $n = 2^k - 1 = \left\lfloor \frac{2^{k+1}-1}{2} \right\rfloor$, and $c_{2,s}(n) = 0$ for $s > k+1$. Thus, $ord_2(K(n)) = 1$.

Conversely, suppose $ord_2(K(n)) = 1$. If m is a k-digit (base 2) number with leading digit 1, then $m \geq \left\lfloor \frac{2^k-1}{2} \right\rfloor + 1 = 2^{k-1}$. Thus, $c_{2,k}(m) = 2$ unless $m = 2^k - 2$ or $2^k - 1$ by Propositions 1.3 and 1.4 or unless $k \leq 2$. We can easily dispense with the small cases by noting that 1 and 3 are of the form $2^k - 1$ and $ord_2(K(2)) = 2$. If $k \geq 3$ and $m = 2^k - 2$ then the base 2 representation of m is a string of $k-1$ 1's followed by a 0. Then $c_{2,r}(m) = 1$ for $1 \leq r \leq k$ (and 0 for larger k), so $ord_2(K(n)) = k > 1$. Hence, $n = 2^k - 1$. □

Corollary 2.4. *For every positive integer $k \neq 2$, there are infinitely many n for which $ord_2(K(n)) = k$. If $ord_2(K(n)) = 2$, then $n = 2$.*

Proof. We consider a few cases. The case $k = 1$ is handled in Theorem 2.3. If $k = 3$, consider $n = 2^j + 1$ where $j > 3$. Then, by Propositions 1.3 and 1.4, $c_{2,r}(n) = 0$ for $r = 1, 3, 4, \ldots j, j+2, \ldots$, $c_{2,2}(n) = 1$ and $c_{2,j+1}(n) = 2$. This means $ord_2(K(n)) = 3$.

Next, suppose $k \geq 4$ and consider $n = 2^j + 2^{k-2} - 2$ where $j \geq k + 1$. Then $c_{2,r}(n) = 1$ for $1 \leq r \leq k - 2$, $c_{2,r}(n) = 0$ for $k - 1 \leq r \leq j$ and $r > j + 1$, and $c_{2,j+1}(n) = 2$. Thus, $ord_2(K(n)) = k$.

Finally, we consider the case $k = 2$. We know that $K(2) = 20$, and $ord_2(20) = 2$. Now from the proof of Theorem 2.3, we have already seen that if m is an r-digit (base 2) number (beginning with 1) where $r \geq 3$, then $c_{2,r}(m) = 2$, unless $m = 2^r - 2$ or $2^r - 1$. If $m = 2^r - 1$, then there are no 0's in the base 2 representation of m, and $ord_2(K(m)) = 1$ by Theorem 2.3. If $m = 2^r - 2$, then there is only one 0 in the base 2 representation and it is in the rightmost position. Furthermore, if $r \geq 3$, then by the proof of Theorem 2.3, $ord_2(K(m)) = r$. So we are left in the case that there are 0's in the base 2 representation of m in at least one position other than the rightmost position. Let s be the position of the rightmost 0 other than in the first digit ($1 < s < r$). Then either $c_{2,s}(m) = 1$ or $c_{2,s-1}(m) = 1$ depending on if the first digit is 1 or 0. In either case, we now have $ord_2(K(m)) > 2$ (since we also had $c_{2,r}(m) = 2$). $\square$

2.2 $K(n) \pmod 3$

Theorem 2.5. *$ord_3(K(n)) = 0$ precisely when n is either 1 or 2 or n is one less than, one more than or two more than a sum of distinct powers of 3 each of which is at least 9.*

Proof. We can restate the theorem by saying that $ord_3(K(n)) = 0$ precisely when $n = 1$ or 2 or, for $n > 2$, the base 3 representation of n has rightmost digit 1, the 3's digit is 0 and the remaining digits are either 1 or 0, or, for $n > 2$, the base 3 representation of n has a string of 2's as its rightmost digits preceded by a 0, and the remaining digits are either 1 or 0. It is straightforward to check that in any of these cases, the least nonnegative residue of n modulo 3^k is either $3^k - 1$ or is between 1 and $\frac{3^k-1}{2} - 1$ (note that the base 3 representation of $\frac{3^k-1}{2}$ consists of all 1's). Thus, $c_{3,k}(n) = 0$ for all k and therefore $ord_3(K(n)) = 0$ for such n.

Conversely, suppose that $ord_3(K(n)) = 0$. Then $c_{3,k}(n) = 0$ for all k. Thus, the least nonnegative residue of n modulo 3^k, i.e. the last k digits of the base 3 representation of n, must either consist of all 2's or must be between 1 and $\frac{3^k-1}{2} - 1$ inclusive (except when $k = 1$ in which case the residue can equal 1). The only numbers that satisfy that criterion are those numbers described. □

Theorem 2.6. *For every nonnegative integer k, there are infinitely many n for which $ord_3(K(n)) = k$.*

Proof. If $k = 0$, we simply refer to Theorem 2.5. Now suppose $k > 0$, and consider $n = 3^k$. Then for $1 \leq r \leq k$, the least nonnegative residue of $n \pmod{3^r}$ is 0. Therefore $c_{3,r}(n) = 1$, and for $r > k$, $c_{3,r}(n) = 0$ since $n < 3^r - 1$. Thus, we have $ord_3(K(n)) = k$. Furthermore, if we now consider $n = 3^j + 3^k$ where $j > k$, we still have $c_{3,r}(n) = 0$ for $r > k$. Thus, in each of these cases $ord_3(K(n)) = k$. □

Next we wish to consider $K(n)$ modulo 3.

Theorem 2.7. *$K(n)$ is never congruent to 1 mod 3.*

Proof. We first note that, by Theorem 2.5, if $n \equiv 0 \pmod 3$, then $K(n) \equiv 0 \pmod 3$. Thus, we only consider $n \equiv 1$ or $2 \pmod 3$.

We now divide into cases.

If $n \equiv 1 \pmod 3$, then we know by Theorem 2.5 that $n = 3^{j_1} + 3^{j_2} + \cdots + 3^{j_i} + 1$ for some $j_1 > j_2 > \cdots > j_r > 1$, so

$$2n + 1 = 2 \cdot 3^{j_1} + 2 \cdot 3^{j_2} + \cdots + 2 \cdot 3^{j_r} + 3.$$

Therefore,

$$f_3\left((2n+1)\right) = 2 \cdot 3^{j_1 - 1} + 2 \cdot 3^{j_2 - 1} + \cdots + 2 \cdot 3^{j_r - 1} + 1.$$

Similarly,

$$f_3\left((n+2)\right) = 3^{j_1 - 1} + \cdots + 3^{j_r - 1} + 1.$$

Since $j_i \geq 2$ for $1 \leq i \leq r$, both $f_3\left((2n+1)\right)$ and $f_3\left((n+2)\right)$ are congruent to $1 \pmod 3$. Thus, combining this with (4), we have

$$K(n) \equiv f_3\left(\binom{2n}{n+1}\right)^2 \frac{f_3\left((2n+1)\right) \cdot 2}{f_3\left(n\right) f_3\left((n+2)\right)} \equiv \frac{1 \cdot 2}{1 \cdot 1} \equiv 2 \pmod 3.$$

If $n \equiv 2 \pmod 3$, then by (4) we have

$$K(n) \equiv f_3\left(\binom{2n}{n+1}\right)^2 \frac{f_3\left((2n+1)\right)\cdot 2}{f_3\left(n\right)f_3\left((n+2)\right)} \equiv \frac{2\cdot 2}{2\cdot 1} \equiv 2 \pmod 3.$$

Thus, in each of these cases, $K(n) \equiv 2 \pmod 3$. □

2.3 $K(n) \pmod 5$

Theorem 2.8. *$ord_5(K(n)) = 0$ precisely when $n = 1$ or n is one less than or one more than a sum of positive powers of 5 each of which is allowed to occur at most twice.*

Proof. We can restate the theorem by saying that $ord_5(K(n)) = 0$ precisely when $n = 1$ or, for $n > 1$, the base 5 representation of n has rightmost digit 1, and the remaining digits are either 2,1 or 0, or, for $n > 1$, the base 5 representation of n has a string of 4's as its rightmost digits, and the remaining digits are either 2, 1 or 0 except that the digit just preceding the string of 4's is not allowed to be 2. It is straightforward to check that in any of these cases, the least nonnegative residue of n modulo 5^k is either $5^k - 1$ or is between 1 and $\frac{5^k-1}{2} - 1$ (note that the base 5 representation of $\frac{5^k-1}{2}$ consists of all 2's). Thus, $c_{5,k}(n) = 0$ for all k and therefore $ord_5(K(n)) = 0$ for such n.

Conversely, suppose that $ord_5(K(n)) = 0$. Then $c_{5,k}(n) = 0$ for all k. Thus, the least nonnegative residue of n modulo 5^k, i.e. the last k digits of the base 5 representation of n, must either consist of all 4's or must be between 1 and $\frac{5^k-1}{2} - 1$ inclusive. The only numbers that satisfy that criterion are those numbers described. □

Theorem 2.9. *For every nonnegative integer k, there are infinitely many n for which $ord_5(K(n)) = k$.*

Proof. If $k = 0$, we simply refer to Theorem 2.8. Now suppose $k > 0$, and consider $n = 5^k$. Then for $1 \leq r \leq k$, the least nonnegative residue of $n \pmod{5^r}$ is 0. Therefore $c_{5,r}(n) = 1$, and for $r > k$, $c_{5,r}(n) = 0$ since $n < 5^r - 1$. Thus, we have $ord_5(K(n)) = k$. Furthermore, if we now consider $n = 5^j + 5^k$ where $j > k$, we still have $c_{5,r}(n) = 0$ for $r > k$. Thus, in each of these cases $ord_5(K(n)) = k$. □

Next we wish to consider $K(n)$ modulo 5.

Theorem 2.10. *$K(n)$ is never congruent to 1 or 4 mod 5.*

Proof. We first note that, by Theorem 2.8, if $n \equiv 0, 2, \text{ or } 3 \pmod 5$, then $K(n) \equiv 0 \pmod 5$. Thus, we only consider values $n \equiv 1 \text{ or } 4 \pmod 5$.

We now divide into cases.

If $n \equiv 1 \pmod 5$, then by (4), we have

$$K(n) \equiv f_5\left(\binom{2n}{n+1}\right)^2 \frac{f_5\left((2n+1)\right) \cdot 2}{f_5\left(n\right) f_5\left((n+2)\right)} \equiv \pm\frac{3 \cdot 2}{1 \cdot 3} \equiv \pm 2 \pmod 5.$$

If $n \equiv 4 \pmod 5$, then

$$K(n) \equiv f_5\left(\binom{2n}{n+1}\right)^2 \frac{f_5\left((2n+1)\right) \cdot 2}{f_5\left(n\right) f_5\left((n+2)\right)} \equiv \pm\frac{4 \cdot 2}{4 \cdot 1} \equiv \pm 2 \pmod 5.$$

Thus, in each of these cases, $K(n) \equiv \pm 2 \pmod 5$. In other words, $K(n)$ is never congruent to 1 or 4 mod 5. □

3 Concluding Thoughts

We conclude by noting the desire to see knot–theoretic proofs of Theorems 2.7 and 2.10. Moreover, we wonder whether there is some significance to the fact that Theorems 2.7 and 2.10 are clearly related to the quadratic residues modulo 3 and 5 (respectively).

4 Acknowledgements

The authors gratefully acknowledge the referee of the paper for valuable suggestions.

References

[1] D. D. Frey and J. A. Sellers, Prime Power Divisors of the Number of $n \times n$ Alternating Sign Matrices, *Ars Combinatoria*, to appear.

[2] J. L. Jacobsen and P. Zinn–Justin, A Transfer Matrix Approach to the Enumeration of Knots, *Journal of Knot Theory and its Ramifications*, **11** (2002), 739–758.

[3] C. T. Long, "Elementary Introduction to Number Theory", 3rd edition, Waveland Press, Inc., Prospect Heights, IL, 1995.