AN ALGEBRAIC TREATMENT OF CONGRUENCES IN NUMBER THEORY

KONSTANTINOS SMPOKOS

Abstract. In this article we will examine the behavior of certain free abelian subgroups of the multiplicative group of the positive rationals and their relationship with the group of units of integers modulo n.

1. Introduction

This paper studies the unit group of integers modulo n in Number Theory. It relates two seemingly unrelated areas of mathematics, which are the multiplicative subgroups of positive rational numbers and the unit group of integers modulo n. In order to study deeper this relationship we will define two subgroups of positive rationals called S_d and Ω_d which carry a lot of information about the unit group of integers modulo d. The central result of this paper is that the quotient group Ω_d/S_d is isomorphic to $U(\mathbb{Z}_d)$, where $U(\mathbb{Z}_d)$ is the unit group of integers modulo d. This theorem is the link that we will use to prove deeper results about the unit group.

The methods that we will use in this paper are purely algebraic. Using these methods we will compute the order of a special subgroup of $U(\mathbb{Z}_d)$ called $U_{d,\lambda}$ for all λ with $\lambda \mid d$, which is equal to the number of natural numbers n such that $n < d$, $gcd(n,d) = 1$ and $n \equiv 1 \,(\mathsf{mod}\, \lambda)$. This number will be shown to be $\frac{\phi(d)}{\phi(\lambda)}$, where ϕ is the Euler's totient function. This result will prove a generalization of Euler's totient formula, i.e. $r^{\phi(d)} \equiv 1 \,(\mathsf{mod}\, d) \forall r \in U(\mathbb{Z}_d)$. This will be generalized as $r^{\frac{\phi(d)}{\phi(\lambda)}} \equiv 1 \,(\mathsf{mod}\, d) \forall r \in U(\mathbb{Z}_d)$ with $r \equiv 1 \,(\mathsf{mod}\, \lambda)$. By putting $\lambda = 1$ we get the Euler's totient formula.

2. Proof of the central theorem

In this section we will define the groups S_d and Ω_d which are very central to this paper and we will prove the central theorem of this paper, that is Ω_d/S_d is isomorphic to $U(\mathbb{Z}_d)$, where $U(\mathbb{Z}_d)$ is the unit group of integers modulo d. We begin with a theorem about free abelian groups.

2010 *Mathematics Subject Classification.* 11A07.

Key words and phrases. Unit group of integers modulo d, positive rational numbers, Euler's totient function.

Theorem 2.1. *Suppose W is a subset of natural numbers such that $0 \notin W$ and for every $w_1, w_2 \in W$ it is true that $w_1 w_2 \in W$. Let $F = \{\frac{w_1}{w_2} |\ w_1, w_2 \in W\}$. Then F is a free abelian group, subgroup of $\mathbb{Q}_{>0}$, where $\mathbb{Q}_{>0}$ is the multiplicative group of positive rational numbers.*

Proof. It is easy to see that $sk \in F$ for every $s, k \in F$ and $\frac{1}{s} \in F$ for every $s \in F$. This means that F is a multiplicative subgroup of $\mathbb{Q}_{>0}$. Also it is easy to see that $\mathbb{Q}_{>0}$ is a free abelian group with basis the prime numbers, i.e. every positive rational number can be written uniquely in the form $p_1^{n_1}...p_s^{n_s}$ where $n_i \in \mathbb{Z}$, $n_i \neq 0$ and p_i primes. So F is a free abelian group.

$\square$

Suppose now d is a natural number. It is easy to see that the set $W_d = \{nd + 1 |\ n \in \mathbb{N}\}$ satisfies the hypothesis of the theorem 2.1. So the set

$$S_d = \{\frac{nd + 1}{md + 1} |\ n, m \in \mathbb{N}\}$$

is a free abelian group, say $S_d = Free(U_d)$ for some $U_d \subseteq S_d$, i.e. every number $q = \frac{nd+1}{md+1}$ where $n, m \in \mathbb{N}$ can be written uniquely in the form $u_1^{\lambda_1}...u_s^{\lambda_s}$ for $u_i \in U_d$ and $\lambda_i \in \mathbb{Z}$. Also if r is a natural number with $gcd(r, d) = 1$ then

$$S_d = \{\frac{nd + 1}{md + 1} |\ n, m \in \mathbb{N}\} = \{\frac{nd + r}{md + r} |\ n, m \in \mathbb{N}\}$$

. This is true because if $\frac{nd+1}{md+1} \in S_d$ then $\frac{nd+1}{md+1} = \frac{ndr+r}{mdr+r}$ and conversely if we have $u = \frac{nd+r}{md+r}$, then since $gcd(r, d) = 1$ there exists k such that $rk \equiv 1 \pmod{d}$, so $u = \frac{ndk+rk}{mdk+rk}$.

Corollary 2.2. *Let $r, d \in \mathbb{N}$ with $gcd(r, d) = 1$. The set*

$$S_d = \{\frac{nd + 1}{md + 1} |\ n, m \in \mathbb{N}\} = \{\frac{nd + r}{md + r} |\ n, m \in \mathbb{N}\}$$

is a free abelian group, $S_d = Free(U_d)$ and for every $n \in \mathbb{N}$ each number $nd + r$ can be written uniquely in the form $nd + r = ru_1^{\lambda_1}...u_s^{\lambda_s}$ for $u_i \in U_d$ and $\lambda_i \in \mathbb{Z}$.

We continue with a definition.

Definition 2.3. Let q a positive rational number. We say that the prime p is a factor of q if in the analysis of q, $q = p_1^{k_1}...p_s^{k_s}$ where $k_i \in \mathbb{Z}$, p_i primes and $k_i \neq 0$, there exists i such that $p_i = p$.

Remark 2.4. We will see that U_d is infinite for each $d \in \mathbb{N}$. Let p a prime number with $p > d$. Then $p \equiv r \pmod d$ for some $r < d$ with $gcd(r, d) = 1$. So by Corollary 2.2 p can be written in the form $ru_1^{\lambda_1}...u_s^{\lambda_s}$ for $u_i \in U_d$ and $\lambda_i \in \mathbb{Z}$. So this means that p is a factor of some $u_i \in U_d$. So finally every prime number greater than d is a factor of some $u \in U_d$, which makes U_d an infinite set. Thus, it is clear that $S_d \cong \oplus_{n \in \mathbb{N}} \mathbb{Z}$.

Definition 2.5. Fix $d \in \mathbb{N}$. We define Ω_d to be the free abelian group generated by all primes p with $gcd(p, d) = 1$.

It is clear that $S_d \cong \Omega_d \cong \oplus_{n \in \mathbb{N}} \mathbb{Z}$.
Now we are in a position to give a full proof of the central theorem of this paper, that is that the quotient group $\Omega_d/S_d \cong U(\mathbb{Z}_d)$.

Theorem 2.6. *The quotient group Ω_d/S_d is isomorphic to $U(\mathbb{Z}_d)$, where $U(\mathbb{Z}_d)$ is the multiplicative group of the units of $\mathbb{Z}_d$ which has order $\phi(d)$, where ϕ is the Euler's totient function.*

Proof. We will prove that $\Omega_d/S_d \cong U(\mathbb{Z}_d)$. Let $q \in \Omega_d$. Then $q = \frac{n}{m}$ where $n, m \in \mathbb{N}$ and $gcd(n, d) = gcd(m, d) = 1$.
Now using Corollary 2.2 we have that n and m can be written in the form $n = ru_1^{\lambda_1}...u_s^{\lambda_s}$ for $u_i \in U_d$ and $\lambda_i \in \mathbb{Z}$, where $S_d = Free(U_d)$ and $m = sx_1^{k_1}...x_l^{k_l}$ where $x_i \in U_d$ and $r, s < d$ with $gcd(r, d) = gcd(s, d) = 1$.
So the number q can be written uniquely in the form $q = \frac{r}{s}y_1^{m_1}...y_t^{m_t}$ where $y_i \in U_d$. So let the function $f : \Omega_d/S_d \to U(\mathbb{Z}_d)$ with $f((\frac{r}{s}y_1^{m_1}...y_t^{m_t})S_d) = rs^{-1}$, where s^{-1} is the multiplicative inverse of s in the group $U(\mathbb{Z}_d)$. It is easy to see that f is an isomorphism. $\square$

3. Applications of the central theorem

In this section we will turn our attention to applications of the central theorem(Theorem 2.7). We will prove some new theorems about the unit group $U(\mathbb{Z}_d)$ for d natural number.

Suppose that we have two positive integers λ, d such that $\lambda \mid d$. Then it is clear that $S_d \leq S_\lambda$ and $\Omega_d \leq \Omega_\lambda$.
Let the function $f : \Omega_d/S_d \to \Omega_\lambda/S_\lambda$ with $f(uS_d) = uS_\lambda$, $u \in \Omega_d$. Then f is well defined since $S_d \leq S_\lambda$ and it is clearly a homomorphism. Also we have

$$Kerf = \left\{uS_d \in \Omega_d/S_d \middle|\ u \in S_\lambda\right\} = (\Omega_d \cap S_\lambda)/S_d.$$

We have shown that $\Omega_d/S_d \cong U(\mathbb{Z}_d)$, where $U(\mathbb{Z}_d)$ is the multiplicative group of the units of $\mathbb{Z}_d$ and also $\Omega_\lambda/S_\lambda \cong U(\mathbb{Z}_\lambda)$. Also it is true that $(\Omega_d/S_d)/Kerf \cong Imf$, so it is clear that $(\Omega_d \cap S_\lambda)/S_d$ is a finite group and $|(\Omega_d \cap S_\lambda)/S_d| \mid \phi(d)$, where ϕ is the Euler's totient function. Also $\frac{\phi(d)}{|(\Omega_d \cap S_\lambda)/S_d|} \mid \phi(\lambda)$. Thus, we have that

$$\frac{\phi(d)}{\phi(\lambda)} \mid |(\Omega_d \cap S_\lambda)/S_d| \mid \phi(d).$$

Also, it is evident that a quotient of $U(\mathbb{Z}_d)$ can be embedded to $U(\mathbb{Z}_\lambda)$.
We will continue with a definition

Definition 3.1. Let n a natural number. We define $\omega(n)$ to be the number of prime divisors of n. For $n = 1$ trivially we define $\omega(1) = 0$.

Now we are in a position to compute the isomorphism type of the quotient group Ω_λ/Ω_d for $\lambda \mid d$.

Proposition 3.2. *Let $\lambda, d \in \mathbb{N}$ such that $\lambda \mid d$. We have*

$$\Omega_\lambda/\Omega_d \cong \mathbb{Z}^{\omega(d)-\omega(\lambda)}$$

Proof. Set $k = \omega(d) - \omega(\lambda)$. Let a function $h : \Omega_\lambda/\Omega_d \to \mathbb{Z}^k$ with $h((p_1^{m_1}...p_k^{m_k})\Omega_d) = (m_1, ..., m_k)$, where $p_1, .., p_k$ are the primes which divide d and do not divide λ. Clearly the number of such primes is $k = \omega(d) - \omega(\lambda)$. Then it is easy to see that h is an isomorphism. □

We will define now a new function $g : S_\lambda/S_d \to \Omega_\lambda/\Omega_d$ with $g(uS_d) = u\Omega_d$, $u \in S_\lambda$. We have that g is well defined, since $S_d \leq \Omega_d$. Clearly g is a homomorphism. Also we have that

$$Kerg = \left\{uS_d \in S_\lambda/S_d | \ u \in \Omega_d\right\} = (\Omega_d \cap S_\lambda)/S_d$$

, which we have shown that it is a finite group.
We are now ready to state and prove the following theorem.

Theorem 3.3. *Let $\lambda, d \in \mathbb{N}$ such that $\lambda \mid d$.*
The quotient group S_λ/S_d is a finite group if and only if $\omega(d) = \omega(\lambda)$.
In this case $|S_\lambda/S_d| = \frac{d}{\lambda}$.

Proof. ($\Leftarrow$) Assume that $\omega(d) = \omega(\lambda)$. Then by Proposition 3.2 we have $\Omega_\lambda/\Omega_d \cong \mathbb{Z}^{\omega(d)-\omega(\lambda)} \cong 1$. So the homomorphism g as defined above has trivial image. So $Kerg =$

S_λ/S_d. But we have shown that $Kerg = (\Omega_d \cap S_\lambda)/S_d$, which we have shown that it is a finite group. So S_λ/S_d is a finite group.
($\Rightarrow$) Assume now that S_λ/S_d is a finite group. Assume that $\omega(d) \neq \omega(\lambda)$. Then there exists a prime p such that $p \mid d$ and p does not divide λ. Now using Theorem 7.9 in [2] we have that there exists a prime q such that $q > p$ and $p \equiv q \,(\mathsf{mod}\, \lambda)$. Then by Corollary 2.2 we have that $\frac{p}{q} \in S_\lambda$. Also $g(\frac{p}{q}S_d) = \frac{p}{q}\Omega_d \neq 1$, since $\frac{p}{q} \notin \Omega_d$ because $p \mid d$. So $Img \neq \{1\}$ and also Img is a free abelian group since $Img \leq \Omega_\lambda/\Omega_d \cong \mathbb{Z}^{\omega(d)-\omega(\lambda)}$ by Proposition 3.2 and Theorem 4 in Section 12.1 in [1]. So Img is an infinite group. But $(S_\lambda/S_d)/Kerg \cong Img$. This means that S_λ/S_d has an infinite quotient. So S_λ/S_d is an infinite group, which is a contradiction. Therefore, finally $\omega(d) = \omega(\lambda)$. Now, in the case where $\omega(d) = \omega(\lambda)$, we have $\Omega_d = \Omega_\lambda$. So we have $(\Omega_d/S_d)/(S_\lambda/S_d) \cong \Omega_d/S_\lambda = \Omega_\lambda/S_\lambda \cong U(\mathbb{Z}_\lambda)$ and also $\Omega_d/S_d \cong U(\mathbb{Z}_d)$. So $\frac{\phi(d)}{|S_\lambda/S_d|} = \phi(\lambda) \Rightarrow |S_\lambda/S_d| = \frac{\phi(d)}{\phi(\lambda)}$. Also, $\phi(d) = d\prod_{p|d}(1-\frac{1}{p})$ and $\phi(\lambda) = \lambda\prod_{p|\lambda}(1-\frac{1}{p})$. But $\omega(d) = \omega(\lambda)$, so $\prod_{p|d}(1-\frac{1}{p}) = \prod_{p|\lambda}(1-\frac{1}{p})$. So $\frac{\phi(d)}{\phi(\lambda)} = \frac{d}{\lambda}$, which gives that $|S_\lambda/S_d| = \frac{d}{\lambda}$. □

Corollary 3.4. *Let λ, d postive integers with $\lambda \mid d$ and $\omega(d) = \omega(\lambda)$. Then for every $n \in \mathbb{N}$ with $n \equiv 1 \,(\mathsf{mod}\, \lambda)$ we have $n^{\frac{d}{\lambda}} \equiv 1 \,(\mathsf{mod}\, d)$.*

Proof. By Theorem 3.3 we have that $|S_\lambda/S_d| = \frac{d}{\lambda}$, so if $n \in \mathbb{N}$ with $n \equiv 1 \,(\mathsf{mod}\, \lambda)$ then $n \in S_\lambda$, so $nS_d \in S_\lambda/S_d$ which gives $(nS_d)^{\frac{d}{\lambda}} = 1$. Therefore $n^{\frac{d}{\lambda}} \in S_d$, so $n^{\frac{d}{\lambda}} \equiv 1 \,(\mathsf{mod}\, d)$. □

Suppose now that we have two positive integers λ, d with $\lambda \mid d$. Set $k = \omega(d) - \omega(\lambda)$. Let $p_1, ..., p_k$ be the primes which divide d but do not divide λ. For each $i \in \{1, ..., k\}$ select a prime q_i such that $q_i \equiv p_i \,(\mathsf{mod}\, \lambda)$ and $q_i > p_j$ for every $j \in \{1, ..., k\}$. This can be done by Theorem 7.9 in [2] since $p_i \in \Omega_\lambda$. We define now a function $w : \mathbb{Z}^k \to S_\lambda/S_d$ with $w(w_1, ..., w_k) = [(\frac{p_1}{q_1})^{w_1} ... (\frac{p_k}{q_k})^{w_k}]S_d$, for $w_i \in \mathbb{Z}$. It is easy to see that w is a homomorphism. Also if $w_1, .., w_k \in \mathbb{Z}$ then $(\frac{p_1}{q_1})^{w_1} ... (\frac{p_k}{q_k})^{w_k} \in S_d \iff w_1 = ... = w_k = 0$, since the primes p_i divide d. This shows that $Kerw = 0$, so w is an embedding.
We are now ready to compute the isomorphism type of the quotient group S_λ/S_d for $\lambda \mid d$. From Theorem 3 of section 5.2 in [1] every finitely generated abelian group can be written as direct sum of cyclic groups. The number of copies of $\mathbb{Z}$(infinite cyclic) in the direct sum decomposition of the finitely generated group G is denoted by $rank(G)$. Also by Theorem 5 in section 12.1 in [1] the torsion group of a finitely generated abelian group G i.e. the set of elements of G which have finite order is isomorphic to the direct sum of the finite cyclic groups occuring in the direct sum decomposition of G.The torsion subgroup of G is

denoted by $Tor(G)$. We have

$$Tor(G) = \{g \in G | \exists n \in \mathbb{N}(g^n = 1)\}$$

Now we will prove the following theorem.

Theorem 3.5. *Let λ, d positive integers such that $\lambda \mid d$. Then*

$$S_\lambda / S_d \cong \mathbb{Z}^{\omega(d)-\omega(\lambda)} \oplus (\Omega_d \cap S_\lambda)/S_d$$

Proof. We have shown that the homomorphism w as defined above is an embedding. This shows that $rank(S_\lambda/S_d) \geq \omega(d) - \omega(\lambda)$. Also if $g : S_\lambda/S_d \to \Omega_\lambda/\Omega_d$ with $g(uS_d) = u\Omega_d$ then we have seen that g is a homomorphism. Also we have seen that $Kerg = (\Omega_d \cap S_\lambda)/S_d$, which we have seen that it is a finite group. Also $(S_\lambda/S_d)/Kerg \cong Img$, which gives $rank(S_\lambda/S_d) - rank(Kerg) = rank(Img)$ and $rank(Kerg) = 0$. Therefore $rank(S_\lambda/S_d) = rank(Img)$. But $Img \leq \Omega_\lambda/\Omega_d \cong \mathbb{Z}^{\omega(d)-\omega(\lambda)}$. So $rank(Img) \leq \omega(d) - \omega(\lambda)$. If we put it all together we have that $rank(S_\lambda/S_d) = \omega(d) - \omega(\lambda)$. Also we have that $Kerg = (\Omega_d \cap S_\lambda)/S_d$ and $(S_\lambda/S_d)/Kerg$ is torsion free. Therefore $Tor(S_\lambda/S_d) \leq (\Omega_d \cap S_\lambda)/S_d$. Also every element of $(\Omega_d \cap S_\lambda)/S_d$ is an element of finite order. Therefore $Tor(S_\lambda/S_d) = (\Omega_d \cap S_\lambda)/S_d$. So finally,

$$S_\lambda / S_d \cong \mathbb{Z}^{\omega(d)-\omega(\lambda)} \oplus (\Omega_d \cap S_\lambda)/S_d.$$

□

Now we will define a subgroup of $U(\mathbb{Z}_d)$ which is called $U_{d,\lambda}$. The importance of this group will be shown later.

Definition 3.6. Let $\lambda, d \in \mathbb{N}$ with $\lambda \mid d$. Then we define

$$U_{d,\lambda} = \{n \in U(\mathbb{Z}_d) | n \equiv 1 \pmod{\lambda}\}$$

Let now $u \in (\Omega_d \cap S_\lambda)/S_d$. Then $u \in S_\lambda$, so there exist $m, n \in \mathbb{N}$ such that $m \equiv n \equiv 1 \pmod{\lambda}$ and $u = \frac{m}{n}$. Also we have $\frac{m}{n} \in \Omega_d$. Pick $r, s < d$ such that $m \equiv r \pmod{d}$ and $n \equiv s \pmod{d}$. It is evident that $r \equiv s \equiv 1 \pmod{\lambda}$. Then $\frac{m}{r}, \frac{n}{s} \in S_d$. So there exists $f \in S_d$ such that $u = \frac{m}{n} = \frac{r}{s} f$. We define now a function $j : (\Omega_d \cap S_\lambda)/S_d \to U_{d,\lambda}$ with $j((\frac{r}{s} f)S_d) = rs^{-1}$, where s^{-1} is the multiplicative inverse of s in the group $U_{d,\lambda}$. Then we can see that j is an isomorphism.

Corollary 3.7. *If $\lambda \mid d$ then $(\Omega_d \cap S_\lambda)/S_d \cong U_{d,\lambda}$*

Corollary 3.8. *If $\lambda \mid d$ then*

$$S_\lambda/S_d \cong \mathbb{Z}^{\omega(d)-\omega(\lambda)} \oplus U_{d,\lambda}.$$

4. The unit group of integers modulo d.

We have now developed the appropriate tools to investigate deeper the group $U(\mathbb{Z}_d)$. We will compute ther order of the group $U_{d,\lambda}$ for $\lambda \mid d$ and this will show a generalization of Euler's totient formula.

Theorem 4.1. *Let $\lambda, d \in \mathbb{N}$ with $\lambda \mid d$. Then $|U_{d,\lambda}| = \frac{\phi(d)}{\phi(\lambda)}$.*

Proof. Let $x = |(\Omega_d \cap S_\lambda)/S_d| = |U_{d,\lambda}| =$ number of natural numbers n such that $n < d$, $gcd(n, d) = 1$ and $n \equiv 1 \,(\mathsf{mod}\, \lambda)$.

We have seen that the function $f : \Omega_d/S_d \to \Omega_\lambda/S_\lambda$ with $f(uS_d) = uS_\lambda$ has $Kerf = (\Omega_d \cap S_\lambda)/S_d$. We will show that $(\Omega_\lambda/S_\lambda)/Imf = \{1\}$.

Let $yImf \in (\Omega_\lambda/S_\lambda)/Imf$. Then $y \in \Omega_\lambda/S_\lambda$. So $y = uS_\lambda$, where $u \in \Omega_\lambda$. Let $u = p_1^{\lambda_1}...p_s^{\lambda_s}$ where p_i are primes and $\lambda_i \in \mathbb{Z}$. Fix $i \in \{1, .., s\}$. Then we consider two cases. Firstly if p_i do not divide d then $p_i \in \Omega_d$. So $p_iS_\lambda \in Imf$. Secondly, if $p_i \mid d$ then pick a prime $q_i > d$ such that $p_i \equiv q_i \,(\mathsf{mod}\, \lambda)$. This can be done because $gcd(p_i, \lambda) = 1$ since $u \in \Omega_\lambda$ and by Theorem 7.9 in [2]. Then we have $\frac{p_i}{q_i} \in S_\lambda$. So $p_iS_\lambda = q_iS_\lambda$ and $q_i \in \Omega_d$. So $q_iS_\lambda \in Imf$, which gives $p_iS_\lambda \in Imf$. So finally in both cases we have $p_iS_\lambda \in Imf$ for every $i \in \{1, .., s\}$. Thus, $(p_1^{\lambda_1}...p_s^{\lambda_s})S_\lambda \in Imf$, which gives $y \in Imf$. This shows $(\Omega_\lambda/S_\lambda)/Imf = \{1\}$. Now we have that $(\Omega_d/S_d)/Kerf \cong Imf = \Omega_\lambda/S_\lambda$. So $\frac{\phi(d)}{x} = \phi(\lambda) \Rightarrow x = \frac{\phi(d)}{\phi(\lambda)}$ and the theorem is proved. □

Corollary 4.2. *There are exactly $\frac{\phi(d)}{\phi(\lambda)}$ natural numbers n such that $n < d$, $gcd(n, d) = 1$ and $n \equiv 1 \,(\mathsf{mod}\, \lambda)$.*

Corollary 4.3. *Let λ, d natural numbers with $\lambda \mid d$. Then for every $m \in \mathbb{N}$ with $m \equiv 1 \,(\mathsf{mod}\, \lambda)$ and $gcd(m, d) = 1$, we have $m^{\frac{\phi(d)}{\phi(\lambda)}} \equiv 1 \,(\mathsf{mod}\, d)$.*

Proof. Suppose m is a natural number with $m \equiv 1 \,(\mathsf{mod}\, \lambda)$ and $gcd(m, d) = 1$. Then we have $m \in S_\lambda$ and $m \in \Omega_d$. So $mS_d \in (\Omega_d \cap S_\lambda)/S_d$ and also by Theorem 4.1 and

Corollary 3.7 the order of $(\Omega_d \cap S_\lambda)/S_d$ is $\frac{\phi(d)}{\phi(\lambda)}$. Thus $m^{\frac{\phi(d)}{\phi(\lambda)}} \in S_d$ which means that $m^{\frac{\phi(d)}{\phi(\lambda)}} \equiv 1 \,(\mathsf{mod}\, d)$. □

We are now ready to state and prove a theorem about the unit group modulo d. This theorem is another property of the group $U_{d,\lambda}$.

Theorem 4.4. *Let $\lambda, d \in \mathbb{N}$ with $\lambda \mid d$. Then $U(\mathbb{Z}_d)/U_{d,\lambda} \cong U(\mathbb{Z}_\lambda)$.*

Proof. Consider the function $h : U(\mathbb{Z}_d) \to U(\mathbb{Z}_\lambda)$ with $h([n]_d) = [n]_\lambda$. We have that h is well defined because if $gcd(n, d) = 1$ then it is true that $gcd(n, \lambda) = 1$ and also because if we have $n \equiv m \,(\mathsf{mod}\, d)$ this implies $n \equiv m \,(\mathsf{mod}\, \lambda)$. So h is well defined. Also obviously h is a homomorphism. Now we have $Kerh = \{[n]_d \in U(\mathbb{Z}_d) |\ n \equiv 1 \,(\mathsf{mod}\, \lambda)\} = U_{d,\lambda}$. Also we have that $U(\mathbb{Z}_d)/U_{d,\lambda} \cong Imh$. But the order of $U(\mathbb{Z}_d)/U_{d,\lambda}$ is $\frac{\phi(d)}{(\frac{\phi(d)}{\phi(\lambda)})} = \phi(\lambda)$. Thus the order of Imh is $\phi(\lambda)$, which gives that $Imh = U(\mathbb{Z}_\lambda)$ and h is surjective. So $U(\mathbb{Z}_\lambda) = \{[n]_\lambda |\ [n]_d \in U(\mathbb{Z}_d)\}$. □

We are now proving the last theorem of this article.

Theorem 4.5. *Let n be a natural number with $n > 1$. Suppose $n = p_1^{\lambda_1} ... p_k^{\lambda_k}$ where p_i distinct primes and λ_i positive integers. Then for every $u_1, ..., u_k \in U(\mathbb{Z}_n)$ there exists $u \in U(\mathbb{Z}_n)$ such that $u \equiv u_i \,(\mathsf{mod}\, p_i^{\lambda_i})$ for every $i \in \{1, .., k\}$.*

Proof. Let the function $l : U(\mathbb{Z}_n) \to \oplus_i (U(\mathbb{Z}_n)/U_{n,p_i^{\lambda_i}})$ with $l(m) = (mU_{n,p_1^{\lambda_1}}, ..., mU_{n,p_k^{\lambda_k}})$. Then clearly l is well defined and it is a homomorphism. Now we have

$$Kerl = \{m \in U(\mathbb{Z}_n) |\ m \equiv 1 \,(\mathsf{mod}\, p_i^{\lambda_i}) \forall i\} = \{1\}.$$

So l is injective. Also we have that $U(\mathbb{Z}_n)/U_{n,p_i^{\lambda_i}} \cong U(\mathbb{Z}_{p_i^{\lambda_i}})$ for every i by Theorem 4.4. So $\oplus_i (U(\mathbb{Z}_n)/U_{n,p_i^{\lambda_i}}) \cong \oplus_i U(\mathbb{Z}_{p_i^{\lambda_i}})$. Now by Lemma $A.3$ in Appendix A in [3] we have that $U(\mathbb{Z}_n) \cong \oplus_i U(\mathbb{Z}_{p_i^{\lambda_i}})$. This means that l is also surjective. Now let $u_1, .., u_k \in U(\mathbb{Z}_n)$. Then

$$(u_1 U_{n,p_1^{\lambda_1}}, ..., u_k U_{n,p_k^{\lambda_k}}) \in \oplus_i (U(\mathbb{Z}_n)/U_{n,p_i^{\lambda_i}})$$

But l is surjective, so there exists $u \in U(\mathbb{Z}_n)$ such that $l(u) = (u_1 U_{n,p_1^{\lambda_1}}, ..., u_k U_{n,p_k^{\lambda_k}})$. This means that $u \equiv u_i \,(\mathsf{mod}\, p_i^{\lambda_i})$ for every $i \in \{1, .., k\}$. □

References

[1] D. S. Dummit and R. M. Foote, *Abstract Algebra*, John Wiley and Sons, Third Edition (2004).

[2] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer International Student Edition, First Edition (1998).

[3] Ian Stewart and David Tall, *Algebraic Number Theory and Fermat's Last Theorem*, CRC Press, Fourth Edition (2015).

Email address: k.smpokos@gmail.com