Which influence does the cardinality of the algebraic structure $\mathbb{Z}_n$ have on the suitability of RSA for four-digit PIN encryption and decryption?

Subject: Mathematics   Word count: 4000 words

Contents page

Introduction

People have many Personal Identification Numbers (PINs) for websites and are unable to store or remember seldom-used PINs. People often use one PIN for multiple websites to reduce the number of PINs to remember, but if a PIN is stolen and used for several websites, then a person whose data has been stolen is unlikely to receive compensation. People may store their PINs electronically or on paper, but paper can be stolen. Therefore, it is important to find a method of encrypting PINs securely only with a calculator to prevent losses as a result of PIN theft. Encrypted PINs may be stored electronically, but not the keys for encryption or decryption. Encryption should not be performed on a hackable computer. Since PINs are real numbers restricted to a few digits (finite elements), encryption of PINs is a problem within discrete and finite mathematics. Integers and finite sets are typical subtopics within Number Theory. Old dials, dice, playing cards, and subtopics within game theory are examples of where finite sets have been applied before.

Examples of cryptosystems are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Public Key Cryptography, such as Diffie-Hellman Key Exchange (DHKE), Elliptic Curve Cryptosystems (ECC), and the RSA cryptosystem. DES and AES were created to encrypt pages of text. ECC would be too time-consuming and vulnerable to calculation errors, so the only two appropriate methods of encryption are the DHKE and RSA (Paar and Pelzl, 2010).

RSA is a cryptosystem designed by Ron Rivest, Adi Shamir, and Leonard Adleman, (Rivest, Shamir and Adleman, n.d.) and is a sub-topic within cryptography, an application of Number Theory. Since DHKE relies on Discrete Logarithm Problem, I used RSA, as RSA relies on integer factorisation, which is more promising, as many people have little knowledge of logarithms.

Aim

The aim is to determine the algebraic structure $\mathbb{Z}_n$'s cardinality so that RSA is suitable for the encryption of four-digit PINs with only a calculator.

Approach

Firstly, RSA's suitability for the PIN encryption will be shown using an example demonstrating RSA encryption and decryption. Secondly, there will be a mathematical analysis of integer rings, Extended Euclidean algorithm, modular arithmetic, Euler's Theorem, and Euler's Phi Function which will allows a deeper understanding of RSA to be gained, to determine the influence of $\mathbb{Z}_n$'s cardinality on RSA's suitability for PIN encryption. This is will allow someone to understand how to securely encrypt their PINs.

Hypothesis 1:

In less than three hours, a four-digit PIN can be encrypted and decrypted, using RSA, with only a calculator.

Example to proof Hypothesis 1:

The product $n_{(p,q)}$ (RSA module) of the chosen prime numbers $p = 149$ and $q = 151$ is:

$$p \cdot q = n_{(p,q)} \quad \textbf{(1)} \qquad \text{and } 149 \cdot 151 = 22499 = n_{(149,151)} \quad \textbf{(2)}$$

One is subtracted from each prime number, and these numbers are multiplied. The product is written as $\varphi_{(n_{(p,q)})}$:

$$(p-1) \cdot (q-1) = \varphi_{(n_{(p,q)})} \quad \textbf{(3)} \quad (149-1) \cdot (151-1) = 22200 = \varphi_{(n_{(149,151)})} = \varphi_{(22499)} \quad \textbf{(4)}$$

A prime number (e) slightly smaller than $\varphi_{(n_{(p,q)})}$ is chosen.

$$e < \varphi_{(n)} < n \quad \textbf{(5)}$$

$$21211 = e \quad \textbf{(6)}$$

The public key consists of e and n. Normally, this key would be published, so that anyone could encrypt messages to be sent to the recipient, but as our task does not involve a sender or recipient, this key is not published:

$$K_{public}(21211, 22499) \quad \textbf{(7)}$$

These first steps are easy to follow. The linear diophantine equation has to be solved:

$$22200x + 21211d = 1 \quad \textbf{(8)} \quad \text{or} \quad \varphi_{(n)}x + ed = 1 \quad \textbf{(9)}$$

using the Extended Euclidean Algorithm:

i	a_i	b_i	q_i	rem_i	x_i	d_i
1	22200	$e = 21211$	1	989	-8686	$405 - (1 \cdot (-8686)) = 9091$
2	$b_1 = 21211$	$q_1 = 989$	21	442	405	$-181 - (21 \cdot 405) = -8686$
3	989	442	2	105	-181	$43 - (2 \cdot -181) = 405$
4	442	105	4	22	43	$-9 - (4 \cdot 43) = -181$
5	105	22	4	17	-9	$7 - (4 \cdot -9) = 43$
6	22	17	1	5	7	$-2 - (1 \cdot 7) = -9$
7	17	5	3	2	-2	$1 - (3 \cdot -2) = 7$
8	5	2	2	1	$d_{i+1} = 1$	$x_{i+1} - q_i \cdot d_{i+1} = 0 - (2 \cdot 1) = -2$
9	2	1	2	0	$x_{i+1} = 0$	$d_{i+1} = 1$

Table 1: Example of the Extended Euclidean Algorithm

In row 1 the larger number in column a_i is divided by the smaller number in column b_i. The result and the remainder are written in columns q_i and rem_i. In row 2, the previous divisor $b_1 = 21211$ is divided by the previous remainder $q_1 = 989$. This process of dividing the previous divisor by the remainder is repeated until the reminder rem_i is 0, as seen in row 9. This is relatively easy.

After calculating all values for columns a_i, b_i, q_i and rem_i, columns x_i and d_i will be completed from the bottom row upwards. To determine the values for x_i and d_i in row i, the equation:

$$a_i \cdot x_i + b_i \cdot d_i = 1 \quad \textbf{(10)}$$

has to be solved. For row 9 with $a_9 = 2$ and $b_9 = 1$, it follows that $x_9 = 0$ and $d_9 = 1$. x_i and d_i must be integers. Each row results in a combination which equals 1. d_9 equates to x_8. To determine d_8, the equation:

$$d_i = x_{i+1} - q_i \cdot d_{i+1} \quad \textbf{(11)}$$

has to be solved. With $i = 8$ it follows that: $d_8 = x_9 - q_8 \cdot d_9 = 0 - (2 \cdot 1) = -2 = x_7$. This process of calculating d_1 using equation (11) is repeated for every row. This step is relatively harder, and requires close attention, to prevent making calculation errors which could severely undermine the security of the PIN's encryption. It has been deduced that $x_1 = -8686$ and $d_1 = 9091$:

$$22200 \cdot -8686 + 21211 \cdot 9091 = 1 \quad \textbf{(12)} \quad \text{and} \quad 9091 = d \quad \textbf{(13)}$$

The private key is:

$$K_{private} = (9091, 22499) \quad \textbf{(14)}$$

To encrypt $T = 6266$, a simple rule must be introduced: a and m chosen should be whole numbers. When a is divided by m there will be a remainder r of $0 : r \equiv a \bmod m$.

With this, and the following identity, the public key in **(7)** will be used to encrypt T:

$$T^e \equiv G \bmod n \qquad \textbf{(15)}$$

$6266^{9091} \bmod 22499$ will be calculated.

As 6266^{9091} is too long for a calculator, the exponent 9091 is written as: $9091 = 8192 + 512 + 256 + 128 + 2 + 1$.

The following lookup table will be used to calculate $6266^{9091} \bmod 22499$:

$$\begin{array}{lclclll}
6266^{1} & \equiv & 6266 & \equiv & 6266 & \mod & 22499 \\
6266^{2} & \equiv & 2001 & \equiv & 2001 & \mod & 22499 \\
6266^{4} & \equiv & 2001^{2} & \equiv & 21678 & \mod & 22499 \\
6266^{8} & \equiv & 21678^{2} & \equiv & 21570 & \mod & 22499 \\
6266^{16} & \equiv & 21570^{2} & \equiv & 8079 & \mod & 22499 \\
6266^{32} & \equiv & 8079^{2} & \equiv & 642 & \mod & 22499 \\
6266^{64} & \equiv & 642^{2} & \equiv & 7182 & \mod & 22499 \\
6266^{128} & \equiv & 7182^{2} & \equiv & 13416 & \mod & 22499 \\
6266^{256} & \equiv & 13416^{2} & \equiv & 19555 & \mod & 22499 \\
6266^{512} & \equiv & 19555^{2} & \equiv & 5021 & \mod & 22499 \\
6266^{1024} & \equiv & 5021^{2} & \equiv & 11561 & \mod & 22499 \\
6266^{2048} & \equiv & 11561^{2} & \equiv & 12661 & \mod & 22499 \\
6266^{4096} & \equiv & 12661^{2} & \equiv & 18045 & \mod & 22499 \\
6266^{8192} & \equiv & 18045^{2} & \equiv & 16497 & \mod & 22499
\end{array}$$

Table 2: Powers of 6266 in modulus 22499

$6266^{9091} \bmod 22499$ is calculated. First, $6266^{8192} \cdot 6266^{512}$ is calculated in modulus 22499. The result is multiplied by 6266^{256} in modulus 22499. This process is repeated to gain the final result.

$$\begin{array}{ccccccc}
6266^{8192} & \cdot & 6266^{512} & \equiv & 16497 & \cdot & 5021 & \equiv \\
82831437-3681 & \cdot & 22499 & \equiv & 12618 & \mod & 22499 & \\
\\
12618 & \cdot & 6266^{256} & \equiv & 12618 & \cdot & 19555 & \equiv \\
246744990-10966 & \cdot & 22499 & \equiv & 20956 & \mod & 22499 & \\
\\
20956 & \cdot & 6266^{128} & \equiv & 20956 & \cdot & 13416 & \equiv \\
281145696-12495 & \cdot & 22499 & \equiv & 20691 & \mod & 22499 & \\
\\
20691 & \cdot & 6266^{2} & \equiv & 20691 & \cdot & 2001 & \equiv \\
41402691-1840 & \cdot & 22499 & \equiv & 4531 & \mod & 22499 & \\
\\
4531 & \cdot & 6266^{1} & \equiv & 4531 & \cdot & 6266 & \equiv \\
28391246-1261 & \cdot & 22499 & \equiv & 20007 & \mod & 22499 &
\end{array}$$

The cipher G is: $6266^{9091} \equiv 20007 \bmod 22499$ **(16)**

This method of calculating, which was not found in the original article demonstrating RSA (Rivest, Shamir and Adleman, n.d.), is not prone to mistakes. This is very important for PIN encryption. 20007 can be stored. To decrypt $G = 20007$, using the private key **(14)**,

$$(T^{e})^{d} \equiv G^{d} \equiv T \bmod n \qquad \textbf{(17)}$$

or $20007^{21211} \bmod 22499$ has to be calculated. The same method used to encrypt 6266 is used to decrypt 20007.

The exponent can be written as:

$$21211 \equiv 16384 + 4096 + 512 + 128 + 64 + 16 + 8 + 2 + 1 \qquad \textbf{(18)}$$

Using **Table 3**,

$$\begin{array}{ccccc}
20007^{1} & \equiv & 20007 & \equiv & 20007 \bmod 22499 \\
20007^{2} & \equiv & 340 & \equiv & 340 \bmod 22499 \\
20007^{4} & \equiv & 340^{2} & \equiv & 3105 \bmod 22499 \\
20007^{8} & \equiv & 3105^{2} & \equiv & 11453 \bmod 22499 \\
20007^{16} & \equiv & 11453^{2} & \equiv & 2039 \bmod 22499 \\
20007^{32} & \equiv & 2039^{2} & \equiv & 17705 \bmod 22499 \\
20007^{64} & \equiv & 17705^{2} & \equiv & 10957 \bmod 22499 \\
20007^{128} & \equiv & 10957^{2} & \equiv & 1185 \bmod 22499 \\
20007^{256} & \equiv & 1185^{2} & \equiv & 9287 \bmod 22499 \\
20007^{512} & \equiv & 9287^{2} & \equiv & 9702 \bmod 22499 \\
20007^{1024} & \equiv & 9702^{2} & \equiv & 15487 \bmod 22499 \\
20007^{2048} & \equiv & 15487^{2} & \equiv & 7829 \bmod 22499 \\
20007^{4096} & \equiv & 7829^{2} & \equiv & 5965 \bmod 22499 \\
20007^{8192} & \equiv & 5965^{2} & \equiv & 10306 \bmod 22499 \\
20007^{16384} & \equiv & 10306^{2} & \equiv & 18356 \bmod 22499
\end{array}$$

Table 3: Powers of 20007 in modulus 22499

$20007^{21211} \bmod 22499$ is calculated:

$$\begin{array}{cccccccc}
20007^{16384} & \cdot & 20007^{4096} & \equiv & 18356 & \cdot & 5965 & \equiv \\
109493540 - 4866 & \cdot & 22499 & \equiv & 13406 & \bmod & 22499 & \\
 & & & & & & & \\
13406 & \cdot & 20007^{512} & \equiv & 13406 & \cdot & 9702 & \equiv \\
130065012 - 5780 & \cdot & 22499 & \equiv & 20792 & \bmod & 22499 & \\
 & & & & & & & \\
20792 & \cdot & 20007^{128} & \equiv & 20792 & \cdot & 1185 & \equiv \\
24638520 - 1095 & \cdot & 22499 & \equiv & 2115 & \bmod & 22499 & \\
 & & & & & & & \\
2115 & \cdot & 20007^{64} & \equiv & 2115 & \cdot & 10957 & \equiv \\
23174055 - 1030 & \cdot & 22499 & \equiv & 85 & \bmod & 22499 & \\
 & & & & & & & \\
85 & \cdot & 20007^{16} & \equiv & 85 & \cdot & 2039 & \equiv \\
173315 - 7 & \cdot & 22499 & \equiv & 15822 & \bmod & 22499 & \\
 & & & & & & & \\
15822 & \cdot & 20007^{8} & \equiv & 15822 & \cdot & 11453 & \equiv \\
181209366 - 8054 & \cdot & 22499 & \equiv & 2420 & \bmod & 22499 &
\end{array}$$

$$\begin{array}{cccccccc} 2420 & \cdot & 20007^{2} & \equiv & 2420 & \cdot & 340 & \equiv \\ 822800-36 & \cdot & 22499 & \equiv & 12836 & \mathrm{mod} & 22499 & \end{array}$$

$$\begin{array}{cccccccc} 12836 & \cdot & 20007^{1} & \equiv & 12836 & \cdot & 20007 & \equiv \\ 256809852-11414 & \cdot & 22499 & \equiv & 6266 & \mathrm{mod} & 22499 & \end{array}$$

The result of this calculation is 6266, the original PIN: (Mathworld.wolfram.com, n.d.)

$$20007^{21211} \equiv 6266 \bmod 22499 \quad \textbf{(19)}$$

Discussion:

Assuming no calculation errors were made, these calculations can be performed in less than three hours, proving Hypothesis 1, which was only the first part of our approach. Now, a deep understanding of the mathematics behind RSA needs to be gained to fulfill our aim, which is to determine a suitable cardinality of $\mathbb{Z}_n$.

Strategy to gain a deep understanding of the mathematics behind RSA

To conduct a mathematical analysis of RSA, groups and rings need to be understood, to understand what $\mathbb{Z}_n$ is. Divisibility and greatest common divisor (gcd), both of which led to the Extended Euclidean Algorithm, the solvability of the linear diophantine equation and Euler's theorem, and Euler's Phi Function $\varphi_{(n)}$, have to be explained to understand the proof of $(T^e)^d \equiv T \bmod n$. Several books about Number Theory and cryptography introduce many topics, from which only a few are useful when gaining a deep understanding of RSA. Relevant topics must be extracted. Also, books about cryptography are often written for engineers, rather than mathematicians, meaning that theorems are introduced, but often not proven. In mathematical books, the theorems are proven at a high level. This could pose some barriers when trying to fulfil the second part of our approach. The following diagram shows the connections between the relevant topics:

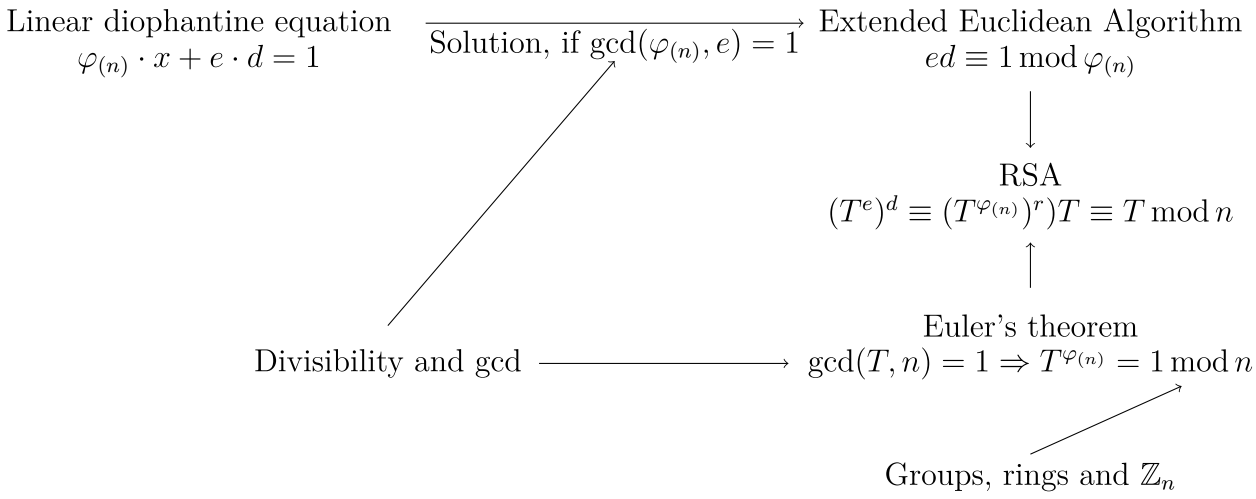
Linear diophantine equation
$\varphi_{(n)} \cdot x + e \cdot d = 1$
Solution, if $\gcd(\varphi_{(n)}, e) = 1$
Extended Euclidean Algorithm
$ed \equiv 1 \bmod \varphi_{(n)}$
RSA
$(T^e)^d \equiv (T^{\varphi_{(n)}})^r)T \equiv T \bmod n$
Euler's theorem
$\gcd(T, n) = 1 \Rightarrow T^{\varphi_{(n)}} = 1 \bmod n$
Divisibility and gcd
Groups, rings and $\mathbb{Z}_n$

Diagram 1: Connections between relevant topics related to RSA

Algebraic structures

To understand $\mathbb{Z}_n$'s cardinality, algebraic structures must be explained. It is suitable to explain the term 'group' first, followed by 'ring', and then $\mathbb{Z}_n$. In both sections, the most relevant theorems from the sources were selected and demonstrated concisely, so that the second part of the approach could be fulfilled easily.

Groups

An algebraic structure $(G, \odot)$ is a semi group, if a set of elements G with one binary operation $\odot$ exists, and if the following two axioms are fulfilled:

1. Set G is closed with respect to operation $\odot$: $\forall\ a, b\ \in\ G\ ,\ \exists\ c\ \in\ G\ ,\ a \odot b = c$ **(20)**

2. The operation is associative: $\forall\ a, b, c\ \in\ G\ ,\ (a \odot b) \odot c = a \odot (b \odot c)$ **(21)**

If the following two additional axioms are fulfilled:

3. An identity n exists: $\exists\ n\ \in\ G\ ,\ \forall\ a\ \in\ G\ ,\ a \odot n = a = n \odot a$ **(22)**

4. An inverse $\bar{a}$ relative to a exists: $\forall\ a\ \in\ G\quad \exists\ \bar{a}\ \in\ G\ ,\ a \odot \bar{a} = n = \bar{a} \odot a$ **(23)**

then the algebraic structure is a group, and, if the following axiom is also true:

5. The operation is commutative: $\forall\ a, b\ \in\ G\ ,\ a \odot b = b \odot a$ **(24)**,

then the group is an abelian group. Elements of the sets in cryptography need not be numbers. If the set contains a finite number of elements, then the group is a finite group (Fine and Rosenberger, 2007).

Rings

Rings will be explained to understand the concept of divisibility. An algebraic structure $(R, +, \cdot)$ is a ring (Buchmann, 1999), if a set of elements R exists with two binary operation $+$ and $\cdot$ and the following axioms are fulfilled:

1. $R, +$ is a commutative group

2. $R, \cdot$ is a semi group

3. Multiplication is distributive over addition:

$\forall\ a, b, c\ \in\ R\ ,\ a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ **(25)**

If the additional axiom is true:

4. Multiplication is commutative: $\forall\ a, b\ \in\ R$ **,** $a \cdot b = b \cdot a$ **(26)**

then the algebraic structure is a commutative ring.

If the following axiom is fulfilled, but axiom 4 is not fulfilled:

5. An identity n exists: $\exists\ n\ \in\ R$ **,** $\forall\ a\ \in\ R$ **,** $a \cdot n = a = n \cdot a$ **(27)**

then the algebraic structure is a ring with an identity.

If all axioms are followed, the set R with the two binary operations is a commutative ring with an identity. Field F is a commutative ring with identity, which fulfils the following additional axiom:

6. A multiplicative inverse exists: $\forall\ a, b\ \in\ F \wedge a \neq 0$**,** $a \cdot b = b \cdot a = 1$ **(28)**,

All calculations to prove Hypothesis 1 were performed within an integer ring $\mathbb{Z}_n$, a set of numbers $\{0, \pm1, \pm2, \pm3 ... n-1\}$ where two operations $+$ and $\cdot$ are defined on them so that $a + b \equiv c \bmod n$ with $a, b, c \in \mathbb{Z}_n$ and $a \cdot b \equiv c \bmod n$ with $a, b, c \in \mathbb{Z}_n$ (Fine and Rosenberger, 2007). The cardinality of $\mathbb{Z}_n$ is:

$$|\mathbb{Z}_n| = n - 1 \quad \mathbf{(29)}$$

Now, the cardinality of $\mathbb{Z}_n$ has been defined, which is important to explain which influence the cardinality of $\mathbb{Z}_n$ has on the suitability of RSA for PIN encryption and decryption, since to determine the influence of a factor on something, the factor must be understood.

Divisibility:

An important definition of divisibility is that for all a and b, there exists a q, such that:

$a, b \in \mathbb{Z}$, $a \mid b$ (a divides b) $\exists \ q \in \mathbb{Z}$ **,** $b = a \cdot q$ **(30)**

a is a factor or divisor of b. If $b > 1 \wedge$ (and) $a = \pm 1 \vee$ (or) $a = \pm b$ then b is prime. Otherwise b is a composite (Fine and Rosenberger, 2007).

$\forall \ a, b \ \in \mathbb{Z}$ **,** $a \mid b \ \Leftrightarrow \exists \ q \in \mathbb{Z}$ **,** $a \cdot q = b$ **(31)**

For all a, a divides 0, such that:

$\forall \ a \ \in \mathbb{Z}$ **,** $a \mid 0$ **(32)** since $0 = a \ \cdot \ 0$, the only number which is divisible by 0 is 0 since $a = 0 \ \cdot \ b \Rightarrow a = 0$ **(33)** (Buchmann, 1999)

The theorems of interest were selected, explained clearly using proper mathematical notation, and proven.

1. For all a, b, and c, when a divides b and b divides c, a divides c:

$a, b, c \ \in \mathbb{Z} \ a \mid b \ \wedge \ b \mid c \Rightarrow a \mid c$ **(34)**

Proof:

$a, b, c \ \in \mathbb{Z} \ a \mid b \ \wedge \ b \mid c \quad \exists \ f, g \in \mathbb{Z}$ **.** $b = fa \wedge c = bg \Rightarrow c = bg = (af)g = a(fg)$ **(35)**

2. When a divides b, ac divides bc:

$a, b, c \ \in \mathbb{Z} \ a \mid b \ \Rightarrow \forall \ c \in \mathbb{Z}$ **,** $ac \mid bc$ **(36)**

Proof:

$a, b, c \ \in \mathbb{Z} \ a \mid b \quad \exists \ f \in \mathbb{Z}$ **,** $b = af \ \Rightarrow \ bc = (af)c = f(ac)$ **(37)**

3. When c divides a and b, c divides $da + eb$:

$a, b, c \ \in \mathbb{Z}\, c \mid a \ \wedge \ c \mid b \Rightarrow \ \forall\, d, e \in \mathbb{Z}\, c \mid da + eb$ **(38)**

Proof:

$a, b, c, d, e \ \in \mathbb{Z}\, c \mid a \wedge c \mid b \ \Rightarrow \ \exists\, f, g \in \mathbb{Z}\, \mathbf{,}\, a = fc \wedge b = gc \Rightarrow \ da{+}eb = dfc{+}egc = (df{+}eg)c$

(39)

4. When a divides b, the absolute of a is smaller than or equal to the absolute of b:

$a, b, \ \in \mathbb{Z}\ a \mid b \ \wedge \ b \neq 0 \Rightarrow |a| \leq |b|$ **(40)**

Proof:

$a, b, \ \in \mathbb{Z}\ a \mid b \ \wedge \ b \neq 0\ \exists\ f \in \mathbb{Z}\ f \neq 0\ \mathbf{,}\ b = af \ \Rightarrow \ |b| = |af| \geq |a|$ **(41)**

5. When a and b divide each other, a equates to b:

$a, b, \ \in \mathbb{Z}\ a \mid b \ \wedge \ b \mid a \Rightarrow |a| = |b|$ **(42)**

Proof:

$a, b, \ \in \mathbb{Z}\ a \mid b \ \wedge \ b \mid a$ **(43)** case 1: $a = 0 \Rightarrow b = 0 \wedge b = 0 \Rightarrow a = 0$ **(44)**

case 2: $a \neq 0 \wedge b \neq 0$ with 4$\Rightarrow |a| \leq |b| \wedge |b| \leq |a| \Rightarrow |a| = |b|$ **(45)**

6. a divides itself: $\forall\ a \ \in \mathbb{Z}\ \mathbf{.}\ a \mid a$ **(46)**

Proof: $a \in \mathbb{Z}\ \mathbf{.}\ a \cdot 1 = a \Rightarrow \exists\ q \in \mathbb{N}\ \mathbf{.}\ a = q \cdot a \Rightarrow a \mid a$ **(47)** (Fine and Rosenberger, 2007)

With these theorems, a lot of progress was made in explaining the influence of the cardinality of $\mathbb{Z}_n$, as divisibility is needed to understand gcd and division with remainder.

Division with remainder:

$a \in \mathbb{Z} \wedge b \in \mathbb{N}\ \exists\ q, r \in \mathbb{Z}\ .\ a = q \cdot b + r \wedge 0 \leq r < b$ **(48)**

To prove the above statement, the existence of a solution has to be shown.

$\frac{a}{b}\ \exists\ q \in \mathbb{N}\ .\ q \leq \frac{a}{b} < q + 1$ **(49)**

multiplication with b: $qb \leq \ a < q \cdot b + b$ **(50)**

substract $-q \cdot b$: $0 \leq a - q \cdot b < b$ **(51)**

with $r = a - q \cdot b$ if q exists, then r exists with

$q, r \in \mathbb{Z} \Rightarrow a = q \cdot b + r$ **(52)**

Now, the uniqueness quantification has to be proven, meaning that only one solution exists.

This has to be proven indirectly.

Assuming that uniqueness quantification does not exist, then:

$q', r' \in \mathbb{Z}\ .\ g \neq g' \vee r \neq r' \wedge a = q'b + r' \wedge 0 \leq r' < b$ **(53)**

rearranging: $r' = a - q' \cdot b$ **(54)** with this: $0 \leq a - q' \cdot b < b$ **(55)**

addition of $+q' \cdot b$: $q'b \leq a < b + q' \cdot b$ **(56)**

division by b: $q' \leq \frac{a}{b} < q' + 1$ **(57)** but $\frac{a}{b}$ can only be between the same two successive numbers $\Rightarrow q' = q$

it could be $r' \neq r$ but $r = a - q \cdot b = a - q' \cdot b = r'$ but this is a false assumption $\lightning$.

Division with remainder is important to understand the Extended Euclidean Algorithm, which solves linear diophantine equations, which is needed to determine the inverse elements in the exponent e and d, whose sizes depend on $\mathbb{Z}_n$'s cardinality (Paar and Pelzl, 2010).

Definitions used:

The following definitions are needed to understand the Extended Euclidean Algorithm.

Set of all divisors:

The set $D_{(a)} = \{x \in \mathbb{N}.\ x \mid a\}$ **(58)** is called set of all divisors.

Prime:

a number $n \in \mathbb{N}$ is a prime if the cardinality of this set is: $|D_{(n)}| = 2$ **(59)** .

Common divisor:

$a, b, \in \mathbb{N}$ every $d \in D_{(a)} \cap D_{(b)}$ **(60)** is called a common divisor of a and b.

Coprime:

$a, b, \in \mathbb{N}$ if $D_{(a)} \cap D_{(b)} = \{1\}$ **(61)**, then a is coprime to b.

Greatest common divisor (gcd):

$a, b, \in \mathbb{N} \wedge D_{(a,b)} = D_{(a)} \cap D_{(b)}\ g \in D_{(a,b)}\ \forall\ t{:}D_{(a,b)}\ .\ t \leq g \Rightarrow g = \text{gcd}(a, b)$ **(62)**

It may be of interest that:

1: $\text{gcd}(1, a) = 1$ **(63)**

Proof: $D_{(1)} = \{1\} \Rightarrow \{1\} \cap D_{(a)} = \{1\}$ **(64)**

2: $\text{gcd}(a, a) = a$ **(65)**

Proof: $D_{(a)} \cap D_{(a)} = D_{(a)}$ **(66)**

3: $\text{gcd}(a, 0) = \mathbb{N}$ **(67)**

since $D_{(0)} = \mathbb{N} \wedge D_{(a)} \cap \mathbb{N} = D_{(a)}$ **(68)** by definition of divisibility.

For example, $7 \mid 0$ since $7 \cdot 0 = 0$

4: $\text{gcd}(a, b) = \text{gcd}(a - b, b)$ **(69)**

This can be proven in two steps.

First, it must be proven that $\text{gcd}(a, b)$ is the divisor of $\text{gcd}(a - b, b)$:

$\text{gcd}(a, b) \mid a \wedge \text{gcd}(a, b) \mid b \Rightarrow \text{gcd}(a, b) \mid a - b$ according to the third rule of divisibility **(38)**.

Substituting c with a results in:

$a \mid b \wedge a \mid c \Rightarrow a \mid a + b\ \vee\ a \mid a - b\ \vee a \mid da + eb \Rightarrow \text{gcd}(a, b) \in D_{(a-b)} \cap D_{(b)}$

Now, it can be proven indirectly that $\text{gcd}(a, b)$ is the biggest divisor of $D_{(a-b)} \cap D_{(b)}$

The false assumption is made: $g \in D_{(a-b)} \cap D_{(b)} \wedge g > \text{gcd}(a, b)$

$\Rightarrow g \mid a - b \wedge g \mid b \Rightarrow g \mid (a - b) + b \Leftrightarrow g \mid a \Rightarrow g \mid a \wedge g \mid b \wedge g > \text{gcd}(a, b)\lightning$

$\Rightarrow \text{gcd}(a, b) = \text{gcd}(a - b, b)$ (Paar and Pelzl, 2010)

This theorem is the basis for the Extended Euclidean Algorithm, which gives a solution to the linear diophantine equation.

Linear diophantine equation:

The linear Diophantine equation:

$$ax + by = c \quad \text{with} \quad a, b, c \in \mathbb{Z} \qquad \textbf{(70)}$$

has a solution if and only if $\gcd(a, b) \mid c$. From the third theorem of divisibility **(38)**, it is easy to understand that $\gcd(a, b)$ not only divides a and b, but also a linear combination of a and b with any $x, y \in \mathbb{Z}$.

So the $\gcd(a, b)$ divides both sides of the equation. The problem lies in the formulation 'if and only if'. The proof has to run in both directions. The first part of the proof states a solution for x and y and then it follows that $\gcd(a, b) \mid c$.

" $\Rightarrow$ ": (x_0, y_0) should be a solution to **(70)**. It can be written that:

$$ax_0 + by_0 = c \qquad \textbf{(71)}$$

$\gcd(a, b)$ divides a and b, according to the third theorem of divisibility **(38)**:

$$\gcd(a, b) \mid (ax_0 + by_0) \Rightarrow \gcd(a, b) \mid c \qquad \textbf{(72)}$$

Second part " $\Leftarrow$ ": If $\gcd(a, b) \mid c$ then, according to the definition of divisibility **(30)**, there is a q that:

$$\gcd(a, b) \mid c \Rightarrow \exists \;\, q : \mathbb{Z} \;\, . \;\, c = q \cdot \gcd(a, b) \qquad \textbf{(73)}$$

From the Extended Euclidean Algorithm it is known that there are (x_0, y_0) so that:

$$ax_0 + by_0 = \gcd(a, b) \qquad \textbf{(74)}$$

Inserting **(72)** in **(71)** results in:

$$c = q(ax_0 + by_0) = a(qx_0) + b(qy_0) \qquad \textbf{(75)}$$

so c is a linear combination of a and b ($qx_0 = x$ and $qy_0 = y$). It follows from this that $\gcd(a, b)$ is the smallest natural number which is a linear combination of a and b, since $ax + by = c$ only has a solution when $\gcd(a, b) \mid c$.

If $c < \gcd(a, b)$, then there would be no solution to $ax + by = c$. A special case of interest is when $ax + by = 1$, then $\gcd(a, b) = 1$ (Paar and Pelzl, 2010).

Euler's Phi Function:

In equation **(3)** Euler's Phi Function was introduced as a product of two primes. The function will be described in more detail, using some examples. Euler's Phi Function $\varphi_{(n)}$ is a function of a natural number n and gives the amount of numbers which are coprime to the argument n (Paar and Pelzl, 2010):

$$\varphi(n) \ := \ \Big|\{a \in \mathbb{N} \,|\, 1 \leq a \leq n \wedge \gcd(a, n) = 1\}\Big| = |\mathbb{Z}_n^*| \quad \textbf{(76)}$$

Example (2): $\varphi_{(6)} = 2$ since:

$\gcd(1, 6) = 1$ and $\gcd(5, 6) = 1$

but $\gcd(2, 6) = 2 \quad \gcd(3, 6) = 3 \quad \gcd(4, 6) = 2 \quad \gcd(6, 6) = 6$

Example (3): $\varphi_{(7)} = 6$ since:

$\gcd(1, 7) = 1 \quad \gcd(2, 7) = 1 \quad \gcd(3, 7) = 1 \quad \gcd(4, 7) = 1 \quad \gcd(5, 7) = 1 \quad \gcd(6, 7) = 1$

but $\gcd(7, 7) = 7$

In Example (4), n is the product of two prime numbers. It can be written as (Stillwell, 2003):

$$\varphi_{(n)} = \varphi_{(pq)} = \varphi_{(p)} \cdot \varphi_{(q)} \quad \gcd(p, q) = 1 \quad \textbf{(77)}$$

Example (4): $\varphi_{(21)} = \varphi_{(3)} \cdot \varphi_{(7)} = 2 \cdot 6 = 12$ since:

$\gcd(1, 21) = 1 \quad \gcd(2, 21) = 1 \quad \gcd(4, 21) = 1 \quad \gcd(5, 21) = 1$

$\gcd(8, 21) = 1 \quad \gcd(10, 21) = 1 \quad \gcd(11, 21) = 1 \quad \gcd(13, 21) = 1$

$\gcd(16, 21) = 1 \quad \gcd(17, 21) = 1 \quad \gcd(19, 21) = 1 \quad \gcd(20, 21) = 1$

but:

$\gcd(3, 21) = 3 \quad \gcd(6, 21) = 3 \quad \gcd(7, 21) = 7 \quad \gcd(9, 21) = 3$

$\gcd(12, 21) = 3 \quad \gcd(14, 21) = 7 \quad \gcd(15, 21) = 3 \quad \gcd(18, 21) = 3$

$\gcd(21, 21) = 21$

Euler's theorem:

Since Euler's Phi Function has been described, Euler's theorem should be proved. This short example of mine will help:

Example (5): $\varphi(8) = 4 \quad S = \{1, 3, 5, 7\}$ Now all elements of S will be multiplied with a with $\gcd(a, 8) = 1$. I have taken a to be 3 and $\bmod 8$ will be applied. All results will then be multiplied together:

$$\begin{array}{rr} 1 \cdot 3 = 3 & 3 \bmod 8 = 3 \\ 3 \cdot 3 = 9 & 9 \bmod 8 = 1 \\ 5 \cdot 3 = 15 & 15 \bmod 8 = 7 \\ 7 \cdot 3 = 21 & 21 \bmod 8 = 5 \end{array}$$

$3 \cdot 1 \cdot 7 \cdot 5 = 105$

Now I take a to be 15 ($\gcd(15, 8) = 1$):

$$\begin{array}{rr} 1 \cdot 15 = 15 & 15 \bmod 8 = 7 \\ 3 \cdot 15 = 45 & 45 \bmod 8 = 5 \\ 5 \cdot 15 = 75 & 75 \bmod 8 = 3 \\ 7 \cdot 15 = 105 & 105 \bmod 8 = 1 \end{array}$$

$1 \cdot 3 \cdot 5 \cdot 7 = 3 \cdot 1 \cdot 7 \cdot 5 = 7 \cdot 5 \cdot 3 \cdot 1 = 105$

Applying $\bmod 8$ causes the same results (1, 3, 5, 7) to occur in different permutations. Since I have not found a proof which is short and easy to understand, I would like to introduce my proof for Euler's theorem (which was inspired by Christian Spannagel's lecture 'Der Satz von Euler'):

$$\gcd(T, n) = 1 \Rightarrow T^{\varphi(n)} \equiv 1 \bmod n \quad \textbf{(78)}$$

Proof:

Let $k_1, k_2, ...k_{\varphi(n)}$ be coprimes to n of $\mathbb{Z}_n$

$$S_1 = \{k_i \in \mathbb{N} \,|\, 1 \leq k_i \leq n \wedge \gcd(k_i, n) = 1\} = \{k_1, k_2, ...k_{\varphi(n)}\} \quad \textbf{(79)}$$

multiplication by T :

$$S_2 = \{Tk_1, Tk_2, ...Tk_{\varphi(p)}\} \quad \textbf{(80)}$$

Since T and $k_1, k_2, ...k_{\varphi(n)}$ are co prime to n, it follows that $\gcd(TK_i, n) = 1$.

The bijection (multiplication with T) results in a permutation:

Proof by contradiction:

It is assumed that:

$$Tk_i \equiv Tk_j \bmod n \quad \textbf{(81)}$$

Here, a division by T is possible since $\gcd(T, n) = 1$. Division by T results in:

$$k_i \equiv k_j \bmod n \quad \textbf{(82)}$$

but every element exists only once:

$$k_i \not\equiv k_j \bmod n \quad \textbf{(83)}$$

so:

$$Tk_i \not\equiv Tk_j \bmod n \quad \textbf{(84)}$$

Now all elements of S_1 are multiplied with each other and the elements of S_2 are multiplied with each other. Since S_1 and S_2 are permutations, I wrote:

$$k_1 \cdot k_2 \cdot k_3 \cdot ... \cdot k_{\varphi(m)} = Tk_1 \cdot Tk_2 \cdot Tk_3 \cdot ... \cdot Tk_{\varphi(m)} \quad \textbf{(85)}$$

or:

$$k_1 \cdot k_2 \cdot k_3 \cdot ... \cdot k_{\varphi(m)} \equiv Tk_1 \cdot Tk_2 \cdot Tk_3 \cdot ... \cdot Tk_{\varphi(m)} \bmod n \quad \textbf{(86)}$$

Both sides will be divided by all elements of S_1 (this is possible since $\gcd(k_i, n) = 1$), resulting in:

$$1 \equiv T \cdot T \cdot T \cdot ... \cdot T \equiv T^{\varphi(m)} \bmod n \quad \textbf{(87)}$$

(Spannagel, 2012) After Euler's theorem was proven, $(T^e)^d \equiv T \bmod n$ should be proven.

Proof of $(T^e)^d \equiv T \bmod n$:

Combining both steps $T^e \equiv G \bmod n$ **(15)** and $G^d \equiv T \bmod n$ **(17)** results in:

$$(T^e)^d = T^{ed} \qquad \mathbf{(88)}$$

e was chosen and d was determined in equation **(11)** so that :

$$[(p-1)\cdot(q-1)]x + e \cdot d = \varphi_{(n)}x + e \cdot d = 1 \ \mathbf{(88)}$$

or:

$$e \cdot d = 1 - \varphi_{(n)}x \qquad \mathbf{(89)}$$

$-x$ is substituted with r:

$$e \cdot d = r \cdot \varphi_{(n)} + 1 \qquad \mathbf{(90)}$$

Using **(87)** and **(89)**, the following is deduced:

$$T^{ed} = T^{(r\cdot\varphi_{(n)}+1)} = T^{(r\cdot\varphi_{(n)})} \cdot T = (T^{\varphi_{(n)}})^r \cdot T \qquad \mathbf{(91)}$$

Now, Euler's Theorem has to be applied.

$$\gcd(T, n) = 1 \Rightarrow T^{\varphi_{(n)}} \equiv 1 \bmod n \qquad \mathbf{(92)}$$

Substitution of $T^{\varphi_{(n)}}$ with 1 results in:

$$(T^e)^d \equiv (T^{\varphi_{(n)}})^r \cdot T \equiv 1^r \cdot T \equiv T \bmod n \qquad \mathbf{(93)}$$

The original PIN has been obtained.

There is a better way to prove, which does not start with the statement to be proven:

$$T = T = 1 \cdot T = 1^r \cdot T \quad \mathbf{(94)}$$

With Euler's theorem **(91)**:

$$T \equiv 1^r \cdot T \equiv (T^{\varphi_{(n)}})^r \cdot T \equiv T^{(r\cdot\varphi_{(n)}+1)} \bmod n \quad \mathbf{(95)}$$

sum up the exponent:

$$exp = r \cdot \varphi_{(n)} + 1 \quad \mathbf{(96)}$$

and substitution:

$$T \equiv T^{(r \cdot \varphi_{(n)}+1)} \equiv T^{exp} \bmod n \quad \textbf{(97)}$$

(RSA encryption, n.d.) With this proof, a deep understanding of RSA has been gained, which is important in answering the research question.

Comparison between the original applications of RSA and the encryption of PINs:

RSA was developed for information encryption on the internet. Only the public key is published. A sender encrypts using the public key $T^e \equiv G \bmod n$. The receiver with the private key calculates $G^d \equiv T \bmod n$. n is so large, that it is impossible to find p and q in a reasonable amount of time, but calculating n is only a multiplication (a trapdoor function). Also, a public key cannot be used to decrypt cipher texts encrypted using the same public key. Successful hacks would usually produce meaningful text. However, PINs are meaningless strings of numbers, so hackers will not know what they are looking for - not even the PIN's length. Brute force is inapplicable as, after several false attempts are made, the PIN of the account is invalid and new PINs must be chosen. For our purpose the public key is not published. Spies would not know the module. With this, and the added security of encrypting PINs without a hackable computer, very large primes are not needed to show how $\mathbb{Z}_n$'s cardinality affects RSA's suitability for PIN encryption.

Influence of Euler's theorem on size of T

If RSA is used for its original intentions, then Euler's theorem will have some practical consequences for the size of T, depending on the cardinality of $\mathbb{Z}_n$. Since T usually represents a string of letters, which changes from message to message, T needs to be changeable and therefore has changing divisors. As a result, every time a message is sent it must be proven again that T and n have no common divisors other than one. However, determining all factors of these two numbers - especially when they are at least 400 digits large - is nearly impossible. Therefore, it is useful to know n's divisors. The easiest way of finding out n's divisors is to make n the product of two prime numbers. This way, it can be ensured that the only divisors of n are the two prime numbers chosen and one.

Since n is the product of the two primes p and q, T should be tested whether it is a multiple of these prime numbers. Of course this makes no sense in the original application of RSA, because senders should test this before sending. They therefore must have knowledge of the two primes and could decrypt other people's messages encrypted using the same public key. However, one of the main advantages of this method is that several senders could use the same public key. Therefore no sender should know these two primes.

This restricts the size of T. If T should have no common divisor other than one with n, and there is no possibility to test whether T is a multiple of p and q, p and q should be larger than T, so that all three numbers will only have one as a common divisor. The example in the first article demonstrating RSA encryption called 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems' does not show these considerations, since $p = 47$ and $q = 59$ were chosen, and 920 was encrypted (Rivest, Shamir and Adleman, n.d.).

It also becomes clear why n should be the product of only two prime numbers and not of more. With every additional multiplicand the RSA module and the value of $\varphi_{(n)}$ becomes larger, but T cannot become larger than the smallest prime multiplicand without additional testing. The only result of using more than two prime multiplicands is a more complex calculation, as the numbers become larger.

The testing above is possible for a person who is using the method of this essay to encrypt PINs, since they will know both prime numbers. They can use numbers for T which are larger than the smallest prime number, because they can test whether T is a multiple of q or p.

$$6266 = 151 \cdot 41 + 75 \quad \textbf{(99)} \quad \text{and} \quad 6266 = 149 \cdot 42 + 8 \quad \textbf{(101)}$$

If T is a multiple of p or q, then the PIN should be disposed of and another PIN should be tested. However, they will still be restricted by the size of n. The PIN was represented by T with $T < n$. If $T > n$, the modulo operation on different values of T would have the same result, which is not useful. For example, $T_1 = 10$ and $T_2 = 20$ both result in $T_1 \equiv T_2 \equiv 0 \bmod 5$. This means that several PINs would have the same ciphertext.

Assume that instead of choosing two prime numbers, a prime number and a composite is chosen. This raises the question of whether RSA would still securely encrypt PINs.

To answer this question, a small example where a prime number and a composite (the product of two prime numbers) is chosen, will be calculated:

Hypothesis 2

RSA encryption and decryption can also be performed when a prime number and a composite number are multiplied to determine n.

To prove this hypothesis, a small example is used:

Example (6):

with $p = 11$ and $q = 247$ $(247 = 13 \cdot 19)$ $\quad n = 11 \cdot 247 = 2717 \quad \varphi_{(2717)} = 10 \cdot 12 \cdot 18 = 2160$

$e = 1783$

i	a_i	b_i	q_i	rem_i	x_i	d_i
1	2160	1783	1	377	-402	$85 - (1 \cdot (-402) = 487$
2	1783	377	4	275	85	$-62 - (4 \cdot 85) = -402$
3	377	275	1	102	-62	$23 - (1 \cdot -62) = 85$
4	275	102	2	71	23	$-16 - (2 \cdot 23) = -62$
5	102	71	1	31	-16	$7 - (1 \cdot -16) = 23$
6	71	31	2	9	7	$-2 - (2 \cdot 7) = -16$
7	31	9	3	4	-2	$1 - (3 \cdot -2) = 7$
8	9	4	2	1	1	$0 - (2 \cdot 1) = -2$
9	4	1	4	0	0	1

$-402 \cdot 2160 + 487 \cdot 1783 = 1 \bmod 2717 \quad d = 478$

Encrypt 1972 : $1972^{1783} \bmod 2717$

$$\begin{array}{ccccc}
1972^{1} & \equiv & 1972 & \equiv & 1972 \mod 2717 \\
1972^{2} & \equiv & 1972^{2} & \equiv & 757 \mod 2717 \\
1972^{4} & \equiv & 757^{2} & \equiv & 2479 \mod 2717 \\
1972^{8} & \equiv & 2479^{2} & \equiv & 2304 \mod 2717 \\
1972^{16} & \equiv & 2304^{2} & \equiv & 2115 \mod 2717 \\
1972^{32} & \equiv & 2115^{2} & \equiv & 1043 \mod 2717 \\
1972^{64} & \equiv & 1043^{2} & \equiv & 1049 \mod 2717 \\
1972^{128} & \equiv & 1049^{2} & \equiv & 16 \mod 2717 \\
1972^{256} & \equiv & 16^{2} & \equiv & 256 \mod 2717 \\
1972^{512} & \equiv & 256^{2} & \equiv & 328 \mod 2717 \\
1972^{1024} & \equiv & 328^{2} & \equiv & 1621 \mod 2717
\end{array}$$

$$1783 = 1024 + 512 + 256 + 128 + 64 + 32 + 16 + 4 + 2 + 1 \quad \mathbf{(101)}$$

$$\begin{array}{cccccccc}
20007^{16384} & \cdot & 20007^{4096} & \equiv & 18356 & \cdot & 5965 & \equiv \\
109493540 - 4866 & \cdot & 22499 & \equiv & 13406 & \text{mod} & 22499 & \\
 & & & & & & & \\
1972^{1024} & \cdot & 1972^{512} & \equiv & 1621 & \cdot & 328 & \equiv \\
531688 - 195 & \cdot & 2717 & \equiv & 1873 & \text{mod} & 2717 & \\
 & & & & & & & \\
1873 & \cdot & 1972^{128} & \equiv & 1873 & \cdot & 16 & \equiv \\
29968 - 11 & \cdot & 2717 & \equiv & 81 & \text{mod} & 2717 & \\
 & & & & & & & \\
81 & \cdot & 1972^{64} & \equiv & 81 & \cdot & 1049 & \equiv \\
84969 - 31 & \cdot & 2717 & \equiv & 742 & \text{mod} & 2717 & \\
 & & & & & & & \\
742 & \cdot & 1972^{32} & \equiv & 742 & \cdot & 1043 & \equiv \\
773906 - 284 & \cdot & 2717 & \equiv & 2278 & \text{mod} & 2717 & \\
 & & & & & & & \\
2278 & \cdot & 1972^{16} & \equiv & 2278 & \cdot & 2115 & \equiv \\
4817970 - 1773 & \cdot & 2717 & \equiv & 729 & \text{mod} & 2717 & \\
 & & & & & & & \\
729 & \cdot & 1972^{4} & \equiv & 729 & \cdot & 2479 & \equiv \\
1807191 - 665 & \cdot & 2717 & \equiv & 386 & \text{mod} & 2717 & \\
 & & & & & & & \\
386 & \cdot & 1972^{2} & \equiv & 386 & \cdot & 757 & \equiv \\
292202 - 107 & \cdot & 2717 & \equiv & 1483 & \text{mod} & 2717 & \\
 & & & & & & & \\
1483 & \cdot & 1972^{1} & \equiv & 1483 & \cdot & 1972 & \equiv \\
2924476 - 1076 & \cdot & 2717 & \equiv & 984 & \text{mod} & 2717 &
\end{array}$$

$$1972^{1783} \equiv 984 \mod 2717 \quad \mathbf{(102)}$$

Decrypt $984 : 984^{487} \mod 2717$

$$\begin{array}{ccccccc}
984^1 & \equiv & 984 & \equiv & 984 & \bmod 2717 \\
984^2 & \equiv & 984^2 & \equiv & 1004 & \bmod 2717 \\
984^4 & \equiv & 1004^2 & \equiv & 9 & \bmod 2717 \\
984^8 & \equiv & 9^2 & \equiv & 81 & \bmod 2717 \\
984^{16} & \equiv & 81^2 & \equiv & 1127 & \bmod 2717 \\
984^{32} & \equiv & 1127^2 & \equiv & 1290 & \bmod 2717 \\
984^{64} & \equiv & 1290^2 & \equiv & 1296 & \bmod 2717 \\
984^{128} & \equiv & 1296^2 & \equiv & 510 & \bmod 2717 \\
984^{256} & \equiv & 510^2 & \equiv & 1985 & \bmod 2717
\end{array}$$

$487 = 256 + 128 + 64 + 32 + 4 + 2 + 1$ **(103)**

$$\begin{array}{ccccccccc}
984^{256} & \cdot & 984^{128} & \equiv & 1985 & \cdot & 510 & \equiv \\
1012350 - 372 & \cdot & 2717 & \equiv & 1626 & \text{mod} & 2717 & \\
 & & & & & & & \\
1626 & \cdot & 984^{64} & \equiv & 1626 & \cdot & 1296 & \equiv \\
2107296 - 775 & \cdot & 2717 & \equiv & 1621 & \text{mod} & 2717 & \\
 & & & & & & & \\
1621 & \cdot & 984^{32} & \equiv & 1621 & \cdot & 1290 & \equiv \\
2091090 - 769 & \cdot & 2717 & \equiv & 1717 & \text{mod} & 2717 & \\
 & & & & & & & \\
1717 & \cdot & 984^{4} & \equiv & 1717 & \cdot & 9 & \equiv \\
15453 - 5 & \cdot & 2717 & \equiv & 1868 & \text{mod} & 2717 & \\
 & & & & & & & \\
1868 & \cdot & 984^{2} & \equiv & 1868 & \cdot & 1004 & \equiv \\
1875472 - 690 & \cdot & 2717 & \equiv & 742 & \text{mod} & 2717 & \\
 & & & & & & & \\
742 & \cdot & 984^{1} & \equiv & 742 & \cdot & 984 & \equiv \\
730128 - 268 & \cdot & 2717 & \equiv & 1972 & \text{mod} & 2717 &
\end{array}$$

$984^{487} \equiv 1972 \bmod 2717$

This example shows proves that PINs can still be encrypted when a prime and a composite number is chosen. Still, the chosen prime number 1783 is not a linear combination of 11, 13, and 19. This section shows not only that RSA can be carried out using a prime and a composite number, when the composite number is coprime to the prime number, and that the cardinality of $\mathbb{Z}_n$ become unnecessarily larger which reduces the suitability of RSA for PIN encryption, but also that there are two cases to examine.

If the user tests that p, q, and T have no common divisor, then the product of p and q determines the size of the PIN ($T < p \cdot q$). This results in a greater suitability, which refers to a small amount of time needed to encrypt and decrypt, when small numbers can be chosen for the RSA module. For example, for a 4-digit PIN, the cardinality of $\mathbb{Z}_n$ must be larger than 9999, but not more than five times larger than 9999, to reduce the time needed to calculate. If no testing is possible or wanted, the size of the PIN determines the smallest prime ($T < p < q < p \cdot q$). The RSA module will be much larger. The cardinality of $\mathbb{Z}_n$ must be at least as large as the product of the next primes after 9999, which are 10007 and 10009. The product is $n = 100160063$. This number is more than five times larger than 9999. The larger the length of the PIN, the greater the difference between the time needed for both methods.

Advantage of calculating in $\mathbb{Z}_n$:

Discrete and finite mathematics play great roles in making RSA encryption strong. If a function were used for encryption then there would be some type of order:

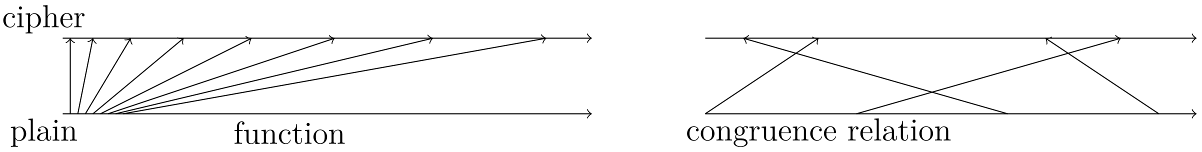

Diagram 2: Difference of function and congruence relation

This makes it easy to break the encryption. The congruence relation used here does not show this order, if the numbers to be encrypted are not very small compared to $\mathbb{Z}_n$'s cardinality. Therefore, to encrypt PINs, n should be no more than 5 times larger than the PINs. In the first example used, 6266 was encrypted to 20007; in the second example, 1972 was encrypted to 984, demonstrating the lack of order, although the same mechanism was used. If the numbers to be encrypted are very small compared to n, an order would still be detectable (Paar and Pelzl, 2010).

Conclusion

The aim of this investigation, which was to determine the algebraic structure $\mathbb{Z}_n$'s cardinality so that RSA is suitable for the encryption of four-digit PINs with only a calculator, was fulfilled by encrypting the PIN 6266. The cipher produced was 20007, and was decrypted back to 6266. The cardinality was 22498.

It was also explained that the cardinality of $\mathbb{Z}_n$ should not be larger than 50000, which would reduce the suitability of RSA, since the time needed to calculate would become unnecessarily long. Also, the important advantage of the congruence relation, which is that no order between the PIN and cipher is shown, is lost. Also, the cardinality should not be smaller than 9999, since several PINs would have the same ciphertext.

A concise derivation for a proof of $(T^e)^d \equiv T \bmod n$ was shown. $(T^e)^d \equiv T \bmod n$ was proven in two ways.

A second example of RSA was presented, to show that under certain conditions, even if a prime and a composite number are used, that RSA can still be easily used for secure encryption and decryption.

Also, a straightforward proof of Euler's theorem was demonstrated. The relationships between the different numbers were explored, such as the influence of prime numbers on the size of T under the aspect of Euler's theorem.

Bibliography

Paar, C. and Pelzl, J. (2010). Understanding Cryptography. 1st ed. Heidelberg: Springer-Verlag Berlin Heidelberg, pp.14, 55, 87, 205, 239, 173.

Rivest, R., Shamir, A. and Alderman, L. (n.d.). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. 1st ed. [ebook] Available at: http://people.csail.mit.edu/rivest/Rsapaper.pdf [Accessed 7 Mar. 2017].

Fine, B. and Rosenberger, G. (2007). Number Theory. 1st ed. Boston, Mass.: Birkhauser, pp.7, 8, 11.

Buchmann, J. (1999). Einführung in die Kryptographie. 1st ed. Berlin: Springer, pp.7, 28.

Mathworld.wolfram.com. (n.d.). RSA Encryption – from Wolfram MathWorld. [online] Available at: http://mathworld.wolfram.com/RSAEncryption.html [Accessed 8 May 2017].

RSA encryption. (n.d.). Proof of the RSA Algorithm - RSA Encryption. [online] Available at: https://sites.google.com/site/danzcosmos/proof-of-the-rsa-algorithm [Accessed 14 Jun. 2017].

Stillwell, J. (2003). Elements of Number Theory. 1st ed. New York: Springer-Verlag New York, Inc., p.56.

Spannagel, C. (2012). Der Satz von Euler. [video] Available at: https://www.youtube.com/watch?v=DU082wcr40A&index=2&list=PL6_AeYXBHF0MUuSPyAOY9JLK2gKWejbmP [Accessed 15 Jul. 2017].