THE ORDER OF A PERFECT k-SHUFFLE

Robert W. Packard
Department of Mathematics, Northern Arizona University, Flagstaff, AZ 86011

Erik S. Packard
Department of Mathematics, Texas Tech University, Lubbock, TX 79407

(*Submitted June 1992*)

When you break open a new deck of 52 cards you might wonder how many times you would have to "perfectly" shuffle the cards to return the deck to its original configuration. Our curiosity about this led ultimately to the contents of this paper. By a perfect shuffle here we mean separate the cards into two piles of 26 cards each, then reorder the cards by alternately taking a card from the first pile then one from the other. We call this a perfect 2-shuffle, which is the same as the out Faro shuffle mentioned in [2], [4], [5], [6], and [9]. The answer to the question above is 8, i.e., the order of a perfect 2-shuffle on 52 cards is 8.

As in [4] and [7], we will generalize the idea of a 2-shuffle to that of a k-shuffle. We will then proceed to the main goal of this paper, which is to produce necessary and sufficient conditions under which the order is large in comparison with the number of cards. We will also give a lower bound for the order. The results, embodied in Theorems 1, 4, and 6, imply certain properties of the graph obtained when one plots order versus deck size. This will, in turn, shed light on question 5 in [9], which asks for reasons for the appearance of such a graph. See also the figures accompanying this paper. In these graphs, it appears as if sets of points line up in straight lines all passing through a common point with more irregularly positioned points above or below these lines. Our concluding remarks indicate how this behavior and much more can be explained. Following these remarks will be found a short description of how we discovered the results communicated in this paper.

Definition 1: Let k and s be integers greater than 1. Take $n = ks$ cards numbered in order 1 through n. Place the cards in k piles of s each, the first pile containing, in order, cards 1 through s, the second pile containing cards $s + 1$ through $2s$, etc., with the last pile containing cards $(k-1)s+1$ through ks. Now, in order, pick up the first card in each pile, then the second, etc., ending with the last card in each pile. The result we call a "perfect k-shuffle." The order of this k-shuffle, $d_k(n)$, will be the minimum number of times the k-shuffle needs to be repeated to return the cards to their original configuration. The order of a card will be the minimum number of k-shuffles needed to return that card to its original position.

In [4] Medvedoff and Morrison show that $d_k(n)$ is the order of k (mod$(n-1)$), i.e., the minimum positive integer r such that $k^r \equiv 1$ (mod$(n-1)$). The key to the proof is in demonstrating that if the cards are numbered 0 through $n-1$, rather than 1 through n, then the card numbered $x \neq 0$ or $n-1$, i.e., an *interior* card, ends up after one perfect k-shuffle in the position formerly occupied by the card numbered kx (mod$(n-1)$). The first and last cards obviously remain unchanged. The fact that $d_k(n) \leq n-2$ is easily deduced from properties of the Euler ϕ-function. It is also not hard to see that the order of a card divides $d_k(n)$ and is the length of the cycle that it is in when the k-shuffle is represented as a member of the permutation group on n objects. It is also true that $d_k(n)$ is the length of the longest cycle and card 2 will always be in such a cycle.

As an example, consider the case $k = 3$ and $s = 5$. The three piles

$$\begin{array}{ccc} 1 & 6 & 11 \\ 2 & 7 & 12 \\ 3 & 8 & 13 \\ 4 & 9 & 14 \\ 5 & 10 & 15 \end{array} \qquad \text{become} \qquad \begin{array}{ccc} 1 & 12 & 9 \\ 6 & 3 & 14 \\ 11 & 8 & 5 \\ 2 & 13 & 10 \\ 7 & 4 & 15 \end{array}$$

after one 3-shuffle. The permutation representation is

$$(1)(2, 4, 10, 14, 12, 6)(8)(3, 7, 5, 13, 9, 11)(15)$$

and $d_3(15) = 6$.

We now produce the promised lower bound for $d_k(n)$. This lower bound is related to Theorem 2 on page 9 in [4].

Theorem 1 If $n = k^t$, then $d_k(n) = t$. Furthermore, if $k^t < n < k^{t+1}$, then $d_k(n) > t+1$. Hence, $d_k(n) = \log_k(n)$ if $n = k^t$ and $d_k(n) > \log_k(n) + 1$ if $k^t < n < k^{t+1}$.

Proof: If $n = k^t$, then $k^t \equiv 1 \pmod{n-1}$ and $k^r \equiv 1 \pmod{n-1}$ with $r < t$ is not possible since $k^r - 1 < n - 1$. So, $d_k(n) = t$. If $n > k^t$, then $u \le t$ implies $k^u - 1 \le k^t - 1 < n - 1$ and $k^u \not\equiv 1 \pmod{n-1}$. Thus, $d_k(n) > t$. Assume $d_k(n) = t+1$ for $k^t < n < k^{t+1}$. Then $k^{t+1} - 1 = m(n-1)$ for some $m > 1$. Then $k^{t+1} = mks - (m-1)$, so that $k|(m-1)$, $k \le m-1$, $k < m$. We also have

$$n = \frac{k^{t+1}-1}{m} + 1 < \frac{k^{t+1}-1}{k} + 1 = k^t + \frac{k-1}{k} < k^t + 1,$$

a contradiction. Thus, $d_k(n) > t+1$ for $k^t < n < k^{t+1}$.

The fact that $d_2(22) = 6$ and $d_3(21) = 4$ shows that $d_k(n) = t+2$ is possible when $k^t < n < k^{t+1}$.

Let us now define what we mean by $d_k(n)$ being large in comparison with n.

Definition 2: If $d_k(n) = n-2$, we say that the k-shuffle is full. If $d_k(n) > (n-2)/2$, we say that it is over half full.

We are interested in circumstances under which the k-shuffle is over half full. The following two theorems follow from the fact that $d_k(n)$ is the order of $k \pmod{n-1}$, the proof of that fact, and elementary number theoretic ideas.

Theorem 2: If the k-shuffle is full, then $p = n-1$ is prime.

Theorem 3: If $p = n-1$ is prime, then all interior cards have order $d_k(n) = (n-2)/c$, where c is the largest positive integer such that $c|(n-2)$ and there is an x such that $x^c \equiv k \pmod{p}$, i.e., c is the largest divisor of $n-2$ such that k is a c-residue modulo p.

The fact that $d_5(110) = 27$ shows that the converse of Theorem 2 does not hold. On the other hand, Theorem 3 is illustrated by the fact that the 108 interior cards appear in four cycles of 27 each, i.e., each interior card has order 27. Furthermore, $28^4 \equiv 5 \pmod{109}$ while 5 is not a c-residue modulo 109 where $4 < c|108$. Although $3^{16} \equiv 5 \pmod{109}$, 16 does not divide 108.

The fact that $d_2(2048) = 11$ and $2047 = 23 \cdot 89$ shows that all interior cards can have the same order without $n-1$ being prime. On the other hand, the fact that $d_2(10) = 6$ and cards 4 and 7 have order 2 shows that, in general, not all interior cards have the same order.

Theorems 2 and 3 together yield the following necessary and sufficient conditions for a k-shuffle to be full. Recall that a is a primitive root of m if $(a, m) = 1$ and a is of order $\phi(m)$ modulo m, where ϕ is the Euler ϕ-function.

Theorem 4: A perfect k-shuffle is full, i.e., $d_k(n) = n-2$ if and only if $p = n-1$ is a prime (odd) and k is a primitive root of p.

Since $d_2(20) = 18$, for example, 2 must be a primitive root of 19. From Theorem 3, we see further that, if $p = n-1$ is prime and k is not a primitive root of p, then $d_k(n) \leq (n-2)/2$ and the k-shuffle is not over half full.

It is interesting that, for some k, there can be no full shuffles. Using quadratic reciprocity, we can show that, if $k \equiv 0$ or 1 (mod 4) and $n-1$ is prime, then k is a quadratic residue modulo p. Thus, Theorems 2 and 3 show lack of fullness. See also Lemma 2 on page 5 of [4]. A computer check suggests the conjecture that, if $k \equiv 2$ or 3 (mod 4), then there is an $n = ks$ such that $d_k(n) = n-2$, i.e., k and s are primitive roots of a prime $p = n-1$. This is similar to Artin's conjecture that, if k is a positive integer that is not a perfect square, then k is a primitive root of infinitely many primes (see [8], p. 81). Not surprisingly, we have made no headway in proving or disproving our conjecture. We can rule out certain cases. Again, using quadratic reciprocity, we can show that, if $k = 4j+2$ and

$$n-1 = ks-1 = p \equiv \pm 1 \pmod 8 \text{ and } j \text{ or } s \text{ is even or}$$
$$n-1 = ks-1 = p \equiv \pm 3 \pmod 8 \text{ and } j \text{ and } s \text{ are odd,}$$

then k is a quadratic residue modulo p and the k-shuffle is not full. Examples include

$$d_{10}(80) = 13, \; d_{14}(168) = 83, \; d_{14}(182) = 45.$$

Furthermore, if $k = 4j+3$, $n-1 = ks-1 = p$, and $s = 4w$, the k-shuffle cannot be full. An example is $d_{11}(44) = 7$. But note that $d_2(44) = 14$, where $20^3 \equiv 2$ (mod 43) and 2 is not a c-residue modulo 43 for $3 < c|42$, is not covered by any of the above cases, all of which employ quadratic residues, while this example involves a *cubic* residue.

We now turn to necessary and sufficient conditions for which a k-shuffle is over half full but not full. From the preceding, it is clear that $n-1$ cannot be prime. We can, in fact, say much more about necessary conditions.

Theorem 5: If $\frac{n-2}{2} < d_k(n) < n-2$, then $n-1 = p^a$, where p is an odd prime and $a \geq 2$.

Before we prove this theorem, we need the following easily verified lemma.

Lemma 1: If k is odd and $a \geq 3$, then $k^{2^{a-2}} \equiv 1 \pmod{2^a}$.

A proof of Theorem 5 is as follows: Suppose $n-1 = hg = ks-1$ with $(h, g) = 1$. In the case in which $h, g > 2$, we have $\phi(h), \phi(g)$ even and

$$\left(k^{\frac{\phi(h)}{2}}\right)^{\phi(g)} \equiv 1 \pmod g, \quad \left(k^{\frac{\phi(g)}{2}}\right)^{\phi(h)} \equiv 1 \pmod h,$$

$$k^{\frac{\phi(h)\phi(g)}{2}} \equiv 1 \pmod{hg} \equiv 1 \pmod{n-1}$$

and

$$d_k(n) \le \frac{\phi(h)\phi(g)}{2} \le \frac{(h-1)(g-1)}{2} = \frac{hg-h-g+1}{2} < \frac{hg-5}{2} = \frac{n-6}{2} < \frac{n-2}{2}.$$

In the case $h=2$, $g>2$, we have k odd,

$$k^{\phi(g)} \equiv 1 \pmod{g}, \quad k^{\phi(g)} \equiv 1 \pmod{h} \quad k^{\phi(g)} \equiv 1 \pmod{hg}$$

and

$$\phi(g) \le g-1 < \frac{n-1}{2},$$

so that

$$d_k(n) \le \phi(g) < \frac{n-1}{2} - \frac{1}{2} = \frac{n-2}{2}.$$

Thus, $n-1=p^a$, where p is a prime and $a \ge 2$. Since $p=a=2$ is impossible, consider $p=2$, $a \ge 3$. Then $n=ks$ is odd, k is odd, and Lemma 1 shows that

$$d_k(n) \le 2^{a-2} = \frac{2^a - 2^{a-1}}{2} < \frac{2^a-1}{2} = \frac{n-2}{2}.$$

Thus, p is odd.

To produce sufficient conditions we utilize a lemma (see [8], pp. 98-99).

Lemma 2: Let p be a prime. Then k is a primitive root of p^2 if and only if k is a primitive root of p^a for all $a \ge 1$.

We can now state and prove the theorem we have been aiming for.

Theorem 6: A perfect k-shuffle is over half full, but not full, i.e., $\frac{n-2}{2} < d_k(n) < n-2$, if and only if $n-1=p^a$, where p is an odd prime, $a \ge 2$, and k is a primitive root of p^2.

Proof: Assume $\frac{n-2}{2} < d_k(n) < n-2$. By Theorem 5, $n-1=p^a$, where p is an odd prime and $a \ge 2$ is necessary. If k is not a primitive root of p^2 then, by Lemma 2, k is not a primitive root of p^a. Thus,

$$d_k(n) = d_k(p^a+1) \le \frac{(p-1)p^{a-1}}{2} = \frac{p^a - p^{a-1}}{2} \le \frac{p^a+1-4}{2} = \frac{n-4}{2} < \frac{n-2}{2}.$$

Thus, k must be a primitive root of p^2.

Conversely, assume that $n-1=p^a$, where p is an odd prime and $a \ge 2$ and k is a primitive root of p^2. Then, by Lemma 2, k is a primitive root of p^a. Thus,

$$d_k(n) = d_k(p^a+1) = (p-1)p^{a-1} > (p-1)\left(p^{a-1} - \frac{1}{p}\right) = \frac{p-1}{p}(p^a-1) = \frac{p-1}{p}(n-2).$$

Since $p \ge 3$, $\frac{p-1}{p} \ge \frac{2}{3} > \frac{1}{2}$, and we are done.

We can draw the following interesting facts from the proof of Theorem 6.

Corollary 1: A k-shuffle is over half full if and only if it is over two-thirds full, i.e.,

$$d_k(n) > \frac{n-2}{2} \text{ if and only if } d_k(n) > \frac{2}{3}(n-2).$$

Furthermore, if the conditions of Theorem 6 hold and $d_k(n) = m(n-2)$, then m increases to 1 as p increases and decreases to $\frac{p-1}{p}$ as a increases.

Before we illustrate Theorem 6, note the following, the proofs of which we leave as a challenge to the reader.

Lemma 3: Let p be prime. If the order of k (mod p^j) = b, then the order of k (mod p^{j+1}) = b or bp and in the latter case the order of k (mod p^r) $= bp^{r-j}$ for all $r \geq j$.

Lemma 4: Let p be prime. If $p^t \equiv 1 \pmod{k}$ and $k|(p^j+1)$, then $k|p^{tr+j}+1$ for all $r \geq 0$.

Lemma 4 is useful in generating sequences of k-shuffles.

Consider the following six examples, each with a slightly different flavor. Notice the relevance of Corollary 1 and Lemmas 3 and 4.

(1) The order of 2 (mod 3^2) = $2 \cdot 3$. Thus, $d_2(3^a+1) = 2 \cdot 3^{a-1}$. Thus, a 2-shuffle on 3^a+1 cards is over half full, over 2/3 full in fact. It is full if $a = 1$, not full if $a \geq 2$. As a increases, the ratio decreases to 2/3.

(2) The order of 2 (mod 7) = 3 and the order of 2 (mod 7^2) = $3 \cdot 7 \neq 6 \cdot 7$. Thus, $d_2(7^a+1) = 3 \cdot 7^{a-1}$. Thus, a 2-shuffle on 7^a+1 cards is half full if $a = 1$ and less than half full if $a \geq 2$.

(3) The order of 3 (mod 5^2) = $4 \cdot 5$. Thus, $d_3(5^{2r+1}+1) = 4 \cdot 5^{2r}$. Thus, a 3-shuffle on $5^{2r+1}+1$ cards is over half full, over 4/5 full in fact. It is full if $r = 0$, not full if $r \geq 1$. As r increases, the ratio decreases to 4/5.

(4) The order of 3 (mod 11) = 5, the order of 3 (mod 11^2) = 5 and the order of 3 (mod 11^3) = $5 \cdot 11 \neq 10 \cdot 11^2$. Thus, $d_3(11+1) = 5$ and $d_3(11^{2r+1}+1) = 5 \cdot 11^{2r-1}$ for $r \geq 1$. Thus, a 3-shuffle on 11 + 1 cards if half full and a 3-shuffle on $11^{2r+1}+1$ cards, $r \geq 1$, is less than half full, much less.

(5) The order of 5 (mod 7^2) = $6 \cdot 7$. Thus, $d_5(7^{4r+2}+1) = 6 \cdot 7^{4r+1}$ for $r \geq 0$. Thus, a 5-shuffle on $7^{4r+2}+1$ cards is over half full, over 6/7 full in fact, with the ratio decreasing to 6/7 as r increases.

(6) The order of 10 (mod 487) = 486, and the order of 10 (mod 487^2) = $486 \neq 486 \cdot 487$. Thus, a 10-shuffle on $487^{4r+2}+1$ cards where $r \geq 0$ is less than half full, much less.

Example (6) was found on page 102 in [8] and shows that k a primitive root of p^2 in Theorem 6, cannot be replaced by k a primitive root of p.

Remarks: If one were to graph the function $y = d_k(n)$, k a constant, plotting y versus n, every time $n = p+1$, p a prime, by Theorems 3 and 4 the points would lie on one of the lines $y = \frac{n-2}{c}$ where $c|n-2$ and $c = 1$ when k is a primitive root of p. See Figure 1 for $k = 2$ and recall examples (1) and (2) above. See Figure 2 for $k = 3$ and recall examples (3) and (4) above. More irregularly positioned points above or below and sometimes on the lines $y = \frac{n-2}{c}$ are supplied examples (1) and (2) above. See Figure 2 for $k = 3$ and recall examples (3) and (4) above. More irregularly positioned points above or below and sometimes on the lines $y = \frac{n-2}{c}$ are supplied when $n - 1$ is composite. In order for points to lie between $y = n-2$ and $y = \frac{n-2}{2}$, n would have to be a $p^a + 1$ with p an odd prime, $a \geq 2$, and k a primitive root of p^2. This is rare and, in fact, sometimes cannot happen, for example, when k is a perfect square. See Figure 3 for $k = 4$. Clearly, no point can be above $y = n-2$. If $k \equiv 0$ or 1 (mod 4), no point will lie on $y = n-2$. See Figure 3 again for $k = 4$. See Figure 4 for $k = 5$ and recall example (5) above. In Figure 1 those points above $y = \frac{n-2}{2}$ are all above $y = \frac{2}{3}(n-2)$ and those near $y = n-2$ are due to large p. In Figure 2 those points above $y = \frac{n-2}{2}$ are all above $y = \frac{4}{5}(n-2)$. In Figure 3 those points just below $y = \frac{n-2}{2}$ are all above $y = \frac{n-2}{3}$. In Figure 4 those points above $y = \frac{n-2}{2}$ are all above $y = \frac{2}{3}(n-2)$ and those near $y = n-2$ are due to large p. By Theorem 1 all points are on or above $y = \log_k(n)$.

We thus have at least a partial explanation for the appearance of the graph in Figure 1 ([9], p. 145) which is for in-shuffles with $k = 2$ but is similar to a graph for out-shuffles talked about in this paper. Since the order of an in-shuffle on n cards is the order of k (mod(n + 1)) as opposed to the order of k (mod(n – 1)) for the order of an out-shuffle on n cards (see [4], p. 6), the lines in Figure 1 ([9], p. 145) are $y = n/c$. In fact that graph is just a translation of the graph in Figure 1 of this paper.

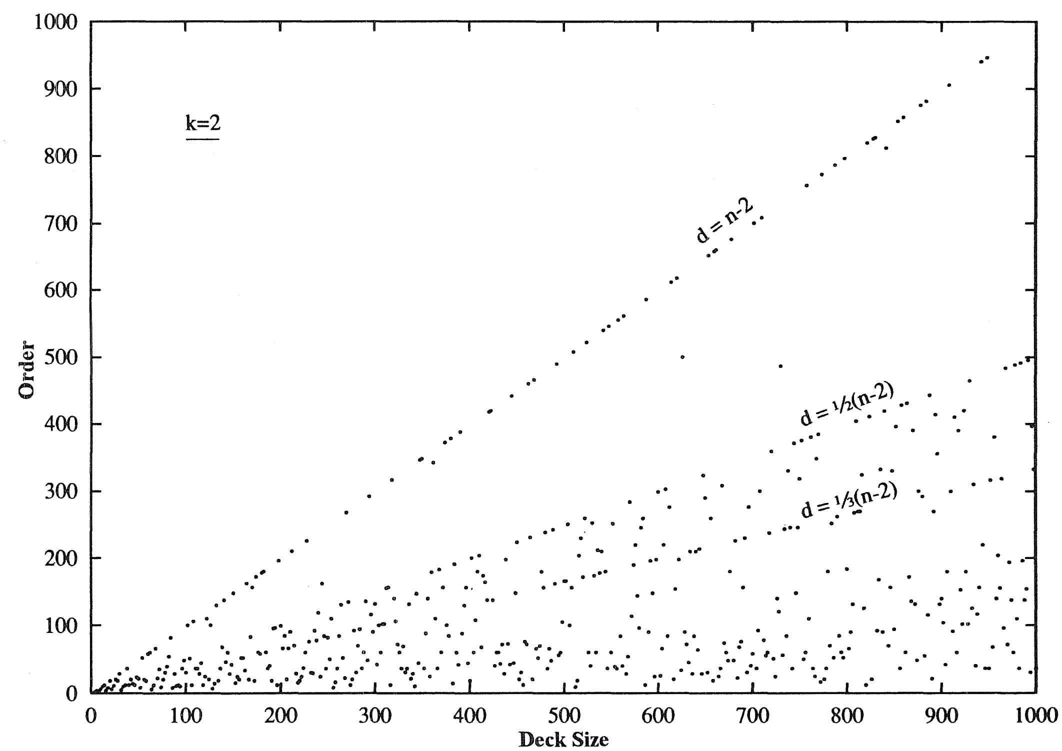

FIGURE 1. Graph of Order vs Deck Size, $k = 2$

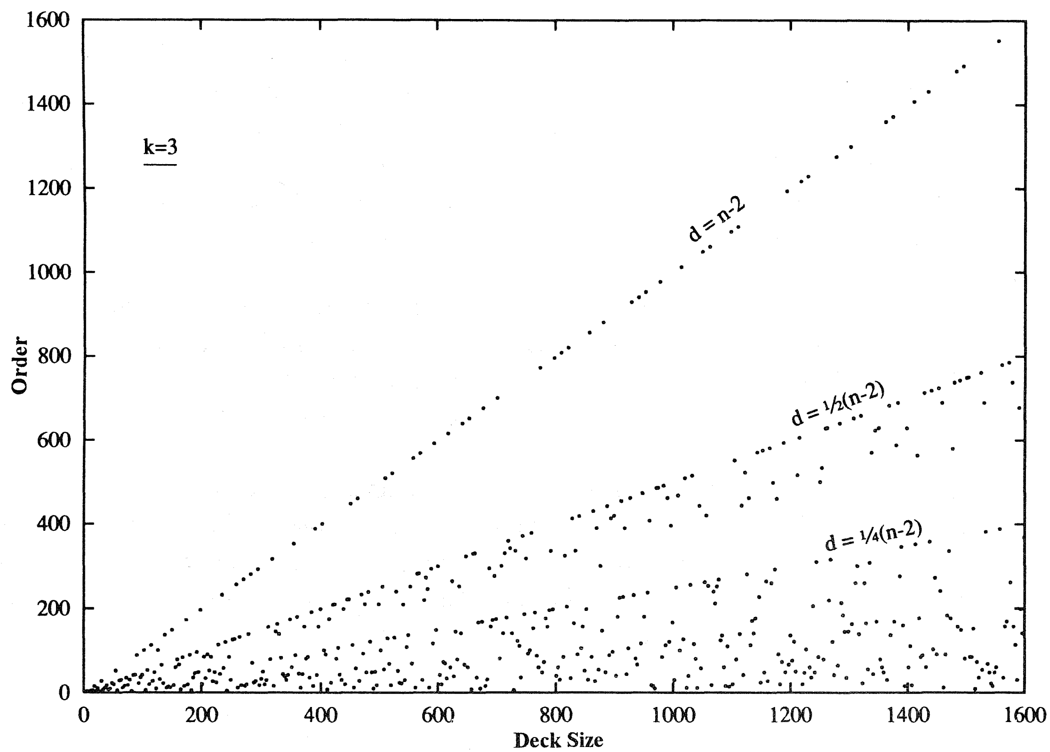

FIGURE 2. Graph of Order vs Deck Size, $k = 3$

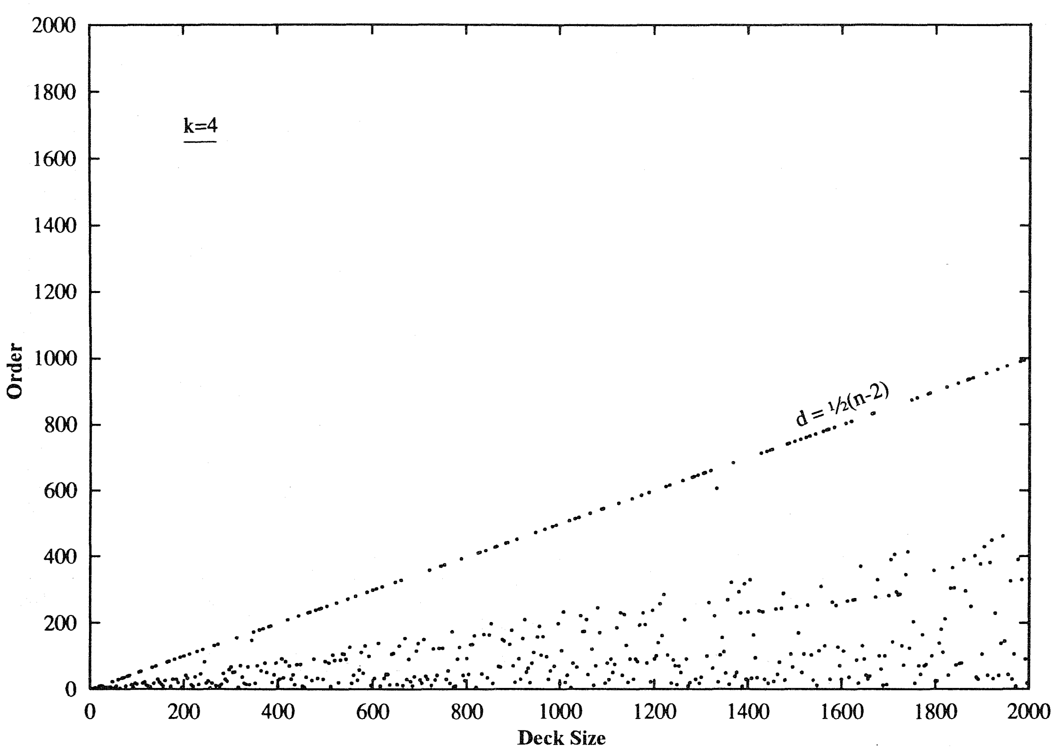

FIGURE 3. Graph of Order vs Deck Size, $k = 4$

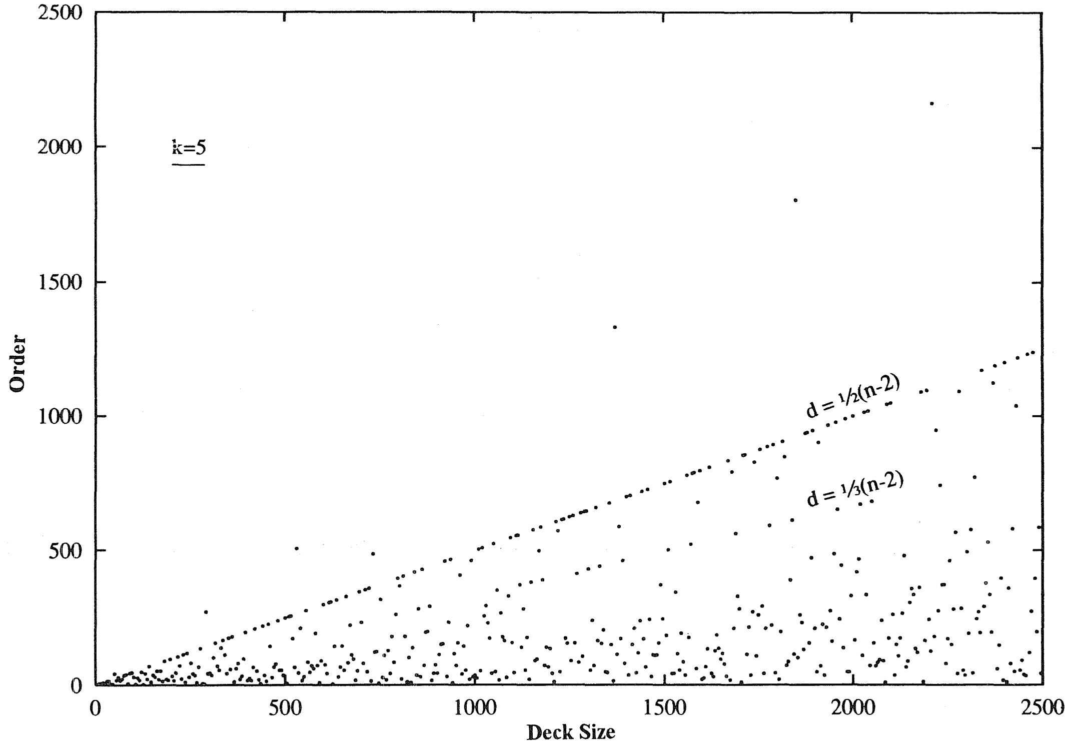

FIGURE 4. Graph of Order vs Deck Size, k = 5

DISCOVERY

After our initial curiosity was aroused, we wrote out a few shuffle permutations by hand for small n. It was not long before we had discovered and proved correct the formula for $d_k(n)$. It was a shock to later see this as Proposition 1 in [4]. A simple program in BASIC produced printouts of $d_k(n)$ using a PC. When we saw what ideas seemed to play significant rules, modifications in the program checked $n-1$ for being prime, $d_k(n)$ for being $n-2$, and $d_k(n)$ for dividing $n-2$. Essentially every result in this paper represents the successful justification of conjectures suggested by the printouts. Early success with techniques from elementary number theory prompted us to continue in that direction.

ACKNOWLEDGMENTS

We are grateful to Dr. William C. Schulz of the Northern Arizona University Department of Mathematics whose computer expertise facilitated the production of the figures in this paper. Dr. Schulz rewrote the code for $d_k(n)$ in C and ran it on a SUN SPARCstation 2. Output from the C program was run into the GNUPLOT plotting program, the POSTSCRIPT output of which was adjusted and sent to a laser printer for final copy. Thanks are also due to two other members of the same department, Dr. Everett L. Walter for his assistance in programming and Dr. Stephen E. Wilson for his helpful observations.

REFERENCES

1. William W. Adams & Larry Joel Goldstein. *Introduction to Number Theory.* Englewood Cliffs, NJ: Prentice-Hall, Inc., 1976.
2. Persi Dianconis, R. L. Graham, & William M. Kantor. "The Mathematics of Perfect Shuffles." *Advances in Appl. Math.* **4** (1983):175-93.
3. Gina Kilata. "Perfect Shuffles and Their Relation to Math." *Science* **216** (1982):505-06.
4. Steve Medvedoff & Kent Morrison. "Groups of Perfect Shuffles." *Math. Magazine* **60.1** (1987):3-14.
5. S. Brent Morris. "The Basic Mathematics of the Faro Shuffle." *Pi Mu Epsilon Journal* **6** (1975):85-92.
6. S. Brent Morris. "Faro Shuffling and Card Placement." *J. Recreat. Math.* **8.1** (1975):1-7.
7. S. Brent Morris Robert E. Hartwig. "The Generalized Faro Shuffle." *Discrete Math.* **15** (1976):333-46.
8. Daniel Shanks. *Solved and Unsolved Problems in Number Theory.* Washington, D.C.: Spartan Books, 1962.
9. "Student Research Projects," ed. Irl C. Bivens. *The College Mathematics Journal* **22.2** (1991):144-47.

AMS Classification Numbers: 10A10