On the Distribution and Products of Totatives

Alma Lindborg

Abstract

This thesis concerns itself with relative primality of integers. It uses the concept of *totatives*, that is, integers relatively prime to a fixed number n, to investigate the distribution and products of those integers.

The thesis presents two sufficient conditions for uniform distribution of totatives, a composite analogy of Wilson's theorem, and some results on partial products, including sufficient conditions for congruence of partial products in composite moduli and the Gauss and Jacobi coefficient theorems for prime moduli.

1 Introduction

The natural numbers are the most ancient of all mathematical objects, and the fascination for and study of integers predates universities and academies. Divisibility of integers has been a subject of study at least since antiquity, with Euclid stating the main features of the fundamental theorem of arithmetic in his *Elements* (book VII).

This thesis is devoted to the study of integers with a special property: that of being relatively prime to a fixed prime or composite number n. By the fundamental theorem of arithmetic, every integer $n > 1$ can be expressed uniquely as a product of primes, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where $p_1, \ldots, p_r$ are distinct primes and $\alpha_i \geq 1$ for $i = 1, 2, \ldots, r$ and $r \geq 1$. If the integer k does not share any prime factors with n, we say that k and n are relatively prime. We shall, however, use a slightly different terminology that is better suited to the purpose of this thesis.

Definition 1.1. *Given an integer n, we say that k* ***is a totative of*** *n if and only if k and n are relatively prime.*

The concept of totatives marks a fruitful path of inquiry, as it leads us to look beyond the *relation*

$$n * k \;\Leftrightarrow\; n \text{ is relatively prime to } k$$

and turn our attention to the *set* of integers relatively prime to a given integer n. Studying totatives, it suffices to consider the interval $1, 2, \ldots, n-1$, for they recur periodically with period n. Indeed, if τ is a totative of n, so is $n + \tau$. This leaves us with the task of investigating $\phi(n)$ numbers, where

$$\phi(n) = n(1 - p_1^{-1})(1 - p_2^{-1}) \cdots (1 - p_r^{-1}) \tag{1.1}$$

denotes Euler's phi-function. This set, which can be identified with the multiplicative subgroup U_n of the ring $\mathbb{Z}_n$, is what we will dissect in this thesis. We shall construct rules for dividing it into subsets and consider the cardinalities of these subsets as well as the products of all elements in the subsets. As we shall see, some interesting results can be obtained for n both prime and composite.

The point of departure of this thesis is two articles, one by Cosgrave and Dilcher [CD11] and one by Lehmer [Leh55]. Most central theorems and proofs in this thesis are presented in their entirety in these articles. However,

there are some (nontrivial) results which I consider to be my own contributions which I have marked with an asterisk [*]. The reader is assumed to have a basic understanding of elementary number theory and group and ring theory.

2 Uniform Distribution of Totatives

An interesting aspect of the subject of totatives (see Definition 1.1) of a given composite number $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, is their distribution over the real line. This section of the thesis will concern itself with defining uniform distribution of totatives, and presenting two sufficient conditions under which the totatives of n are uniformly distributed.

It is clear that for a prime p, by any definition the totatives must be uniformly distributed over the interval $1, 2, \ldots, p-1$, as in fact all integers in this interval are totatives of p. To define uniform distribution of totatives for a composite number n, let us divide the interval $1, 2, \ldots, n$ into k subintervals of equal length, $[nq/k, n(q+1)/k]$ where $q = 0, 1, \ldots, k-1$ (here, we shall assume $n > k$). We can easily conclude that every totative belongs to exactly one of these subintervals, for if a totative would belong to two subintervals, it would occupy a common end point of two subintervals, i.e. it would be of the form nq/k. But if nq/k is a totative, then n must divide k, which is impossible since $n > k$. If every subinterval contains the same number of totatives, we say that the totatives of n are uniformly distributed with respect to k.

Following Lehmer [Leh55], we define the partial totient function $\phi(k, q, n)$ by

$$\phi(k, q, n) = |S_q|\,, \tag{2.1}$$

where $S_q = \{\tau \mid nq/k < \tau < n(q+1)/k,\ \gcd(\tau, n) = 1\}$.

It is clear that

$$\sum_{q=0}^{k-1} \phi(k, q, n) = \sum_{q=0}^{k-1} |S_q| = \phi(n). \tag{2.2}$$

Lehmer also introduces the function

$$E(k, q, n) = \phi(n) - k\phi(k, q, n). \tag{2.3}$$

This function can be conceived of as the excess of totatives of n over the amount of totatives there would be if they were everywhere as densely distributed as over the subinterval $[nq/k, n(q+1)/k]$.

If the totatives of n are uniformly distributed with respect to k, this implies that $E(k, q, n) = 0, \quad q = 0, 1, \ldots, k-1$. A necessary condition for this to happen is that k divides $\phi(n)$; indeed, this is a necessary condition for $E(k, q, n)$ to equal zero even for a single value of q.

In conjunction with Lehmer [Leh55], we make the following observations.

Theorem 2.1. *If $n > k$, $E(k,q,n) = E(k,k-q-1,n)$ for $q = 0,1,\ldots,k-1$.*

Proof. Follows directly from the fact that if τ is a totative of n, so is $n-\tau$. □

Theorem 2.2. *If $k^2|n$, then $E(k,q,n) = 0$ for $q = 0,1,\ldots,k-1$.*

Proof. Let $n = hk^2$ and first consider the totatives of hk. If τ is a totative of hk, then clearly $\tau + qhk$ is a totative of hk^2 for $q = 0,1,\ldots,k-1$, so for each totative τ of hk there exist k totatives of hk^2 of the form $\tau + qhk$. But then all totatives of hk^2 must be of this form, as there are $k\phi(hk) = \phi(hk^2)$ such totatives. It is then clear that the totatives of n are uniformly distributed with respect to k. □

We have thus found one sufficient condition for uniform distribution of totatives of n with respect to k, namely that $k^2|n$. Before proceeding to presenting the second sufficient condition for uniform distribution, we need to prepare the ground by investigating some properties of the function $E(k,q,n)$. In doing so, we shall make use of the Möbius μ-function, which is defined by

$$\mu(p^\alpha) = \begin{cases} -1 & \text{if } \alpha = 1, \\ 0 & \text{if } \alpha > 1 \end{cases}$$

for prime power arguments, and is *multiplicative*, meaning that for $p_i \neq p_j$,

$$\mu(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = \mu(p_1^{\alpha_1})\mu(p_2^{\alpha_2}) \cdots \mu(p_r^{\alpha_r}),\ r \geq 1.$$

Lemma 2.3. *Let $f(x,n)$ be the number of totatives of n which do not exceed x. Then*

$$f(x,n) = \sum_{d|n} \mu(d) \left[\frac{x}{d}\right],$$

where $[y]$ denotes the greatest integer not exceeding y.

Proof. [*] Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the prime factorization of n. Consider the set $S = \{m \in \mathbb{Z} \mid \gcd(m,n) = 1,\ 1 \leq m \leq x\}$, and the sets

$$A_{p_i} = \{m \in \mathbb{Z} \mid m = p_i k,\ 1 \leq m \leq x\}, \quad i = 1,2,\ldots,r,$$

which each contain all integers between 1 and x *not* relatively prime to the given prime factor p_i of n. Clearly we have

$$|A_{p_i}| = \left[\frac{x}{p_i}\right] \quad \text{and} \quad S = \{1,2,\ldots,[x]\} \setminus \cup_{i=1}^{r} A_{p_i}.$$

We also observe that for each i, $A_{p_i} \subseteq \{1, 2, \ldots, [x]\}$. and so

$$|S| = |\{1, 2, \ldots, [x]\}| - |\cup_{i=1}^{r} A_{p_i}|.$$

Now, by the inclusion-exclusion principle,

$$|\cup_{i=1}^{r} A_{p_i}| = \sum_{i=1}^{r} |A_{p_i}| - \sum_{1 \le i < j \le r} \left|A_{p_i} \cap A_{p_j}\right| + \sum_{1 \le i < j < k \le r} \left|A_{p_i} \cap A_{p_j} \cap A_{p_k}\right| + \cdots$$
$$\cdots + (-1)^{r-1} |\cap_{i=1}^{r} A_{p_i}|. \tag{2.4}$$

As $A_{p_i} \cap A_{p_j} = \{m \in \mathbb{Z} \mid m = p_i p_j k,\ 1 \le m \le x\}$, $\left|A_{p_i} \cap A_{p_j}\right| = \left[\frac{x}{p_i p_j}\right]$. We have a similar formula for the cardinality of each intersection up to

$$|\cap_{i=1}^{r} A_{p_i}| = \left[\frac{x}{\prod_{i=1}^{r} p_i}\right].$$

Hence we get

$$|S| = [x] - \sum_{i=1}^{r} |A_{p_i}| + \sum_{1 \le i < j \le r} \left|A_{p_i} \cap A_{p_j}\right| + \cdots + (-1)^r |\cap_{i=1}^{r} A_{p_i}| =$$
$$[x] - \sum_{i=1}^{r} \left[\frac{x}{p_i}\right] + \sum_{1 \le i < j \le r} \left[\frac{x}{p_i p_j}\right] - \cdots + (-1)^r \left[\frac{x}{\prod_{i=1}^{r} p_i}\right] = \mu(1) \left[\frac{x}{1}\right] +$$
$$\sum_{i=1}^{r} \mu(p_i) \left[\frac{x}{p_i}\right] + \sum_{1 \le i < j \le r} \mu(p_i p_j) \left[\frac{x}{p_i p_j}\right] + \ldots + \mu\left(\prod_{i=1}^{r} p_i\right) \left[\frac{x}{\prod_{i=1}^{r} p_i}\right] =$$
$$\sum_{d | p_1 p_2 \cdots p_r} \mu(d) \left[\frac{x}{d}\right].$$

The sum produced is taken over exactly all the square-free divisors of n. But as we know that $\mu(d) = 0$ if $p^2 \mid d$ for any prime p, we can do the summation over *all* divisors of n without changing the result. We thus have

$$|S| = \sum_{d | p_1 p_2 \cdots p_r} \mu(d) \left[\frac{x}{d}\right] = \sum_{d | n} \mu(d) \left[\frac{x}{d}\right].$$

□

Theorem 2.4. $E(k, q, n) = \sum_{\delta | n} \left(\delta + k \left[\frac{q\delta}{k}\right] - k \left[\frac{(q+1)\delta}{k}\right]\right) \mu(n/\delta)$.

Proof. By Lemma 2.3, we have

$$f(x,n) = \sum_{\delta|n} \left[\frac{x}{\delta}\right] \mu(\delta) = \sum_{\delta|n} \left[\frac{\delta x}{n}\right] \mu(n/\delta).$$

This gives us

$$\phi(k,q,n) = \sum_{\delta|n} \left(\left[\frac{\delta(q+1)}{k}\right] - \left[\frac{\delta q}{k}\right] \right) \mu(n/\delta).$$

The formula now follows from equation (2.3). □

Theorem 2.5. *The totatives of n are uniformly distributed with respect to k if $p \mid n$, where $p \equiv 1 \pmod{k}$ is a prime.*

Proof. It is sufficient to show that $\phi(k,q,n)$ is independent of q, given the conditions above. Let $n = p^\alpha m,\ p \equiv 1 \pmod{k}$, $p \nmid m$. Then

$$\phi(k,q,n) = \sum_{\delta|m} \mu(m/\delta) g(k,q,p^\alpha,\delta), \tag{2.5}$$

where

$$g(k,q,p^\alpha,\delta) = \sum_{v=0}^{\alpha} \left(\left[\frac{p^v \delta(q+1)}{k}\right] - \left[\frac{p^v \delta q}{k}\right] \right) \mu(p^{\alpha-v}).$$

Since $\mu(p^\beta) = 0$ for $\beta > 1$, we have

$$g(k,q,p^\alpha,\delta) = \left[\frac{p^\alpha \delta(q+1)}{k}\right] - \left[\frac{p^\alpha \delta q}{k}\right] - \left[\frac{p^{\alpha-1} \delta(q+1)}{k}\right] + \left[\frac{p^{\alpha-1} \delta q}{k}\right].$$

Let $p^\alpha = kr + 1$, $p^{\alpha-1} = ks + 1$. Then

$$\begin{aligned}
\left[\frac{p^\alpha \delta q}{k}\right] &= r\delta q + \left[\frac{\delta q}{k}\right], \\
\left[\frac{p^{\alpha-1} \delta q}{k}\right] &= s\delta q + \left[\frac{\delta q}{k}\right], \\
\left[\frac{p^\alpha \delta(q+1)}{k}\right] &= r\delta q + r\delta + \left[\frac{\delta(q+1)}{k}\right], \\
\left[\frac{p^{\alpha-1} \delta(q+1)}{k}\right] &= s\delta q + s\delta + \left[\frac{\delta(q+1)}{k}\right].
\end{aligned}$$

Substituting, we find that

$$g(k, q, p^\alpha, \delta) = (r - s)\delta = \delta\phi(p^\alpha)/k.$$

Since this is independent of q, the theorem follows. □

Concluding this section, we have presented Lehmer's definition of uniform distribution of totatives, and two sufficient conditions under which the totatives of n are uniformly distributed with respect to k.

3 Products of Totatives

In this section, we shall turn our attention to products of totatives of a given number n, and their values (mod n). We shall use Wilson's famous theorem concerning the value of $(p-1)!$ (mod p) for a prime p as a point of departure for our enquiry, and develop analogies for composite numbers.

3.1 Wilson's Theorem

Wilson's theorem together with its converse, proved by Lagrange, states that p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}. \tag{3.1}$$

It is one of the most essential theorems in elementary number theory, and we shall omit its proof here. Instead, we proceed by noting an interesting implication of Wilson's theorem. For any odd prime p, we can exploit the symmetry relation $k \equiv (-1)(p-k) \pmod{p}$ to rewrite the factorial $(p-1)!$ so as to produce

$$(p-1)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p} \tag{3.2}$$

which, using Wilson's result, implies that

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}. \tag{3.3}$$

This result marks the first step in our investigation of partial products, which will be the main subject of the last section of the thesis. Before further pursuing the subject, we shall now turn to composite number analogies of Wilson's theorem.

3.2 Composite Number Analogies of Wilson's Theorem

As, for a composite number n, $(n-1)!$ contain factors of n and thus cannot be congruent to ± 1 (mod n), we shall once again restrict ourselves to the totatives of n when we present a composite analogue of Wilson's theorem. The theorem was first proved by Gauss, but is actually a consequence of a more general structural feature of abelian groups of finite order. The theorem will therefore be presented as a corollary of the more general result below.

Theorem 3.1. *Let G be a multiplicative abelian group of finite order. Then*

$$\prod_{a\in G} a = \begin{cases} g & \text{if } G \text{ has exactly one element } g \text{ of order 2,} \\ 1 & \text{otherwise.} \end{cases}$$

Proof. [*****] By the fundamental theorem of finitely generated abelian groups,

$$G \simeq \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_r^{k_r}} = H$$

where $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = |G|$, p_i not necessarily distinct primes.

Let $\psi : G \to H$ be an isomorphism and ψ^{-1} its inverse.

$$\psi\left(\prod_{a\in G} a\right) = \sum_{a\in G} \psi(a) = \sum_{b\in H} b = \left(\left[\left(\prod_{j\neq i} {p_j}^{k_j} \right) \frac{{p_i}^{k_i}({p_i}^{k_i}+1)}{2} \right]_{{p_i}^{k_i}} \right)_{i=1}^{r}.$$

We notice that for every odd prime, $(p_i^{k_i}+1)/2$ is an integer and so the product within brackets becomes a multiple of ${p_i}^{k_i}$ and vanishes. So if all p_i are odd, then the sum will become $([0]_{{p_i}^{k_i}})_{i=1}^{r}$.

If at least two of the primes p_i equal 2, then for each p_i the product $\prod_{j\neq i} {p_j}^{k_j}$ contains a factor 2, and the product within brackets will again be a multiple of ${p_i}^{k_i}$ and vanish for all i.

In the final case, where exactly one of the p_i equals 2, say p_m, then in the m:th position we get that

$$\left[\prod_{j\neq m} {p_j}^{k_j} \frac{2^{k_m}(2^{k_m}+1)}{2} \right]_{2^{k_m}} = \left[(2l+1)2^{k_m-1}(2^{k_m}+1) \right]_{2^{k_m}},$$

for some $l \in \mathbb{Z}$. (Here we have used the fact that p_i is odd for all $i \neq m$ and hence their product is also odd.) This expression simplifies to $\left[2^{k_m-1}\right]_{2^{k_m}}$. In the remaining positions the products will vanish, as all primes in these positions are odd. Therefore, in this case the sum will be

$$\left([0]_{p_1^{k_1}}, \ldots, [0]_{p_{m-1}^{k_{m-1}}}, [2^{k_m-1}]_{2^{k_m}}, [0]_{p_{m+1}^{k_{m+1}}}, \ldots, [0]_{p_r^{k_r}} \right) = h.$$

It is easy to see that $2h = \left([0]_{p_i^{k_i}}\right)_{i=1}^{r}$ and that h must be the only element of order 2 in the additive abelian group H. Assume for a contradiction that there is another element $\hat{h}$ of order 2 in H. If $\hat{h} = \left([b_i]_{p_i^{k_i}}\right)_{i=1}^{r}$, at least one of the b_i must be nonzero and satisfy $[2b_i]_{p_i^{k_i}} = [0]_{p_i^{k_i}}$. As 2 is a unit in $\mathbb{Z}_{p_i^{k_i}}$ for all $i \neq m$, we must have zero everywhere except in the m:th position. Now, as $2\hat{h} = \left([0]_{p_i^{k_i}}\right)_{i=1}^{r}$, we must have $[2b_m]_{2^{k_m}} = [0]_{2^{k_m}}$, so $b_m = 2^{k_m-1}$. But then $\hat{h} = h$.

Concluding the argument, we have

$$\sum_{b\in H} b = \begin{cases} h & \text{if } h \text{ is the unique element in } H \text{ of order 2,} \\ \left([0]_{p_i^{k_i}}\right)_{i=1}^{r} & \text{otherwise.} \end{cases}$$

We now apply ψ^{-1} to $s = \sum_{b\in H} b$.
In the case $s = \left([0]_{p_i^{k_i}}\right)_{i=1}^{r}$, s is the additive identity element, and any isomorphism must map it to an identity element. In a multiplicative group, this element is by convention called 1. Hence we have $\prod_{a\in G} a = \psi^{-1}(s) = 1$.

In the case $s = h$, we have $\psi^{-1}(s) = \psi^{-1}(h) = g$, where g is the unique element in G of order 2, as ψ^{-1} is an isomorphism from H to G. □

Corollary 3.2. *For any integer $n \geq 2$ we have*

$$\prod_{\substack{1\leq j\leq n-1 \\ \gcd(j,n)=1}} j \equiv \begin{cases} -1 \pmod{n} & \textit{for } n = 2, 4, p^\alpha, \textit{ or } 2p^\alpha, \\ 1 \pmod{n} & \textit{otherwise,} \end{cases}$$

where p is an odd prime and α is a positive integer.

Proof. [*] First, identify the integers a_i in the product (mod n) with the remainder classes $[a_i]_n$ in the multiplicative group U_n of units in $\mathbb{Z}_n$. Clearly we can construct a bijection f by letting $f(a_i) = [a_i]_n$. Let

$$P = \prod_{\substack{1\leq j\leq n-1 \\ \gcd(j,n)=1}} j,$$

and consider the values of n for which we want to prove that $P \equiv -1 \pmod{n}$. The case $n = 2$ is trivial, but the other values of n for which

the congruence should hold are exactly those for which n has a primitive root, say r, and then $U_n = \langle [r]_n \rangle$. As $|U_n| = \phi(n) \equiv 0 \pmod 2$ for $n > 2$, there exists a $u \in U_n$ such that $u = \left[r^{\frac{\phi(n)}{2}} \right]_n$. By Euler's generalization of Fermat's theorem, $u^2 = [1]_n$, and thus $|\langle u \rangle| = 2$.

Now suppose there exists another element v in U_n, $v \neq u$, such that $|\langle v \rangle| = 2$. Then $v = r^l$ for some l such that $1 \leq l \leq \phi(n)$, $2l \equiv 0 \pmod{\phi(n)}$. But then we must have $l = \phi(n)/2$, which implies that $v = u$. So u must be the unique element of order 2 in U_n. Using Theorem 3.1, and the fact that $(-1)^2 \equiv 1 \pmod n$, for this choice of n we must have

$$\prod_{a \in U_n} a = [u]_n \Rightarrow f^{-1}\left(\prod_{a \in U_n} a \right) = f^{-1}\left([u]_n \right) \Rightarrow P \equiv -1 \pmod n.$$

We shall now consider the cases $n = 2^{2+\alpha}$, $n = 2^{1+\alpha} p_1^\beta m$, $n = p_1^\alpha p_2^\beta m$, where α and β are positive integers, p_1, p_2 odd primes, $\gcd(m, p_i) = 1$ for $i = 1, 2$ and $\gcd(m, 2) = 1$. As there is at least one element of order 2 in U_n (namely $[-1]_n$), by Theorem 3.1 it is sufficient to show that there are at least two elements of order 2 in U_n to prove that $P \equiv 1 \pmod n$. We begin by showing that this is true for $m = 1$.

Consider $n = 2^{2+\alpha}$. $|U_n| = 2^{\alpha+1}$. As $\alpha + 1 \geq 2$ and U_n is not cyclic (n has no primitive root), we must have

$$U_n \simeq \mathbb{Z}_{2^{k_1}} \times \cdots \times \mathbb{Z}_{2^{k_r}},\ k_1 + \cdots + k_r = \alpha + 1,\ r \geq 2.$$

As each group $\mathbb{Z}_{2^{k_i}}$ contains an element of order 2 and there are at least two such groups, $\mathbb{Z}_{2^{k_1}} \times \cdots \times \mathbb{Z}_{2^{k_r}}$ contains at least two elements of order 2 and, by isomorphism, so does U_n.

In both of the two remaining cases, n is a product of two distinct prime powers p^k, with $\phi(p^k)$ even. We shall now show that

$$U_{p_1^{\alpha_1} p_2^{\alpha_2}} \simeq U_{p_1^{\alpha_1}} \times U_{p_2^{\alpha_2}}.$$

By the Chinese Remainder Theorem for principal ideal domains (cf. Corollary 14.5 in [Hun12]), there exists a ring isomorphism

$$\varphi : \mathbb{Z}_{p_1^{\alpha_1} p_2^{\alpha_2}} \to \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}}.$$

Observe that $U_{p_1^{\alpha_1} p_2^{\alpha_2}} \subseteq \mathbb{Z}_{p_1^{\alpha_1} p_2^{\alpha_2}}$ and let $x \in U_{p_1^{\alpha_1} p_2^{\alpha_2}}$, $\varphi(x) = (x_1, x_2)$. Then $\varphi(1) = \varphi(x x^{-1}) = \varphi(x)\varphi(x^{-1}) = (x_1, x_2)(x_1, x_2)^{-1} = (1, 1)$.

Consider the equation $(x_1, x_2)(x_1, x_2)^{-1} = (1, 1)$. To obtain 1 in both positions of the right hand side, both x_1 and x_2 must have inverses and

must be multiplied by them, as multiplication in direct products of groups is always done coordinatewise. Hence $(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1})$.
So $x \in U_{p_1^{\alpha_1} p_2^{\alpha_2}} \Rightarrow x_1 \in U_{p_1^{\alpha_1}}$, $x_2 \in U_{p_2^{\alpha_2}}$.

As φ is injective and surjective, it maps every element of $U_{p_1^{\alpha_1} p_2^{\alpha_2}}$ to an element in the direct product of the respective groups of units for $p_1^{\alpha_1}$ and $p_2^{\alpha_2}$. So the restriction of φ to $U_{p_1^{\alpha_1} p_2^{\alpha_2}}$ is a group isomorphism to $U_{p_1^{\alpha_1}} \times U_{p_2^{\alpha_2}}$.

Now, as we have seen before that $U_{p_1^{\alpha_1}}$ and $U_{p_2^{\alpha_2}}$ each contain an element of order 2, their direct product must contain at least two elements of order 2 (in fact, at least three) and by Theorem 3.1 we thus have

$$\prod_{a \in U_{p_1^{\alpha_1} p_2^{\alpha_2}}} [a]_{p_1^{\alpha_1} p_2^{\alpha_2}} = [1]_{p_1^{\alpha_1} p_2^{\alpha_2}} \Rightarrow P \equiv 1 \pmod{p_1^{\alpha_1} p_2^{\alpha_2}}.$$

For $m > 1$, we can use the same argument to show that

$$U_{m p_1^{\alpha_1} p_2^{\alpha_2}} \simeq U_m \times U_{p_1^{\alpha_1}} \times U_{p_2^{\alpha_2}},$$

so if $U_{p_1^{\alpha_1} p_2^{\alpha_2}}$ contains at least two elements of order 2, so does $U_{m p_1^{\alpha_1} p_2^{\alpha_2}}$ and hence $P \equiv 1 \pmod{n}$ in this case too.

□

4 Partial Products

This section is devoted to the exploration of partial products, a subject which was touched upon slightly already in section 3.1 (more specifically, by equation (3.2)). Here, a more general definition and also some interesting results will be provided.

For a prime p, define the partial product $\Pi_j^{(M)}$ as the j:th of the products obtained by dividing $(p-1)!$ into M parts. That is,

$$\Pi_j^{(M)} = \left((j-1)\frac{p-1}{M}+1\right)\left((j-1)\frac{p-1}{M}+2\right)\cdots\left(j\cdot\frac{p-1}{M}\right).$$

As is evident from the definiton, p only has partial products with respect to M if $p \equiv 1 \pmod{M}$.

Exploiting the same symmetry relation as in equation (3.2), it is clear that

$$\Pi_{M-j}^{(M)} \equiv \pm\Pi_j^{(M)} \pmod{p}, \quad j = 1, 2, \ldots, \left[\frac{M-1}{2}\right].$$

When M is odd, the "central" product $\Pi_{(M+1)/2}^{(M)}$ plays a somewhat special role, as there is generally no simple relation between its value and the values of other partial products. For fixed M, Cosgrave and Dilcher [CD11] suggest that computations have so far not been able to produce a prime p for which all partial products are congruent. Instances where two of the partial products $\Pi_j^{(M)}$, $j = 1, 2, \ldots, \left[\frac{M+1}{2}\right]$ are congruent have however been found.

4.1 Composite Moduli

If one is interested in finding conditions under which the partial products of a certain modulus are all congruent, one should then perhaps leave the prime moduli behind and instead turn one's attention to the composite moduli. This is what we will do here, and later on we shall see that this search is indeed more fruitful.

For a composite modulus n, we may define $\Pi_j^{(M)}$ as the product of all totatives of n in the interval $\left[(j-1)\frac{(n-1)}{M}+1, j\frac{n-1}{M}\right]$, and the *Gauss factorial* $N_n!$ by

$$N_n! = \prod_{\substack{1\le j\le N\\ \gcd(j,n)=1}} j.$$

If the partial products are all congruent (mod n), it must follow that

$$\left(\frac{n-1}{M}\right)_n ! \equiv \Pi_j^{(M)} \pmod{n}, \quad j = 1, 2, \ldots, M. \tag{4.1}$$

By definition, the equation is always satisfied for $j = 1$. Departing from this deifinition, we will now present two interesting theorems on sufficient conditions for congruence of the partial products $\Pi_j^{(M)}$. The proof of the first of the theorems relies on a lemma, the proof of which is somewhat technical and therefore omitted (for details, see [CD11]).

Lemma 4.1. *Let $M \geq 2$ and $n \equiv 1 \pmod{M}$, $n = p^\alpha q^\beta w$ for distinct primes $p, q \equiv 1 \pmod{M}$, $\alpha, \beta \geq 1$, and $\gcd(pq, w) = 1$. Then for $i = 1, 2, \ldots, M$ we have*

$$\left(i\frac{n-1}{M}\right)_n ! \equiv \frac{\varepsilon^{i\frac{p-1}{M}}}{p^{iA}} \pmod{q^\beta w}, \quad A = \frac{p^{\alpha-1}}{M}\phi(q^\beta w), \tag{4.2}$$

where

$$\varepsilon = \begin{cases} -1 & \text{if } w = 1 \\ 1 & \text{if } w > 1. \end{cases}$$

Theorem 4.2. *Let $M \geq 2$ be an integer, and suppose that n has at least two distinct prime factors congruent to $1 \pmod{M}$. Then (4.1) holds, i.e. the partial products are all congruent $\pmod{n}$.*

Proof. We start off by observing that every partial product $\Pi_j^{(M)}$ can be written as a quotient of two Gauss factorials, namely

$$\Pi_j^{(M)} = \frac{(j\frac{n-1}{M})_n!}{\big((j-1)\frac{n-1}{M}\big)_n!}, \quad j = 1, 2, \ldots, M, \tag{4.3}$$

with the convention that $0_n! = 1$.

Combining the congruence (4.3) with (4.2), we get

$$\Pi_j^{(M)} \equiv \frac{\varepsilon^{\frac{p-1}{M}}}{p^A} \pmod{q^\beta w}, \quad A = \frac{p^{\alpha-1}}{M}\phi(q^\beta w). \tag{4.4}$$

Since we can interchange p^α and q^β, we also have

$$\Pi_j^{(M)} \equiv \frac{\varepsilon^{\frac{q-1}{M}}}{q^B} \pmod{p^\alpha w}, \quad B = \frac{q^{\beta-1}}{M}\phi(p^\alpha w). \tag{4.5}$$

We can now apply the Chinese Remainder Theorem to (4.4) and (4.5) to determine a unique value of $\Pi_j^{(M)}$ modulo $p^\alpha q^\beta w = n$, which is independent of j. This completes the proof of the theorem.

□

Theorem 4.3. *Let $M \geq 2$ be an integer, and suppose that the positive integer n has at least three distinct prime factors $\equiv 1 \pmod{M}$. Then*

$$\Pi_j^{(M)} \equiv 1 \pmod{n} \quad \textit{for} \quad j = 1, 2, \ldots, M. \tag{4.6}$$

Proof. We begin by rewriting A in (4.4) by using the multiplicativity of Euler's phi-function and the fact that $q \equiv 1 \pmod{M}$.

$$A = \frac{p^{\alpha-1}}{M}\phi(q^\beta)\phi(w) = p^{\alpha-1}\frac{(q-1)q^{\beta-1}}{M}\phi(w) = C\phi(w)$$

for some integer C. As $p \nmid w$, it follows from Euler's generalization of Fermat's little theorem that

$$p^{iA} = \left(p^{iC}\right)^{\phi(w)} \equiv 1 \pmod{w}.$$

Consider the quotient $\frac{\varepsilon^{i\frac{p-1}{M}}}{p^{iA}}$. We know that the denominator is congruent to 1 $\pmod{w}$. If $w > 1$, $\varepsilon = 1$ and then the numerator is also congruent to 1 $\pmod{w}$. If $w = 1$ the numerator is trivially congruent to 1 $\pmod{w}$. So in either case, by (4.4) we have

$$\left(i\frac{n-1}{M}\right)_n ! \equiv 1 \pmod{w} \quad \text{and} \quad \Pi_j^{(M)} \equiv 1 \pmod{w}. \tag{4.7}$$

Now, let $n = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\bar{w}$, where p_1, p_2, p_3 are distinct primes with $p_i \equiv 1 \pmod{M}$, $\alpha_i \geq 1$ for $i = 1, 2, 3$, and $\gcd(p_1p_2p_3, \bar{w}) = 1$. Replace w in (4.7) with w_i, $w_i = p_i^{\alpha_i}\bar{w}$, $i = 1, 2, 3$. This gives $\Pi_j^{(M)} \equiv 1 \pmod{w_i}$ for $i = 1, 2, 3$. The congruences (4.6) then follow directly from the Chinese Remainder Theorem. □

4.2 Revisiting the Primes: The Gauss and Jacobi Binomial Coefficient Theorems

Although we have already suggested that there might not be any prime for which all the partial products $\Pi_j^{(M)}$ are congruent $\pmod{p}$ for a fixed M, there are interesting relationships between the quotients of partial products and the representation of p as a sum of squares.

4.2.1 $Q_4(p)$ and the Gauss Binomial Coefficient Theorem

Let us first turn our attention to the case when we have four partial products. As we have already taken note of, $\Pi_{M-j}^{(M)} \equiv \pm\Pi_j^{(M)} \pmod{p}$, so the interesting relationship here is the quotient $Q_4(p) = \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}}$. For $p \equiv 1 \pmod 4$, $\Pi_1^{(4)} = \frac{p-1}{4}!$ and $\Pi_1^{(4)}\Pi_2^{(4)} = \frac{p-1}{2}!$, so

$$Q_4(p) = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2} = \frac{\frac{p-1}{2}!}{\left(\frac{p-1}{4}!\right)^2} = \binom{\frac{p-1}{2}}{\frac{p-1}{4}}.$$

By a classic theorem of Fermat (see for instance [Bur02]), if p is a prime and congruent to 1 (mod 4), it can be represented as a sum of two squares a^2 and b^2, where a, $b \neq 0$ are integers. Choose a such that $a \equiv 1 \pmod 4$. It is obvious that there is always such a choice of a, as one of a^2 and b^2 must be congruent to 1 (mod 4).

We can now state Gauss's binomial coefficient theorem as follows.

Theorem 4.4. *Let the prime p and integer a be as above. Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod{p}.$$

The proof of the theorem is nonelementary and will not be stated here. An interesting application of the theorem, however, is the following result.

Corollary 4.5. $\Pi_2^{(4)} \not\equiv \pm\Pi_1^{(4)} \pmod{p}$ *for all* $p \equiv 1 \pmod 4$.

Proof. To prove this, assume for a contradiction that $Q_4(p) \equiv \pm 1 \pmod{p}$. On the other hand, by Theorem 4.4 we know that $Q_4(p) \equiv 2a \pmod{p}$, so $2a \equiv \pm 1 \pmod{p}$. The smallest possible value of a is then $\frac{p-1}{2}$. But as $p = a^2 + b^2$, we must have $|a| < \sqrt{p}$, and since $\sqrt{p} < \frac{p-1}{2}$ for $p > 5$, this is impossible. So there are no solutions of the congruence $2a \equiv \pm 1 \pmod{p}$, which was what we had to show. □

4.2.2 $Q_3(p)$ and Jacobi's Binomial Coefficient Theorem

For primes $p \equiv 1 \pmod 6$ we consider

$$Q_3(p) = \frac{\Pi_2^{(3)}}{\Pi_1^{(3)}} = \frac{\Pi_1^{(3)}\Pi_2^{(3)}}{\left(\Pi_1^{(3)}\right)^2} = \frac{\left(2\frac{p-1}{3}\right)!}{\left(\frac{p-1}{3}!\right)^2} = \binom{2\frac{p-1}{3}}{\frac{p-1}{3}}.$$

Jacobi's binomial coefficient theorem gives us a formula for $Q_3(p)$ analogue to Gauss's formula for $Q_4(p)$. The expression of p as a sum of squares is, however, less straightforward for $p \equiv 1 \pmod 6$. We will therefore use the following two lemmas to present the result.

Lemma 4.6. *Let $p \equiv 1 \pmod 6$, p prime. Then $\exists\ x, y \in \mathbb{Z} : p = x^2 + 3y^2$.*

Proof. [*] By Theorem 9.10 in [Bur02], if p is a prime and $p \neq 3$, then

$$(3 \mid p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}, \end{cases}$$

where the Legendre symbol $(3 \mid p)$ equals 1 if 3 is a quadratic residue of p (i.e. if there exists a such that $a^2 \equiv 3 \pmod p$), and $(3 \mid p) = -1$ otherwise.

Let $p = 6m + 1$, m an integer. By Theorem 9.2 in [Bur02] we know that $(-1 \mid p) = (-1)^{\frac{p-1}{2}} = (-1)^{3m}$, $m \in \mathbb{Z}$. If m is even, then $p \equiv 1 \pmod{12}$ and $(-1)^{3m} = 1$. If m is odd, then $p \equiv -5 \pmod{12}$ and $(-1)^{3m} = -1$.

Combining the results for $(3 \mid p)$ and $(-1 \mid p)$ we get

$$(-3 \mid p) = (-1 \mid p)(3 \mid p) = \begin{cases} 1 \cdot 1 = 1 & \text{if } p \equiv 1 \pmod{12} \\ (-1)(-1) = 1 & \text{if } p \equiv -5 \pmod{12}. \end{cases}$$

So for all $p \equiv 1 \pmod 6$ $\exists\ a : a^2 \equiv -3 \pmod p$. Naturally, we must have $\gcd(a, p) = 1$, and by Thue's lemma, the congruence $ax \equiv y \pmod p$ admits a solution (x_0, y_0) where $0 < |x_0|, |y_0| < \sqrt{p}$.
Squaring the congruence, it follows that

$$(ax_0)^2 \equiv y_0^2 \text{ (mod p)} \Rightarrow -3x_0^2 \equiv y_0^2 \text{ (mod p)}.$$

We can thus conclude that

$$3x_0^2 + y_0^2 = kp, \tag{4.8}$$

where $k \geq 1$ is an integer. As $0 < |x_0| < \sqrt{p}$ and $0 < |y_0| < \sqrt{p}$, we obtain $0 < 3x_0^2 + y_0^2 < 4p$. Thus, the only possible values of k are $1, 2$ or 3.

If $k = 3$, then it follows that $3 \mid y_0 \Rightarrow y_0 = 3y_1$ for some $y_1 \in \mathbb{Z}$. This gives $3x_0^2 + (3y_1)^2 = 3p \Rightarrow x_0^2 + 3y_1^2 = p$, and then we can choose $(x_0,\ y_1)$ as a solution of the equation.

If $k = 2$, then $3x_0^2 + y_0^2 = 2p$ and we must have $x_0 \equiv y_0 \pmod 2$. If $x_0 \equiv y_0 \equiv 0 \pmod 2$, then $x_0 = 2x_2$, $y_0 = 2y_2$ and (4.8) becomes

$$3(2x_2)^2 + (2y_2)^2 = 2p \Leftrightarrow 4(3x_2^2 + y_2^2) = 2p \Rightarrow 2 \mid p.$$

This leads to a contradiction, as $p \equiv 1 \pmod 6$.

If $x_0 \equiv y_0 \equiv 1 \pmod 2$, then $x_0 = 2x_3 + 1$ and $y_0 = 2y_3 + 1$, $x_3, y_3 \in \mathbb{Z}$. Then the left hand side of (4.8) will equal $3(2x_3+1)^2+(2y_3+1)^2 = 3(4x_3^2+4x_3+1)+(4y_3^2+4y_3+1) = 4n+4 \equiv 0 \pmod 4$ (n an integer). Again, the left hand side of (4.8) is a multiple of 4, which implies that p is a multiple of 2 and hence leads to a contradiction. In case $k = 1$, (4.8) gives the required representation. □

Lemma 4.7. *Let $p \equiv 1 \pmod 6$, p prime. Then there exist three distinct solutions (x_i, y_i), $i = 0, 1, 2$, $x_i, y_i > 0$ of the equation*

$$x^2 + 3y^2 = 4p. \tag{4.9}$$

Proof. [*] By Lemma 4.6, we know that there exist positive integers a and b such that $a^2 + 3b^2 = p$. Consider the ring

$$\mathbb{Z}[\sqrt{-3}] = \left\{x + y\sqrt{-3} \;\mid\; x, y \in \mathbb{Z}\right\}.$$

Let N be the norm in $\mathbb{Z}[\sqrt{-3}]$, defined by

$$N(x + y\sqrt{-3}) = (x + y\sqrt{-3})\overline{(x + y\sqrt{-3})} = x^2 - (-3)y^2 = x^2 + 3y^2.$$

By Theorem 10.19 in [Hun12], $N(\alpha\beta) = N(\alpha)N(\beta)$. If we choose a and b as above, then $N(a + b\sqrt{-3}) = p$, and $4p = 4N(a + b\sqrt{-3}) = N(2)N(a + b\sqrt{-3}) = N(2a + 2b\sqrt{-3})$. So $(2a, 2b)$ is a solution of the equation.

Now consider the larger ring $\mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{-3}}{2}$. Clearly,

$$\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\omega], \text{ as } \mathbb{Z}[\sqrt{-3}] = \{x + y\omega \mid x \in \mathbb{Z},\, y \in 2\mathbb{Z}\}.$$

We see that $N(\omega) = \frac{1}{4}(-1 + \sqrt{-3})(-1 - \sqrt{-3}) = 1$. So in $\mathbb{Z}[\omega]$ and for k a positive integer, we have

$$4p = N(2)N(\omega^k)N(a + b\sqrt{-3}) = N\left(2\omega^k(a + b\sqrt{-3})\right).$$

It is thus possible to obtain more solutions by multiplying our first solution $(2a, 2b)$ by powers of ω. We may also note that

$$\omega^2 = \left(\frac{-1+\sqrt{-3}}{2}\right)^2 = \frac{-1-\sqrt{-3}}{2} = -1-\omega \text{ and}$$

$$\omega^3 = \omega\omega^2 = \omega(-1-\omega) = 1.$$

This implies that the relevant powers of ω to multiply our solution by is ω and ω^2. Now, 2ω, $2\omega^2 \in \mathbb{Z}[\sqrt{-3}]$ as $2 \in 2\mathbb{Z}$, and hence the product will be an element of $\mathbb{Z}[\sqrt{-3}]$.
Multiplication by ω gives

$$2\omega(a+b\sqrt{-3}) = (-1+\sqrt{-3})(a+b\sqrt{-3}) = -\left((a+3b)+(b-a)\sqrt{-3}\right).$$

Similarly, multiplying by ω^2, we get

$$2\omega^2(a+b\sqrt{-3}) = (-1-\sqrt{-3})(a+b\sqrt{-3}) = -\left((a-3b)+(a+b)\sqrt{-3}\right).$$

Collecting the results obtained by multiplying our original solution by ω and ω^2, and requiring both coordinates to be positive in our new solutions, we have found two additional solutions of the equation $4p^2 = x^2 + 3y^2$, namely $(x_1, y_1) = (|a+3b|, |a-b|)$, $(x_2, y_2) = (|a-3b|, |a+b|)$. These two solutions together with the solution $(x_0, y_0) = (|2a|, |2b|)$ represent the desired three solutions of the equation. □

It can be shown that there are no further solutions of (4.9).

We shall now show that for $p \equiv 1 \pmod 6$, there is a solution (r, s) of (4.9) such that

$$4p = r^2 + 3s^2, \quad r \equiv 1 \pmod 3, \quad s \equiv 0 \pmod 3.$$

Let

$$(x_0, y_0) = (|2a|, |2b|),\ (x_1, y_1) = (|a+3b|, |a-b|),\ (x_2, y_2) = (|a-3b|, |a+b|)$$

and recall that

$$x_i^2 + 3y_i^2 = 4p. \tag{4.10}$$

We have to show that there is only one choice of y_i such that $y_i \equiv 0 \pmod 3$, which will then uniquely determine r. First note that $3 \nmid a$, for otherwise

the left-hand side of equation (4.10) would be a multiple of 3, which cannot be true since $p \equiv 1 \pmod 6$.

In the case $b \equiv 0 \pmod 3$, then $y_0 \equiv 0 \pmod 3$, and as $3 \nmid a$ we must have $3 \nmid y_1$, $3 \nmid y_2$.

In the case $b \equiv \pm 1 \pmod 3$, as $3 \nmid a$ we must either have $a \equiv b \pmod 3$ or $a \equiv -b \pmod 3$. If $a \equiv b \pmod 3$, then $3 \mid y_1$ and $3 \nmid y_i$ for $i \neq 1$. If $a \equiv -b \pmod 3$, then $3 \mid y_2$ and $3 \nmid y_i$ for $i \neq 2$.

Now, in each individual case we must have $x_i \equiv \pm 1 \pmod 3$ for the corresponding value of i. For that x_i, choose $r = x_i$ or $r = -x_i$ so that $r \equiv 1 \pmod 3$. We shall now proceed to stating Jacobi's binomial coefficient theorem, which will give us an explicit expression of $Q_3(p)$.

Theorem 4.8. *Let p and r be as above. Then*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p.$$

As with Gauss's binomial coefficient theorem, we shall leave the proof aside and turn to a direct consequence of the theorem, namely the following result.

Corollary 4.9. $\Pi_2^{(3)} \not\equiv \Pi_1^{(3)} \pmod p$ *for* $p \equiv 1 \pmod 6$.

Proof. Assume for a contradiction that the two partial products were indeed congruent. Then we would have $r \equiv -1 \pmod p$, and as $r = -1$ is impossible since $r \equiv 1 \pmod 3$, the smallest possible solution of the congruence is $r = p - 1$. But as we must have $|r| < 2\sqrt{p}$, and we have seen that $2\sqrt{p} < p - 1$ for $p > 5$, this solution is also impossible. □

References

[Bur02] David M. Burton, *Elementary Number Theory*, 5 ed., McGraw-Hill, 2002.

[CD11] John B. Cosgrave and Karl Dilcher, *An Introduction to Gauss Factorials*, The American Mathematical Monthly **118** (2011), no. 9, 812–829.

[Hun12] Thomas W. Hungerford, *Abstract Algebra*, 3 ed., Brooks/Cole, 2012.

[Leh55] D.H. Lehmer, *The distribution of totatives*, Canadian Journal of Mathematics **7** (1955), 347–357.