[1].

GENERATOR AND APPLICATIONS

THEOPHILUS AGAMA

Abstract. In this paper we introduce a complex space, which we choose to call the space of generators $\mathcal{M}$. This space is basically a complex space $\mathbb{C}$ equipped with the bilinear map $\langle ; \rangle : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ called the generator. We study a particular example of this space and define the generator on any two element in the space as

$$\langle a; b\rangle := ab + a + b.$$

1. Introduction and motivation

Devising a very efficient algorithm for factorizing sufficiently large composites is one of the biggest and long-standing problem at the heart of modern mathematics and it's allied areas such as cryptography. Many more of these methods ranging from the classical to the modern methods, including the method of eliptic curves found in the literature (See [2], [3], [4]) are in full use. In this paper, we develop a method for carrying out such an activity, but with a somewhat poor running-time argument. By writing any odd number, say $N > 1$ as a generator $\langle a; b\rangle$, we can write

$$\langle a; b\rangle = d_1\langle 1; 1\rangle + d_2\langle 1; 0\rangle$$

The factors of N can be obtained by finding an equivalent representation of the generator of the form

$$\langle a; b\rangle = s_1\langle 1; 1\rangle + s_2\langle 1; 0\rangle,$$

so that $\gcd(s_1, s_2) > 1$, thereby guaranteeing at least a factor of N.

2. The space of generators

Definition 2.1. Let $\mathbb{C}$ be a bilinear map $\langle ; \rangle : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ such that for $a, b, c \in \mathbb{C}$

(i) $\langle a; b\rangle = \langle b; a\rangle$

(ii) $\langle a; 0\rangle = a$

(iii) $\langle a; b + c\rangle = \langle a; b\rangle + \langle a; c\rangle - \langle a; 0\rangle$,

[1] And here is the beginning of the second paragraph.

Date: November 28, 2018.

2000 *Mathematics Subject Classification.* Primary 54C40, 14E20; Secondary 46E25, 20C20.

Key words and phrases. generator; generator space; prime; composite.

then $\langle ; \rangle$ is said to be a generator on $\mathbb{C}$. The space of complex numbers equipped with a generator $\langle ; \rangle$ is a generator space. The pair $\mathcal{M} = (\mathbb{C}, \langle ; \rangle)$ is called the space of generators

There are many examples of generator spaces. It can very easily be seen that by taking the space of complex numbers equipped with the bilinear map $\langle a; b\rangle := a + b$ is a generator space, by definition 2.1. Another good example of a generator space could be the space of complex numbers with the bilinear map $\langle a; b\rangle := ab + a + b$. In the following sequel we examine the complex generator space with generator defined by $\langle a; b\rangle := ab + a + b$.

3. An example of a generator space

In this section we give an example of a generator space. We show that by defining the generator of any two elements $a, b \in \mathbb{C}$ as $\langle a; b\rangle := ab + a + b$, then the pair $(\mathbb{C}, \langle ; \rangle)$ is a complex generator space. It turns out that this particular example of a generators space has some other properties and whose generator is endowed with some other identities that a general generator space might not have.

Proposition 3.1. *The space of complex numbers $\mathbb{C}$ equipped with the bilinear map $\langle ; \rangle : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ defined by $\langle a; b\rangle = ab + a + b$ is a generator space.*

Proof. It suffices to show that definition 2.1 holds in this setting. First, by definition 2.1, we can write $\langle a; b\rangle = ab + a + b = ba + b + a = \langle b; a\rangle$ and the first part of the definition holds trivially. Again, by setting $b = 0$ in the definition of $\langle a; b\rangle$ the second axiom is also satisfied trivially. Now

$$\begin{aligned}\langle a; b + c\rangle &= a(b + c) + a + b + c \\ &= ab + ac + a + b + c \\ &= (ab + a + b) + (ac + a + c) - a \\ &= \langle a; b\rangle + \langle a; c\rangle - \langle a; 0\rangle,\end{aligned}$$

where we have used again the definition of $\langle a; b\rangle$ on $\mathbb{C}$. This completes the proof of the proposition. □

It turns out that the above generator space is one among the many space of complex generators. The setting may vary somewhat, depending on the application. One may also take the space in definition 2.1 to be $\mathbb{R}$. In such case we have a real space of generators. By using the complex generator space in Proposition 3.1, we can introduce some other properties that a general generator space may not have. By keeping the above setting, we examine those properties in the following sequel.

Theorem 3.1. *Let $\mathbb{C}$ be the complex space equipped with the bilinear map $\langle ; \rangle : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$, defined by $\langle a; b\rangle = ab + a + b$, then the following remain valid*

(i) $\langle a; a\rangle = 0$ *if and only if* $a = 0$ *for* $a \in \mathbb{C}^+$.

(ii) $\overline{\langle a; b\rangle} = \langle \overline{a}; \overline{b}\rangle$.

(iii) $\langle a; \langle b; c\rangle\rangle = \langle a; b\rangle + \langle a; c\rangle + \langle a; bc\rangle - 2\langle a; 0\rangle$.

(iv) $\langle a; b + c\rangle = \langle a; \langle b; c\rangle\rangle - \langle a; bc\rangle + \langle a; 0\rangle$

(v) $\langle a; \lambda b\rangle = \lambda\langle a; b\rangle + (\lambda - 1)\langle a; 0\rangle$ *for* $\lambda \in \mathbb{Z}^+$.

Proof. The first property is trivial and follows immediately. Now, for (ii) we have

$$\begin{aligned}\overline{\langle a; b\rangle} &= \overline{ab + a + b}\\ &= \overline{ab} + \overline{a} + \overline{b}\\ &= \overline{a}\overline{b} + \overline{a} + \overline{b}\\ &= \langle \overline{a}; \overline{b}\rangle.\end{aligned}$$

Also for (iii), we have the following

$$\begin{aligned}\langle a; \langle b; c\rangle\rangle &= \langle a; bc + b + c\rangle\\ &= \langle a; bc\rangle + \langle a; b + c\rangle - \langle a; 0\rangle\\ &= \langle a; bc\rangle + \langle a; b\rangle + \langle a; c\rangle - \langle a; 0\rangle - \langle a; 0\rangle\\ &= \langle a; b\rangle + \langle a; c\rangle + \langle a; bc\rangle - 2\langle a; 0\rangle.\end{aligned}$$

Again, (iv) follows by subtracting (iii) from (iii) in definition 2.1. Since, by Proposition 3.1, the above definition on the complex space $\mathbb{C}$ is a generator space, the property (iv) follows immediately. □

Remark 3.2. Next we prove that in any such space, taking the generator on any two elements reduces to taking the generator on the elements in the set $\{0, 1, i\}$. Before then we launch the following Lemma, which establishes the relationship between the generator on any two elements of the set.

Lemma 3.3. *Let* $\langle ; \rangle : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ *such that* $\langle a; b\rangle = ab + a + b$. *Then the following relations hold:*

(i) $\langle -1; i\rangle = -\langle 1; 0\rangle$.

(ii) $\langle 1; -i\rangle = -\langle i; i\rangle$.

(iii) $\langle -1; 1\rangle = -\langle 1; 0\rangle$.

(iv) $\langle -1; -1\rangle = -\langle 1; 0\rangle$.

(v) $\langle -i; -i\rangle = -\langle 1; i\rangle$.

Proof. Let $\langle a; b\rangle : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$. Then it follows that $\langle -1; i\rangle = -1 + i - i = -\langle 1; 0\rangle$. Similarly, $\langle 1; -i\rangle = 1 - i - i = 1 - 2i = -\langle i; i\rangle$ and (ii) follows immediately. For (iii), we observe that $\langle -1; 1\rangle = -1 - 1 + 1 = -\langle 1; 0\rangle$. Again $\langle -1; -1\rangle = 1 - 1 - 1 = -\langle 1; 0\rangle$. For (v) we observe that $\langle -i; -i\rangle = -1 - 2i = -\langle 1; i\rangle$, and the proof of the lemma is complete. □

Remark 3.4. It is important to notice that, none of these generators are linear combination of the other. That is, by viewing the generators as vectors with scalar field $\mathbb{R}$, we conclude that they are linearly independent. Next we show that any generator on any two elements of $\mathbb{C}$ can actually be reduced to taking the generators on the two elements sets $\{1,0\}$, $\{1,1\}$,$\{i,i\}$ and $\{1,i\}$.

Theorem 3.5. *Let $\langle;\rangle : \mathbb{C}\times\mathbb{C} \longrightarrow \mathbb{C}$ be defined by $\langle a;b\rangle = ab+a+b$. Then there exist some $d_1,d_2,d_3,d_4 \in \mathbb{C}$ such that*

$$\langle a;b\rangle = d_1\langle 1;0\rangle + d_2\langle 1;1\rangle + d_3\langle 1;i\rangle + d_4\langle i;i\rangle.$$

Proof. Let $a,b \in \mathbb{C}$ and take their generator given by $\langle a;b\rangle$. There exist some $b_1,b_2 \in \mathbb{C}$ such that we can write

$$\begin{aligned}\langle a;b\rangle &= \langle a;b_1+b_2\rangle \\ &= \langle a;b_1\rangle + \langle a;b_2\rangle - \langle a;0\rangle \\ &= \langle a;b_1\rangle + \langle a;b_2\rangle - a\langle 1;0\rangle,\end{aligned}$$

where we have used Theorem 3.1. By inducting on these decomposition and using Lemma 3.3, we will arrive at the required representation. □

4. Applications to solutions of diophantine equations and the goldbach problem

Theorem 4.1. *The equation $ab+a+b=0$ has no non-trivial solution in the region spanned by the line joining the points $2i-1$, $2i+1$ and 3 to the origin.*

Proof. Let us set $\langle a;b\rangle = ab+a+b$ for $a,b \in \mathbb{C}$. Then by Theorem 3.1, $\langle;\rangle$ is a generator on $\mathbb{C}$ and by Theorem 3.5, we can write

$$\langle a;b\rangle = d_1\langle 1;0\rangle + d_2\langle 1;1\rangle + d_3\langle 1;i\rangle + d_4\langle i;i\rangle,$$

where $d_1,d_2,d_3,d_4 \in \mathbb{C}$. By moving to the region spanned by the line joining the complex numbers $2i-1$, $2i+1$ and 3 to the origin, we can take $d_1=0$ and it follows that

$$\langle a;b\rangle = d_2\langle 1;1\rangle + d_3\langle 1;i\rangle + d_4\langle i;i\rangle.$$

The generators $\langle 1;1\rangle$, $\langle 1;i\rangle$ and $\langle i;i\rangle$ are linearly independent vectors, thus if $\langle a;b\rangle = ab+a+b=0$, then it follows that $d_1=d_2=d_3=d_4=0$. This can only happen if $a=b=0$, thereby ending the proof. □

It is a well-known result of Rommanof (See [1]) that any number can be partitioned into a bounded number of primes. We give a some what different proof of a weaker version of this result using the real space of generators. We give a precise statement as follows:

Theorem 4.2. *For any positive integer n, there exist some primes $p_1, p_2, \ldots, p_r$ and some integer a such that*

$$n = p_1 + p_2 + \cdots + p_r + a^k$$

for some $k \in \mathbb{N}$.

Proof. Let us specify $\langle ; \rangle : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ defined by

$$\langle a; b\rangle := a + b.$$

It is easy to see, first of all, that $\langle ; \rangle$ is a generator on $\mathbb{R}$. Without loss of generality, let N be any odd number, then we can write $N = \langle 1; N_1\rangle$, where $N_1 > 2$ is even. There exist some $N_2 < N_1$ such that $N_2 + 1 = p_1$ where p_1 is some prime. Thus we can write

$$\begin{aligned} N &= \langle 1; N_1 + M_1\rangle \\ &= \langle 1; N_1\rangle + \langle 1; M_1\rangle - \langle 1; 0\rangle \\ &= p_1 + \langle 1; M_1\rangle - \langle 1; 0\rangle. \end{aligned}$$

If $\langle 1; M_1\rangle = p_2$, where p_2 is prime, then we can write $N+1 = p_1+p_2$ and the result holds. Otherwise, there must exist some $N_2 < M_1$ such that $N_2 + 1 = p_3$, where p_3 is prime. Then in such a case, we can write

$$\begin{aligned} N &= p_1 + \langle 1; N_2 + M_2\rangle - \langle 1; 0\rangle \\ &= p_1 + \langle 1; N_2\rangle + \langle 1; M_2\rangle - 2\langle 1; 0\rangle \\ &= p_1 + p_2 + \langle 1; M_2\rangle - 2\langle 1; 0\rangle. \end{aligned}$$

Since the sequence $M_1 > M_2 > \cdots M_n \cdots$ is decreasing, the result follows immediately by induction. □

5. Application to Factorization and primality testing

In this section we examine a method for deciding when a number is prime or composite. There are vast array of methods in the literature - both classical and modern - for deciding when a given number is prime and for factorizing [2, 3, 4]. In the following sequel we develop a method for decomposing any number into smaller prime factors.

Definition 5.1. Let $\langle ; \rangle : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ be defined by $\langle a; b\rangle = ab + a + b$. Then $\langle ; \rangle$ is a real generator and we can write

$$\langle a; b\rangle = d_1\langle 1; 1\rangle + d_2\langle 1; 0\rangle.$$

Then the representation $s_1\langle 1; 1\rangle + s_2\langle 1; 0\rangle$ is said to be equivalent to the representation $d_1\langle 1; 1\rangle + d_2\langle 1; 0\rangle$ if and only if

$$d_1 - d_2 \equiv s_1 - s_2 \pmod 4,$$

and $\langle a; b\rangle = s_1\langle 1; 1\rangle + s_2\langle 1; 0\rangle$.

Definition 5.2. Let $\langle ; \rangle ; \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ such that $\langle a; b\rangle = ab + a + b$. Then we can write

$$\langle a; b\rangle = d_1\langle 1; 1\rangle + d_2\langle 1; 0\rangle,$$

Then we say $\langle a; b\rangle$ is prime if there is no equivalent representation of the generator of the form $\langle a; b\rangle = s_1\langle 1; 1\rangle + s_2\langle 1; 0\rangle$ such that $\gcd(s_1, s_2) > 1$.

5.1. **The method.** Suppose we have a number $n > 1$. If $n = p^k$ where p is prime, then we have nothing to do. Without loss of generality, let us assume n is odd and that $n \neq p^k$. Then we can write $n = \langle a; b\rangle$ for some $a, b \in \mathbb{Z}$. We can write

$$\langle a; b\rangle = d_1\langle 1; 1\rangle + d_2\langle 1; 0\rangle,$$

for some $d_1, d_2 \in \mathbb{Z}$. If there exist no other equivalent representation of the generator $\langle a; b\rangle$, then it certainly must be prime. Otherwise, there exist some $\lambda_1, \mu_1 \in \mathbb{Z}$ with $\gcd(\lambda_1, \mu_1) > 1$ such that

$$\langle a; b\rangle = \lambda_1\langle 1; 1\rangle + \mu_1\langle 1; 0\rangle.$$

Then it follows by definition 5.1 that $d_1 - d_2 \equiv \lambda_1 - \mu_1 \pmod 4$. Since $\gcd(\lambda_1, \mu_1) > 1$, we can write $d_1 - d_2 \equiv \gcd(\lambda_1, \mu_1)(\lambda_2 - \mu_2) \pmod 4$. The usphot is that the representation $d_1\langle 1; 1\rangle + d_2\langle 1; 0\rangle$ is equivalent to the representation

$$\gcd(\lambda_1, \mu_1)\lambda_2\langle 1; 1\rangle + \gcd(\lambda_1, \mu_1)\mu_2\langle 1; 0\rangle.$$

Thus the problem reduces to finding an equivalent representation for the representation $\lambda_2\langle 1; 1\rangle + \mu_2\langle 1; 0\rangle$. If there is no such equivalence, then it must certainly be a prime, then we stop the process and carry out the process on the components that are not prime. Otherwise, there exist some $\lambda_3, \mu_3 \in \mathbb{Z}$ with $\gcd(\lambda_3, \mu_3) > 1$ such that $\lambda_3\langle 1; 1\rangle + \mu_3\langle 1; 0\rangle$ is equivalent to $\lambda_2\langle 1; 1\rangle + \mu_2\langle 1; 0\rangle$, and it follows that

$$\begin{aligned}\lambda_2 - \mu_2 &\equiv \lambda_3 - \mu_3 \pmod 4 \\ &\equiv \gcd(\lambda_3, \mu_3)(\lambda_4 - \mu_4) \pmod 4.\end{aligned}$$

It follows that

$$d_1 - d_2 \equiv \gcd(\lambda_1, \mu_1)\gcd(\lambda_3, \mu_3)(\lambda_4 - \mu_4) \pmod 4,$$

and it follows that

$$\langle a; b\rangle = \gcd(\lambda_1, \mu_1)\gcd(\lambda_3, \mu_3)\lambda_4\langle 1; 1\rangle + \gcd(\lambda_1, \mu_1)\gcd(\lambda_3, \mu_3)\mu_4\langle 1; 0\rangle.$$

This process terminates, since the sequence $\lambda_1 - \mu_1 > \lambda_3 - \mu_3 > \lambda_5 - \mu_5 > \cdots 1$ is decreasing and it is positive. Thus we can write

$$\begin{aligned}n &= \gcd(\lambda_1, \mu_1)\gcd(\lambda_3, \mu_3)\cdots\gcd(\lambda_{2k-1}, \mu_{2k-1}) \\ &= n_1 n_3 \cdots n_{2k-1}.\end{aligned}$$

If each of the components n_i is prime then we have obtained a prime decomposition of n. Otherwise we iterate the process on the composite factors until we obtain a complete decomposition of n into prime factors.

5.1.1. *Example.* Suppose we seek to obtain a complete factorization of $n = 143$. Then we first write 143 as a generator, given by $\langle 71; 1\rangle$ Applying Theorem 3.1, we can write

$$\begin{aligned} 143 &= \langle 71; 1\rangle \\ &= \langle\langle 5; 11\rangle; 1\rangle \\ &= \langle 1; 5\rangle + \langle 1; 11\rangle + \langle 1; 55\rangle - 2\langle 1; 0\rangle \\ &= 5\langle 1; 1\rangle - 4\langle 1; 0\rangle + 11\langle 1; 1\rangle - 10\langle 1; 0\rangle + 55\langle 1; 1\rangle - 54\langle 1; 0\rangle - 2\langle 1; 0\rangle \\ &= 71\langle 1; 1\rangle - 70\langle 1; 0\rangle. \end{aligned}$$

The generator $\langle 71; 1\rangle = 66\langle 1; 1\rangle - 55\langle 1; 0\rangle$ is equivalent to the generator $71\langle 1; 1\rangle - 70\langle 1; 0\rangle$, since $71 + 70 \equiv 66 + 55 \pmod 4$. Thus we have that

$$\begin{aligned} 143 &= 66\langle 1; 1\rangle - 55\langle 1; 0\rangle \\ &= 11(6\langle 1; 1\rangle - 5\langle 1; 0\rangle). \end{aligned}$$

By definition 5.2 the representation $6\langle 1; 1\rangle - 5\langle 1; 0\rangle$ is prime, and it follows that $143 = 11(6\langle 1; 1\rangle - 5\langle 1; 0\rangle) = 11 \cdot 13$.

References

1. A. Carmen Cojocaru and M.Ram Murty *An introduction to sieve methods and their applications*, **vol. 66**, Cambridge University Press, 2005.
2. D.H. Lehmer and R.E. Powers, *On factoring large numbers,* Bulletin of the American Mathematical society **vol. 37** (1931), 770–776.
3. H.W Lenstra, *Factoring integers with elliptic curves,* Annals of Mathematics **126** (1987) (3), 649–673.
4. S.S Wagstaff, *The joy of factoring*, Student mathematical library, **vol. 68**, AMS, 2013.

Department of Mathematics, African Institute for Mathematical science, Ghana

E-mail address: theophilus@aims.edu.gh/emperordagama@yahoo.com