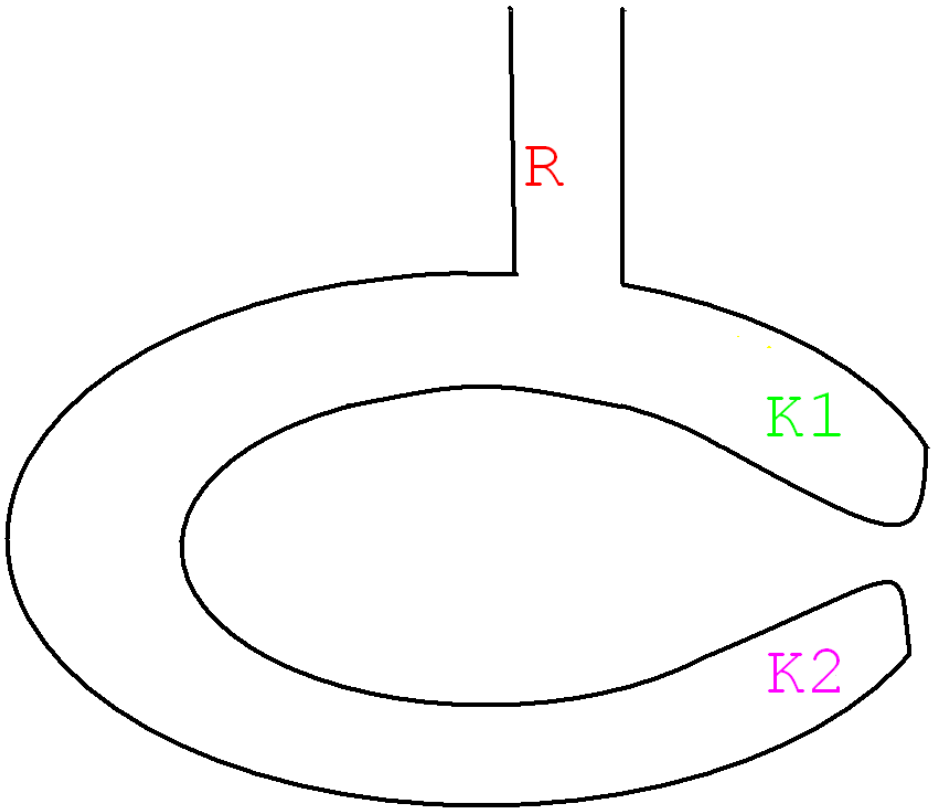
Liczby pierwsze na straży tajemnic

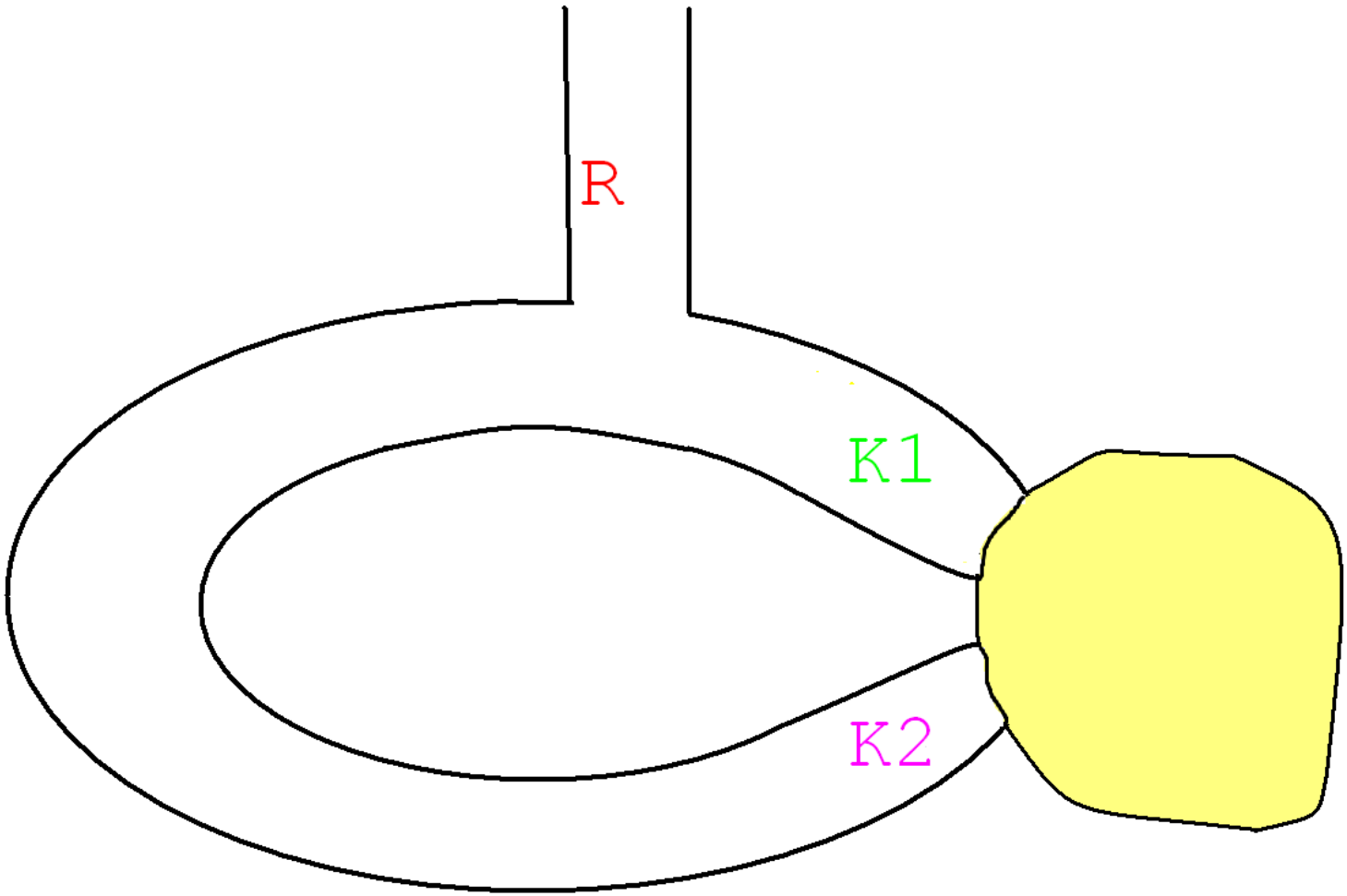
Barbara Roszkowska-Lech

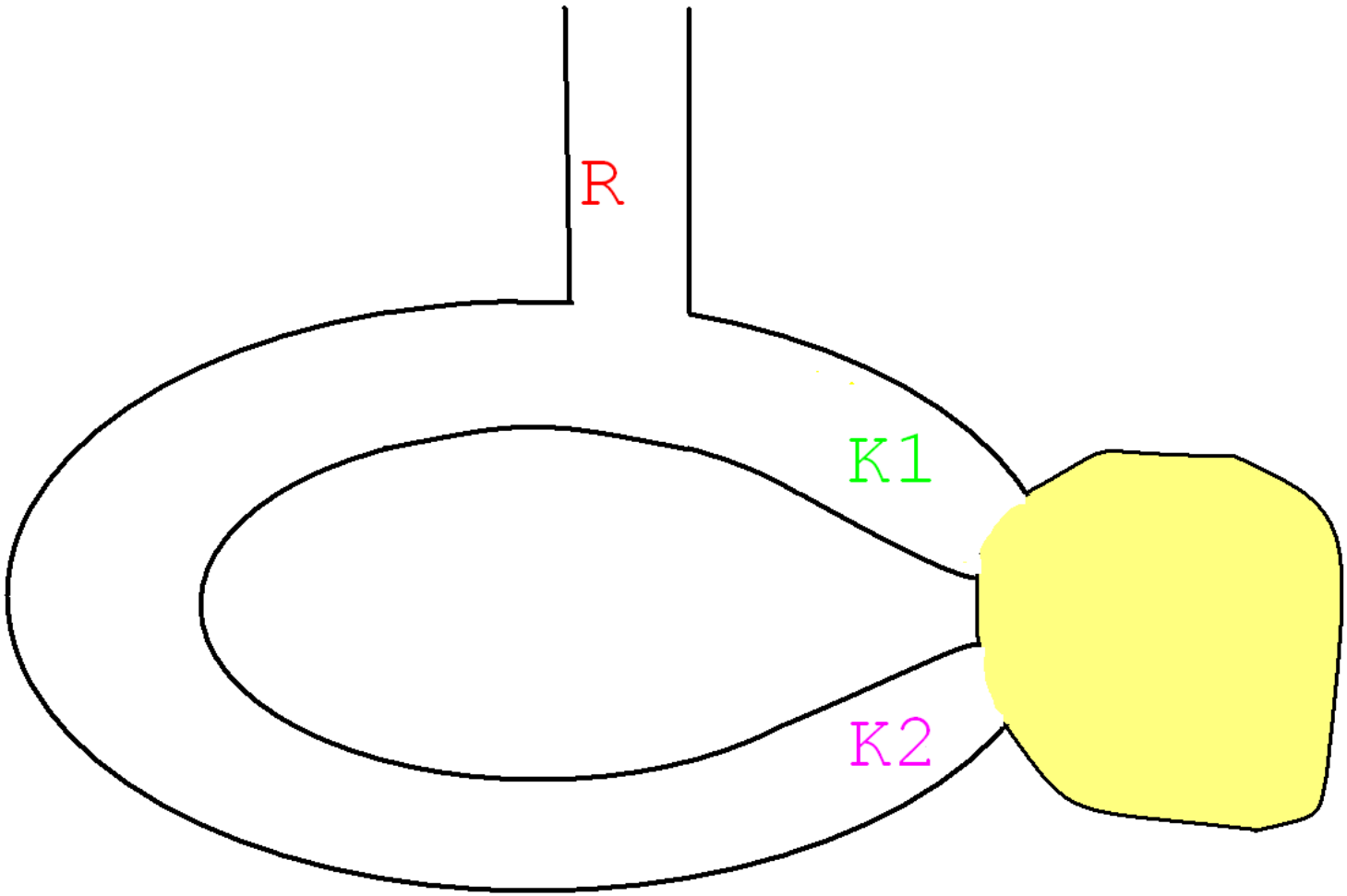
MATEMATYKA DLA CIEKAWYCH ŚWIATA

Liczby rzadzą światem

Ali-Baba


R
K1
K2


R
K1
K2


R
K1
K2

Szukamy pierwiastów kwadratowych mod n

Mamy daną liczbę całkowitą $1 \leq y \leq n - 1$

Szukamy pierwiastów kwadratowych mod n

Mamy daną liczbę całkowitą $1 \leq y \leq n-1$
Chcemy znaleźć liczbę całkowitą x, taką że

$$y \equiv_n x^2$$

Szukamy pierwiastów kwadratowych mod n

Mamy daną liczbę całkowitą $1 \leq y \leq n-1$
Chcemy znaleźć liczbę całkowitą x, taką że

$$y \equiv_n x^2$$

Przykład

Niech $n = 7$. Kongruencja $y \equiv_n x^2$ ma rozwiązanie wtedy i tylko wtedy, gdy $y \in \{1, 4, 2\}$.
Ponadto, dla każdego y z tego zbioru bedą istniały dokładnie dwa rozwiązania tej kongruencji.

Przykład

Niech $n = 7$. Kongruencja $y \equiv_n x^2$ ma rozwiązanie wtedy i tylko wtedy, gdy $y \in \{1, 4, 2\}$.
Ponadto, dla każdego y z tego zbioru bedą istniały dokładnie dwa rozwiązania tej kongruencji.

Definicja

Liczbę całkowitą a względnie pierwszą z liczbą n nazywamy resztą kwadratową modulo n, wtedy i tylko wtedy, gdy istnieje liczba całkowita x, taka że

$$x^2 \equiv_n a.$$

Przykład

Resztami kwadratowymi mod 11 są:

Przykład

Resztami kwadratowymi mod 11 są:

$$1, 4, 9, 5, 3.$$

Przykład

Resztami kwadratowymi mod 11 są:

$$1, 4, 9, 5, 3.$$

Reszty kwadratowe mod 15 to

Przykład

Resztami kwadratowymi mod 11 są:

$$1, 4, 9, 5, 3.$$

Reszty kwadratowe mod 15 to

$$1, 4.$$

Przykład

Resztami kwadratowymi mod 11 są:

$$1, 4, 9, 5, 3.$$

Reszty kwadratowe mod 15 to

$$1, 4.$$

Reszty kwadratowe modulo liczby pierwsze

Twierdzenie

Jest dokładnie $\frac{p-1}{2}$ reszt kwadratowych mod liczba pierwsza $p > 2$.

Reszty kwadratowe modulo liczby pierwsze

Twierdzenie

Jest dokładnie $\frac{p-1}{2}$ reszt kwadratowych mod liczba pierwsza $p > 2$.

Twierdzenie

Niech p będzie liczbą pierwszą $a \neq 0$. Kongruencja $x^2 \equiv_p a$ ma dwa rozwiązania, jeśli a jest resztą kwadratową mod p.

Przykład

$$2^2 \equiv_{15} 4,$$

Przykład

$$2^2 \equiv_{15} 4,$$

$$7^2 \equiv_{15} 4,$$

Przykład

$$2^2 \equiv_{15} 4,$$

$$7^2 \equiv_{15} 4,$$

$$8^2 \equiv_{15} 4,$$

Przykład

$$2^2 \equiv_{15} 4,$$

$$7^2 \equiv_{15} 4,$$

$$8^2 \equiv_{15} 4,$$

$$13^2 \equiv_{15} 4$$

Reszty kwadratowe mod n=pq

Niech $n = pq$, gdzie p oraz q liczby pierwsze. Jeśli liczba całkowita y jest kwadratem pewnej liczby całkowitej x modulo n to istnieją dokładnie cztery takie liczby x.

Reszty kwadratowe mod n=pq

Niech $n = pq$, gdzie p oraz q liczby pierwsze. Jeśli liczba całkowita y jest kwadratem pewnej liczby całkowitej x modulo n to istnieją dokładnie cztery takie liczby x.

Wynika stąd, że wśród liczb od 1 do n-1 istnieje dokładnie $\frac{n-1}{4}$ liczb będacych kwadratami mod n.

Reszty kwadratowe mod n=pq

Niech $n = pq$, gdzie p oraz q liczby pierwsze. Jeśli liczba całkowita y jest kwadratem pewnej liczby całkowitej x modulo n to istnieją dokładnie cztery takie liczby x.

Wynika stąd, że wśród liczb od 1 do n-1 istnieje dokładnie $\frac{n-1}{4}$ liczb będacych kwadratami mod n.
Załóżmy, że liczba y jest kwadratem mod n i chcemy znaleźć którąkolwiek liczbę całkowitą x taką, że

$$y \equiv_n x^2.$$

Chińskie Twierdzenie o resztach

Twierdzenie

Dla parami względnie pierwszych modułów $m_1, m_2, \ldots, m_r$, oraz liczb całkowitych $a_1, a_2, \ldots a_r$ układ kongruencji

$$x \equiv_{m_1} a_1$$

$$x \equiv_{m_2} a_2$$

$$\vdots$$

$$x \equiv_{m_r} a_r$$

ma dokładnie jedno rozwiązanie modulo $M = m_1 \cdot \ldots \cdot m_r$.

- Nie jest znana żadna **efektywna** metoda znajdowania któregokolwiek pierwiastka z y modulo n, jeśli znamy tylko n oraz y.

- Nie jest znana żadna **efektywna** metoda znajdowania któregokolwiek pierwiastka z y modulo n, jeśli znamy tylko n oraz y.
- Umiemy znaleźć wszystkie cztery pierwiastki z liczby y modulo n, jeśli dane są liczby p, q, y

- Nie jest znana żadna **efektywna** metoda znajdowania któregokolwiek pierwiastka z y modulo n, jeśli znamy tylko n oraz y.
- Umiemy znaleźć wszystkie cztery pierwiastki z liczby y modulo n, jeśli dane są liczby p, q, y
- Znajomość wszystkich czterech pierwiastków jest równoważna znajomości rozkładu liczby n na iloczyn.

Ali-Baba udowadnia, że zna pierwiastek kwadratowy mod $n = pq$

Ali-Baba wybiera losowo liczbę

$$x, \quad 1 \leq x \leq n - 1$$

oraz oblicza

$$x^2 \equiv_n y.$$

Ali-Baba udowadnia, że zna pierwiastek kwadratowy mod $n = pq$

Ali-Baba wybiera losowo liczbę

$$x, \quad 1 \leq x \leq n - 1$$

oraz oblicza

$$x^2 \equiv_n y.$$

Liczbę y ogłasza publicznie i twierdzi, że zna conajmniej jeden pierwiastek kwadratowy z tej liczby i potrafi każdego przekonać, że taki pierwiastek zna.

Ali-Baba udowadnia, że zna pierwiastek kwadratowy mod $n = pq$

- Ali-Baba wybiera losowo liczbę w, $1 \leq w \leq n-1$ oraz oblicza $w^2 \equiv_n z$. Liczbę z przesyła Weryfikatorowi.

Ali-Baba udowadnia, że zna pierwiastek kwadratowy mod $n = pq$

- Ali-Baba wybiera losowo liczbę w, $1 \leq w \leq n-1$ oraz oblicza $w^2 \equiv_n z$. Liczbę z przesyła Weryfikatorowi.
- Weryfikator prosi Ali-Babę o podanie liczby w lub iloczynu xw mod n.

Ali-Baba udowadnia, że zna pierwiastek kwadratowy mod $n = pq$

- Ali-Baba wybiera losowo liczbę w, $1 \leq w \leq n-1$ oraz oblicza $w^2 \equiv_n z$. Liczbę z przesyła Weryfikatorowi.
- Weryfikator prosi Ali-Babę o podanie liczby w lub iloczynu xw mod n.
- Weryfikator sprawdza: w pierwszym przypadku czy $w^2 \equiv_n z$, a w drugim czy $(xw)^2 \equiv_n yz$?

Ali-Baba udowadnia, że zna pierwiastek kwadratowy mod $n = pq$

- Ali-Baba wybiera losowo liczbę w, $1 \leq w \leq n-1$ oraz oblicza $w^2 \equiv_n z$. Liczbę z przesyła Weryfikatorowi.
- Weryfikator prosi Ali-Babę o podanie liczby w lub iloczynu xw mod n.
- Weryfikator sprawdza: w pierwszym przypadku czy $w^2 \equiv_n z$, a w drugim czy $(xw)^2 \equiv_n yz$?
- Powtarzają procedurę kilkakrotnie. Jeśli za każdym razem odpowiednia równość jest prawdziwa Weryfikator jest przekonany, że Ali-Baba zna pierwiastek kwadratowy z y

Cel

Dzielimy sekret

$$D$$

pomiędzy n osób
z których każde k jest w stanie odtworzyć D.

Użyteczne wielomiany

- Wybieramy dużą liczbę pierwszą p taką, że $p > n$ oraz $p > D$,

Użyteczne wielomiany

- Wybieramy dużą liczbę pierwszą p taką, że $p > n$ oraz $p > D$,
- Wybieramy losowo k-1 liczb $w_1, \ldots, w_{k-1}$ mniejszych od p,

Użyteczne wielomiany

- Wybieramy dużą liczbę pierwszą p taką, że $p > n$ oraz $p > D$,
- Wybieramy losowo k-1 liczb $w_1, \ldots, w_{k-1}$ mniejszych od p,
- Definiujemy funkcję $w(x) = D + \sum_{i=1}^{k-1} w_i x^i$,

Użyteczne wielomiany

- Wybieramy dużą liczbę pierwszą p taką, że $p > n$ oraz $p > D$,
- Wybieramy losowo k-1 liczb $w_1, \ldots, w_{k-1}$ mniejszych od p,
- Definiujemy funkcję $w(x) = D + \sum_{i=1}^{k-1} w_i x^i$,
- Obliczamy wartości $w(1), w(2), \ldots, w(n)$ mod p

Użyteczne wielomiany

- Wybieramy dużą liczbę pierwszą p taką, że $p > n$ oraz $p > D$,
- Wybieramy losowo k-1 liczb $w_1, \ldots, w_{k-1}$ mniejszych od p,
- Definiujemy funkcję $w(x) = D + \sum_{i=1}^{k-1} w_i x^i$,
- Obliczamy wartości $w(1), w(2), \ldots, w(n)$ mod p
- i-tej osobie przekazujemy wartość $w(i)$.

Dzielenie sekretu po chińsku

- Ustalamy ciag liczb parami względnie pierwszych $1 < m_1 < m_2 < \ldots < m_n$, spełniających warunek

$$m_1 m_2 \ldots m_k > D > m_n m_{n-1} \ldots m_{n-k+2}.$$

Dzielenie sekretu po chińsku

- Ustalamy ciag liczb parami względnie pierwszych $1 < m_1 < m_2 < \ldots < m_n$, spełniających warunek

$$m_1 m_2 \ldots m_k > D > m_n m_{n-1} \ldots m_{n-k+2}.$$

- Obliczamy fragmenty sekretu do podziału S_i, takie że $D \equiv_{m_i} S_i$.

Dzielenie sekretu po chińsku

- Ustalamy ciag liczb parami względnie pierwszych $1 < m_1 < m_2 < \ldots < m_n$, spełniających warunek

$$m_1 m_2 \ldots m_k > D > m_n m_{n-1} \ldots m_{n-k+2}.$$

- Obliczamy fragmenty sekretu do podziału S_i, takie że $D \equiv_{m_i} S_i$.
- Obliczamy $M = m_1 m_2 \ldots m_n$

Dzielenie sekretu po chińsku

- Ustalamy ciag liczb parami względnie pierwszych $1 < m_1 < m_2 < \ldots < m_n$, spełniających warunek

$$m_1 m_2 \ldots m_k > D > m_n m_{n-1} \ldots m_{n-k+2}.$$

- Obliczamy fragmenty sekretu do podziału S_i, takie że $D \equiv_{m_i} S_i$.
- Obliczamy $M = m_1 m_2 \ldots m_n$
- Udział i-tej osoby to (S_i, m_i, M)

Dziękuję za uwagę