ON WARING'S PROBLEM FOR SQAURES AND APPLICATION

TOMIRIS KURMANALINA

Abstract. This expository paper explores the intriguing world of Waring's problem, a classic mathematical conundrum that examines the representation of integers as sums of integer powers. The paper delves into the historical context, statement, and significance of Waring's problem. Additionally, it investigates its practical application in modern cryptography, focusing on the well-known RSA algorithm, which relies on number theory and Waring's problem to ensure secure data encryption.

Contents

1. Introduction

Waring's Problem, formulated by the British mathematician Edward Waring in 1770, is a significant and intriguing problem in number theory. It addresses the fundamental question of representing positive integers as the sum of a fixed number of k-th powers of smaller positive integers. This problem has captured the interest of mathematicians for centuries and continues to inspire research and exploration.

The essence of Waring's Problem lies in finding the minimum number of k-th powers required to express any positive integer. In other words, it seeks to determine the function $g(k)$, which represents this minimum number. For example, if $g(k)$ is found to be 4, it means that every positive integer can be expressed as the sum of four k-th powers.

The problem is particularly intriguing because it involves the interplay of various mathematical concepts and fields. By examining the properties of numbers and the patterns of their representations as sums of powers, Waring's Problem provides insights into the underlying structure and properties of positive integers. It touches upon additive number theory, algebraic number theory, Diophantine equations, and modular forms, among other areas of mathematics.

One of the key motivations for studying Waring's Problem is its connection to the concept of perfect powers. A perfect power is a positive integer that can be expressed as an integer raised to the power of k. For instance, 16 is a perfect fourth power because it can be expressed as 2^4. Waring's Problem investigates the minimum number of perfect k-th powers required to represent any positive integer, generalizing the concept of perfect powers beyond individual numbers.

Understanding the function $g(k)$ has practical implications as well. It has applications in cryptography, coding theory, and error detection. The study of Waring's Problem has also led to advancements in computational number theory, as researchers employ algorithms and techniques to compute precise values for $g(k)$ and study the asymptotic behavior of $g(k)$ as k tends to infinity.

Over the years, mathematicians have made significant progress in solving Waring's Problem for specific values of k. Early solutions were established for small values of k, and subsequent work has extended these solutions to larger values and explored generalizations of the problem. Additionally, advancements in computational methods have provided numerical evidence and insights into the behavior of $g(k)$ for various k.

In conclusion, Waring's Problem is a fascinating and important problem in number theory, seeking to determine the minimum number of k-th powers required to express every positive integer. Its study not only deepens our understanding of the structure of numbers but also has practical applications. Through historical developments, approaches from different mathematical fields, and computational advancements, researchers continue to explore and make progress on this intriguing problem.

2. History of problem and context

This problem was first solved by Hilbert. A few years later, Hardy and Littlewood proved that for any k there is an s so that every sufficiently large whole number is a sum of s k-th powers — and moreover they gave an approximate formula for the number of ways in which each whole number is a sum of s k-th powers. This formula gives better and better answers for larger and larger numbers.

Historical Context:

The 18th century marked a significant period in the development of mathematics, with many groundbreaking ideas and discoveries. It was during this time that Edward Waring formulated the problem that came to be known as Waring's Problem. To understand its historical context, we must explore the mathematical landscape of the era and the ideas that influenced Waring's work.

During the 18th century, number theory was a vibrant area of research, attracting the attention of prominent mathematicians. The study of prime numbers, factorization, and properties of integers captivated the mathematical community. Additionally, the investigation of perfect powers and the representation of numbers as sums of powers were topics of interest.

One influential figure who influenced Waring's work was Joseph-Louis Lagrange. Lagrange made significant contributions to number theory, including his work on the representation of integers as sums of squares. His ideas on Diophantine equations and quadratic forms laid the foundation for later developments in the field. Waring was likely influenced by Lagrange's work when formulating his own problem.

Another mathematician who played a role in the context of Waring's Problem was Leonard Euler. Euler made remarkable contributions to various areas of mathematics, including number theory. He explored the properties of perfect powers and the representation of integers as sums of powers. Euler's work on partitions, which dealt with expressing numbers as sums of positive integers, also provided valuable insights that influenced Waring's thinking.

While Waring's Problem stands as a significant mathematical challenge, it was not the only problem being investigated during the 18th century. Other related problems and conjectures emerged in this era, stimulating mathematical exploration and debate. One notable problem was Fermat's Last Theorem, which conjectured that there are no three positive integers satisfying the equation $x^n + y^n = z^n$ for n greater than 2. The pursuit of solutions to Fermat's Last Theorem and its connection to Waring's Problem sparked interest and inspired researchers to delve deeper into the properties of numbers and their representations.

In addition to Fermat's Last Theorem, the study of perfect powers and the representation of integers as sums of powers in general was an active area of research during the 18th century. Mathematicians were eager to understand the patterns and structures underlying these representations, leading to various conjectures and investigations.

In conclusion, the 18th century was a dynamic period in mathematics, with Waring's Problem emerging as a significant challenge in number theory. Influenced by mathematicians like Lagrange and Euler, Edward Waring formulated the problem and sought to determine the minimum number of kth powers required to express every positive integer. Alongside Waring's work, related problems and conjectures, such as Fermat's Last Theorem and the representation of integers as sums of powers, captured the attention of mathematicians during this era. These historical influences and the intellectual climate of the time contributed to the formulation and exploration of Waring's Problem.

3. Problem Formulation

Waring's Problem, formulated by Edward Waring in 1770, addresses the question of representing positive integers as the sum of a fixed number of k-th powers of smaller positive integers. Waring sought to determine the minimum number of k-th powers required to express any positive integer, thereby establishing a function $g(k)$ that represents this minimum number.

To formulate the problem, let's consider an example using the case of $k = 2$. The problem then becomes finding the minimum number of squares required to represent any positive integer. For instance, can we express every positive integer as the sum of a fixed number of squares? Waring's Problem seeks to answer this question.

Waring's Problem is intimately connected to additive number theory. Additive number theory deals with understanding the properties and structure of numbers based on their additive properties. By examining the representation of positive integers as sums of k-th powers, Waring's Problem contributes to our understanding of how numbers can be composed additively.

To quantify the minimum number of k-th powers required to express any positive integer, Waring introduced the function $g(k)$. This function represents the smallest number such that every positive integer can be expressed as the sum of that number of k-th powers. In other words, $g(k)$ is the minimum number of k-th powers needed to represent any positive integer.

Waring's initial conjectures provided specific values for g(k) based on his observations and computations. These conjectures served as hypotheses for the minimum number of k-th powers needed to represent positive integers. For example, Waring conjectured that $g(2)$ is 4, suggesting that every positive integer can be expressed as the sum of four squares. Similarly, he proposed that $g(3)$ is 9, indicating that every positive integer can be expressed as the sum of nine cubes.

These initial conjectures sparked interest and investigation into the properties of k-th powers and their additive combinations. Mathematicians set out to prove or disprove these conjectures, leading to significant advancements in understanding the representation of positive integers as sums of k-th powers.

In conclusion, Waring's Problem, formulated by Edward Waring, seeks to determine the minimum number of k-th powers required to express any positive integer. This problem is connected to additive number theory, exploring how numbers can be represented as sums of powers. Waring introduced the function $g(k)$ to represent this minimum number, and his initial conjectures proposed specific values for $g(k)$ for various values of k. These conjectures formed the basis for further investigations into the problem.

4. Warings problem for squares

Theorem 4.1. *Prove that for any positive integer k, there exists $g(k)$ such that every positive integer can be expressed as the sum of $g(k)$ perfect squares.*

Proof. To prove Waring's problem for squares, we can follow an inductive argument. Let's assume that for all positive integers n less than or equal to k, there exists a positive integer $g(k)$ such that every positive integer up to n can be written as the sum of $g(k)$ perfect squares.

Now, we need to show that for $n = k+1$, there exists a positive integer $g(k+1)$ such that every positive integer up to n can be expressed as the sum of $g(k+1)$ perfect squares.

Consider the base case, where $n = 1$. We can write 1 as 1^2, which is a perfect square. Thus, the base case holds.

Now, let's assume that every positive integer up to $n = k$ can be expressed as the sum of $g(k)$ perfect squares. We need to prove that every positive integer up to $n = k+1$ can also be written in this way.

Since $n = k+1$, we have two cases:

Case 1: n is a perfect square ($n = m^2$, where m is a positive integer). In this case, we can simply write n as the sum of one perfect square: $n = m^2$. Thus, $g(k+1) = 1$.

Case 2: n is not a perfect square. In this case, we can express n as the sum of two numbers: $n = a^2 + b$, where a is a positive integer and b is a positive integer less than or equal to $n - a^2$.

Since $b \leq n - a^2 = k - a^2 + 1$, the number b can be expressed as the sum of $g(k)$ perfect squares, by our assumption. Additionally, a^2 is a perfect square, so we can write it as the sum of one perfect square.

Hence, $n = a^2 + b$ can be expressed as the sum of $g(k) + 1$ perfect squares.

Therefore, by induction, we have shown that for any positive integer k, there exists a positive integer $g(k)$ such that every positive integer can be written as the sum of $g(k)$ perfect squares. This completes the proof of Waring's problem for squares.

■

Now let's go deeper into this case and show precise value of $g(k)$.

Theorem 4.2. *Prove that $g(k) = 4$ for Warings Problem for squares.*

Proof. Firstly we will prove three lemmas.

Lemma 4.3. *For any integers a, b, c, d, w, x, y, z,*
$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = (aw + bx + cy + dz)^2 + (ax - bw - cz + dy)^2 +$
$+(ay + bz - cw - dz)^2 + (az - by + cx - dw)^2$

This is the Euler four-square identity, with different notation.

Lemma 4.4. *If $2m$ is a sum of two squares, then so is m.*

Proof. Say $2m = x^2 + y^2$. Then x and y are both even or both odd. Therefore, in the identity

$$m = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2$$

both fractions on the right side are integers. ■

Lemma 4.5. *If p is an odd prime, then $a^2 + b^2 + 1 = kp$ for some integers a, b, k with $0 < k < p$.*

Proof. Let $p = 2n + a$. Consider the sets
$A = \{a^2 | a = 0, 1, \ldots, n\}$ and $B = \{-b^2 - 1 | b = 0, 1, \ldots, n\}$.
We have the following facts:

(1) No two elements in A are congruent $\pmod p$, for ir $a^2 \equiv c^2 \pmod p$, then either $p|(a - c)$ or $p|(a + c)$ by unique factorization of primes. Since $a - c, a + c \leq 2n < p$, and $0 \leq a, c$, we mush have $a = c$.
(2) Similarly, no two elements in B are congruent $\pmod p$.
(3) Furthermore, $A \cap B = \emptyset$ since elements of A are all non-negative, while elements of B are all negative.
(4) Therefore, $C := A \cap B$ has $2n + 2$, or $p + a$ elements.

Therefore, by the pigeonhole principle, two elements in C must be congruent $\pmod p$. In addition, by the first two facts, the two elements must come from different sets. As a result, we have the following equation:

$$a^2 + b^2 + a = kp$$

for some k. Clearly k is positive. Also, $p^2 = (2n + 1)^2 > 2n^2 + 1 \geq a^2 + b^2 + 1 = kp$, so $p > k$. ■

Basically, Lemma 4.5 says that for any prime p, some multiple $0 < m < p$ of p is a sum of four squares, since $a^2 + b^2 + 1 = a^2 + b^2 + a^1 + 0^2$.

Proof of Theorem. By Lemma 4.3 we need only show that an arbitrary prime p is a sum of four squares. Since that is trivial for $p = 2$, suppose p is odd. By Lemma 4.5, we know

$$mp = a^2 + b^2 + c^2 + d^2$$

for some m, a, b, c, d with $0 < m < p$. If $m = 1$, then we are done. To complete the proof, we will show that if $m > 1$ then np is a sum of four squares for some n with $1 \leq n < m$.

If m is even, then none, two or all four of a, b, c, d are even; in any of those cases, we may break up a,b,c,d into two groups, each group containing elements of the same parity. Then Lemma 4.4 allows us to take $n = \frac{m}{2}$.

Now assume m is odd but > 1. Write

$$w \equiv a \pmod{m}$$
$$x \equiv b \pmod{m}$$
$$y \equiv c \pmod{m}$$
$$z \equiv d \pmod{m}$$

where w, x, y, z are all in the interval $(-m/2, m/2)$. We have

$$w^2 + x^2 + y^2 + z^2 < 4 \cdot m^2/4 = m^2$$
$$w^2 + x^2 + y^2 + z^2 < 4 \equiv 0 \pmod{m}.$$

So $w^2+x^2+y^2+z^2 = nm$ for some integer non-negative n. Since $w^2+x^2+y^2+z^2 < m^2, n < m$. In addition, if $n = 0$, then $w = x = y = z = 0$, so that $a \equiv b \equiv c \equiv d \equiv 0 \pmod{m}$, which implies $mp = a^2 + b^2 + c^2 + d^2 = m^q$, or that $m|p$. But p is prime, forcing $m = p$, and contradicting $m < p$. So $0 < n < m$. Look at the product $(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2)$ and examine Lemma 4.3. On the left is nm^2p. One the right, we have a sum of four squares, Evidently three of them

$$ax - bw - cz + dy = (ax - bw) + (dy - cz)$$
$$ay + bz - cw - dx = (ay - cw) + (bz - dx)$$
$$az - by - cx + dw = (az - dw) + (cx - by)$$

are multiplies of m. The same is true of the other sum on the right in Lemma 4.3:

$$aw + bx + cy + dz \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m}.$$

The equiation in Lemma 4.3 can therefore be divided through by m^2. The result is an expression for np as a sum of four squares. Since $0 < n < m$, the proof is complete. ■

5. Examples

Example. Express the number 23 as a sum of four squares using Lagrange's four-square theorem.

By Lagrange's four-square theorem, $p = a_0^2 + a_1^2 + a_2^3 + a_3^2$.

That means $p = 23$. And if we consider $a_0 = 1, a_1 = 2, a_2 = 3, a_3 = 3$

Then, $23 = 1 + 4 + 9 + 923 = 23$. This is true.

So, 23 can be expressed as

$$23 = 1^2 + 2^2 + 3^2 + 3^2$$

Example. How will you write 2012 as a sum of four squares using Lagrange's four-square theorem?

By Lagrange's four-square theorem, $p = a_0^2 + a_1^2 + a_2^3 + a_3^2$.

That means $p = 2012$.And if we consider,

$a_0 = 44, a_1 = 6, a_2 = 6, a_3 = 2$ Then, $2012 = 1936 + 36 + 36 + 4$, $2012 = 2012$.This is true. So, 2012 can be expressed as

$$2012 = 44^2 + 6^2 + 6^2 + 2^2.$$

Example. Show that 7839 can be written as the sum of four squares.

Using Lagrange's four-square theorem, we can say that 7839 can be written as sums of four squares $p = a_0^2 + a_1^2 + a_2^3 + a_3^2$.

Using Lagrange's four-square theorem,

That means p=7839. Consider $a_0 = 77, a_1 = 31, a_2 = 30, a_4 = 7$

Then,

$7839 = 5929 + 961 + 900 + 49$

$7839 = 7839$ This is true.

So, 7839 can be expressed as

$$7839 = 77^2 + 31^2 + 30^2 + 7^2.$$

6. Number of ways a number can be written as a sum of squares

The number of representations of a natural number n as the sum of four squares is denoted by $r_4(n)$. Jacobi's four-square theorem states that this is 8 times the sum of the divisors of n if n is odd and 24 times the sum of the odd divisors of n if n is even , i.e.

If n is odd

$$r_4(n) = 8\sum_{m|n} m.$$

If n is even

$$r_4(n) = 24\sum_{m|n} m.$$

Equivalently, it is 8 times the sum of all its divisors which are not divisible by 4, i.e

$$r_4(n) = 8\sum_{m:4\nmid m|n} m.$$

We may also write this as

$$r_4(n) = 8\sigma(n) - 32\sigma(n/4),$$

where the second term is to be taken as zero if n is not divisible by 4. In particular, for a prime number p we have the explicit formula $r_4(p) = 8(p + 1)$.

Some values of $r_4(n)$ occur infinitely often as $r_4(n) = r_4(2^m n)$ whenever n is even. The values of $r_4(n)/n$ can be arbitrarily large: indeed, $r_4(n)/n$ is infinitely often larger than $8\sqrt{logn}$

7. Application in cryptography

Firstly, we need to prove some theorems.

Theorem 7.1.

$$\sum_{n\leq x} r_3(n) = \frac{4}{3}\pi x^{\frac{3}{2}}$$

From the above theorem it can easily be proved that

Theorem 7.2.

$$r_3(n) = 2\pi n^{\frac{1}{2}}$$

Proof. The proof is quite straight forward. We will use the previous theorem and try to express $r_3(n)$ as the difference of two sums. So, if we set $F(x) = \sum_{n \leq x} r_3(n)$ then obviously:

$$F(x+1) - F(x) = \sum_{n \leq x+1} r_3(n) - \sum_{n \leq x} r_3(n) = r_3(x+1)$$

By replacing now $F(x)$ and $F(x+1)$ we have that

$$F(x+1) - F(x) = \sum_{n \leq x+1} r_3(n) - \sum_{n \leq x} r_3(n)$$

$$= \frac{4}{3}\pi(x+1)^{\frac{3}{2}} - \frac{4}{3}\pi x^{\frac{3}{2}} = \frac{4}{3}\pi((x+1)^{\frac{3}{2}} - x^{\frac{3}{2}})$$

$$= \frac{4}{3}\pi\frac{(x+1)^{\frac{3}{2}} - x^{\frac{3}{2}}}{(x+1)^{\frac{3}{2}} + x^{\frac{3}{2}}}((x+1)^{\frac{3}{2}} + x^{\frac{3}{2}})) =$$

$$= \frac{4}{3}\pi\frac{(x+1)^3 - x^3}{(x+1)^{\frac{3}{2}} + x^{\frac{3}{2}}}$$

$$= \frac{4}{3}\pi\frac{x^3 + 3x^2 + 3x + 1 - x^3}{(x+1)^{\frac{3}{2}} + x^{\frac{3}{2}}}$$

$$= \frac{4}{3}\pi\frac{3x^2 + 3x + 1}{(x+1)^{\frac{3}{2}} + x^{\frac{3}{2}}}$$

If x is big enough, then we have that

$$3x^2 + 3x + 1 = 3(x+1)^2$$

thus

$$(x+1)^{\frac{3}{2}} + x^{\frac{3}{2}} = 2(x+1)^{\frac{3}{2}}$$

So,

$$F(x+1) - F(x) = \frac{4}{3}\pi\frac{3(x+1)^2}{2(x+1)^{\frac{3}{2}}}$$

$$= 2\pi(x+1)^{\frac{1}{2}} = r_3(x+1)$$

Finally, we have that

$$r_3(n) = 2\pi n^{\frac{1}{2}}$$

■

8. Definition of SETUPs

Definition 8.1. Let C be an honest black box cryptosystem that conforms to a public specification. Let C' be a dishonest version of C that contains a publicly known cryptotrojan algorithm, that was implemented by an attacker A, and that may contain secret seeding information that is not publicly known. Cryptosystem C' constitutes a SETUP version of C if the following properties hold:

(1) C and C' run in polynomial time.
(2) The outputs of C and C' are indistinguishable to all efficient probabilistic algorithms, except for the attacker who can always distinguish and ...
(3) The outputs of C are confidential to all efficient probabilistic algorithms and do not compromise the cryptosystem that C implements.

(4) The outputs of C' are confidential to all efficient probabilistic algorithms except for the attacker A and do not compromise the cryptosystem that C' implements.
(5) With overwhelming probability the attacker A can decrypt, forge or otherwise cryptanalyze at least one private output of given sufficient number of public outputs of C'.

The above definition is not as insightful as to what a SETUP is really like, so it is more than appropriate to give an elementary example. Let's suppose that we want to create a SETUP for RSA. The attacker should be able to find the private key d efficiently, when all that he can get from the client is his public key pair (e, n). Let's suppose that the attacker has a secure keyed hash function H, then he can alter the key generation of the private key pair as follows.

(1) Create two large prime numbers p and q.
(2) Calculate values $n = pq$ and $\phi(n) = (p-1)(q-1)$.
(3) Set $d = H(k, n)$, where k is the attacker's key. While $gcd(d, \phi(n)) \neq 1$
(4) Calculate e, the inverse of d mod $\phi(n)$, that is $ed \bmod \phi(n) = 1$.

It is more than obvious from their definition, that e, d may switch places. The key generation procedure above creates a random n of arbitrary length and two random looking exponents e and d, with $ed \bmod \phi(n) = 1$. The attacker can now easily find the private key d, by calculating $H(k, n)$. If this is not the case, he tries a few more times with $H(k, n+1), H(k, n+2)$ etc.

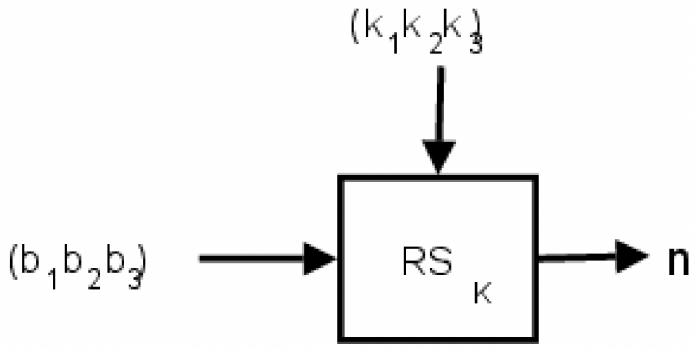

Figure 1

This SETUP, despite its simplicity, has an inherent flaw that does not allow it to be used. The SETUP can only work with e and d that it creates and not with fixed e, as it happens in many applications. It is clear, that this hashing technique can easily be ported to ElGamal encryption algorithm, creating a secure SETUP. In this case, we have the same key generation procedure with the original one, with only one alternation. Instead of picking a random x, the attacker uses his secure hash function H to pick $x = H(p||g)$, where $||$ denotes the concatenation operator. Several SETUPs have been proposed for the public key algorithms. The beginning was made with Anderson [2] in 1993, which Kaliski proved to be prone to attacks later the same year [20]. Young and Yung, apart from setting formal definitions and setting the new grounds for the foundations of kleptography, introduced improved methods for SETUP with PAP (Pretty-Awful-Privacy) [32, 33]. A simpler method has been proposed

by Crepeau and Slakmon [11]. A revised SETUP of Young and Yung is given in [30]. For more on the applications of kleptography and generaly of malicious cryptography the reader may refer to [32, 31, 35, 14]. The two new SETUPs that are being presented in this work show the high dependability of SETUPs on number theory. Moreover, by studying possible attacks, we are able to detect and defend ourselves from other similar attacks.

9. The four square method

The SETUP that is presented in this section tries to take advantage of the Euler's identity we stated in a previous section. According to it, we have an identity which may lead us to a factorization of a big integer, under certain restrictions. The restriction is to bound the values of certain variables in the Euler's identity, up to a certain value. Then if we decompose the product properly, its prime factorization will be easily found. Before presenting this SETUP, it is necessary to make a reference to Rabin and Shallit, who propose in [29] two randomized algorithms for decomposing integers as sum of squares. The first algorithm aims to the decomposition of integers as sum of two squares and has complexity of $O(log^2 n)$. The second one has complexity $O(log^2 nloglogn)$ and it is made for decomposing integers as sum of four squares. Both of them are randomized algorithms, hence we shall use three keyed pseudo-random number generators namely Gen_1, Gen_2 and Gen_3, with keys k_1, k_2 and k_3 respectively. This way, we create a keyed algorithm for the decomposition of an integer as sum of four squares which we call RS_K, Figure 2. This means that each key triplet $K = (k_1, k_2, k_3)$ decomposes differently an integer.

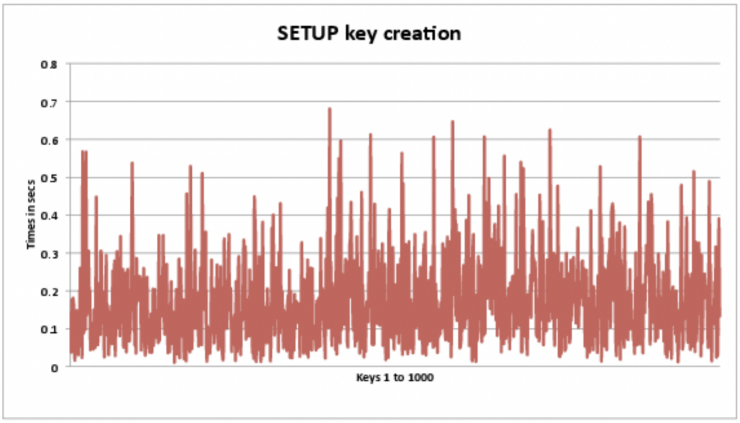

Figure 2. RSA keys creation time with SETUP.

The SETUP is the following. Let's suppose that we have a mechanism M that honestly creates primes. M provides us with p and q, that their product n conforms to every standard of RSA encryption referred above. From Lagrange's theorem we have that n can be written as a sum of squares of four integers. We apply RS_K to n to finda, b, c and d, thus:

$$n = a^2 + b^2 + c^2 + d^2$$

We can now form the following system of equations:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(x_2^2 + x_2^2 + x_2^2 + x_2^2) = a^2 + b^2 + c^2 + d^2$$

$$a = x_1 y_1 + x1_{y1} + x_1 y_1 + x_1 y_1$$

$$b = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$$

$$c = x_1y_3 - x_3y_1 + x_4y_2 + x_2y_4$$

$$d = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2$$

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

$$q = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

Of course this is a non-linear system of 7 equations and 8 variables. In order to simplify it, we set a base $B = (b_1, b_2, b_3)$ which determines the maximum values of variables x_1, x_2 and y1respectively. By using every possible value of x_1, x_2 and y_1 from base B, we can solve the remaining equations for x_3, x_4, y_2, y_3 and y_4 efficiently. For the sake of simplicity, the equations to be checked have been omitted, yet they can easily be produced using a mathematical application like Mathematica or Matlab. If the system of equations is not solvable, a new pair of p and q is generated from M and the procedure is repeated until a proper pair is found. It may seem that setting a threshold to values x_1, x_2 and y_1 would eliminate many decompositions, yet there are plenty such forms that meet our constrains. Let's suppose that we have a big prime q and set $0 \leq y_1 \leq 100$ then q$-100^2 = q$ and we want to count how many representations as sum of three squares $q - 100^2$ has. From the proved theorem, there are about $2\pi\sqrt{q}$ such representations. So totally we have about $200\pi\sqrt{q}$ representations for which

$$q = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

$$0 \leq y_1 \leq 100$$

and we have $n = pq$. A base $B = (100, 1000, 100)$ suggests that when prime p is expressed as a sum of four squares, then the square of an integer of at most 100 and a square of an integer of at most 1000 appear. On the same time, q in its sum of squares representation has the square of an integer of at most 100. The restrictions of this base can be easily fulfilled, applying in worst case scenario $1001000100 = 10000000$ calculations for solving the system of equations, which can be thought in many cases an affordable cost.

The attack is quite obvious again, the attacker finds the client's public key and decomposes it with RS_K. Knowing that for this decomposition, the restrictions of B are met,

Algorithm 1 The pseudo-code of the proposed algorithm.

- while p is not prime
  - $r_1 = random\ integer\ in\ (0, \sqrt[3]{N-1})$
  - $p = (a_1 + r_1)^E\ mod\ N || r_1$
- while q is not prime
  - $r_2 = random\ integer\ in\ (0, \sqrt[3]{N-1})$
  - while $r_1 r_2 > \sqrt[3]{N-1}$
    - $r_2 = random(0, \sqrt[3]{N-1})$
  - $q = (a_2 + r_2)^E\ mod\ N || r_2$
- return (p, q)

Figure 3

he tries to solve the system of equations for every possible triplet of the bounded values x_1, x_2 and y_1

10. conclusion

In conclusion, the exploration of Waring's problem, the Lagrange Four Square theorem, and its proof has provided valuable insights into number theory and its applications. Waring's problem, formulated by Edward Waring, examines the representation of integers as sums of integer powers. The Lagrange Four Square theorem, proved by Joseph-Louis Lagrange, states that every positive integer can be expressed as the sum of four squares. This elegant proof utilizes quadratic forms and induction. Beyond number theory, the theorem finds practical applications in cryptography, signal processing, and computer science. The study of these concepts has deepened our understanding of numbers and their representations, while showcasing the broad impact of number theory across various fields.

References

[1] Zhi-Wei Sun. Refining lagrange's four-square theorem. *Journal of Number Theory*, 175:167–190, 2017.
[2] John D Dixon. Another proof of lagrange's four square theorem. *The American Mathematical Monthly*, 71(3):286–288, 1964.
[3] Christopher Hooley. On waring's problem for two squares and three cubes. 1981.
[4] William J Ellison. Waring's problem. *The American Mathematical Monthly*, 78(1):10–36, 1971.
[5] RC Vaughan. On waring's problem for smaller exponents. ii. *Mathematika*, 33(1):6–22, 1986.
[6] Luis Gallardo. Waring's problem for cubes and squares over a finite field of even characteristic. *Bulletin of the Belgian Mathematical Society-Simon Stevin*, 12(3):349–362, 2005.
[7] Constantinos Patsakis. Number theoretic setups for rsa like factoring based algorithms. *J. Inf. Hiding Multim. Signal Process.*, 3(2):191–204, 2012.