NUMBER-THEORETIC ANALYSIS AND EXTENSIONS OF "THE MOST COMPLICATED AND FANTASTIC CARD TRICK EVER INVENTED"

KURT EISEMANN
Computer Center, San Diego State University, San Diego, CA 92182

1. Introduction. This paper presents a mathematical analysis, simplification, and extensions of a card trick based on number theory, and involving congruences, power residues, inverse permutations, relative primality, associated integers, and primitive roots, as well as mystery and surprise. The card trick, described by the philosopher and mathematician Charles Sanders Peirce [**1**], has been resurrected by Martin Gardner [**2**], who characterizes it as "surely the most complicated and fantastic card trick ever invented," stating that "for a teacher who wants to motivate student interest in congruence arithmetic, it is superb." A mathematical analysis shows it to be based on number-theoretic properties; it should therefore be of particular interest to mathematicians.

We shall first describe the performer's manipulations, incorporating a significant simplification, followed by mathematical validation, an extension, and generalization.

2. Initial set-up. The Ace, Jack, Queen, and King of a deck will be designated respectively as the face values 1, 11, 12 and 13. For any deck facing upward, the sequence of its cards is enumerated by starting at the bottom of the deck and proceeding towards the top. All dealings take place by holding a deck face down, turning over its top card, and placing it on the table face up.

From a deck of cards, select the spades from Ace through Queen (12 cards), to be called the "black" deck, and the hearts from Ace through King (13 cards), the "red" deck. Sequence the black deck so that the face values of successive cards represent the successive power residues modulo 13 of its primitive root 2. Cut the deck arbitrarily, yielding, let us say, the sequence $\{b_n\}$ shown in Fig. 1. Next, sequence the red deck as follows: Because the Ace of spades is in position number 9, place the 9 of hearts as the first card of the red deck. As the 2 of spades is in position number 10, place the 10 of hearts as the second card of the red deck. Proceed similarly for each successive face value of spades. At the end, append the King of hearts to the red deck. The sequence of spades thus yields a corresponding deck of hearts as shown in Fig. 1.

Black deck:	$b_n = 3$	6	12	11	9	5	10	7	1	2	4	8	
Position numbers	$n = 1$	2	3	4	5	6	7	8	9	10	11	12	
Red deck:	$r_n = 9$	10	1	11	6	2	8	12	5	7	4	3	13

FIG. 1. Initial corresponding decks.

3. Reciprocity. The two card decks have a pointer property that is mutual: For convenient reference, deal the deck of spades face down from left to right into rows of 5, 5, 2 cards, respectively. Ask a spectator to name any card of *spades*; say it is the 4. In the deck of *hearts*,

Kurt Eisemann, born in Nuremberg, escaped the German persecutions. Unable to afford the cost of high school, he worked full time from age 14 and after work taught himself high school and advanced college math, physics, engineering, etc. At 18 he passed the London University external matriculation exams with honors. He came to the U.S. at age 24. Albert Einstein, on learning of his passion for mathematics and autodidactics, arranged through Jekuthiel Ginsburg (editor of *Scripta Mathematica*) for Eisemann's acceptance and a scholarship at Yeshiva University, despite the lack of high school. Einstein had a friend finance basic subsistence during studies. Yeshiva University awarded Eisemann a B.A. summa cum laude after only two years. He earned his M.S. from M.I.T. (with scholarships) and Ph.D. from Harvard, both in Applied Mathematics. Publications are in linear programming, operations research, numerical analysis, and applied math. He enjoys constructing personalized magic squares, simplifying algorithms for Rubik's Revenge 4th order cube, and Charlie Chaplin.

count to the 4th card and show it to be the Jack (11). This indicates that the desired 4 of spades is the 11th card in the black deck. Show the audience that this is true, and repeat for other face values named by the audience. Similarly ask the audience to name any face value of *hearts*; say it is the 2. The second card of the deck of *spades*, which is a 6, indicates that the desired 2 of hearts is the 6th card in the red deck.

Before demonstrating the reciprocity property of the two decks, however, first apply the quasi-randomization described in the next section.

4. Red k-shuffle. Let the audience cut the red deck (into two parts, reassembled in reverse order) an arbitrary number of times, and then name an arbitrary positive integer k (< 13), say $k = 5$. From the red deck, deal k cards from left to right so as to form the bottom cards of k heaps. Continue dealing the remainder of the deck onto the k heaps by sequentially sweeping from left to right, keeping visible the upper parts of covered cards. Fig. 2 illustrates the result for the deck from Fig. 1.

8	12	5	7	4
3	13	9	10	1
11	6	2		

FIG. 2. The red deck, cut so as to start with face value 8, dealt into $k = 5$ heaps.

The heaps, arranged in vertical columns of overlapping cards, must now be carefully assembled in a particular manner: Counting heaps left to right from 1 to k (here, 5), suppose the last heart fell onto heap number z ($= 3$ in Fig. 2). Let a member of the audience point to an arbitrary heap, say number i_1. Starting at the designated heap i_1, pick up the entire heap, count heaps cyclically z positions towards the right, reaching, say, position number i_2, and place all cards from your hand on top of heap i_2. Remember that the count must NOT be i_1 positions, but z positions. Always counting z heap position numbers (NOT *remaining* heaps) towards the right, start from position i_2 and repeat the procedure, continuing until all heaps have been consolidated into a single deck. While accuracy in identifying the proper sequence of heaps is critical for success, the selection should be made nonchalantly and appear to randomize. At the end, cut once so as to bring the King to the end of the deck (to the top when the deck is held face up), ostensibly "because the King has no counterpart in the black deck." This constitutes our new, "shuffled" red deck, to be designated as the sequence $\{R_n\}$. See the illustration in Fig. 3 below.

The foregoing procedure will be termed a "(red) *k-shuffle*." Show to the audience that it radically rearranges the sequence of cards. We shall see later that $\{R_n\}$ is independent of the cuts applied to the red deck and of the choice of i_1.

When the last card falls nearer the rightmost heap, it is convenient to apply instead an equivalent, alternative method of assembly that is easier for this case: Count position numbers cyclically towards the *left*, beginning with the label 0 (NOT 1) for the rightmost heap. For Fig. 2, this alternative method yields $z = 2$ and heaps are accumulated by successive placements upon every zth heap position counted cyclically towards the *left*. The final result is the same as before.

The k-shuffle of the red deck requires a corresponding manipulation of the black deck that is surprisingly simple: Determine the new position number n of the Ace of hearts, then inconspicuously cut the black deck so that face value n occupies the first position. Alternatively, peek at the first red card R_1 ($= 6$ here); pick up the black deck and, reviewing it, inconspicuously cut it so that its Ace occupies position number R_1 ($= 6$). Denote the resulting sequence of spades as $\{B_n\}$ —see Fig. 3.

Black deck:	$B_n =$	11	9	5	10	7	1	2	4	8	3	6	12	
Red deck:	$R_n =$	6	7	10	8	3	11	5	9	2	4	1	12	13

FIG. 3. Pair of decks after a red 5-shuffle.

Point out to the audience that the red cards have been cut, rearranged into k piles, assembled, cut again, and that the number of heaps (k) and starting point for reassembly (i_1) have been chosen *by the audience*. Yet, reciprocity is now seen to hold between the new sequence of hearts and the deck of spades, and is demonstrated, for any number of black or red cards, to the surprise of the audience.

To heighten the effect, perform two or three k-shuffles, each with a different k, before demonstrating the preservation of reciprocity. Thus with the red deck, alternate cuts by the audience and k-shuffles (various k). Apply the performer's single cut of each deck only once, at the end. No matter how often the red deck is cut and k-shuffled, reciprocity between the rearranged red and the black deck persists, seemingly by sheer miracle.

5. Mathematical validation.

a. *Reciprocity*. For a black deck sequenced arbitrarily, consider a corresponding red deck prepared as described in Section 2. Thus if, in the black deck, the face value n appears in position number i, so that $b_i = n$, the red deck correspondingly shows in position n the face value i by construction, so that $r_n = i$. Conversely, if we start with the red deck ($r_n = i$), then the black deck must correspondingly show $b_i = n$. The indicator relationship must therefore necessarily be mutual.

A somewhat deeper proof of reciprocity may be obtained by considering permutations: Let b denote the permutation of the sequence $\{b_n\}$ into the sequence of successive integers $n = 1$ to 12, i.e.,

$$\underline{b} = (b \to n) = \binom{b}{n} = \begin{pmatrix} 3 & 6 & 12 & 11 & 9 & 5 & 10 & 7 & 1 & 2 & 4 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{pmatrix}.$$

Ignoring r_{13}, similarly for the sequence $\{r_n\}$ define $\underline{r} = (r \to n) = \binom{r}{n}$, and $\underline{x} = (n \to r) = \binom{n}{r}$. By construction, also $\underline{r} = (n \to b) = \binom{n}{b}$. We now find that

$$\underline{b} \cdot \underline{r} = \binom{b}{n}\binom{n}{b} = I = \binom{r}{n}\binom{n}{r} = \underline{r} \cdot \underline{x},$$

whence firstly, $\underline{r}$ and $\underline{b}$ are mutual inverses; and secondly, $\underline{x} = \underline{b}$, i.e., $\binom{n}{r} = \binom{b}{n}$. Thus in Fig. 1, *every* vertically positioned pair of numbers [such as $\binom{3}{1}$] found in rows 1 and 2 is also found in rows 2 and 3.

As the relationship between an arbitrary sequence $\{b_i\}$ and its pointers $\{r_n\}$ must necessarily be mutual, the surprising feature of the card trick does not consist in the mutuality of the indicator relationship, but rather in its *persistence* under shuffling! This astonishing permanence is due to the structure devised for the black deck.

b. *Basic formulae*. Preparation of the initial deck was specified by Peirce and by Gardner via a tedious procedure. Inspection of the result reveals it to represent a cyclic permutation of the successive powers modulo 13 of its primitive root 2. This observation formed the clue to all else.

Referring to Fig. 1, let

$f =$ the face value of the first card immediately following (cyclically) the Ace of spades (here, the primitive root f = 2).

$e =$ the number of cards lying at the end of the black deck beyond the Ace of spades (here $e = 3$).

$x(n) =$ the index of $n \bmod 13$.

By construction of the black deck, position number i is occupied by a spade with face value

(1) $$b_i = f^{i'} \pmod{13} \quad \text{where } i' = i + e \pmod{12}.$$

Equivalently, a specified face value $n = b_i$ is found in position number $i \equiv x(n) - e \pmod{12}$.

By construction of the red deck, position number n is occupied by a heart of face value

(2) $$r_n = i \equiv x(n) - e \pmod{12}.$$

c. *Red-shuffle*. We shall approach the investigation of what takes place with the deck of hearts in successive steps:

Step 1. Consider a card deck of diamonds sequenced from 1 to $p = 13$ subjected to a k-shuffle. With k heaps, the last card falls on heap z, where $p = mk + z$ (for some integer m). z will always be relatively prime to z, because any common factor would also divide p. Hence none of the cyclic counts of k position numbers will end on a vacant position until all heaps have been taken up. Heap no. i has as its bottom card the face value i, its top card $mk + i$ when $i \leqslant z$, or $(m-1)k + i$ when $i > z$. Within each heap, successive cards have the common difference k. When heap no. i is placed on top of heap no. $i + z \pmod{k}$, the difference d between the bottom card of the former and the top card of the latter is as follows:

$$\text{When } i + z > k: \quad d = i - [mk + (i + z - k)] \quad = k - p \equiv k \bmod p;$$
$$\text{When } i + z \leqslant k: \quad d = i - [(m-1)k + (i + z)] \quad = k - p \equiv k \bmod p.$$

The scheme for the formation and reassembly of heaps thus assures that successive cards will have a constant difference $k \pmod{p}$ not only *within* each heap but also *between* heaps. The k-shuffle thus amounts to considering the original card deck arranged in a circle, repeatedly counting off k positions cyclically, and extracting the cards occupying the successive kth positions. Because k is relatively prime to $p = 13$, each count of k cannot reach a vacant position but lands on a spot occupied by a card, until all p cards have been selected.

Step 2. Any number of initial cuts of the deck of diamonds, and different choices of an arbitrary heap to begin the reassembly of the heaps, merely amount to cyclical permutations of the deck, which have no effect on the substance of the procedure. Cut of the final deck so that the King is in the last position thus results in the identical sequence for all the preceding variations in execution.

Step 3. What has been described above for the deck of diamonds shows what happens with the *position numbers* of the deck of hearts; namely, all variants of the intriguing procedure yield the identical result: Transformation of the sequence $\{r_n\} = r_1, r_2, \ldots, r_{13}$ into the sequence $\{R_n\} = r_k, r_{2k}, r_{3k}, \ldots, r_{13k}$, where all subscripts are modulo 13.

d. *The red and black decks*. What changes are needed in the black deck to maintain reciprocity? Applying (2) to the new deck,

$$R_n = r_{nk} \equiv x(nk) - e \pmod{12}.$$

Use of the fundamental property of indices for primes (see e.g., [3]),

$$x(nk) \equiv x(n) + x(k) \pmod{p-1},$$

yields

$$R_n \equiv r_n + r_k + e = r_n + (R_1 + e) \pmod{12}.$$

Thus the effect of the k-shuffle is to increase (mod 12) the face value of each card of the red deck by the *same* constant!

At the outset, $r_n = i$ corresponded to $b_i = n$. For the new sequence, $R_n = j$ will require the correspondence $B_j = n$ where $j \equiv i + (R_1 + e) \pmod{12}$. This means that the original black deck is updated to correspond to the shuffled red deck by merely moving $R_1 + e \pmod{12}$ cards from the bottom of the black deck to its top! This cyclic permutation is effected in the manner described in Section 4.

From (2), the number of black cards to be moved is

$$m \equiv r_k + e \equiv x(k) \pmod{12},$$

i.e., depends only on k (for fixed f) and is independent of the starting configuration of the two decks. Moreover, if the black deck is to be updated by the movement of m cards, where m is specified, the requisite number of heaps for the corresponding k-shuffle of the red deck is given from the preceding by $k \equiv f^m \pmod{13}$.

6. Extension. An understanding of the mathematical relationships underlying Peirce's card trick allows an immediate extension: Suppose that a k-shuffle is applied not to the deck of hearts but to the deck of spades! What rearrangement will be required for the red deck to maintain reciprocity? Let us first describe the procedure, followed by mathematical validation.

Quietly note the face value of the last card of spades. Then have the audience cut the deck any number of times. Let someone pick for k one of the numbers 5, 7 or 11 (no other number will do); say $k = 5$. Apply a k-shuffle to the deck of spades. At the end, cut the deck so that the originally last card is restored to last place.

Now take a deck of diamonds with face values sequenced from 1 to 12. It is vital to remember that *the King of diamonds must be discarded at this point*. Apply a k-shuffle to the deck of diamonds, using the *same* k. Either begin reassembly with the heap that contains the last card (Queen) or cut the final deck so that the Queen occupies the last place. Now append the King of diamonds.

To illustrate, we take the decks of Fig. 3 as our new starting point (relabelling them b_n and r_n respectively). With $k = 5$, the result is shown in the first four rows of Fig. 4.

Shuffled spades:	B_n	= 7	3	5	4	11	1	6	10	8	9	2	12		
Hearts:	r_n	= 6	7	10	8	3	11	5	9	2	4	1	12	13
Position number	n	= 1	2	3	4	5	6	7	8	9	10	11	12	13
Diamonds after shuffle:	d_n	= 5	10	3	8	1	6	11	4	9	2	7	12	13
Diamonds at the end:	D_n	= 6	11	2	4	3	7	1	9	10	8	5	12	13

FIG. 4. Black 5-shuffle applied to the decks of Fig. 3.

Deal the resulting deck of diamonds into successive positions 1 to 13 from left to right, preferably face down and grouped 5 cards per row for easy reference. Now pick up the deck of *hearts* face down and deal it one card at a time. For each card, if the face value of the heart dealt is m, pick out from the table and set aside the diamond in position m face up into a single pile. The resulting deck of diamonds $\{D_n\}$, shown in Fig. 4, is our new red deck to go with the shuffled black deck. Demonstrate to the audience that despite the shuffles, reciprocity between all cards of the new black and red decks continues to hold!

The procedures of Sections 4 and 6 may be repeated any number of times, with any choices of k (for black-shuffles, from the numbers 5, 7, 11 only) without affecting the reciprocity of the black and red decks.

7. Validation of the extension. Let $f, e, x(n)$ as defined in Section 5b refer to our present starting decks of Fig. 3 (now relabelled b_n, r_n), and let $F, E, X(n)$ refer to the corresponding quantities for the new decks B_n, D_n of Fig. 4. As in Step 3 of Section 5c, the black k-shuffle amounts to rearranging the deck $b_1, b_2, \ldots, b_{12}$ to the sequence $\{B_n\} = b_k, b_{2k}, \ldots, b_{12k}$, here done with 12 cards so that the subscripts here are modulo 12. The face value of the first card immediately following (cyclically) the Ace of spades is now $F = f^k = 2^5 \equiv 6 \pmod{13}$, so that the spades now form a cyclic permutation of the successive powers mod 13 of its primitive root 6. We have $B_j = F^{j+E} = f^{k(j+E)}$ and also $B_j = b_{jk} = f^{jk+e}$, whence $kE \equiv e \pmod{12}$, and $B_j \equiv b_{12} \cdot F^j \pmod{13}$.

Let us relate the red deck R_n, required for reciprocity with B_j, to the starting deck r_n: For a fixed $n = B_j = b_{jk}$ we find from (2) and the analogous $R_n = j \equiv X(n) - E \pmod{12}$ that

$$x(n) \equiv kj + e \equiv k[X(n) - E] + e \pmod{12},$$

whence

$$r_n \equiv k \cdot R_n \pmod{12}. \tag{3}$$

Since $k^2 \equiv 1 \pmod{12}$ for $k = 1, 5, 7, 11$, the solution of (3) yields the requirement

$$R_n \equiv k \cdot r_n \pmod{12}. \tag{4}$$

The k-shuffle applied to the deck of 12 diamonds sequenced in natural order resulted in the sequence $\{d_n\} = k, 2k, \ldots, 12k$ (mod 12) (see Fig. 4). The subsequent selection from position numbers $r_1, r_2, \ldots, r_{12}$ then furnished diamonds with face values $k \cdot r_1, k \cdot r_2, \ldots$ (mod 12), i.e., precisely the sequence of values required by (4).

Note that the k-shuffle of the black deck is restricted to the values $k = 5, 7, 11$ because these are the only integers (other than the trivial 1) relatively prime to $p - 1 = 12$, a condition required for nondegeneracy of the procedure (see end of Step 1, Section 5c). It always leads to a cyclic permutation of successive power residues of one of the primitive roots $F = 2, 6, 7, 11$. A total of 48 different arrangements of the pairs of decks may thus be obtained.

8. Generalization. Generalization of the procedure to arbitrary primes p is now made obvious by the analysis above: For an arbitrary prime p, take a black deck of $p - 1$ cards arranged in an arbitrary cyclic permutation of successive power residues mod p of one of its primitive roots f, together with a correspondingly sequenced red deck of p cards. Apply k-shuffles of the red deck with arbitrary k, because every $k < p$ is relatively prime to p. Corresponding to it is a cyclic permutation of the black deck. Demonstrate the persistence of reciprocity.

If you wish to apply k-shuffles to the black deck, k must be chosen from the integers relatively prime to $p - 1$. In this case $p - 1 = km + z$ (for some integer m), and z will always be relatively prime to k, because any common factor would also be a common factor of $p - 1$ and k, contrary to the choice of k. Nondegeneracy of the black k-shuffle is therefore assured. However, an interesting complication now appears: If the black deck is k-shuffled, the auxiliary deck (diamonds) must be h-shuffled, where generally $h \neq k$. It is seen from (3) that its solution

$$R_n \equiv h \cdot r_n \pmod{12}$$

in reality requires h to satisfy $h \cdot k \equiv 1 \pmod{p-1}$, i.e., $h = k^{-1} \pmod{p-1}$. Thus h and k must be "associated integers." For practical values of p, a short table of corresponding admissible values k and h and of all relevant primitive roots is shown in Fig. 5.

Red deck: $p =$ Black deck: $p - 1 =$	11 10	13 12	17 16	23 (Hearts & Diamonds) 22 (Spades & Clubs)
k (rel.prime to $p - 1$):	1 3 7 9	1 5 7 11	1 3 5 7 9 11 13 15	1 3 5 7 9 13 15 17 19 21
$h = k^{-1}$ (mod $p - 1$):	1 7 3 9	1 5 7 11	1 11 13 7 9 3 5 15	1 15 9 19 5 17 3 13 7 21
f = prim.roots of p:	2 6 7 8	2 6 7 11	3 5 6 7 10 11 12 14	5 7 10 11 14 15 17 19 20 21

FIG. 5. Corresponding numerical values.

With k-shuffles of p red and $p - 1$ black cards, a total of $(p-1)\phi(p-1)$ different arrangements (where ϕ denotes Euler's totient function) of the pairs of decks may be obtained, all of which display reciprocity.

As is seen from Fig. 5, for a handy little deck of 10 black cards a 7-shuffle of the spades requires a 3-shuffle of the diamonds (and vice versa). This feature may be utilized to thwart the boasts of a would-be imitator: "Simplify" the above deck of 12 black cards to a deck of only 10 black cards (sequenced in successive powers mod 11 of its primitive root 2) and demonstrate by k-shuffling the red deck. Record the two final deck sequences. Then challenge him (possibly with a bet) to continue, requesting a 7-shuffle of the black deck. After he fails (because he consistently saw you use only $h = k$ with the larger deck), you can restore the two decks as recorded, do it "right" for the audience (this time with the surprise $h = 3 \neq k$), and win your bet!

References

1. Charles S. Peirce, Collected Papers, vol. 4.
2. Martin Gardner, Mathematical Games, Scientific American, July 1978.
3. Oystein Ore, Number Theory and its History, McGraw-Hill, 1948.