

One Hundred Prisoners and a Light Bulb

*Hans van Ditmarsch, LORIA / CNRS / Univ. of Lorraine, France
& IMSc, Chennai, India (associate)*

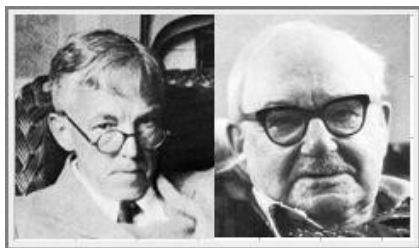
- ▶ Muddy Children — details
- ▶ Consecutive Numbers — details
- ▶ Sum and Product
- ▶ Russian Cards
- ▶ Monty Hall — details
- ▶ One Hundred Prisoners and a Light Bulb — details
- ▶ Gossip

Why are logic puzzles relevant for research in logic?
What is the origin of these puzzles?

Hardy & Littlewood

- Hardy and Littlewood are 20th century British mathematicians.
- Hardy wrote *A Mathematician's Apology* for a general audience.
- Littlewood wrote *A Mathematician's Miscellany*.
- Hardy starts with a non-trivial mathematical problem:
there are infinitely many prime numbers (classical / Euclid)
- Littlewood starts with the **Muddy Children problem** (modern).

Three ladies, A, B, C in a railway carriage all have dirty faces and are all laughing. It suddenly flashes on A: why doesn't B realize C is laughing at her? — Heavens, I must be laughable. (...)



Muddy Children



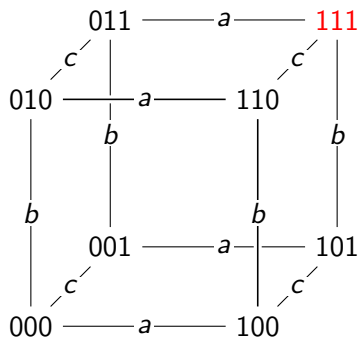
Muddy Children

A group of children has been playing outside and are called back into the house by their father. The children gather round him. As one may imagine, some of them have become dirty from the play and in particular: they may have mud on their forehead. Children can only see whether other children are muddy, and not if there is any mud on their own forehead. All this is commonly known, and the children are, obviously, perfect logicians. Father now says: "At least one of you has mud on his or her forehead." And then: "Will those who know whether they are muddy step forward." If nobody steps forward, father keeps repeating the request. What happens?

Three Muddy Children

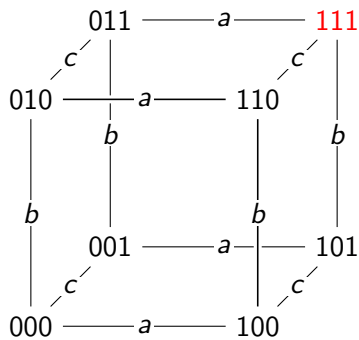
- The children can see each other.

Three Muddy Children



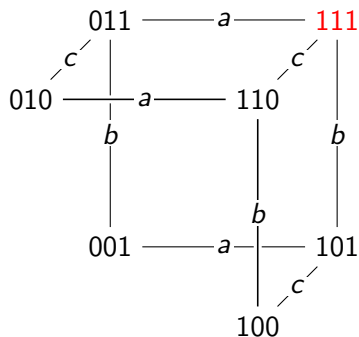
- The children can see each other.

Three Muddy Children



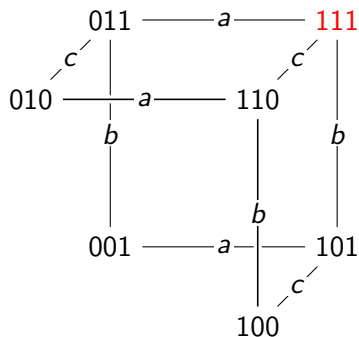
- The children can see each other.
- At least one of you has mud on his or her forehead.

Three Muddy Children



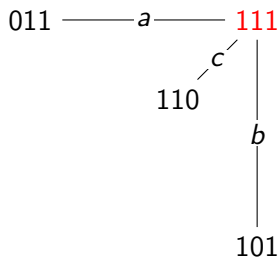
- The children can see each other.
- At least one of you has mud on his or her forehead.

Three Muddy Children



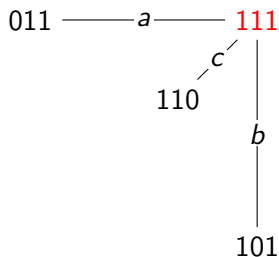
- The children can see each other.
- At least one of you has mud on his or her forehead.
- Will those who know whether they are muddy step forward?

Three Muddy Children



- The children can see each other.
- At least one of you has mud on his or her forehead.
- Will those who know whether they are muddy step forward?

Three Muddy Children



- The children can see each other.
- At least one of you has mud on his or her forehead.
- Will those who know whether they are muddy step forward?
- Will those who know whether they are muddy step forward?

Three Muddy Children

111

- The children can see each other.
- At least one of you has mud on his or her forehead.
- Will those who know whether they are muddy step forward?
- Will those who know whether they are muddy step forward?

Three Muddy Children

111

- The children can see each other.
- At least one of you has mud on his or her forehead.
- Will those who know whether they are muddy step forward?
- Will those who know whether they are muddy step forward?
- Will those who know whether they are muddy step forward?

On the origin of Muddy Children

- ▶ Kraitchik, *Mathematical Recreations*, 1942
- ▶ Littlewood, *A Mathematician's Miscellany*, 1953
- ▶ van Tilburg, *Doe wel en zie niet om*, Katholieke Illustratie, 1956 (Do well and don't look back, Catholic Illustrated J)
- ▶ Moses, Dolev and Halpern, *Cheating husbands and other stories: a case study in knowledge, action, and communication*, Distributed Computing, 1986

On the origin of Muddy Children

- ▶ Kraitchik, *Mathematical Recreations*, 1942
- ▶ Littlewood, *A Mathematician's Miscellany*, 1953
- ▶ van Tilburg, *Doe wel en zie niet om*, Katholieke Illustratie, 1956 (Do well and don't look back, Catholic Illustrated J)
- ▶ Moses, Dolev and Halpern, *Cheating husbands and other stories: a case study in knowledge, action, and communication*, Distributed Computing, 1986

Similar riddles appeared in the 1940s in:

- ▶ Penguin Problems Book, 1940; 2nd Penguin Problems B, 1944

and many variations since (more in this talk!), as recent as 2015:

- ▶ Cheryl's Birthday (Singapore Math Olympiad, 10 April 2015)
https://en.wikipedia.org/wiki/Cheryl's_Birthday
<https://www.facebook.com/barteld.kooi.7/videos/1722881727938456/>

but also **MUCH BEFORE** the 1940s:

- ▶

On the origin of Muddy Children



On the origin of Muddy Children

German translation of Rabelais' Gargantua and Pantagruel:
Gottlob Regis, *Meister Franz Rabelais der Arzeney Doctoren
Gargantua und Pantagruel, usw.*, Barth, Leipzig, 1832.

Ungelacht pftetz ich dich. Gesellschaftsspiel. Jeder zwickt seinen rechten Nachbar an Kinn oder Nase; wenn er lacht, giebt er ein Pfand. Zwei von der Gesellschaft sind nämlich im Complot und haben einen verkohlten Korkstöpsel, woran sie sich die Finger, und mithin denen, die sie zupfen, die Gesichter schwärzen. Diese werden nun um so lächerlicher, weil jeder glaubt, man lache über den anderen.

I pinch you without laughing. Parlour game. Everybody pinches his right neighbour into chin or nose; if one laughs, one must give a pledge. Two in the round have secretly blackened their fingers on a charred piece of cork, and hence will blacken the faces of their neighbours. These neighbours make a fool of themselves, since they both think that everybody is laughing about the other one.

Consecutive numbers



Consecutive numbers



Consecutive numbers

Anne and Bill are each going to be told a natural number. Their numbers will be one apart. The numbers are now being whispered in their respective ears. They are aware of this scenario. Suppose Anne is told 2 and Bill is told 3.

The following truthful conversation between Anne and Bill now takes place:

- ▶ *Anne: "I do not know your number."*
- ▶ *Bill: "I do not know your number."*
- ▶ *Anne: "I know your number."*
- ▶ *Bill: "I know your number."*

Explain why is this possible.

- ▶ *Consecutive Numbers is also known as the Conway Paradox.*
- ▶ *Peter van Emde Boas, Jeroen Groenendijk, Martin Stokhof, The Conway Paradox: its solution in an epistemic framework. 1984.*

Consecutive Numbers

*Suppose Anne has been told 2 and Bill has been told 3.
How we represent the model of uncertainty:*

01 — b — 21 — a — 23 — b — 43 — a — ...

Consecutive Numbers

*Suppose Anne has been told 2 and Bill has been told 3.
How we represent the model of uncertainty:*

01 — b — 21 — a — 23 — b — 43 — a — \dots

- ▶ Anne: "I do not know your number."

Consecutive Numbers

*Suppose Anne has been told 2 and Bill has been told 3.
How we represent the model of uncertainty:*

01 — b — 21 — a — 23 — b — 43 — a — ...

- ▶ Anne: "I do not know your number."

21 — a — 23 — b — 43 — a — ...

Consecutive Numbers

*Suppose Anne has been told 2 and Bill has been told 3.
How we represent the model of uncertainty:*

01 — b — 21 — a — 23 — b — 43 — a — ...

- ▶ Anne: "I do not know your number."

21 — a — 23 — b — 43 — a — ...

- ▶ Bill: "I do not know your number."

Consecutive Numbers

*Suppose Anne has been told 2 and Bill has been told 3.
How we represent the model of uncertainty:*

01 — b — 21 — a — 23 — b — 43 — a — ...

- ▶ Anne: "I do not know your number."

21 — a — 23 — b — 43 — a — ...

- ▶ Bill: "I do not know your number."

23 — b — 43 — a — ...

Consecutive Numbers

*Suppose Anne has been told 2 and Bill has been told 3.
How we represent the model of uncertainty:*

01 — b — 21 — a — 23 — b — 43 — a — ...

- ▶ Anne: "I do not know your number."

21 — a — 23 — b — 43 — a — ...

- ▶ Bill: "I do not know your number."

23 — b — 43 — a — ...

- ▶ Anne: "I know your number."

Consecutive Numbers

*Suppose Anne has been told 2 and Bill has been told 3.
How we represent the model of uncertainty:*

01 — b — 21 — a — 23 — b — 43 — a — ...

- ▶ Anne: "I do not know your number."

21 — a — 23 — b — 43 — a — ...

- ▶ Bill: "I do not know your number."

23 — b — 43 — a — ...

- ▶ Anne: "I know your number."

23

Consecutive Numbers

*Suppose Anne has been told 2 and Bill has been told 3.
How we represent the model of uncertainty:*

01 — b — 21 — a — 23 — b — 43 — a — ...

- ▶ Anne: "I do not know your number."

21 — a — 23 — b — 43 — a — ...

- ▶ Bill: "I do not know your number."

23 — b — 43 — a — ...

- ▶ Anne: "I know your number."

23

- ▶ Bill: "I know your number."

Consecutive Numbers

*Suppose Anne has been told 2 and Bill has been told 3.
How we represent the model of uncertainty:*

01 — b — 21 — a — 23 — b — 43 — a — ...

- ▶ Anne: "I do not know your number."

21 — a — 23 — b — 43 — a — ...

- ▶ Bill: "I do not know your number."

23 — b — 43 — a — ...

- ▶ Anne: "I know your number."

23

- ▶ Bill: "I know your number."

23

Sum and product



Sum and product

A says to S and P : I have chosen two integers x, y such that $1 < x < y$ and $x + y \leq 100$. In a moment, I will inform S only of $s = x + y$, and P only of $p = xy$. These announcements remain private. You are required to determine the pair (x, y) .

He acts as said. The following conversation now takes place:

1. P says: "I do not know it."
2. S says: "I knew you didn't."
3. P says: "I now know it."
4. S says: "I now also know it."

Determine the pair (x, y) .

Sum and product

A says to S and P : I have chosen two integers x, y such that $1 < x < y$ and $x + y \leq 100$. In a moment, I will inform S only of $s = x + y$, and P only of $p = xy$. These announcements remain private. You are required to determine the pair (x, y) .

He acts as said. The following conversation now takes place:

1. P says: "I do not know it."
2. S says: "I knew you didn't."
3. P says: "I now know it."
4. S says: "I now also know it."

Determine the pair (x, y) .

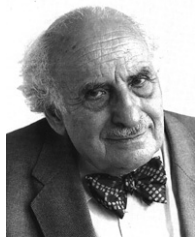
- If the numbers were 2 and 3, then P deduces the pair from their product: $6 = 2 \cdot 3$ and $6 = 1 \cdot 6$, but the numbers are larger than 1 (two integers x, y such that $1 < x < y$ and $x + y \leq 100$).
- If the numbers were prime, then P deduces the pair, because of the unique factorization of the product.

Sum and product — history

Originally stated, in Dutch, by Hans Freudenthal.

Nieuw Archief voor Wiskunde 3(17):152, 1969.

Became popular in AI by way of John McCarthy, Martin Gardner.



— Jan Plaza, *Logics of Public Communications*, 1989.

— Born, Hurkens and Woeginger, *The Freudenthal Problem and its Ramifications* (Parts I/II/III), Bulletin of the EATCS, 2006/7/8.

— van Ditmarsch, Ruan, Verbrugge, *Sum and Product in Dynamic Epistemic Logic*. Journal of Logic and Computation, 2007.

Russian cards



Russian cards



Russian Cards

From a pack of seven known cards 0, 1, 2, 3, 4, 5, 6 Alice and Bob each draw three cards and Cath gets the remaining card. How can Alice and Bob openly inform each other about their cards, without Cath learning of any of their cards who holds it?

- ▶ Presented at Moscow Mathematics Olympiad 2000.
- ▶ Thomas Kirkman, *On a problem in combinations*, Cambridge and Dublin Mathematical Journal 2: 191-204, 1847.
- ▶ David Fernandez and Valentin Goranko, *Secure aggregation of distributed information*, Discrete Applied Mathematics, 2015.



Monty Hall



Playing with probabilities — What is the best question?

Anthony and Barbara play the following game. First, Barbara selects a card from an ordinary set of 52 playing cards. Then, Anthony guesses which card Barbara selected. If he guesses correctly, Barbara pays him 100 euros. If he guesses incorrectly, Anthony pays Barbara 4 euros. To make the game a bit more interesting, Anthony is allowed to ask a yes/no question before he guesses, and Barbara has to answer his question truthfully. Which question is better: “Do you have a red card?” or “Do you have the Queen of hearts?”?

Playing with probabilities — What is the best question?

Anthony and Barbara play the following game. First, Barbara selects a card from an ordinary set of 52 playing cards. Then, Anthony guesses which card Barbara selected. If he guesses correctly, Barbara pays him 100 euros. If he guesses incorrectly, Anthony pays Barbara 4 euros. To make the game a bit more interesting, Anthony is allowed to ask a yes/no question before he guesses, and Barbara has to answer his question truthfully. Which question is better: “Do you have a red card?” or “Do you have the Queen of hearts?”?

Red card?	Yes/No	$\frac{1}{2} \cdot \frac{1}{26}$	+	$\frac{1}{2} \cdot \frac{1}{26}$	=	$\frac{1}{26}$
Queen of Hearts?	Yes/No	$\frac{1}{52} \cdot \frac{1}{1}$	+	$\frac{51}{52} \cdot \frac{1}{51}$	=	$\frac{1}{26}$

What the question is does not matter!
Only the number of answers matter.

Playing with probabilities — Monty Hall problem

Marilyn vos Savant

1975 — 1990

Suppose you're on a game show, and you're given the choice of three doors. Behind one door is a car, behind the others, goats. You pick a door, say #1, and the host, who knows what's behind the doors, opens another door, say #3, which has a goat. He says to you, "Do you want to pick door #2?" Is it to your advantage to switch your choice of doors?

Craig F. Whitaker
Columbia, Maryland

Playing with probabilities — Monty Hall problem

Marilyn vos Savant

1975 — 1990

Suppose you're on a game show, and you're given the choice of three doors. Behind one door is a car, behind the others, goats. You pick a door, say #1, and the host, who knows what's behind the doors, opens another door, say #3, which has a goat. He says to you, "Do you want to pick door #2?" Is it to your advantage to switch your choice of doors?

Craig F. Whitaker
Columbia, Maryland

Yes, it is...

Playing with probabilities — Monty Hall problem

Marilyn vos Savant

1975 — 1990

Suppose you're on a game show, and you're given the choice of three doors. Behind one door is a car, behind the others, goats. You pick a door, say #1, and the host, who knows what's behind the doors, opens another door, say #3, which has a goat. He says to you, "Do you want to pick door #2?" Is it to your advantage to switch your choice of doors?

Craig F. Whitaker
Columbia, Maryland

Yes, it is...

However, some people find it hard to accept the correct solution.

Monty Hall problem

Suppose you're on a game show, and you're given the choice of three doors. Behind one door is a car, behind the others, goats. You pick a door, say #1, and the host, who knows what's behind the doors, opens another door, say #3, which has a goat. He says to you, "Do you want to pick door #2?" Is it to your advantage to switch your choice of doors?

- ▶ Probability $1/3$ that the car is behind door #1.
- ▶ Probability $1/3$ that the car is behind door #2.
- ▶ **Do not switch! Your probability increased to $1/2$!**
- ▶ **The host opening a door does not change prior probabilities!**

Monty Hall problem

Suppose you're on a game show, and you're given the choice of three doors. Behind one door is a car, behind the others, goats. You pick a door, say #1, and the host, who knows what's behind the doors, opens another door, say #3, which has a goat. He says to you, "Do you want to pick door #2?" Is it to your advantage to switch your choice of doors?

- ▶ Probability $1/3$ that the car is behind door #1.
- ▶ Probability $1/3$ that the car is behind door #2.
- ▶ **Do not switch! Your probability increased to $1/2$!**
- ▶ **The host opening a door does not change prior probabilities!**

- ▶ Probability $1/3$ that the car is behind door #1. If you do not switch, you win the car. If you switch, you lose the car.
- ▶ Probability $2/3$ that the car is **not** behind door #1. If you do not switch, you lose the car. **If you switch, you win the car.**
- ▶ Not switch: $\frac{1}{3} \cdot 1 + \frac{2}{3} \cdot 0 = \frac{1}{3}$. Switch: $\frac{1}{3} \cdot 0 + \frac{2}{3} \cdot 1 = \frac{2}{3}$. **Switch!**

Responses to the solution of the Monty Hall problem

You blew it, and you blew it big! Since you seem to have difficulty grasping the basic principle at work here, I'll explain. After the host reveals a goat, you now have a one-in-two chance of being correct. Whether you change your selection or not, the odds are the same. There is enough mathematical illiteracy in this country, and we don't need the world's highest IQ propagating more. Shame!

Scott Smith, Ph.D.
University of Florida

Responses to the solution of the Monty Hall problem

You blew it, and you blew it big! Since you seem to have difficulty grasping the basic principle at work here, I'll explain. After the host reveals a goat, you now have a one-in-two chance of being correct. Whether you change your selection or not, the odds are the same. There is enough mathematical illiteracy in this country, and we don't need the world's highest IQ propagating more. Shame!

Scott Smith, Ph.D.
University of Florida

You're in error, but Albert Einstein earned a dearer place in the hearts of people after he admitted his errors.

Frank Rose, Ph.D.
University of Michigan

Responses to the solution of the Monty Hall problem

You are utterly incorrect about the game show question, and I hope this controversy will call some public attention to the serious national crisis in mathematical education. If you can admit your error, you will have contributed constructively towards the solution of a deplorable situation. How many irate mathematicians are needed to get you to change your mind?

E. Ray Bobo, Ph.D.
Georgetown University

Responses to the solution of the Monty Hall problem

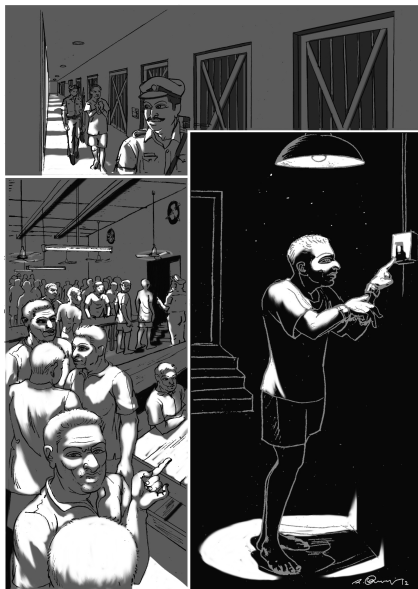
You are utterly incorrect about the game show question, and I hope this controversy will call some public attention to the serious national crisis in mathematical education. If you can admit your error, you will have contributed constructively towards the solution of a deplorable situation. How many irate mathematicians are needed to get you to change your mind?

E. Ray Bobo, Ph.D.
Georgetown University

You made a mistake, but look at the positive side. If all those Ph.D.s were wrong, the country would be in some very serious trouble.

Everett Harman, Ph.D.
U.S. Army Research Institute

One hundred prisoners and a light bulb



One hundred prisoners and a light bulb

A group of 100 prisoners, all together in the prison dining area, are told that they will be all put in isolation cells and then will be interrogated one by one in a room containing a light with an on/off switch. The prisoners may communicate with one another by toggling the light-switch (and that is the only way in which they can communicate). The light is initially switched off. There is no fixed order of interrogation, or interval between interrogations, and at any stage the same prisoner will later be interrogated again. When interrogated, a prisoner can either do nothing, or toggle the light-switch, or announce that all prisoners have been interrogated. If that announcement is true, the prisoners will (all) be set free, but if it is false, they will all be executed. While still in the dining room, and before the prisoners go to their isolation cells (forever), can the prisoners agree on a protocol that will set them free?

100 prisoners — not a solution

Let there be **one** prisoner:

Protocol: *If a prisoner enters the interrogation room, he announces that all prisoners have been interrogated.*

Let there be **two** prisoners:

Protocol: *If a prisoner enters the interrogation room and the light is off, he turns it on; if a prisoner enters the interrogation room and the light is on, and he has not turned on the light at a previous interrogation, he announces that all prisoners have been interrogated.*

Let there be **three** prisoners:

Protocol: ...

100 prisoners — solution Protocol for $n \geq 3$ prisoners

The n prisoners appoint one amongst them as the **counter**. The non-counting prisoners are the **followers**. The followers follow the following protocol: the first time they enter the room when the light is off, they turn it on; on all other occasions, they do nothing. The counter follows a different protocol. When the light is on when he enters the interrogation room, he turns it off. When he turns off the light for the $(n - 1)$ st time, he announces that everybody has been interrogated.

100 prisoners — solution Protocol for $n \geq 3$ prisoners

The n prisoners appoint one amongst them as the **counter**. The non-counting prisoners are the **followers**. The followers follow the following protocol: the first time they enter the room when the light is off, they turn it on; on all other occasions, they do nothing. The counter follows a different protocol. When the light is on when he enters the interrogation room, he turns it off. When he turns off the light for the $(n - 1)$ st time, he announces that everybody has been interrogated.

Let us picture a number of executions of this protocol for $n = 3$. The upper index: state of the light. The lower index: the number of times the light has been turned off. Anne is the counter.

— ${}^0\text{Bob}^1\text{Anne}_1^0\text{Caro}^1\text{Anne}_2^0$
— ${}^0\text{Anne}^0\text{Bob}^1\text{Caro}^1\text{Anne}_1^0\text{Bob}^0\text{Anne}_1^0\text{Caro}^1\text{Caro}^1\text{Bob}^1\text{Bob}^1\text{Anne}_2^0$
— ${}^0\text{Bob}^1\text{Anne}_1^0\text{Bob}^0\text{Caro}^1\text{Bob}^1\text{Anne}_2^0$

If the scheduling is fair, then the protocol will terminate.

Followers can also count

A follower may know before the counter that everybody has been interrogated. E.g., follower Bob may know it before counter Anne:

— ${}^0\text{Bob}{}^1\text{Anne}{}^0_1\text{Bob}{}^0\text{Caro}{}^1\mathbf{Bob}{}^1\text{Anne}{}^0_2$

When will you get out of prison?

Assume a single interrogation per day takes place.

When can the prisoners expect to be set free from prison?

When will you get out of prison?

Assume a single interrogation per day takes place.

When can the prisoners expect to be set free from prison?

non-counter / counter / another non-counter / counter / etc.

$\frac{99}{100}$ / $\frac{1}{100}$ / $\frac{98}{100}$ / $\frac{1}{100}$ / etc.

$\frac{100}{99}$ / $\frac{100}{1}$ / $\frac{100}{98}$ / $\frac{100}{1}$ / etc.

Summation:

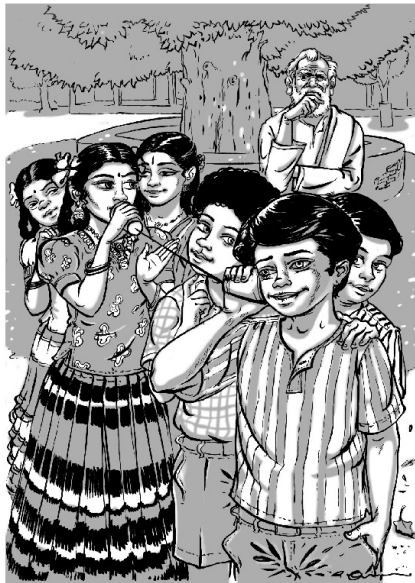
$$\sum_{i=1}^{99} \left(\frac{100}{i} + \frac{100}{1} \right) = 99 \cdot 100 + 100 \cdot \sum_{i=1}^{99} \frac{1}{i} = 9,900 + 518 \text{ days} \approx 28.5 \text{ years}$$

This can be reduced to around 9 years. The minimum is unknown.

Relation to **Coupon Collector's Problem** (De Moivre):

$$n \cdot \sum_{i=1}^n \frac{1}{i} = n \cdot H_n \text{ where } H_n \text{ is the harmonic number.}$$

Gossip



Gossip: agents exchanging secrets

Six friends each know a secret. They can call each other. In each call they exchange all the secrets they know. How many calls are needed for everyone to know all secrets?

Gossip: agents exchanging secrets

Six friends each know a secret. They can call each other. In each call they exchange all the secrets they know. How many calls are needed for everyone to know all secrets?

First consider four friends a, b, c, d who hold secrets A, B, C, D .
Four calls $ab; cd; ac; bd$ distribute all secrets.

$$\begin{aligned} A.B.C.D &\xrightarrow{ab} AB.AB.C.D \xrightarrow{cd} AB.AB.CD.CD \xrightarrow{ac} \\ &ABCD.AB.ABCD.CD \xrightarrow{bd} ABCD.ABCD.ABCD.ABCD \end{aligned}$$

Now consider friends a, b, c, d, e, f with secrets A, B, C, D, E, F .
Eight calls $ae; af; ab; cd; ac; bd; ae; af$ distribute all secrets.

[Peer-to-peer communication; epidemiology; semantic web; ...]

Gossip: agents exchanging secrets

Six friends each know a secret. They can call each other. In each call they exchange all the secrets they know. How many calls are needed for everyone to know all secrets?

First consider four friends a, b, c, d who hold secrets A, B, C, D .
Four calls $ab; cd; ac; bd$ distribute all secrets.

$$\begin{aligned} A.B.C.D &\xrightarrow{ab} AB.AB.C.D \xrightarrow{cd} AB.AB.CD.CD \xrightarrow{ac} \\ &ABCD.AB.ABCD.CD \xrightarrow{bd} ABCD.ABCD.ABCD.ABCD \end{aligned}$$

Now consider friends a, b, c, d, e, f with secrets A, B, C, D, E, F .
Eight calls $ae; af; ab; cd; ac; bd; ae; af$ distribute all secrets.

[Peer-to-peer communication; epidemiology; semantic web; ...]

cd : How does c know that she should call d , and not a or b ?
We need *knowledge-based gossip protocols*.

One Hundred Prisoners and a Light Bulb: the book

authors: Hans van Ditmarsch and Barteld Kooi

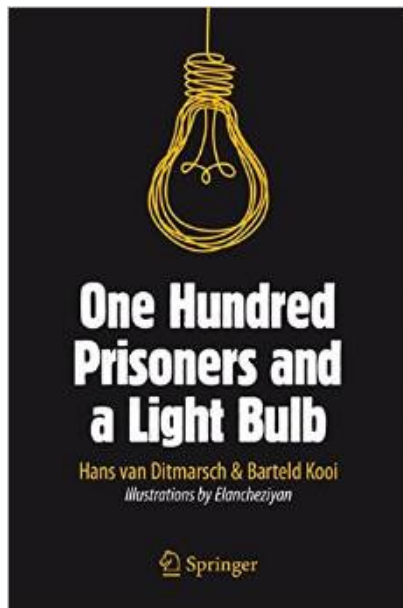
illustrations: Elanchezian



More information:

<http://personal.us.es/hvd/lightbulb.html>

More inform. : <http://personal.us.es/hvd/lightbulb.html>



More inform. : <http://personal.us.es/hvd/lightbulb.html>

