Math-O-Trick: Assignment

Gaurish Korpal

Prove the following statements based on your understanding of Bachet-1, Bachet-2 and Bachet-3. Definitions and useful theorems (from arithmetic) are given on the other side of this page.

1. Given a deck of $2n$ cards, s in-riffle-shuffle will restore the original order just when $2^s \equiv 1 \pmod{2n+1}$.
2. If you in-riffle-shuffle $2n$ cards $2n$ times, and $2n+1$ is prime, then cards will come back to their original order.
3. In you out-riffle-shuffle $2n$ cards $2n-2$ times, where $2n-1$ is prime, the cards will come back to their original order.
4. The number of Monge's shuffles required to restore the original order is the smallest s for which $2^s \equiv \pm 1 \pmod{4n+1}$.
5. If $4n+1$ is prime, then $2n$ Monge's shuffles of a $2n$ card deck restore the original order.
6. The number of bases (like base-2=binary, base-10=decimal, etc.) modulo a prime number p in which $1/p$ has the cycle length k is just the same as the number of fractions
$$\frac{0}{p-1}, \frac{1}{p-1}, \ldots, \frac{p-2}{p-1}$$
that have least denominator k.
7. For a permutation π of $\{1, 2, 3, \ldots, N\}$ the following four properties are equivalent:
   (a) π is a Gilbreath permutation, defined as: Fix a number between 1 and N, call it j. Deal the top j cards into a pile face-down on the table, reversing their order. Now, riffle shuffle (need not be perfect-riffle-shuffle) the j cards with the remaining $N-j$ cards.
   (b) For each j, the top j cards
   $$\{\pi(1), \pi(2), \ldots, \pi(j)\}$$
   are distinct modulo j.
   (c) For each j and k with $kj \leq N$, the j cards
   $$\{\pi((k-1)j+1), \pi((k-1)j+2), \ldots, \pi(kj)\}$$
   are distinct modulo j.
   (d) For each j, the top j cards are consecutive in $1, 2, 3, \ldots, N$.

References

[1] Conway, J. H. and Guy R. K. *The Book of Numbers.* Copernicus, Springer-Verlag: New York. 1996

[2] Diaconis P. and Graham R. *Magical Mathematics: The Mathematical Ideas That Animate Great Magic Tricks.* Princeton University Press: Princeton and Oxford. 2012

Hints:

- The symbol $a \equiv b \pmod{n}$ is read as "a is congruent to b, modulo n" and is equivalent to saying that both the integers a and b leave same remainder when divided by some integer n.
- If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then:
  - $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
  - $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$
  - $a_1 a_2 \equiv b_1 b_2 \pmod{n}$
- The symbol $\gcd(a, b) = 1$ means that the greatest common divisor of the integers a and b is 1, i.e. a and b don't have any common divisor other than 1.
- Let the prime number p be 7, then following are the different representations of $\frac{1}{7}$:

base (b)	representation	cycle length
2	0.001001001001001...	3
3	0.01021201021201...	6
4	0.021021021021021...	3
5	0.032412032412032...	6
6	0.05050505050505...	2
7	0.1	terminating
8	0.11111111111111...	1
9	0.12512512512512...	3
10	0.142857142857142...	6

  So, the cycle length is

$$\begin{array}{lll} 6 & \text{for the 2 cases when} & b \equiv 3, 5 \pmod{7} \\ 3 & \text{for the 2 cases when} & b \equiv 2, 4 \pmod{7} \\ 2 & \text{for the 1 case when} & b \equiv 6 \pmod{7} \\ 1 & \text{for the 1 case when} & b \equiv 1 \pmod{7} \end{array}$$

- Number of fractions among $\frac{0}{6}, \frac{1}{6}, \ldots, \frac{5}{6}$ with lowest denominator

$$\begin{array}{lll} 6 & \text{are the 2 fractions} & \frac{1}{6}, \frac{5}{6} \\ 3 & \text{are the 2 fractions} & \frac{1}{3}, \frac{2}{3} \\ 2 & \text{is the 1 fraction} & \frac{1}{2} \\ 1 & \text{is the 1 fraction} & \frac{0}{1} \end{array}$$

- For any positive integer $m \leq n$, the number of fractions from $\frac{0}{n}, \frac{1}{n}, \ldots, \frac{n-1}{n}$ has m as least possible denominator is given by Euler's totient function, $\phi(m)$. It's value can be calculated using the formula:

$$\phi(m) = m \times \left(1 - \frac{1}{p}\right) \times \left(1 - \frac{1}{q}\right) \times \left(1 - \frac{1}{r}\right) \times \cdots$$

  where $p, q, r, \ldots$ are the distinct prime factors of m. For example, $\phi(3) = \phi(6) = 2$ and $\phi(1) = \phi(2) = 1$.
- A group G is a finite or infinite set of elements together with a binary operation that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.
- We denote the *group* of integers modulo n under multiplication operation by $(\mathbb{Z}/n\mathbb{Z})^{\times}$ and the number of elements in this group is $\phi(n)$. For example, $(\mathbb{Z}/7\mathbb{Z})^{\times} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.
- Permutation of a finite set X is a bijective map from the set X to itself. The number of permutations of a set of cardinality n is $n! = 1 \times 2 \times \cdots \times (n-1) \times n$.
- [Fermat's little theorem] If p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p. In the notation of modular arithmetic, $a^p \equiv a \pmod{p}$. For example, if $a = 2$ and $p = 7$, $2^7 = 128$ and $128 - 2 = 7 \times 18$ is an integer multiple of 7. And if $\gcd(a, p) = 1$ then we can write $a^{p-1} \equiv 1 \pmod{p}$, which is a special case of: $a^{\phi(n)} \equiv 1 \pmod{n}$ for any integer n with $\gcd(a, n) = 1$.

Answers to Math-O-Trick Assignment

Hitesh Kumar

March 9, 2017

1. It is a simple observation that a card moves to position $2x \mod(2n+1)$ after an in-riffle-shuffle, where x is the initial position of the card in the deck of $2n$ cards. Say the original order is restored after s in-riffle-shuffles. This means, after s in-riffle-shuffles, card at position 1 is back to position 1 i.e. $2^s * 1 \equiv 1 \mod(2n+1)$. Conversely, if $2^s \equiv 1 \mod(2n+1)$ holds for some natural number s then $2^s x \equiv x \mod(2n+1)$ for all natural numbers x, which implies that the card at position x is back to its original position after s in-riffle-shuffles. Hence, s in-riffle-shuffles restore the order of $2n$ cards iff $2^s \equiv 1 \mod(2n+1)$.

2. We know that if p is a prime and a is an integer such that $\gcd(p,a) = 1$ then $a^{p-1} \equiv 1 \mod(p)$. If $2n+1$ is prime then by above theorem, $2^{2n} \equiv 1 \mod(2n+1)$ since $\gcd(2, 2n+1) = 1$ for all natural numbers n. Hence, by the result in Q.1, the claim is straightforward.

3. In the case of out-riffle-shuffle, the position of first and last cards in the deck of $2n$ cards, never changes. The $2n-2$ remaining cards behave as if an in-riffle-shuffle has been applied. So, by the result in Q.2, we can say that the original order will be restored after $2n-2$ out-riffle-shuffles if $2n-1$ is prime.

4. Let us label the cards from 1 to $2n$ where 1 is at the bottom of the deck of $2n$ cards. Then the Monge's shuffle corresponds to the following permutation (say p) :

$$\begin{array}{ll} 1 \mapsto 2n & 2 \mapsto 1 \\ 3 \mapsto 2n-1 & 4 \mapsto 2 \\ . & . \\ . & . \\ 2n-1 \mapsto n+1 & 2n \mapsto n \end{array}$$

   Consider the inverse permutation p^{-1}:

$$\begin{array}{ll} 1 \mapsto 2 & n+1 \mapsto 2n-1 \\ 2 \mapsto 4 & n+2 \mapsto 2n-3 \\ . & . \\ . & . \\ n \mapsto 2n & 2n \mapsto 1 \end{array}$$

   Note that, p^{-k} takes the card originally at position x to $\min\{a,b\}$ where a and b are the least positive residues $\mod(4n+1)$ of $2^k x$ and $-2^k x$ respectively.
   So, if the order of cards is restored by m applications of p^{-1} then for a given $1 \le x \le 2n$, either $2^m x \equiv x \mod(4n+1)$ or $-2^m x \equiv x \mod(4n+1)$ holds. (1)
   We know that m is the order of p iff m is the order of p^{-1}. Also by (1), m is the order of p^{-1} iff m is the least number such that $2^m \equiv 1 \mod(4n+1)$ or $-2^m \equiv 1 \mod(4n+1)$. It follows that order of p is m i.e. m is the minimum number of Monge's shuffles required to restore the order iff m is the least number such that $2^m \equiv \pm 1 \mod(4n+1)$.

5. We know that, if p is a prime and a is an integer such that $\gcd(a,p) = 1$, then $a^{(p-1)/2} \equiv \pm 1 \mod(p)$. If $4n+1$ is prime then simple application of the result in Q.4 and the statement above, proves the claim.

6. Let, b be denote a base and p be a prime. Let, $1/p$ has a cycle of length $k \geq 1$ i.e. $1/p = 0.a_1a_2...a_ka_1...$, (where $a_1, a_2, ..., a_k$ are non-negative integers, not all zero which form the smallest repeating unit in $1/p$), then $b^k/p = a_1a_2...a_k + 1/p$ which implies $b^k \equiv 1 \mod(p)$. Suppose, s is the smallest positive integer such that $b^s \equiv 1 \mod(p)$, then $s \leq k$. Suppose $s < k$. Then, $b^s \equiv 1 \mod(p)$ implies $1/p = 0.a_1a_2...a_sa_1...$ i.e. cycle length of $1/p$ is s which is less than k, a contradiction. Hence, the cycle length k of $1/p$ is the smallest positive integer such that $b^k \equiv 1 \mod(p)$ if $\gcd(b, p) = 1$.
   Now, let m be the number of bases b modulo p such that $1/p$ has cycle length k in base b. It means that m is the number of solution classes of the congruence relation $b^k \equiv 1 \mod(p)$. Or in other words, m is the number of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ with order k. We know that, in a finite cyclic group, number of elements of order k is $\phi(k)$, where ϕ is the Euler totient function. Hence, $m = \phi(k)$.
   Again, for $0 \leq x \leq p-2$, $x/(p-1)$ has least denominator k iff $(xk/(p-1), k) = 1$. Hence, $\phi(k)$ gives the number of fractions in $\frac{0}{p-1}, \frac{1}{p-1}, ..., \frac{p-2}{p-1}$, that have least denominator k. So, the claim holds.

7. Given that π is a permutation of $\{1, 2, 3, ..., N\}$.

   Let π be a Gilbreath permutation. Then, π is given by the interlacing of sub-permutations A and B where $A = (t+1, t+2, ..., N)$ and $B = (t, t-1, ..., 1)$ with $0 \leq t \leq N$.
   Consider, the sub-permutation $P = (\pi((k-1)j+1), \pi((k-1)j+2), ..., \pi(kj))$ for k and j such that $kj \leq n$. Define, $s =\mid B \cap P \mid \geq 0$ and $r =\max B \cap P$ if $s > 0$ else $r := 0$.
   Then, $r, r-1, ..., r-s+1 \in B \cap P$ and $(k-1)j+r+1, (k-1)j+r+2, ..., (k-1)j+r+j-s-1, (k-1)j+r+j-s \in A \cap P$. (1)
   Let, $a < b \in P$.
   Case 1 : $a, b \in A$
   By (1), $1 \leq b-a < j$ which implies $b \not\equiv a \mod(j)$.
   Case 2 : $a, b \in B$
   Similar to Case 1.
   Case 3 : $a \in B$ *and* $b \in A$
   By (1), $a = r-x$ where $0 \leq x \leq s-1$ and $b = (k-1)j+r+y$ where $1 \leq y \leq j-s$. Then, $b-a \equiv y+x \mod(j)$ But $1 \leq y+x \leq j-1$. It follows that $b \not\equiv a \mod(j)$.
   Hence, (a)⇒(c).

   If we take $k = 1$ then (c)⇒(b).

   Assume (b). Now, (d) is true for $j = 1$. Let (d) be true for some $j \geq 1$ i.e. $\{\pi(1), \pi(2), ..., \pi(j)\} = \{a, a+1, ..., a+j-1\}$ for some $a \geq 1$. We claim that $\pi(j+1)$ is equal to $a-1$ or $a+j+1$. If not, then $\pi(j+1)$ equals $a-x$ or $a+j+x$ for some $x > 1$. If $\pi(j+1) = a-x$ then $\pi(j+1) \equiv a-x+j+x-1 \equiv a+j-1 \mod(j+x-1)$ which contradicts (b). Similarly, if $\pi(j+1) = a+j+x$ then $\pi(j+1) \equiv a+1+j+x-1 \equiv a+1 \mod(j+x-1)$ which contradicts (b). Therefore, $\{\pi(1), \pi(2), ..., \pi(j), \pi(j+1)\} = \{a, a+1, ..., a+j\}$ for some $a \geq 1$.
   Hence, (b)⇒(d).

   Assume (d). We've seen that $\pi(j+1)$ equals $\max\{\pi(1), \pi(2), ..., \pi(j)\}+1$ or $\min\{\pi(1), \pi(2), ..., \pi(j)\}-1$ where $1 \leq j \leq N-1$. It is then clear that either $\pi = (1, 2, ..., N)$ or π can be partitioned into two sub-permutations $A = (t, t+1, t+2, ..., N)$ and $B = (t-1, t-2, ..., 1)$, where $t = \pi(1) > 1$, by adding $\pi(j+1)$ to A if $\pi(j+1) > t$ else adding $\pi(j+1)$ to B, sequentially. In either case π is a Gilbreath permutation.
   Hence, (d)⇒(a)

   In total, (a)⇒(c)⇒(b)⇒(d)⇒(a).