BÖLÜM 17

$\mathbb{Z}_n$ HALKALARI VE $\mathbb{Z}_n^*$ GRUPLARI

Bu bölümü bitirdiğinizde,

- $\mathbb{Z}_n^*$ grubu ve $\mathbb{Z}_n$ halkası
- Euler φ-fonksiyonu
- Gauss Teoremi
- birimin kökleri
- ilkel kökler
- Artin Tahmini
- şifreleme
- RSA şifreleme yöntemi

hakkında bilgi sahibi olabileceksiniz.

BÖLÜM 17

$\mathbb{Z}_n$ HALKALARI VE $\mathbb{Z}_n^*$ GRUPLARI

$n \in \mathbb{N}$, $n \geq 2$ olmak üzere, $\mathbb{Z}_n$, n modunda toplama işlemi ile; $\mathbb{Z}_n^*$, n modunda çarpma işlemi ile, sonlu Abel gruplarının en önemli örnekleri arasındadır. $\mathbb{Z}_n$ nin halka yapısı da sayılar teorisinde ayrı bir öneme sahiptir.

Bu bölümde, $\mathbb{Z}_n$ halkası ve $\mathbb{Z}_n^*$ grubunun yapısını ele alacağız. Bölüm 5'te

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \ (x, n) = 1\}$$

olarak tanımlanmış olan $\mathbb{Z}_n^*$ grubu, $\mathbb{Z}_n$ halkasının tüm tersinir elemanlarından ibarettir. Bu grubun mertebesinin, Euler $\varphi-$fonksiyonu'nun tanımına yol açtığını anımsayınız: $\varphi(n) = |\mathbb{Z}_n^*|$.

$\mathbb{Z}_n^*$ ın tanımından, her asal sayı p ve her $r \in \mathbb{N}$ için

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$

olduğu görülür.

Teorem 10.2 nin ikinci sonucunda, eğer $n_1, n_2, \ldots, n_k$ doğal sayıları ikişer ikişer aralarında asal ve $n = n_1 n_2 \cdots n_k$ ise, $\mathbb{Z}_n$ grubu ile $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ grubunun izomorf olduğunu görmüştük. Aşağıda, $\mathbb{Z}_n$ ve $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ arasındaki bu izomorfizmin aslında bir halka izomorfizmi olduğunu göreceğiz ve Çin Kalan Teoremi'nin kanıtında tanımlanmış olan bu izomorfizmi, burada tekrar sergileyeceğiz. Bunu yaparken, aşağıdaki lemmadan yararlanacağız.

Lemma 1. *n ve s doğal sayılar, $s \mid n$ olsun. $\mathbb{Z}_n$ nin bir x elemanının s ile bölümünden elde edilen en küçük negatif olmayan kalan*

x_s olmak üzere,

$$f_s \ : \ \mathbb{Z}_n \ \longrightarrow \ \mathbb{Z}_s \quad , \quad f_s(x) = x_s$$

ile tanımlanan fonksiyon bir örten halka homomorfizmidir. Ayrıca,

$$f_s(\mathbb{Z}_n^*) = \mathbb{Z}_s^*$$

dır.

Kanıt. $x \in \mathbb{Z}_n$ olsun. x ve s ye bölme algoritmasını uygulayalım:

$$x = q_s s + x_s \quad ; \quad q_s \in \mathbb{Z} \ , \ x_s \in \mathbb{Z}_s.$$

Böylece, x in s ile bölümünden elde edilen en küçük negatif olmayan kalan, x_s, $\mathbb{Z}_s$ içinde tek türlü belirlidir. Başka bir deyişle, f_s, iyi tanımlı bir fonksiyondur. f_s nin, toplama ve çarpma işlemlerini koruduğu ve örten olduğu kolayca gösterilebilir. Ayrıca, $x \in \mathbb{Z}_n^*$, yani x ve n aralarında asal ise, x_s ve s de aralarında asaldır. Böylece, $f_s(x) = x_s \in \mathbb{Z}_s^*$ dır. Bu, $f_s(\mathbb{Z}_n^*) = \mathbb{Z}_s^*$ olduğunu gösterir. ∎

Tanım 1. Lemma 1'de tanımlanan f_s ye $\mathbb{Z}_n$ den $\mathbb{Z}_s$ ye $(mod\ s)$ *indirgeme homomorfizmi* denir. □

Teorem 1. *Eğer $n_1, \ \ldots \ , n_k$ doğal sayıları ikişer ikişer aralarında asal ve $n = n_1 \ \cdots \ n_k$ ise, $\mathbb{Z}_n$ ve $\mathbb{Z}_{n_1} \oplus \ \cdots \ \oplus \ \mathbb{Z}_{n_k}$ halkaları izomorftur. Dolayısıyla,*

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{n_1}^* \oplus \ \cdots \ \oplus \ \mathbb{Z}_{n_k}^*$$

dır.

Kanıt. Her $i = 1, \ldots, k$ için, $f_{n_i}, \ (mod\ n_i)$ indirgeme homomorfizmi olmak üzere, $\mathbb{Z}_n$ den $\mathbb{Z}_{n_1} \oplus \ \cdots \ \oplus \ \mathbb{Z}_{n_k}$ ye

$$f \ : \ \mathbb{Z}_n \ \longrightarrow \ \mathbb{Z}_{n_1} \oplus \ \cdots \ \oplus \ \mathbb{Z}_{n_k} \ , \ f(x) = (f_{n_1}(x), \ \ldots \ , f_{n_k}(x))$$

ile tanımlanan fonksiyon, iyi tanımlı olup toplama ve çarpma işlemlerini korur. Ayrıca, Çin Kalan Teoremi'nin kanıtında görüldüğü üzere, bu fonksiyon, bire-bir ve örtendir. Sonuç olarak, f, bir halka izomor-

fizmidir. f nin $\mathbb{Z}_n^*$ a kısıtlanışı düşünülüp Lemma 1 uygulanırsa,

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{n_1}^* \oplus \cdots \oplus \mathbb{Z}_{n_k}^*$$

olduğu görülür. ∎

Teorem 1 den, Euler $\varphi-$fonksiyonu'nun bazı özelliklerini ifade eden ve uygulamada çok kullanılan bazı sonuçlar çıkaracağız. Teorem 1'de görülen grupların mertebeleri hesaplanarak aşağıdaki sonuç elde edilir.

Sonuç 1. *Eğer $n_1, \ldots, n_k$ ikişer ikişer aralarında asal doğal sayılar ve $n = n_1 \cdots n_k$ ise,*

$$\varphi(n_1 \cdots n_k) = \varphi(n_1) \cdots \varphi(n_k)$$

dir. ∎

Sonuç 2. *Eğer $p_1, \ldots, p_k$ farklı asal sayılar; $r_1, \ldots, r_k$ pozitif tamsayılar ve $n = p_1^{r_1} \cdots p_k^{r_k}$ ise,*

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{{p_1}^{r_1}}^* \oplus \cdots \oplus \mathbb{Z}_{{p_k}^{r_k}}^*$$

dır. ∎

Sonuç 3. *$p_1, \ldots, p_k$ farklı asal sayılar ve $n = p_1^{r_1} \cdots p_k^{r_k}$ ise,*

$$\varphi(n) = n(1 - \tfrac{1}{p_1}) \cdots (1 - \tfrac{1}{p_k})$$

dir.

Kanıt. Sonuç 2 ve Euler φ-fonksiyonu'nun bu bölümün başlangıcında verilen özelliği kullanılarak,

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k}) = (p_1^{r_1} - p_1^{r_1-1}) \cdots (p_k^{r_k} - p_k^{r_k-1}) \\ &= p_1^{r_1}(1 - \tfrac{1}{p_1}) \cdots p_k^{r_k}(1 - \tfrac{1}{p_k}) = n(1 - \tfrac{1}{p_1}) \cdots (1 - \tfrac{1}{p_k}).\end{aligned}$$ ∎

n doğal sayısının asal çarpanlara ayrılışı $n = p_1^{r_1} \cdots p_k^{r_k}$ ise,

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{{p_1}^{r_1}}^* \oplus \cdots \oplus \mathbb{Z}_{{p_k}^{r_k}}^*$$

olacağından, $\mathbb{Z}_n^*$ gruplarının yapısını belirlemek için, p bir asal sayı olmak üzere, $\mathbb{Z}_{p^r}^*$ ın yapısını belirlemek yeterli olacaktır. Bu doğrultudaki temel sonuç 1800 yıllarında C. F. Gauss tarafından elde edilmiştir.

Teorem 2 (Gauss). *(i)* $\mathbb{Z}_2^* = \{1\}$, $\mathbb{Z}_4^* \cong \mathbb{Z}_2$ *dir.*

(ii) *Her* $r \geq 3$ *için* $\mathbb{Z}_{2^r}^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{r-2}}$ *dir.*

(iii) *Her tek asal sayı* p *ve her* $r \geq 1$ *için* $\mathbb{Z}_{p^r}^* \cong \mathbb{Z}_{p^r - p^{r-1}}$ *dir.*

Kanıt. *(i)* $\mathbb{Z}_2^* = \{1\}$ ve $\mathbb{Z}_4^* = \{1, 3\} \cong \mathbb{Z}_2$ olduğu açıktır.

(ii) Her $r \geq 1$ için $\varphi(2^r) = |\mathbb{Z}_{2^r}^*| = 2^r - 2^{r-1} = 2^{r-1}$ dir. Bununla beraber, eğer x, tek(çift olmayan) tamsayı ise, tümevarımla, her $r \geq 3$ için

$$x^{2^{r-2}} \equiv 1 \pmod{2^r}$$

olduğu kolayca görülür. Bu nedenle, $\mathbb{Z}_{2^r}^*$ ın bir elemanının mertebesi, en çok 2^{r-2} olabilir ve $\mathbb{Z}_{2^r}^*$ devirli değildir. Yine tümevarımla, her $r \geq 3$ için ($5 \in \mathbb{Z}_{2^r}^*$ olduğuna dikkat ediniz)

$$5^{2^{r-3}} \equiv (1 + 2^{r-1}) \pmod{2^r}$$

olduğu ve böylece, 5 in, $\mathbb{Z}_{2^r}^*$ içinde mertebesinin 2^{r-2} olduğu görülür. Ek olarak, her $r \geq 3$ için $(2^{r-1} - 1) \in \mathbb{Z}_{2^r}^* \setminus < 5 >$ olup bu elemanın $\mathbb{Z}_{2^r}^*$ içindeki mertebesi 2 dir. Buradan,

$$\mathbb{Z}_{2^r}^* = < 2^{r-1} - 1 > \times < 5 > \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{r-2}}$$

olduğu görülür.

(iii) p bir tek asal sayı olsun. Önce $\mathbb{Z}_p^*$ ın devirli olduğunu kanıtlayacağız. Bunun için, $\mathbb{Z}_p^*$ a Sonlu Abel Gruplarının Temel Teoremi'ni uygulayalım. Her $i = 2, \ldots, s$ için $m_i \mid m_{i-1}$ olacak biçimde öylc $m_1, \ldots, m_s > 1$ doğal sayıları bulunabilir ki

$$\mathbb{Z}_p^* \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$

dir. O halde, $m_1 \cdots m_s = p - 1$ olup $\mathbb{Z}_p^*$ ın her elemanının mertebesi, m_1 i böler. Başka bir deyişle, her $x \in \mathbb{Z}_p^*$ için $x^{m_1} = 1$ dir. $x^{m_1} = 1$

denkleminin $\mathbb{Z}_p$ cismi içinde en çok m_1 tane çözümü vardır. Bu nedenle, $|\mathbb{Z}_p^*| = m_1 = p-1$ ve $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ dir. Sonuç olarak, $\mathbb{Z}_p^*$ devirlidir. Şimdi, her $r > 1$ için $\mathbb{Z}_{p^r}^*$ ın devirli olduğunu gösterelim. $\mathbb{Z}_p^* =< a >$ olsun. σ_p, $\mathbb{Z}_{p^r}$ den $\mathbb{Z}_p$ ye $(mod\ p)$ indirgeme homomorfizmi olmak üzere, $\sigma_p(b) = a$ olacak biçimde bir $b \in \mathbb{Z}_{p^r}^*$ seçelim. b nin mertebesi, $\mathbb{Z}_{p^r}^*$ ın mertebesi olan $\varphi(p^r) = p^{r-1}(p-1)$ i böler ve homomorf görüntüsü olan a nın mertebesinin de bir katıdır. Bu nedenle,

$$|b| = p^k(p-1) \quad , \quad 0 \leq k \leq r-1$$

dir. Eğer $k = r-1$ ise, $|b| = p^{r-1}(p-1)$ ve $\mathbb{Z}_{p^r}^* =< b >$ devirlidir. Aksi halde, $|b| \mid p^{r-2}(p-1)$ olacağından, $b^{p^{r-2}(p-1)} = 1$ dir. Bu takdirde, $c = b + p \in \mathbb{Z}_{p^r}^*$ alalım. O zaman, $\sigma_p(c) = a$ olup $\mathbb{Z}_{p^r}$ içinde Binom açılımı ile,

$$\begin{aligned} c^{p^{r-2}(p-1)} = (b+p)^{p^{r-2}(p-1)} &= b^{p^{r-2}(p-1)} + p^{r-1}(p-1)b^{p^{r-2}(p-1)-1} \\ &= 1 - p^{r-1}b^{p^{r-2}(p-1)-1} = 1 - p^{r-1}b^{-1} \neq 1 \end{aligned}$$

olduğu görülür. c nin mertebesi de $p^{r-1}(p-1)$ i bölüp a nın mertebesinin bir katı olduğundan ve $c^{p^{r-2}(p\ \ 1)} \neq 1$ olduğundan, $|c| = p^{r\ \ 1}(p-1)$ ve $\mathbb{Z}_{p^r}^* =< c >$ dir. ∎

Örnek 1. Yukarıdaki sonuçlar kullanılarak,

$$\mathbb{Z}_{720}^* \cong \mathbb{Z}_{2^4}^* \oplus \mathbb{Z}_{3^2}^* \oplus \mathbb{Z}_5^* \cong (\mathbb{Z}_2 \oplus \mathbb{Z}_4) \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_4$$

yazılabilir. Böylece, $\mathbb{Z}_{720}^*$ ın bir elemanının mertebesi, 1, 2, 3, 4, 6, 12 sayılarından biridir. □

Örnek 2. $\mathbb{Z}_{720}^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$ nın mertebesi 12 olan elemanlarının sayısı şöyle belirlenebilir: Mertebesi 12 olan $(a,b,c,d) \in \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$ elemanlarından

$|d| = 6,\ |c| = 4$ olanların sayısı: $2 \cdot 4 \cdot 2 \cdot 2 = 32$ tane,

$|d| = 6,\ |c| \in \{1,2\},\ |b| = 4,$ olanların sayısı: $2{\cdot}2{\cdot}2{\cdot}2 = 16$ tane,

$|d| = 3,\ |c| = 4$ olanların sayısı: $2 \cdot 4 \cdot 2 \cdot 2 = 32$ tane,

$|d| = 3,\ |c| \in \{1,2\},\ |b| = 4,$ olanların sayısı: $2{\cdot}2{\cdot}2{\cdot}2 = 16$ tane,

toplam, 96 tane vardır. □

Teorem 2 nin sayılar teorisindeki *ilkel kök* kavramı ile yakın ilişkisi vardır.

Tanım 1. Eğer $\mathbb{Z}_n^*$ içinde, mertebesi $\varphi(n)$ olan bir eleman varsa, o elemana *n modunda ilkel kök* denir. □

n modunda ilkel kök bulunması için gerek ve yeter koşul, $\mathbb{Z}_n^*$ ın devirli grup olmasıdır. $\mathbb{Z}_n^*$ devirli ve $x \in \mathbb{Z}_n^*$ ise, x in n modunda ilkel kök olması için gerek ve yeter koşul, x ın $\mathbb{Z}_n^*$ ı üretmesidir. Dolayısıyla, n modunda ilkel köklerin sayısı, ya sıfır ya da $\varphi(\varphi(n))$ dir.

Teorem 2 ye göre, 2 ve 4 modunda ilkel kökler vardır; $r \geq 3$ için 2^r modunda ilkel kök yoktur; 2 den büyük her p asal sayısı ve her $r \geq 1$ için, p^r modunda ilkel kök vardır.

Örnek 3. $\mathbb{Z}_4^* = \{1, 3\} =< 3 >$ olduğundan 3 elemanı, 4 modunda ilkel köktür. $\mathbb{Z}_4^*$ içinde 4 modunda başka ilkel kök yoktur. $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7\} =< 2 >$ olduğundan, 2, 9 modunda ilkel köktür. 9 modunda $\varphi(\varphi(9)) = \varphi(6) = 2$ adet ilkel kök vardır ve bunlar, 2, $2^5 = 5$ tir. □

Teorem 1 ile onun ilk sonucu ve Teorem 2 kullanılarak n modunda ilkel kök bulunan tüm n doğal sayılarından oluşan kümenin

$$\{1, 2, 4\} \cup \{p^r : p, r \in \mathbb{N}, p \text{ asal}, \ p > 2\} \cup \{2p^r : p, r \in \mathbb{N}, p \text{ asal}, \ p > 2\}$$

olduğu görülür(Bak. Alıştırma 17).

Bir a tamsayısının n ile bölümünden elde edilen en küçük negatif olmayan kalan, n modunda ilkel kök ise, a tamsayısı n modunda ilkel köktür denir. Bu bağlamda, n modunda kongruent olan ilkel kökler, özdeş sayılır. E. Artin'in ilkel köklerle ilgili, ünlü bir tahmini şöyledir:

Artin Tahmini. *Tamkare olmayan ve -1 den farklı olan her tamsayı, sonsuz çoklukta p asal sayısı için p modunda ilkel köktür.*

E. Artin'in bu tahmini henüz bir tane tamsayı için dahi kanıtlanamamıştır.

Bu bölümü, konumuzla doğrudan olmasa da dolaylı olarak bağlantılı olan bir şifreleme örneği ile bitireceğiz.

Örnek 4 (*RSA* Şifreleme Sistemi). Tarihin çok eski dönemlerinden beri bir yerden başka bir yere aktarılan bilgi veya gönderilen haberin istenmeyen kimselerin eline geçmemesi için şifreleme yöntemleri kullanıldığı bilinir. Şifrelemede en önemli husus, şifrelemenin güvenli olması, yani istenmeyen kişi veya kurumlar tarafından çözülememesidir. Şifrenin, istenmeyen kişi veya kurumlarca çözülmesine, şifrenin *kırılması* da denir.

Son zamanlarda çok kullanılan güvenli şifreleme yöntemlerinden biri, 1970'lerin ortalarında, R. Rivest, A. Shamir ve L. Adleman tarafından geliştirilen ve *RSA Sistemi* olarak bilinen şifreleme yöntemidir.

RSA sisteminde, haberleşen kişilerden her biri, kendisine gönderilecek mesajın nasıl şifreleneceğini kimseden gizlemez, açıkça ilan eder. Başka bir deyişle, alıcı durumundaki kişiye gönderilecek mesajın nasıl şifreleneceği bilgisi herkeste vardır; ancak, şifrelenmiş mesajın nasıl çözüleceği bilgisi sadece alıcısında vardır. Sistem öyle yapılandırılmıştır ki, mesajların nasıl şifreleneceği hakkındaki bilgiden, şifrelenmiş mesajın nasıl çözüleceğine dair bir ipucu dahi elde etmek, kısa süre içinde imkânsızdır.

RSA sistemi, temelde, yeteri kadar büyük; örneğin, 100 veya daha çok basamaklı asal sayılar bulmak ve tamsayıları çarpmak için elverişli yöntemlerin bulunduğu; ancak, büyük sayıların, örneğin, 200 veya daha çok basamaklı sayıların, asal çarpanlarına ayrılması için elverişli yöntemler bulunmadığı gerçeğine dayanır. Haberleşecek kişilerden her biri, p ve q gibi yeterince büyük, iki farklı asal sayı ve $m = okek(p-1, q-1)$ olmak üzere, bir $r \in \mathbb{Z}_m^*$ seçer. Bu kişi, $n = pq$ çarpımını hesaplar, n ve r sayılarını ilan ederek, kendisine gönderilecek bir M mesajının sayısallaştırılarak $M^r \ (mod\ n)$ olarak şifrelenmesini ister. Ayrıca, $\mathbb{Z}_m^*$

içinde r nin tersini, yani $rs \equiv 1 \ (mod\ m)$ olan $s \in \mathbb{Z}_m^*$ elemanını bulur ve gelecek mesajları çözmek için saklar. Bir mesajın nasıl sayısallaştırılacağını aşağıda göreceğiz. Burada, r, n ve $M^r \ (mod\ n)$ herkes tarafından bilinmesine rağmen, M nin hesabı, yani şifrenin çözülmesi, sadece n nin asal çarpanlarına ayrılışının pq olduğunu ve dolayısıyla m ve s sayılarını bilen kişi tarafından yapılabilir. Bu kişi, kendisine gönderilen $M^r \ (mod\ n)$ yi alınca, hemen $(M^r)^s \ (mod\ n)$ yi hesaplar ve mesajı çözer. Çünkü,

$$M^{p-1} \equiv 1 \ (mod\ p) \quad \text{ve} \quad M^{q-1} \equiv 1 \ (mod\ q)$$

olduğundan,

$$M^m \equiv 1 \ (mod\ n)$$

dir ve $rs = 1 + tm,\ t \in \mathbb{Z}$ ifadesinden,

$$(M^r)^s \equiv M \ (mod\ n)$$

olduğu görülür.

RSA sistemini basit bir örnekle açıklamak için $p = 41$ ve $q = 73$ asal sayılarını seçelim. Uygulamada, seçilecek asal sayıların 100 veya daha çok basamaklı olması gerektiğini biliyoruz; ancak, bizim seçtiğimiz bu küçük asal sayılar da sistemin nasıl yapılandığını görmemizi sağlayacaktır. p ve q yu seçerken, pq çarpımının 2929 dan küçük olmamasına özen gösterdiğimizi belirtmeliyiz. Bunun nedeni, aşağıda mesajlar sayısallaştırılırken anlaşılacaktır. Seçtiğimiz p ve q asal sayıları ile,

$$m = okek(40, 72) = 360 \quad , \quad n = 41 \cdot 73 = 2993$$

tür. $r = 7 \in \mathbb{Z}_{360}^*$ alalım. 7 nin $\mathbb{Z}_{360}^*$ içinde tersi, örneğin, Öklid Algoritması ile hesaplanırsa, $s = 103$ bulunur. Bize mesaj göndereceklerin kullanması için, 7 ve 2993 sayılarını ilan ederiz. Şimdi, bize, *SİL* mesajının gönderileceğini varsayalım. Bu sözcüğü sayısallaştırmak için, Türkçe alfabenin harfleri 01 den 29 a kadar numaralanır:

A: 01; ...; *İ*: 12; *J*: 13; *K*: 14; *L*: 15; ...; *S*: 22; ; ...; *Z*: 29.

Boşluk da belirtilmek istenince boşluğu göstermek için, 00 kullanılır. Sözcükteki her harfin yerine, o harfe karşılık gelen sayı yazılır. Buna

göre *SİL* sözcüğü, 221215 sayısına karşılık gelir. Şifrelenmiş mesajlarda karışıklığı önlemek için, gerekirse boşluklar kullanılarak, mesajlar, dört basamaklı bloklar halinde gösterilir. Her dörtlü blok iki harfe veya bir harf ile bir boşluğa karşılık gelecektir. Örneğin, *SİL* mesajı, 2212 ve 1500 blokları halinde gösterilecek ve bu bloklar ayrı ayrı şifrelenerek gönderilecektir. Bu mesajların şifrelenmiş biçimleri şöyle bulunur:

$$2212^7 \equiv 2127 \ (mod\ 2993) \quad , \quad 1500^7 \equiv 2529 \ (mod\ 2993).$$

Bu hesaplamalar için basit bir hesap makinesi yeterli olur. Bize gelen şifrelenmiş mesaj, 2127 ve 2529 bloklarına karşılık gelen $RVUZ$ dir. Bu mesajın çözülmesi için

$$2127^{103} \ (mod\ 2993) \quad \text{ve} \quad 2529^{103} \ (mod\ 2993)$$

ün hesaplanması gerekmektedir. Bu hesaplar için, yine hesap makinesi kullanılarak, aşağıdaki adımlar izlenebilir:

$$2127^{10} \equiv 2582 \ (mod\ 2993) \quad , \quad 2529^{10} \equiv 1034 \ (mod\ 2993)$$

$$2127^{100} \equiv 1313 \ (mod\ 2993) \quad , \quad 2529^{100} \equiv 2377 \ (mod\ 2993)$$

$$2127^{3} \equiv 1146 \ (mod\ 2993) \quad , \quad 2529^{3} \equiv 17 \ (mod\ 2993)$$

$$2127^{103} \equiv 1313 \cdot 1146 \ (mod\ 2993) \equiv 2212 \ (mod\ 2993)$$

$$2529^{103} \equiv 2377 \cdot 17 \ (mod\ 2993) \equiv 1500 \ (mod\ 2993).$$

Böylece, 2212 ve 1500 bloklarını yan yana getirerek, gönderilen mesajın *SİL* olduğunu anlarız. □