The Chinese Labyrinth

by Dr. Carsten Elsner

December 24, 2020

Redesigned and SageMath samples added by the CrypTool Team,
see: www.cryptool.de
Thanks to: https://www.heise.de/ct/Redaktion/bb/story/Labyrinth.htm

Primes reveal a lot of surprising features of natural numbers. You will learn some of them here as part of an interesting historic adventure, where the *Great Khan* is interested in more than the pure intellectual abilities of his intended officials and advisors.

Job Interview in *K* …

Mark Johnson is 24 years old and has a Harvard computer science diploma in the bag (however, at the moment it is lying in front of him on the table). He is beginning his job search with optimism and self-confidence. Of course he considers himself such an experienced computer specialist that the managers in the local technology center won’t be able to resist his résumé. But right now, the professor is sitting across from him with a mischievous smile. The professor, leader of the technology institute, has just completed the job interview and has asked him to wait outside: “I would like to confer with my assistant. Could you give us a moment, please?”

This is one of the leading research departments for cryptography and computer-aided encryption techniques. New procedures are programmed here to be run on high-performance computers, which run for days, weeks or months

calculating the factors of huge numbers. So very large, non-prime numbers (called compound numbers) are broken down into their prime factors (divisors) – a task which is necessary for breaking modern encrypted messages. Finding such divisors is not done by random searching, but uses clever tricks and algorithms, in order to cut down computing time. The professor is seeking someone with the knowledge to assist him.

“This guy isn’t a total moron, but is his programming talent really of such a great use for us?”, the pale-faced assistant cautiously asked, after Markus had left the room. “His knowledge of computers would seem to be sufficient”, answered the professor. “And as for the rest, we’ll just have to put him to a test. The young man just needs to have this cocky pride of his broken a bit – and with that, I’ll be glad to help.” The assistant turned with a questioning look to his boss, whose face, once again, wore the mischievous smile as he looked through his desk drawers.

“It must be here somewhere…” The professor was known for utilizing unusual methods in selecting new colleagues and research assistants. So the assistant knew he should just wait and see, what his boss was cooking up this time. “Ah – there it is!” The professor pulled out a few sheets of paper. “When I was working on my doctorate I gave this text to my students.” Again, he grinned mischievously. “And it was a hard experience for each of them. I won’t spare Mr. Johnson the headache. If he can solve this by tomorrow, he’ll get the position. Would you please call him back in again!”

As the over-confident applicant sat back down across from the professor and his assistant, the papers were handed to him. But to his surprise they weren’t the expected employment contract. With carefully played, but unexaggerated drama, the professor explained to him: “A well-known German historian has discovered some medieval manuscripts in a library in Padua. From the style and content of the

writing, it seems certain they are part of a journal kept by Marco Polo. In this document, Marco Polo described one of his strangest adventures in China – a mission which enabled him to rise to the position of advisor to the *Great Khan*. Unfortunately, it appears the last pages of the manuscript are missing. According to his notes Polo gained his position in the *Great Khan's* court through the ability to recognize certain large numbers as non-prime."

From the baffled look on Mark Johnson's face the professor could tell he had many questions, but he simply pointed to the papers: "It's all there in your hand. What you have is a translation of the manuscript sent to me by the historian. If you can reveal the secret of the fifth chamber by tomorrow afternoon, you are our man! Moreover, you will help to shine a light into a little-known period of the life story of this well-traveled Venetian. Don't be surprised: we are regularly confronted with such problems, which come to us

from all over the world. But leave your computer switched off – Marco Polo had, at most, an abacus with him.”

The professor rose and extended his hand before the applicant could raise any questions. “I’ll see you tomorrow afternoon at 3 o’clock”, he said. The interview was over. Before the young man knew what had happened, he was back outside the office door. His optimism had already suffered a heavy blow. He returned to the hotel with a hollow feeling in his gut, extended his stay by one day, shut himself in his room, and became completely immersed in the manuscript, hoping for the best.

Job Application at Khan's

It happens that I must still write an account of that ominous day on which I learned the grace of His Eminency, the *Great Khan*, the son of the sun. In this country, those nominated for public office are subjected to most strenuous testing – the higher the office, the more extensive and difficult the test. Because the *Great Khan* wished to have me as a personal advisor, an honor normally only bestowed upon Mandarins above the 37th degree in the imperial court, I had to undergo the intended test along with two competitors: these were the imperial court astronomer, the honorable and widely esteemed master Hyan Li Pu, as well as the famous mathematician, master Wan Chi, who was summoned from the Kiangnan province.

On that morning, as our strict orders dictated, the three of us appeared in a hall, where a Mandarin of the 38th degree explained the test. He spoke in a formal dialect, which I found

difficult to completely understand, but, thankfully, I was able to get the main points:

"Honorable men," he said, "may the Gods be with you today, for you are about to enter a labyrinth whose gate will be closed behind you. Your life depends, then, only on your cleverness, but …" (here the Mandarin bowed to a group of nearby courtiers) "you must also be fearless. With luck, you may find the exit and, once again, see the light of day." He bowed again… "Those of you who, by wits and skill, find the exit, will share the office. But now, listen closely: Each time you reach a chamber, you will find two potential paths to continue your course… but pay close attention now; as soon as one of you has left the chamber, all exits from it will be closed within moments. Either you all choose the same path or, if you wish, you may separate. But any who hesitate and stay behind will be trapped for eleven years, because before this time, nobody may apply for this office and be examined in this labyrinth.

But again, woe to you who choose the wrong exit from a chamber! Then too, you will find yourself caught in a dead-end. Only the correct exit leads to a new chamber."

I felt more and more uncomfortable as the Mandarin continued his words of warning. "Your intelligence alone will guide you to the correct decision. You must remember: In each of the five chambers, you will find something which can be divided, or not. Any who believe the thing is divisible shall take the exit on the left – any of another opinion will take the path on the right. And now I ask you: Are there any among you who will refuse the test?"

I was torn. I knew I had no real choice in the matter. My refusal would have conflicted with the *Great Khan's* wish to subject me to this test, which would have meant a certain death sentence. My only hope was to enter the labyrinth and pray for a happy return. So I nodded to the Mandarin, to indicate my assent. Neither of the

others said a word, but both simply shook their heads. “So then,” the Mandarin intoned, “it is decided.”

A gong sounded and the Mandarin led us to the entrance of the dangerous labyrinth. With throbbing heart and weak knees, I followed the others through the gate and turned around one last time. The Mandarin bowed, the gong was struck again, and with a deafening rattle and slam, the door went down, sealing the entrance.
I crossed my breast, did a quick prayer, and joined the others, who were leading the way, apparently unflustered. As the Mandarin had described, the dark corridor soon ended in a room lit by two torches.

Chamber One

On both walls of the chamber, dark openings yawned, indicating our exit possibilities. Except for that, I couldn’t see anything of importance, and had to follow the gaze of my companions to find the object of our first task… they were both staring at the opposite wall, on which were painted some characters. Though I’m not completely inexperienced in reading Chinese, out of politeness, I asked Master Wan for a translation. The otherwise distinguished man gave me a condescending look, then informed me, “There is only one number: 8633.” I was perplexed …our very lives depended on whether we found the divisors of this number, or not. Then I wondered if Master Wan had even told me the right number. We were, after all, applying for the same office. But I was soon convinced he’d spoken the truth and began thinking about the problem. Somewhat irresolutely, but to break the silence, I finally opened discussion.

“Do either of you gentlemen have a suggestion?” Master Li looked witheringly at me before replying, seeming a bit reluctant to share his knowledge, with one so ignorant as me, in matters of such great importance. “If we consider this number to be the area of a rectangle, then if two divisors exist, then neither can be larger than the side of a square.” This made sense to me.

“So,” master Wan took over, “if there is a divisor to this number, then …” (I could see he was doing some quick mental arithmetic) “… we will find one which is less than 93, so it should suffice to test only the numbers which, in your experience,” he looked askance at me “are known primes, to see if they divide into our number.”

I marveled at the genius of the two Chinese men and, feeling a bit demoralized, as I still hadn’t added anything to the solution, I shifted my gaze to the side. In the corner of the room, then, I noticed a barely discernible object on the ground and,

on going to it, I found it was an abacus, beside which lay a few pieces of chalk. “Perhaps this will be of some use?” I offered, feeling my spirits rise from at least being able to help in some small way.

Master Li took it from me immediately, and without a word, began moving the balls back and forth. I could sense his impatience and recognized a certain presumption that the Chinese clearly had, that an Italian couldn’t be trusted in the use of this traditional device for calculation. After a few minutes, Master Li impassively announced, “8633 is the product of 89 and 97, so is non-prime.”

“So,” offered Master Wan, “we should take the right exit, if you worthy men would like to lead the way!”

I immediately saw through his intention. I knew we’d been told to take the left passage if a number was found to be divisible and was certain I could count on my memory about this point and tried to find a

polite response. If Master Li and I had done as he suggested, and started down that passage, he'd have taken the other entrance at the last moment and left us to a certain death by asphyxiation or starvation. Master Li, it was clear, also saw through his trickery and corrected him with barely suppressed anger, in order to avoid an open argument before we had even left the first chamber. Only too rapidly and without retort, Wan entered the left passage, following master Li.. I came after the two hastily, and had hardly entered the darkness, when I felt the rush of air caused by the rumbling wall falling behind me. I was in pitch-black darkness. My head hit the low ceiling before I began again with greater care, to make laborious progress, groping at the walls as I went. Ahead of me, at some distance, I could hear the two Chinese, who were now engaged in a loud and vociferous argument, probably surrounding the incident, which had just occurred in the first chamber.

Chamber Two

Suddenly my foot came down on something. Even in the darkness, it was clear these were balls. The quarrel must have turned physical and, moreover, the abacus was now broken! I saw our hopes fading. At last I saw a faint light at the end of the tunnel and soon stood beside the two squabblers in the second chamber. They had both calmed down again as rapidly as they had clashed. Only now did I remember that I had put a piece of chalk from the first chamber into my right sleeve, and my every hope now hung on this seemingly insignificant thing.

“In this chamber we are welcomed by the number three million, two hundred forty thousand, increased by one,” Master Li informed me.

“Heaven help us!” I cried out. “The numbers just get larger and larger. I dare not think of what awaits us in the fifth chamber, if we should even make it so far.”

“Dear honorable master, before whom we bow in the dust,” answered Master Wan in the obsequious language of his custom. “Everything can be understood through rational thinking. The selection of this number for your educated and worldly eyes is not without reason. This number was written there for us, so let’s put our heads together.” Despite our threatened position, I smiled inwardly at this stilted officialese, but felt flattered, nevertheless. I looked furtively at Master Li, who looked rather questioningly at Master Wan and did not seem to share his optimism at all.

The events in this chamber happened unexpectedly in only moments, because Master Li lost control. Master Wan, who was not only an outstanding mathematician, but also experienced at performing complex mental arithmetic, explained his reasoning, as he stared at the characters on the wall. “18 times 18 is 324; therefore 3240000 is 1800 squared. And the double of 1800 results in 3600, which is the

square of 60.” I could follow the calculations, but did not at all understand what this had to do with factoring 3240001. The look on Master Li’s face gave evidence of the same confusion.

Unimpressed, Master Wan continued. “Our number there is not only the square of 1800, increased by one, but also the sum of the square of 1799 and the square of 60.” Finally, he looked from the wall at Master Li and myself, grinning like a small child, and announced, “The number is, therefore, non-prime.”

Master Li had clearly lost his patience. “Would the Master be so kind as to give us a divisor for this number?” He shouted, clearly distrusting the other mathematician. “First you break the abacus, then now act as if you know everything!”

“I cannot give you any actual divisors, but only know that they must exist,” answered Master Wan, serenely.

“I’ve had enough of this nonsense!”

screamed Li, his voice cracking with rage. “May the Gods protect me from this Charlatan!” And in a sudden fury, he dashed from the chamber through the right exit, which closed immediately behind him.

“Come!” Wan grabbed my arm and pulled me toward the left passage, which we barely reached, before this wall, too, fell down. Not for one moment had I been able to follow Master Wan’s reasoning, and doubted that I would be able to get a longer explanation here in the labyrinth. So, holding my tongue, I was only relieved, after another bout of groping in the dark, to see another chamber.

“May God have mercy on his soul,” I said, solemnly, speaking of Master Li. But Master Wan appeared nonplussed.

Chamber Three

I took a deep breath, still fighting my growing fear. Master Wan was already busy with the characters on the wall. He turned to me and said, “Most honorable friend, in all humility, I dare say that we will have no problems here.” He pointed at the wall. “We are asked to multiply all numbers from one to a hundred with each other, then increase the result by one.” Wan looked at me expectantly. I fumbled to remove the chalk from the long sleeve of my Chinese robe, and began, on the side wall, to write out this calculation.

“Would you forgive an ignorant farmer for daring to interfere?” I was increasingly irritated by Master Wan’s scornfully arrogant tone. “But can you imagine, how large this number is going to be and how likely you are to make a mistake its calculation?” I stopped and shook my head. “With your Arabic number system, you would certainly need more than one hundred

figures to write it out. Let me humbly ask: Is 101 a prime number?”

“But that number isn’t even here,” I answered reproachfully.

“Please, just answer my question! Is 101 a prime number? It certainly is. And moreover, it divides our enormous number! Follow me into the left passage, if you are ready to honor my poor sense of reason.”

Again, I was astonished. In the previous chamber, Wan had recognized that the number was non-prime, without being able to name a divisor, while here, he was able to name a factor for a number he hadn’t seen at all. I began to doubt his reason, but his confident appearance left me no other choice. So, turning, I followed him into the low-ceilinged tunnel, through which we progressed only by stooping.

Chamber Four

Soon we reached the fourth chamber, which proved that Wan had, despite my doubts, been right again. With confidence in the master, I translated the characters on the wall. “Now count the scales of the great dragon’s armor. There are one more than the result you get from multiplying two with itself thirty-two times. Beware the great dragon!” I looked expectantly at Master Wan, but got a fright. The man who had always been so self-assured had suddenly turned pale.

Wan sat down on the chamber floor, his head hanging, and spoke with bitter irony, “Now, in the wise man from far Europe, I fear I will finally meet my master, because here, I am clueless. From my knowledge, it would be assumed that the number of the scales is prime. But more than that, I can’t guess. What ways do you have in Europe for determining the scales of the great dragon? But woe, if you prove to be the braggart and fraud I’ve already

assumed for some time now!”

I answered him quietly: “Master! I am not a scholar like you, nor did I study higher mathematics in Paris or my homeland.” I continued, even more quietly, “I’m afraid that I, too, have no answer for you.”

Chamber Five

Master Wan seemed to have expected no more from me. I had to watch as this heretofore-so-proud man cried quietly to himself. As he still sat there, whimpering some minutes later, I felt I had to come to some kind of decision: “We are here in the next-to-last chamber. If we simply ignore the characters on the wall and select a course arbitrarily, then in the event of a lucky choice, we might proceed to the last chamber. Likewise, there, if we have to do the same, we have one chance in four of survival. However, if we should part ways here, then one of us will be able to select the way out of this labyrinth after choosing from only two possibilities. Shall we draw lots then?”

After some time, Master Wan slowly raised his head. “I agree.” We tossed a coin and Lady Luck assigned me the left course once again. I gave Master Wan my hand to bid him farewell, but his weak handshake and the anxious

look on his face betrayed his lack of confidence.

“Now then!” Without further words, I quickly entered the left passage and the wall fell down behind me, isolating me in darkness. The feeling of lucky relief I had, upon finally seeing another light at the end of the tunnel, was indescribable. I stumbled, a bit groggily, into the fifth chamber and collapsed, exhausted, in the corner. In my inner eye, I could see the gruesome scenes which must have been taking place only a short distance away from me, behind the thick walls. Then I felt fear on realizing that with one last false choice, the same fate could await me. I was appalled by the inhumanity of these barbarian officials, who, without compassion, would leave to rot any who failed in the course, by an instant’s wrong decision – the same path by which they had successfully ascended, though perhaps only by lucky accident. I wondered whether they felt some kind of perverse joy at another’s misfortune when they found,

after years, the decayed remnants of a fellow candidate. After such gloomy thoughts, I fell asleep and dreamed things I can’t describe.

Finally, I woke up and struggled to my feet. I felt a weight as if lead filled my body and brain. But I grabbed a torch and lit up the characters on the opposite wall. The translation came with difficulty, although I had some experience. Finally I read, “Multiply four by itself fifteen times, and then fifteen by itself four times. Your results add together to yield divine harmony and thereby will you decide your fate!” What sarcasm! Anyone who doesn’t recognize the “divine harmony” is thus rewarded for his courage with the loss of his life and may not serve the *Great Khan*. Well, well! I took the directive to add the results as a simple task of addition and worked on the wall with the chalk:

$$
\begin{aligned}
&\overbrace{4 \cdot 4 \cdot \ldots \cdot 4}^{15 \text{ times}} + 15 \cdot 15 \cdot 15 \cdot 15 \\
&= 1024 \cdot 1024 \cdot 1024 + 225 \cdot 225 \\
&= 1\,073\,792\,449
\end{aligned}
$$

I prayed to God that the result was correct. But I completely lost my courage as I considered this huge number. If there should be any divisors, they would have to be small, otherwise I would have no chance of finding them. I squatted down in the corner again, and began to scribble on the walls. When I needed more room, I used my sleeve to make space, then continued on. I desperately tried all the small prime numbers known to me, but always remained unsuccessful – none divided evenly. I pressed on with haste, unable to pull myself together to work in peace of mind. With my growing desire to find a divisor, also grew my fear of overlooking one through an error in calculation. But nothing led to the desired result: 1073792449 remained, despite my best

efforts, without a divisor. It became increasingly clear that I would have to accept this figure as prime.

Chamber Five, ctd.

But who would choose, in a situation of life or death, not to test all possibilities? So I persisted in my calculations without thinking about the fact that I simply couldn’t test all possible divisors here at all. Finally, when I had checked 293, my efforts reached a sudden end; the chalk ran out on me. I collapsed in the corner. How long I lay there, I do not know. In my head raged a horrific storm. Finally, and only by the greatest effort of will, did I force myself to find a moment of peace to assess my position. I had two reasons for choosing the right exit from the chamber: firstly, a number, if it isn’t prime, would, in most cases, have a relatively small factor, which I’d been unable to find. And secondly, prime numbers had not been found in any of the previous chambers, so to decide that this number was prime would surely be intended as a test of courage, since calculations alone, with a number of this size, could not

prove this solution. But could I truly wager my life on this conclusion?

In the end, lacking neither the will-power nor the knowledge to further weigh the pros and cons of the situation, I decided to take the right exit. But I sat there for what seemed an eternity, not daring to continue on the decided course of action. What went through my head, my hand shall not try to repeat on paper. But finally, after a desperate prayer, I hastily crossed the threshold and immediately banged my head into an obstacle. I must have knocked myself half-unconscious, because I never even noticed the wall rushing down behind me. When the throbbing pain finally began to diminish, I was again close to despair. It was so dark that I couldn’t see a hand held in front of my face, and the ceiling was so low that I could only progress by bending down. Finally I had to lower myself onto my hands and knees and crawl. Through my mind, only one thought repeated: “You erred now, after all, and guessed your way into a dead-end.

Such a low tunnel can surely have no exit! Soon you are certain to meet your terrible fate.”

I have to admit, I not only crawled on all fours like a dog, but also whined like one. I had lost all pride and dignity. It served me right for my nonsense a while earlier when I’d coolly suggested to Wan that we separate, when I’d sounded so wise and clever in my own ears. Now I was simply mistaken and would pay for this mistake with my life. As if in confirmation of this thought, my hands suddenly met with a wall before me. A short, plaintive cry escaped from my lips and I fell on my stomach, my head in my hands.

I have no idea how long I lay there like that, but suddenly I noticed there was light in front of me. Lifting my head, I saw that the wall in front of me had disappeared and found myself looking into the round face of the 38th degree Mandarin. Some servants pulled me from where I lay and I discovered I was in a great

hall. To my astonishment, masters Wan and Li were also sitting there, both of them crying like two small children, without any restraint. Not a shred remained of their former pride. Their experience must have been as my own and they, too, must have believed themselves close to death. But why aren’t they trapped? Surely only I had found the correct way? A loud gong sounded, pulling me from these thoughts.

Exit

Startled, I turned around and saw behind me that the whole length of the wall was filled with many openings, closed by wooden flaps. From one of these trapdoors, the servants had just pulled me. The Mandarin bowed to me and announced with the reserved smile, for which the Chinese are capable: “I’ll save you the trouble of counting: There are 32 doors!” Only gradually did I realize the almost unbelievable significance of this number for the labyrinth test. “I congratulate, the most honorable man. Because you are all here again, you may also believe that there are no dead-ends in the labyrinth. Each passage leads into a new chamber. By the will of our gentle leader, the life of all pretenders to the office may not be threatened by their choices.”

The bewildered look on my face prompted the Mandarin to continue his explanation: “How wise the Khan is

not to merely test your mathematical ability! At each chamber of the labyrinth, the guard who closed the passages also listened to your conversations. Any who desire such a high office, must not only have courage and reason, but must also possess the rare quality of being able to listen to the arguments of others and weigh them on their merits, despite their personal convictions. In this labyrinth, we break the pride of the candidates, look behind the mask of their practiced politeness and so determine whether they only seek their own advantage.” To masters Wan and Li, who were still sitting, exhausted on the floor, the Mandarin continued: “Get up, Masters! The last part of your test will now take place. In his brilliant justice, the imperial leader awaits your answer to the question of the divisibility of the number you found in the last chamber. You have all been in a fifth chamber, and in each was the same number. So now, follow me!”

Getting Back

The legend ends at this point. The next afternoon, just before three, a pale young man knocked timidly at the professor’s office. The door was immediately opened, by the mischievous-looking professor, who greeted him: “Come in, Mr. Johnson! I’m very excited to learn how Marco Polo gained his position in the *Great Khan’s* court.” The door was closed behind the candidate, and in the anteroom an aghast secretary remarked: “Now the old man’s completely off his rocker!”

The End

Dear reader, the story ends here. If you wish a fuller resolution, slip into the role of Mark Johnson and solve the secret of the fifth chamber. If you solve this puzzle, Johnson gets the job, and otherwise …

Explanations and Hints

Marco Polo lived from 1254 till 1324 A.D. and was known for his travels to China. At the court of the Chinese imperator he has to face an examination: Together with two competitors he has to go through a labyrinth with five chambers. In each chamber the candidates have to solve tasks, which all deal with the divisibility of natural numbers. Especially exciting is the secret of the fifth chamber.

First Chamber/Hints

Here they make a simple estimation of the potential prime factors of a given number: If the given number is not prime, then at least one of its prime factors cannot be greater than the square root of the given number.

This estimation is the basis of an historical algorithm invented to find primes: If you know the primes below

10 (i.e. 2, 3, 5 and 7) then you get all primes between 10 and $10 \cdot 10 = 100$ by eliminating integers in the range from 10 to 100 in the following way: First you cross out all multiples of 2 (i.e. all even numbers), then all multiples of 3, of 5, and finally all multiples of 7. That's all. Some numbers will be crossed out several times (like 30, which is a multiple of 2, 3 and 5). What remains will be the 21 primes between 10 and 100. This is the sieve of Eratosthenes (3rd century B.C.).

Second Chamber/Hints

Here, master Wan applied a more sophisticated theorem regarding prime numbers.

First he proved that the given number 3 240 001 can be written in two essentially different ways as sum of two squares of natural numbers:

$$1800^2+1 = 1800^2+1^2 = 3\,240\,001 = 1799^2+60^2$$

It is easy to calculate the left construction (182 = 324). The right side can be calculated from the left via the second binomial formula:

$$a^2 - 2ab + b^2 = (a-b)^2 \qquad | + 2ab$$
$$a^2 + b^2 = (a-b)^2 + 2ab$$

$$1800^2 + 1^2 = (1800-1)^2 + 2 \cdot 1800$$

Secondly, prime number theory tells us two things about a prime > 2 which can be expressed as a sum of two squares:

a) such a prime must leave a remainder of 1 when dividing it by 4. This criteria is fulfilled by 3240001.

b) such a prime does have only *one* such form as a sum of two squares (besides changing the order of the two summands).

So, the given number 3240001 cannot be a prime, because there do exist two different forms as the sum of two

squares. Indeed: $3\,240\,001 = 1741 \cdot 1861$, actually both factors being prime.

Third Chamber/Hints

In this chamber master Wan applied what has become known as the Theorem of Wilson (Sir John Wilson, 1741-1793)[1]. Even today this is, theoretically, the easiest way to determine whether an integer number is prime: An integer $n > 1$ is prime, if and only if n is a divisor of the product of all numbers from 1 to $(n-1)$, increased by 1. In other words: An integer $n > 1$ is prime, if and only if:

$(n-1)! \equiv -1 \mod n$ or rather $(n-1)! + 1 \equiv 0 \mod n$.

The sign $\equiv$ means, that the left side is congruent to the right side according to the given *modulus*. In elementary school you would say: *a is congruent to b modulo n if the*

[1]This theorem was firstly proven in the year 1770 by Joseph-Louis Lagrange (1736-1813).

remainder of the division of a by n equals b, e.g.: $11 \equiv 2 \ mod 3$

With the numbers of the puzzle of Chamber 3 we have in one direction:

Because the integer $n = 101$ is prime, it divides the number

$$z := 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot 99 \cdot 100 + 1$$

Applied in the other direction this means: you first calculate $z = 100! + 1$, and if $n = 101$ divides z, then 101 is prime.

As master Wan mentioned, the product of the first $(n - 1)$ integers grows very fast (mathematicians today call this product a factorial). So unfortunately, the Wilson criterion is not suitable for practically proofing that a large integer n is prime.

Example: Even for the prime number 71 the number to check $70! + 1$ has more than 99 decimal digits. But for small numbers Wilson can easily be verified: 5 is prime, because 5 divides $4! + 1 = 25$ (but 6 is not prime,

because 6 does not divide $5! + 1 = 121$). Example: The number z above, used in the third chamber and derived from the 3 digit number $n = 101$, has 158 decimal digits ($z \approx 9.33 \times 10^{157}$)! If someone wants to use the Wilson criterion to find out whether $n = 101$ is prime, he first must calculate this huge number z.

Without a computer that's not possible.

Nowadays with SageMath this takes less than a second:

```
sage: factorial(100)+1
CPU times: user 23 µs, sys: 8 µs, total: 31 µs
Wall time: 33.9 µs
933262154439441526816992388562667004
 907159682643816214685929638952175999
 993229915608941463976156518286253699
 697920827223758251185210916864000000
 000000000000000000001
```

This number is divisible by 101, which follows from the factorisation:

```
sage: factor(factorial(100)+1)
sage: factor(factorial(100)+1)
```

```
101 * 14303 * 149239 * 3504330071706
 16328107072379 * 12352868165729972
 513985030175343787083485124007714
 531212405629054224878413923822303
 271959567362883048251014777364474
 07
```

Splitting $z = 100! + 1$ into its prime factors takes a bit longer than the computation of z. With `sage:%time factor(factorial(100)+1)!` it is possible to get information on how long it takes. The MacMini on which this text was edited took about 3 minutes for this task:

```
CPU times: user 3min 1s, sys: 182 ms
 , total: 3min 1s
Wall time: 3min 1s
```

Here you can get a feeling for which dimensions (order of magnitude) the factorial can be realistically computed on modern PCs: Calculating the factorial $z = \left(10^7\right)!$ succeeds after a few seconds and results in $1.20 \times 10 \cdot 10^{65\,657\,059}$ – a number of 65 657 060 decimal digits. But if you tried to calculate the factorial

$z = \left(10^8\right)!$ 20 years ago the program tried for some hours and then stopped with an overflow statement. Today in 2020 with SageMath we have with `sage:%time x=factorial(10**8)!` the following computing time:

```
CPU times: user 49.5 s, sys: 1.87 s, total: 51.3 s
Wall time: 51.9 s
```

Mind that if you use `sage:%time factorial(10**8)!` (without the assignment `x=...`) it takes much longer because SageMath not only computes the result but also prints it to the screen. The number $\left(10^8\right)!$ has about eight hundred million decimal digits.

The computation of $\left(10^9\right)!$ is not so fast any more:

```
sage:%time factorial(10**9)!
```

```
CPU times: user 11min 43s, sys: 4min 16s, total: 16min
Wall time: 22min 51s
```

For $(10^{10})!$ we cannot do the computation anymore with SageMath on

the 8GB Mac Mini. After about an hour the program crashes an we get this error message:

```
/pathtosage/Contents/Resources/sage/
src/bin/sage-python: line 2: 2305
Killed: 9sage -python "$@"
```

To estimate the magnitude or number of decimal digits of factorials one can use the Formula of Stirling:

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

If we round the base 10 logarithm of that number to the next lower integer, we get the number of decimal digits $d_{n!}$ of $n!$. So in the case $n = 10$ the factorial $10^{10}! = 10\,000\,000\,000!$ has approximately 96 billion decimal digits:

```
sage: def stirling(n):
....:     ef=e.n()
....:     pif=pi.n()
....:     x=sqrt(2*pif*n)*((n/ef)**n
  )
....:     return x
....:
sage: stirling(10**10)
```

```
2.32579597597705e95657055186
sage: log(stirling(10**10),10)
9.56570551863666e10
```

For comparison: The number of atoms in the universe (the Eddington Number) is approximately 10^{80}, that are 81 decimal digits.

Today we test primality for numbers with more than 100 decimal digits (cf. e.g. https://primes.utm.edu/largest.html). If we wanted to use the Wilson criterion for this test, we would have to be able to compute at least $(10^{100})!$. Even the stirling approximation from above doesn't go there:

```
sage: stirling(10**100)
+infinity
```

If you plug $n = 10^{100}$ into the stirling formula and compute the approximation of the number of digits by hand, you get nearly 10^{102}. That is, for n with more than hundred decimal digits the factorial $n!$ has more digits than there are atoms in the universe.

Clearly, the Wilson criterion is of no practical use for large numbers.

Master Wan only could judge so fast, because within the task it was explained how the number *z* was constructed.

Chamber Four/Hints

The fourth chamber deals with the famous *fermat numbers* (Pierre de Fermat, 1601-1665) that are obtained by increasing specific powers of two by one, namely those powers of two whose exponent is itself a power of two:

$$F_n = 2^{(2^n)} + 1$$

Now we know that the conjecture which master Wan mentioned is wrong. For a long time it was assumed that all fermat numbers are prime numbers. But Leonhard Euler (1707-1783) disproved this conjecture for n=5:

```
sage: def f(n):
....:     return(2**(2**n)+1)
....:
sage: for i in range(6):
....:     print(f'F_{i}=2**(2**{i})+1=2**{2**i}={f(i)}={factor(f(i))}')
....:
....:
F_0=2**(2**0)+1=2**1=3=3
F_1=2**(2**1)+1=2**2=5=5
F_2=2**(2**2)+1=2**4=17=17
F_3=2**(2**3)+1=2**8=257=257
F_4=2**(2**4)+1=2**16=65537=65537
F_5=2**(2**5)+1=2**32=4294967297=641 * 6700417
```

The number F_5 is the number of interest in the fourth chamber. As you can see, it is divisible by 641. Euler did not find that factor by dividing F_5 successively by all prime numbers $2, 3, 5, 7, \ldots$ He found a mathematical trick, namely that every prime divisor of F_5 has the form $64 \cdot k + 1$:

```
sage: for k in range(11):
....:     print(f'k={k}: 64*{k}+1={64*k+1}={factor(64*k+1)}')
```

```
....:
k=0: 64*0+1=1=1
k=1: 64*1+1=65=5 * 13
k=2: 64*2+1=129=3 * 43
k=3: 64*3+1=193=193
k=4: 64*4+1=257=257
k=5: 64*5+1=321=3 * 107
k=6: 64*6+1=385=5 * 7 * 11
k=7: 64*7+1=449=449
k=8: 64*8+1=513=3^3 * 19
k=9: 64*9+1=577=577
k=10: 64*10+1=641=641
```

Euler only had to do five divisions by hand, since from the list above only the prime numbers come into question as divisors.

The sixth and seventh fermat number were factored into prime factors not before 1855 resp. 1970:

```
F_6=2**(2**6)+1=2**64=18446744073709▸
 ▸551617=274177 * 67280421310721
F_7=2**(2**7)+1=2**128=3402823669209▸
 ▸384634633746074317682114 57=5964958▸
 ▸9127497217 * 5704689200685129054 72▸
 ▸1
```

Even today neither we have a proof that the numbers $F_0, F_1, \ldots F_4$ are the only prime Fermat numbers nor do we know whether there exist infinitely many primes of this form. For all $n \geq 5$ no Fermat number proved to be prime yet. Many details about Fermat numbers can be found at http://www.prothsearch.net/fermat.html.

Primality tests of *very* large random numbers do not work yet. But there are very efficient algorithms for certain forms of numbers. Because there were no new large primes found with pure Fermat numbers, especially the GIMPS[2] project looks at *Mersenne* numbers. These are numbers of the form

$$2^p - 1$$

with p itself being a prime.

There the current prime records were achieved with numbers of that form.

```
sage: def mersenne(n):                    1
....:     for i in range(1,n):            2
....:         if is_prime(i):             3
```

[2] Great Internet Mersenne Prime Search

```
....:             print(f'{i}: 2**{i}-1={2**i-1}={factor(2**i-1)}')
....:
sage: mersenne(30)
2: 2**2-1=3=3
3: 2**3-1=7=7
5: 2**5-1=31=31
7: 2**7-1=127=127
11: 2**11-1=2047=23 * 89
13: 2**13-1=8191=8191
17: 2**17-1=131071=131071
19: 2**19-1=524287=524287
23: 2**23-1=8388607=47 * 178481
29: 2**29-1=536870911=233 * 1103 * 2089
```

Below 10000 there are only 22 such primes p.

```
sage: def countmersenne(N):
....:     count=0
....:     for i in range(1,N):
....:         if is_prime(i):
....:             if is_prime(2**i-1):
....:                 count=count+1
....:     return(count)
....:
sage: %time countmersenne(10000)
```

```
CPU times: user 9h 7min 26s, sys: 12
 s, total: 9h 7min 38s
Wall time: 9h 7min 39s
22
```

The biggest known integers proven to be prime are Mersenne prime numbers:

$$2^{82\,589\,933} - 1$$

This prime number has 24 862 048 decimal digits (found in 2018). For comparison: In 2005 the “only” 7 816 230 digit number $2^{25\,964\,951} - 1$ was proved to be prime.

Further details about the search for prime generating formulas can be found in the CrypTool Book (https://www.cryptool.org/images/ctp/documents/CT-Book-en.pdf) in chapter 3.

Fifth Chamber – First Hint

The number in the fifth chamber is the product of the two primes 29 153

and 36 833. Behind this lies a deeper secret.

You can find out, why for any natural number $n > 1$ the sum of the nth power of 4 and the 4th power of n is always a compound number (or composite number). To affirm that, it is not necessary to calculate the result $N = 1\,073\,792\,449$).

Maybe in other circumstances and without the make-believed peril to life Marco Polo would have been able to see that.

Assistance:

Please try the following (more or less self-evident) attempt of factoring a sum:

$$N = n^4 + 4^n \quad \text{for } n = 15$$

$$15^4 + 4^{15} = \left(15^2 + 15a + 2^{15}\right) \cdot \left(15^2 - 15a + 2^{15}\right)$$

The right hand side is now multiplied with the help of the distributive law:

$$
\begin{aligned}
&\left(15^2 + 15a + 2^{15}\right) \cdot \left(15^2 - 15a + 2^{15}\right) \\
&= 15^4 - 15^3 a + 2^{15} \cdot 15^2 + 15^3 a - 15^2 a^2 + 2^{15} \cdot 15a \\
&+ 2^{15} \cdot 15^2 - 2^{15} \cdot 15a + 4^{15} \\
&= 15^4 + 2^{15} \cdot 15^2 - 15^2 a^2 + 2^{15} \cdot 15^2 + 4^15 \\
&= 15^4 + 2^{16} \cdot 15^2 - 15^2 a^2 + 4^{15} \\
&= 15^4 + \underbrace{(2^8)^2 \cdot 15^2 - 15^2 a^2}_{\stackrel{!}{=}0} + 4^{15}
\end{aligned}
$$

Since the middle part must vanish if we want to get to $15^4 + 4^{15}$, it follows:

$$a = 2^8 = 256$$

With this we can easily and without any technical device determine a composition of $15^4 + 4^{15}$ into factors:

$$
\begin{aligned}
15^2 \pm 15a + 2^{15} &= 225 \pm 15 \cdot 256 + 32\,768 \\
&= \begin{cases} 225 + 3840 + 32768 &= 3683 \\ 225 - 3840 + 32768 &= 2915 \end{cases}
\end{aligned}
$$

So it is not only easy to answer the question (prime or not prime), but also to determine the two factors. Those factors *don't* need to be prime in general, but here they are:

```
sage: factor(15**4+4**15)
29153 * 36833
```

Behind this approach lies – mathematically – the decomposition of the polynomial $f(x) = x^4 + 4^n$ into two quadratic polynomials with integer coefficients. For this to be possible, n has to be odd. We look in to this in more detail in the second hint to the fifth chamber later on.

Marco Polo's probabilistic assumption, that small divisors dominate in compound numbers, was proven later. For any natural number $a > 1$ the following can be proven/shown (see literature [5]):

Within the first m natural numbers $1, 2, 3, \ldots, m$ the proportion of numbers with prime factors all above a relative to all numbers $\leq m$ (i.e. the fraction of the quantity of natural

numbers from 1 to m which only have prime factors $\geq a$, divided by m) converges to the following product for $m \to \infty$:

$$(*)\ \left(1-\tfrac{1}{2}\right)\cdot\left(1-\tfrac{1}{3}\right)\cdot\left(1-\tfrac{1}{5}\right)\cdot\left(1-\tfrac{1}{7}\right)\cdot\left(1-\tfrac{1}{11}\right)\cdot\ldots\cdot\left(1-\tfrac{1}{p}\right)$$

Here p is the biggest prime below a. This limit and therefore the percentage of numbers with prime factors all above a will become smaller and smaller with increased values of a. For example: Because 7 is the biggest prime below 10, the relative portion of the first m numbers with prime factors all above 10, for a growing m approaches

$$\left(1-\tfrac{1}{2}\right)\cdot\left(1-\tfrac{1}{3}\right)\cdot\left(1-\tfrac{1}{5}\right)\cdot\left(1-\tfrac{1}{7}\right)=\tfrac{8}{35}=0{,}228\,571\ldots$$

So only about 23 % of all numbers $1, 2, 3, \ldots, m$ (with a given big m) have *no* prime factors $2, 3, 5$ and 7.

The following SageMath listing shows how one can get a list of all $z \in \{7, \ldots, 50\}$ for which all prime divisors are ≥ 7:

```
#list numbers z with a<=z<=m with only large prime divisors
sage: def lst(a,m):
....:     l=[z for z in range(a,m+1) if all(z%p!=0 for p in prime_range(a))]
....:     return(l)
....:
sage: lst(7,50)
[7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49]
```

Here the 49 is the only non-prime. If you want to get a list with only those non-primes, you can do it like this:

```
#list numbers z with a<=z<=m with only large pr.div's, but leave out the primes
sage: def lst_lop(a,m):
....:     return([z for z in lst(a,m) if is_prime(z)==False])
....:
sage: lst_lop(7,50)
[49]
```

This is interesting especially for large *m*:

```
sage: lst_lop(11,200)
```

```
[121, 143, 169, 187]
```

To be able to make the above formula (∗) (see p. 55) plausible, one does not have to know the list lst(a,m) explicitly, but the number of its elements:

```
#count numbers z with a<=z<=m with only large prime divisors
sage: def cnt(a,m):
....:     count=0
....:     for z in range(a,m+1):
....:         if all(z%p!=0 for p in prime_range(a)):
....:             count=count+1
....:     return(count)
....:
sage: cnt(11,200)
46
sage: cnt(7,50)
13
```

Now you can calculate the fraction of the quantity of those numbers relative to *m*:

```
#fraction of cnt(a,m) relative to m
sage: def frac(a,m):
....:     return(cnt(a,m)/m)
```

```
....:
sage: frac(11,200)
23/100
```

Now we are ready to compare that fraction for large m and $a = 11$ with the product $(1-\frac{1}{2})\cdot\ldots\cdot(1-\frac{1}{7}) = \frac{8}{35}$:

```
sage: frac(11,100).n()
0.210000000000000
sage: frac(11,200).n()
0.230000000000000
sage: frac(11,1000000).n()
0.228570000000000
sage: 8/35.n()
0.228571428571429
```

The general case with arbitrary a and m:

```
#product to which frac(a,m) converges for m-->infty
sage: def prdct(a):
....:     x=1
....:     for p in prime_range(a):
....:         x=x*(1-1/p)
....:     return(x)
....:
sage: frac(53,100000).n()
0.138970000000000
```

```
sage: prdct(53).n()
0.138704092635850
```

Remark about another “fraction”:

The percentage of primes within the first m natural numbers ($m \geq 2$) is below $\frac{2}{\ln(m)}$. Here $ln(m)$ is the natural logarithm of the number m. So, as m increases this percentage approaches zero: Primes become increasingly rare within the first m numbers if m gets larger.

Here, we wish you much luck to figure out the deeper secret of the fifth chamber by yourself! As a remainder: The question was about the possibility to factor the polynomial $f(x) = x^4 + 4^n$ for positive integers n.

Fifth Chamber – Second Hint and Solution

The theorem is:

$N := n^4 + 4^n$ is compound (non-prime) for all natural numbers $n > 1$

Proof:

Case 1: n even

Here clearly N is also even, since we can factor out 2 from $n^4 + 4^n$. Further $N > 2$, ergo N is non-prime (or compound).

For an odd $n > 1$ the polynomial $f(x) = x^4 + 4^n$ can be written as a product of two polynomials with integer coefficients:

$$f(x) = (x^2 + 2^{\frac{n+1}{2}} \cdot x + 2^n) \cdot (x^2 - 2^{\frac{n+1}{2}} \cdot x + 2^n)$$

$$\begin{aligned}
& (x^2 + 2^{\frac{n+1}{2}} \cdot x + 2^n) \cdot (x^2 - 2^{\frac{n+1}{2}} \cdot x + 2^n) \\
= \; & x^4 - 2^{\frac{n+1}{2}} x^3 + 2^n x^2 \\
& + 2^{\frac{n+1}{2}} x^3 - \left(2^{\frac{n+1}{2}}\right)^2 x^2 + 2^{\frac{n+1}{2}} \cdot 2^n x \\
& + 2^n x^2 - 2^n \cdot 2^{\frac{n+1}{2}} x + \left(2^n\right)^2 \\
= \; & x^4 + (2 \cdot 2^n - 2^{2 \cdot \frac{n+1}{2}}) x^2 + 2^{2 \cdot n} \\
= \; & x^4 + (2^{n+1} - 2^{n+1}) x^2 + 4^n \\
= \; & x^4 + 4^n = f(x)
\end{aligned}$$

With SageMath it is easy to factor polynomials:

```
sage: def pn(n):
....:     return(x^4+4^n)
....:
sage: for i in range(10):
```

```
....:     print(f'{i}: {pn(i)}={factor(pn(i))}')
....:
....:
0: x^4 + 1=x^4 + 1
1: x^4 + 4=(x^2 + 2*x + 2)*(x^2 - 2*x + 2)
2: x^4 + 16=x^4 + 16
3: x^4 + 64=(x^2 + 4*x + 8)*(x^2 - 4*x + 8)
4: x^4 + 256=x^4 + 256
5: x^4 + 1024=(x^2 + 8*x + 32)*(x^2 - 8*x + 32)
6: x^4 + 4096=x^4 + 4096
7: x^4 + 16384=(x^2 + 16*x + 128)*(x^2 - 16*x + 128)
8: x^4 + 65536=x^4 + 65536
9: x^4 + 262144=(x^2 + 32*x + 512)*(x^2 - 32*x + 512)
```

You can see that those polynomials with even n don't split over $\mathbb{Z}$. But we want to mention that the polynomial $f(x)$ indeed splits into factors if we allow the coefficients to be complex numbers:

```
sage: R.<x>=ZZ[]
sage: def pn(n):
```

```
....:     return(x^4+4^n)
....:
sage: factor(pn(4))
x^4 + 256
sage: pn(4).change_ring(QQ).factor()
x^4 + 256
sage: pn(4).change_ring(CC).factor()
(x - 2.82842712474619 - 2.8284271247
 4619*I) * (x - 2.82842712474619 +
 2.82842712474619*I) * (x + 2.82842
 712474619 - 2.82842712474619*I) *
 (x + 2.82842712474619 + 2.82842712
 474619*I)
```

Here the coefficients are rounded of course. If one wants to get the exact coefficients of the linear factors (i.e. the roots or zeros) of $f(x)$ over $\mathbb{C}$, this is possible with SageMath like this:

```
sage: f=pn(4)
sage: roots=f.roots(QQbar,
  multiplicities=False)
sage: algroots=[roots[i].
  radical_expression() for i in
  range(len(roots))]
sage: algroots
[-4*(-1)^(1/4), 4*I*(-1)^(1/4), -4*I
```

```
▸*(-1)^(1/4), 4*(-1)^(1/4)]
```

If we go back to the number N which is computed by plugging n into $f(x)$ (i.e. $x = n$), this gives an explicit decomposition of the number $N = n^4 + 4^n$ for odd n:

$$N = n^4 + 4^n = (n^2 + 2^{\frac{n+1}{2}} \cdot n + 2^n) \cdot (n^2 - 2^{\frac{n+1}{2}} \cdot n + 2^n)$$

To complete the observation make sure that both factors above are > 1 for $n > 1$. It follows that N is composite.

Examples:

```
sage: def pl(n): #the plus-factor
....:     return(n^2+2^((n+1)/2)*n+2▸
 ▸^n)
....:
sage: def mi(n): #the minus factor
....:     return(n^2-2^((n+1)/2)*n+2▸
 ▸^n)
....: }
sage: for i in srange(3,16,2):
....:     print(f'{i}: N={i}^4+4^{i▸
 ▸}={pl(i)*mi(i)}={pl(i)}*{mi(i)}')
....:
3: N=3^4+4^3=145=29*5
```

```
5: N=5^4+4^5=1649=97*17
7: N=7^4+4^7=18785=289*65
9: N=9^4+4^9=268705=881*305
11: N=11^4+4^11=4208945=2873*1465
13: N=13^4+4^13=67137425=10025*6697
15: N=15^4+4^15=1073792449=36833*29153
```

The factors of this composition need not be primes. But for $n = 15$ this happens to be the case:

```
sage: factor(13^4+4^13)
5^2 * 37 * 181 * 401
sage: factor(15^4+4^15)
29153 * 36833
```

I don’t know who first offered this problem or who first solved it, but it is used as an exercise for students in number theory.

References

[1] G. Hardy / E.M. Wright: *An Introduction to the Theory of Numbers, fifth ed.,* Clarendon Press, Oxford (1984).

[2] K. Prachar: *Primzahlverteilung,* Springer-Verlag, Berlin – Göttingen – Heidelberg (1957).

[3] A.E. Ingham: *The Distribution of Primes Numbers,* Cambridge Tracts in Mathematics and Mathematical Physics, no. 30 (1990).

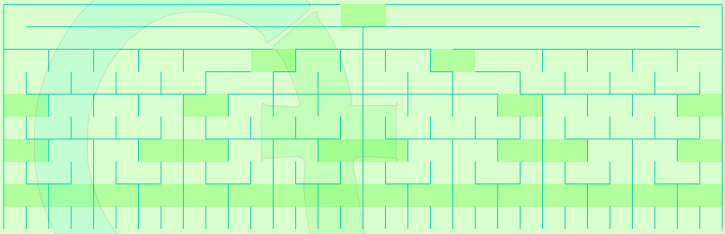
[4] D.M. Bressoud / S. Wagon: *A Course in Computational Number Theory,* Springer-Textbooks (with CD-ROM) (2000).

[5] R. Warlimont: *Eine Bemerkung zu einem Ergebnis von N.G. de Bruijn,* Monatshefte für Mathematik 74 (1970), 273-276.

[6] http://www.utm.edu/research/primes/notes

I’d like to take this opportunity to gracefully say thanks

- to Dr. C. Elsner, who developed the first draft of this hints,
- to G. Kramarz - von Kohout for his support with this hints and
- to Lowell Montgomery who very carefully helped fine tuning the translation which we started using two different translation robots.



Bernhard Esslinger and Doris Behrendt