A generalization of Euler’s Criterion
to composite moduli

József Vass

Department of Algebra and Number Theory, Eötvös Loránd University
Pázmány Péter sétány 1/C, H-1117 Budapest, Hungary
e-mail: vass@cs.elte.hu

Received: 2 July 2015 Revised: 25 July 2016 Accepted: 28 July 2016

Abstract: A necessary and sufficient condition is provided for the solvability of a binomial congruence with a composite modulus, circumventing its prime factorization. This is a generalization of Euler’s Criterion through that of Euler’s Theorem, and the concepts of order and primitive roots. Idempotent numbers play a central role in this effort.

Keywords: Binomial congruences, Power residues, Generalized primitive roots.

AMS Classification: 11A15, 11A07, 11C08.

1 Introduction

1.1 Overview

The solvability of binomial congruences of the form $x^k \equiv a \pmod{m}$, $k \in \mathbb{N}$, $a \in \mathbb{Z}_m$ where the modulus $m$ is any integer, is generally reduced using the Chinese Remainder Theorem to a system of congruences with prime power moduli, for which solvability can be decided with well-known techniques. Since the algorithmic complexity of prime factorization is high, it may be worthwhile to explore an alternative path.

This path will be set by idempotent numbers $e^2 \equiv e \pmod{m}$ which are projections to divisors of $m$ sharing the same prime power factors, enabling us to bypass the Chinese Remainder Theorem. Their relevance will emerge with our generalization of Euler’s Theorem, which is the basis for the concepts of order, orbit, and index generalized to composite moduli as well. A useful generalization of primitive roots is subsequently suggested. The mentioned alternative path must somehow avoid the fact that genuine primitive roots which generate all coprime residues do not
exist for a general modulus. Indeed this is accomplished with a critical theorem, leading to a theoretical equivalence condition for the solvability of such a congruence, similar to Euler’s Criterion. Such criteria for power residues may lead to practical reciprocity laws.

For an overview of congruences see Andrews [2], and of reciprocity see Lemmermeyer [10]. For a more complete discussion of composite moduli via idempotent numbers, see Vass [21].

1.2 Preliminaries

Notation 1.1. Let \( \mathbb{N} \) denote the set of integers greater than or equal to 1. Let the prime numbers be denoted as \( p_i, \ i \in \mathbb{N} \) in ascending order. Denote the prime factorization of \( m \in \mathbb{N} \) as \( m = p_1^{\alpha_1} \cdots p_i^{\alpha_i} \cdots (\alpha_i \geq 0) \). Denote \( \mathbb{Z}_m := \{1, \ldots, m\} \) and let \( a \) mod \( m \) be the number \( b \in \mathbb{Z}_m \) for which \( a \equiv b \) (mod \( m \)). For \( A \subset \mathbb{Z}_m \), \( a \in \mathbb{Z} \) write \( a \in_m A \) iff \( (a \mod m) \in A \). Let \( (a, b) \) denote the greatest common divisor of the numbers \( a, b \in \mathbb{N} \). For \( A \subset \mathbb{N} \) let \( \gcd(a : a \in A) \) denote the greatest common divisor of all the elements in \( A \). Let \( [a, b] \) denote the least common multiple. Let \( \varphi(m) \) denote Euler’s totient function.

Theorem 1.1. (Euler’s Theorem [5]) \( \forall m \in \mathbb{N}, \ a \in \mathbb{Z}_m, \ (a, m) = 1 : \ a^{\varphi(m)} \equiv 1 \) (mod \( m \)).

Theorem 1.2. (Euler’s Criterion [3, 4]) Take a modulus \( m \) of the form \( 2, 4, p^\alpha \) or \( 2^\alpha p^\alpha \) with an odd prime number \( p \) and \( \alpha \in \mathbb{N} \) (i.e. a primitive root exists). Then \( a \in \mathbb{Z}_m, \ (a, m) = 1 \) is a \( k \)-th power residue \( (k \in \mathbb{N}) \), meaning \( x^k \equiv a \) (mod \( m \)) is solvable for \( x \in \mathbb{Z}_m \) if and only if

\[
a^{\frac{\varphi(m)}{[\varphi(m), k]}} \equiv 1 \pmod{m}.
\]

The proof of the above criterion relies heavily on the existence of a primitive root for moduli of the above form. So to find a similar criterion for composite moduli, the challenge becomes to avoid the need for a primitive root.

2 Idempotent and regular numbers

2.1 Order

Definition 2.1. A residue \( e \in \mathbb{Z}_m \) is an idempotent number modulo \( m \) if \( e^2 \equiv e \) (mod \( m \)), and let \( E_m \) denote their set.

It is easy to show that their cardinality is \( |E_m| = 2^N \) where \( N \) is the number of distinct prime power factors of \( m \) (so if \( m \) is a prime power, then \( E_m = \{1, m\} \)). The notation \( e \) comes from the first letter of the Hungarian word for “unit”, since as stated in Theorem 2.2 certain subsets of \( \mathbb{Z}_m \) form abelian groups with an idempotent number as their unit element.

Theorem 2.1. (Generalization of Euler’s Theorem) \( \forall m \in \mathbb{N}, \ a \in \mathbb{Z}_m : \ a^{\varphi(m)} \in_m E_m. \)

Proof. Take any \( i \in \mathbb{N} \) index for which \( \alpha_i > 0 \) in the prime factorization of \( m \). Let us consider two cases, depending on whether \( p_i \) divides \( a \) or not. Supposing first that \( p_i \mid a \)

\[
\alpha_i = 1 + (\alpha_i - 1) \leq 2^{\alpha_i-1} \leq p_i^{\alpha_i-1} \leq p_i^{\alpha_i-1}(p_i - 1) \leq \varphi(m)
\]
we may conclude that \( a^{\varphi(m)} \equiv 0 \pmod{p_i^{\alpha_i}} \). On the other hand, if \( p_i \nmid a \) then by Euler’s Theorem 1.1 and \( \varphi(p_i^{\alpha_i}) \mid \varphi(m) \) we get that \( a^{\varphi(m)} \equiv 1 \pmod{p_i^{\alpha_i}} \). Thus in both cases, for any \( i \) index \( a^{\varphi(m)}(a^{\varphi(m)} - 1) \equiv 0 \pmod{p_i^{\alpha_i}} \) implying that \( a^{\varphi(m)} \pmod{m} \) is idempotent. \( \square \)

Various other generalizations exist, such as the one by László Rédei [18]: \( \forall m \in \mathbb{N}, a \in \mathbb{Z}_m : a^m \equiv a^{m-\varphi(m)} \pmod{m} \), by José Morgado [13, 14, 15], and others [23, 16, 9, 11, 7, 17].

**Definition 2.2.** For \( a \in \mathbb{Z} \) let its order modulo \( m \) be the smallest \( n \in \mathbb{N} \) power for which \( a^n \equiv a \pmod{m} \). Let \( |a|_m \) denote this power, which exists due to the above theorem.

### 2.2 Regularity

**Definition 2.3.** [22, 12, 13, 21, 1, 19, 20] The residue \( a \in \mathbb{Z}_m \) is said to be regular modulo \( m \) if \( a^{[a]_m+1} \equiv a \pmod{m} \). Let \( R_m \) denote the set of all regular residues modulo \( m \). For \( e \in \mathbb{E}_m \) denote \( \mathbb{R}^e_m := \{ a \in \mathbb{R}_m : a^{[a]_m} \equiv e \pmod{m} \} \).

Among many interesting facts, it is true that all residues are regular modulo \( m \) iff \( m \) is square-free. Several equivalent definitions may be given for regularity. Perhaps the most straightforward one is that \( a \) is regular iff there exists some power \( n > 1 \) for which \( a^n \) is congruent to \( a \). In essence, \( a \in \mathbb{R}_m \) iff \( p_i \mid a \) implies \( p_i^{\alpha_i} \mid a \). Note that \( \mathbb{R}^1_m \) is a reduced residue system modulo \( m \).

**Proposition 2.1.** For any \( a \in \mathbb{R}_m, k, l \in \mathbb{N} \) the following hold:

1. \( a^k \in \mathbb{E}_m \Rightarrow |a|_m \mid k \),
2. \( |a|_m \mid \varphi(m) \),
3. \( a^k \equiv a^l \pmod{m} \iff k \equiv l \pmod{|a|_m} \),
4. \( |a^k|_m = |a|_m/(k, |a|_m) \).

**Proof.**

1. Let \( q, r \in \mathbb{N} \cup \{0\} \) be such that \( k = q|a|_m + r, \ 0 \leq r < |a|_m \). Then

\[
    a^k \equiv (a^{[a]_m})^q \cdot a^r \equiv a^{[a]_m} \cdot a^r \equiv a^r \pmod{m}
\]

so \( a^r \in \mathbb{E}_m \), which can only be if \( r = 0 \), by the definition of order.

2. Follows from 1.

3. Clearly we have

\[
    a^k \equiv a^l \pmod{m} \Rightarrow a^{k \varphi(m) - l} \equiv a^l \varphi(m) \pmod{m}.
\]

Since \( a^{l \varphi(m)} \in \mathbb{E}_m \) then by 1. and 2. we have

\[
    0 \equiv k + l \varphi(m) - l \equiv k - l \pmod{|a|_m} \Rightarrow k \equiv l \pmod{|a|_m}.
\]

*See the author’s master’s thesis [21] for the proofs, in which regular numbers were named and investigated independently of the works of von Neumann [22] and José Morgado [12], of which the author used to be unaware.
Now if \( l \geq k \) and \( k \equiv l \pmod{|a|_m} \), then for some \( q \geq 0 \), we have \( l = k + q|a|_m \), so

\[
a^k \equiv a^{k+q|a|_m} \equiv a^k a^{|a|_m} \equiv a^k \pmod{m}
\]

where the last congruence holds, because \( a \) is regular.

4. Considering the congruence

\[
(a^k)^{|a|_m/m} = (a^{|a|_m})^{k/m} \in_m E_m
\]

we have \( |a^k|_m \leq |a|_m / (k, |a|_m) \) by the definition of order. Also by 1. we have

\[
a^{kl} \in_m E_m \Rightarrow |a|_m | kl \iff |a|_m / (k, |a|_m) \mid l
\]

so we have \( |a^k|_m \geq |a|_m / (k, |a|_m) \).

**Proposition 2.2.** A number \( a \in \mathbb{Z}_m \) is regular if and only if the following equivalence holds

\[
a^k \equiv a^l \pmod{m} \iff k \equiv l \pmod{|a|_m} \ (k, l \in \mathbb{N}).
\]

**Proof.** By Proposition 2.1, we have that if \( a \) is regular, then the equivalence holds. On the other hand, if the equivalence holds, then with \( k := |a|_m + 1 \), \( l := 1 \) we have that \( a \) is regular. ☐

**Definition 2.4.** Denote \( a^0 := a^{|a|_m} \pmod{m} \). Let the **inverse** of \( a \in R_m \) be the residue \( a^{-1} := a^{|a|_m-1} \pmod{m} \), and for any \( n \in \mathbb{N} \) denote \( a^{-n} := (a^{-1})^n \pmod{m} \).

**Theorem 2.2.** For all \( e \in E_m \) the structure \( \langle R^e_m; \{ e, \cdot, -1 \} \rangle \) is an abelian group.

**Proof.** The properties to be shown are mostly trivial, except for maybe one. We need to show that for all \( a \in R^e_m \) there exists a unique \( b \in R^e_m \) such that \( ab \equiv e \pmod{m} \).

Let \( b := a^{|a|_m-1} \pmod{m} \). It is obvious that \( ab \equiv e \pmod{m} \). Now, let us suppose that there exists some other \( b' \in R^e_m \) such that \( ab' \equiv e \pmod{m} \). Then we have

\[
a(b - b') \equiv 0 \pmod{m} \Rightarrow 0 \equiv a^{|a|_m-1} \cdot a(b - b') \equiv e(b - b') \equiv b^{|a|_m-1} - (b')^{|a|_m-1} \equiv b - b' \pmod{m}.
\]

**Proposition 2.3.** For any \( a \in R_m \), \( n \in \mathbb{N} \), \( i, j \in \mathbb{Z} \) we have

\[
(a^n)^{-1} \equiv a^{-n} \pmod{m} \quad \text{and} \quad a^{i+j} \equiv a^i \cdot a^j \pmod{m}.
\]

**Proof.** The first statement is equivalent to saying that

\[
(a^n)^{|a|_m-1} \equiv a^{|a|_m-n} \pmod{m}
\]

which by Proposition 2.2 is equivalent to (when \( n \frac{|a|_m}{(n, |a|_m)} - n \neq 0 \))

\[
\frac{n}{(n, |a|_m)} |a|_m - n \equiv n|a|_m - n \pmod{|a|_m}
\]

12
and this congruence clearly holds. In the omitted case
\[ n \frac{|a|_m}{(n, |a|_m)} - n = 0 \iff |a|_m \mid n \]
so for some \( k \in \mathbb{N} \), we have
\[ a^{-n} \equiv a^{n|a|_m-n} = a^{(n-k)|a|_m} \equiv a^0 \equiv (a^n)^{-1} \pmod{|a|_m}. \]

For the second property, we can distinguish four different cases (for nonzero exponents):

The case of \( i, j > 0 \) is trivial. The case of \( i, j < 0 \):
\[ a^{i+j} = a^{-|i+j|} \equiv (a^{-1})^{|i+j|} = (a^{-1})^{|i|} \cdot (a^{-1})^{|j|} \equiv a^{-|i|} \cdot a^{-|j|} \equiv a^i \cdot a^j \pmod{m}. \]

The case of \( j \geq |i| \):
\[ a^{i+j} = a^{j-|i|} \Rightarrow a^j = a^{i+j} \cdot a^{|i|} \Rightarrow a^{i+j} \equiv a^j \cdot (a^{|i|})^{-1} \equiv a^j \cdot a^{-|i|} \equiv a^i \cdot a^j \pmod{m}. \]

The case of \( j < |i| \):
\[ a^{i+j} \equiv a^{-|i|} \equiv a^{-(|i|-j)} \equiv (a^{|i|-j})^{-1} \equiv (a^{|i|} \cdot a^{-j})^{-1} \pmod{m} \]

where the last congruence is true with the application of the previous case. Lastly
\[ (a^{|i|} \cdot a^{-j}) \cdot (a^{-|i|} \cdot a^j) \equiv (a^{|i|})(a^{|i|})^{-1}(a^j)^{-1} \equiv (a^{|a|_m})^{|i|+j} \equiv a^{|a|_m} \pmod{m} \]

so by the unicity of the inverse (previous theorem), we have
\[ (a^{|i|} \cdot a^{-j})^{-1} \equiv a^{-|i|} \cdot a^j \equiv a^i \cdot a^j \pmod{m}. \]

The case of \( i > 0, \ j < 0 \) is similar to the previous two. \( \square \)

### 2.3 Orbit

**Definition 2.5.** Let the orbit of \( a \in \mathbb{Z}_m \) be the set \( \langle a \rangle_m := \{ a^n \mod m : 1 \leq n \leq |a|_m \} \).

**Proposition 2.4.** For any \( b, c \in \mathbb{R}_m, \ n, k \in \mathbb{N} \) we have
\[ b^n, b^k \in \langle c \rangle_m \iff b^{(n,k)} \in \langle c \rangle_m. \]

**Proof.** First suppose that \( b^n \equiv c^i, \ b^k \equiv c^j \pmod{m} \). Without hurting generality, we may suppose that there exist \( x, y \geq 0 \) such that \( (n, k) = nx - ky \). So we have
\[ b^{(n,k)} = b^{nx-ky} = b^{nx} \cdot b^{-ky} \equiv b^{nx} \cdot (b^{ky})^{-1} \equiv (c^i)^x \cdot (c^j)^{-y} \pmod{m} \]
with the application of Proposition 2.3.

Now, let us suppose that \( b^{(n,k)} \equiv c^i \pmod{m} \). Then we have
\[ b^n \equiv b^{(n,k) \frac{n}{(n,k)}} \equiv (c^i)^{\frac{n}{(n,k)}} \pmod{m} \]
and also \( b^k \in \langle c \rangle_m \) similarly. \( \square \)
Definition 2.6. For \( e \in E_m \), \( b, c \in R_m^e \), denote
\[
D_m(b, c) := \gcd(n \in \mathbb{N} : 1 \leq n \leq |b|_m, b^n \equiv_m (c)_m).
\]

Proposition 2.5. If \( e \in E_m \), \( b, c \in R_m^e \), then \( D_m(b, c) \mid |b|_m \) and
\[
b^k \equiv_m (c)_m \iff D_m(b, c) \mid k.
\]
Furthermore \( b^{D_m(b,c)} \equiv_m (c)_m \) and
\[
\langle b \rangle_m \cap (c)_m = \langle b^{D_m(b,c)} \rangle_m \quad \text{and} \quad |\langle b \rangle_m \cap (c)_m| = \frac{|b|_m}{D_m(b, c)}.
\]

Proof. Applying Proposition 2.4 inductively \( b^{D_m(b,c)} \equiv_m (c)_m \) must hold. Now supposing that \( D_m(b, c) \mid k \) we have
\[
b^k \equiv (b^{D_m(b,c)})^\frac{k}{D_m(b,c)} \equiv_m (c)_m.
\]
If \( b^k \equiv_m (c)_m \) then with \( k' := k \mod |b|_m \) we have \( b^{k'} \equiv_m (c)_m \) so \( D_m(b, c) \mid k' \) by definition, and from this it follows that \( D_m(b, c) \mid k \).

By the first property now proven, we get the second one
\[
\langle b \rangle_m \cap (c)_m = \langle b^{D_m(b,c)} \rangle_m.
\]
It is also true that \( D_m(b, c) \mid |b|_m \) since
\[
b^{|b|_m} \equiv e \equiv e^{\mid c \mid_m} \equiv_m (c)_m
\]
so lastly, we have that
\[
|\langle b \rangle_m \cap (c)_m| = |\langle b^{D_m(b,c)} \rangle_m| = |b|_m = \frac{|b|_m}{D_m(b, c)}.
\]

2.4 Index

Definition 2.7. [6, 24] If it exists for \( a, b \in \mathbb{Z}_m \), let the index \( \text{ind}^m_b a \) denote the smallest \( n \in \mathbb{N} \), for which \( b^n \equiv a \pmod{m} \). Let this existence be denoted as \( \exists \text{ind}^m_b a \). For \( a \in R_m \) let its primitive order be the number \( \omega_m(a) := \max\{|b|_m : b \in R_m, \exists \text{ind}^m_b a\} \).

If \((a, m) = 1 \) and a primitive root exists modulo \( m \), then clearly \( \omega_m(a) = \varphi(m) = |g|_m \) for any primitive root \( g \in R_m^1 \). Thus a number \( g \in R_m \) may be considered a “generalized primitive root” if \( \omega_m(g) = |g|_m \) (see [21] for further discussion).

Proposition 2.6. For any \( k \in \mathbb{N} \), \( e \in E_m \), \( a, b \in R_m^e \), \( \exists \text{ind}^m_b a \) we have the equivalence
\[
(k, |b|_m) \mid \text{ind}^m_b a \iff a^{\frac{|b|_m}{(k, |b|_m)}} \equiv_m E_m.
\]

Proof. The equivalence can be deduced as follows.
\[
e \equiv a^{\frac{|b|_m}{(k, |b|_m)}} \equiv b^{\text{ind}^m_b a \frac{|b|_m}{(k, |b|_m)}} \equiv b^{\text{ind}^m_b a \frac{|b|_m}{(k, |b|_m)}} \pmod{m}
\]
\[
\iff |b|_m \mid b^{\text{ind}^m_b a \frac{|b|_m}{(k, |b|_m)}} \iff \text{ind}^m_b a \frac{|b|_m}{(k, |b|_m)} \in \mathbb{N} \iff (k, |b|_m) \mid \text{ind}^m_b a.
\]

14
Proposition 2.7. If \( e \in \mathbb{E}_m \), \( a, b \in \mathbb{R}_m^e \), \( (|a|_m, |b|_m) = 1 \) then \( |ab|_m = |a|_m \cdot |b|_m \).

Proof. We readily see that \((ab)^{|a|_m, |b|_m} \equiv e \pmod{m}\) implying \( |ab|_m \mid |a|_m \cdot |b|_m \). For the other direction of division, we first deduce

\[
e \equiv (ab)^{|a|_m, |b|_m} \equiv e \cdot b^{\lfloor |a|_m/\varphi(m) \rfloor \cdot |b|_m} \quad \text{(mod m)} \quad \Rightarrow \quad |b|_m \mid |a|_m \cdot |ab|_m \quad \Rightarrow \quad |b|_m \mid |ab|_m
\]

and similarly \( |a|_m \mid |ab|_m \) also holds, implying that \( |a|_m \cdot |b|_m \mid |ab|_m \). \( \square \)

Lemma 2.1. Given \( u, v, w \in \mathbb{N} \), \( w \mid (u, v) \) there exist \( u_{1,2}, v_{1,2}, w_{1,2} \in \mathbb{N} \) such that \( u = u_1u_2, v = v_1v_2, w = w_1w_2\) and \((u, v) = u_2v_1\) and \( w_1 \mid u_1, w_2 \mid u_2 \). Lastly, observe that \( 1 = (u_1, u_2) = (v_1, v_2) = (w_1, w_2) = (u_1, v_2) = (u_2, v_1) \) as required.

Proof. Letting \( C := (u, v) \), \( U := u/C \), \( V := v/C \) we have \((U, V) = 1\). Partitioning \( C \) according to the prime factors of \( U \) and \( V \), there must exist \( A, B \in \mathbb{N} \) \((C = AB)\) such that \((A, B) = 1 \equiv (A, V) = (B, U)\). Clearly \( u = AUB \), \( v = AVB \) so defining \( u_1 := AU \), \( u_2 := B \), \( v_1 := A \), \( v_2 := VB \) then due to \( w \mid C = AB = u_2v_1 \) there must exist \( w_{1,2} \in \mathbb{N} \) \((w = w_1w_2)\) such that \( w_1 \mid u_1, w_2 \mid u_2 \) and clearly \( v_1 \mid u_1, v_2 \mid u_2 \). Lastly, observe that \( 1 = (u_1, u_2) = (v_1, v_2) = (w_1, w_2) = (u_1, v_2) = (u_2, v_1) \) as required. \( \square \)

This lemma resembles Kalmár’s Four-Number Theorem [8] which can be employed to show the Fundamental Theorem of Arithmetic, while bypassing the need for the concepts of the “greatest common divisor” or the “least common multiple”, which are two typical approaches. Similarly, our quest to show a generalization of Euler’s Criterion hinges on this lemma and the theorem below to be shown with it, bypassing this time the lack of a cyclical generator (a “genuine” primitive root) for most composite moduli.

Theorem 2.3. Suppose that \( e \in \mathbb{E}_m \), \( a, b, c \in \mathbb{R}_m^e \) and \( a \in \langle b \rangle_\mathbb{m} \cap \langle c \rangle_\mathbb{m} \). Then there exists some \( d \in \mathbb{R}_m^e \) for which \( a \in \langle d \rangle_\mathbb{m} \) and \( |d|_\mathbb{m} = |b|_\mathbb{m}, |c|_\mathbb{m} \).

Proof.\(^\dagger\) By Proposition 2.5 we have

\[
\langle b \rangle_\mathbb{m} \cap \langle c \rangle_\mathbb{m} = \langle b_{D_m(b,c)} \rangle_\mathbb{m} = \langle c_{D_m(c,b)} \rangle_\mathbb{m}
\]

so there exists some \( K \in \mathbb{N} \) such that

\[
\langle b_{D_m(b,c)} \rangle_\mathbb{m} K \equiv c_{D_m(c,b)} \pmod{m}.
\]

Therefore from

\[
|b_{D_m(b,c)}|_\mathbb{m} = |\langle b \rangle_\mathbb{m} \cap \langle c \rangle_\mathbb{m}| = |c_{D_m(c,b)}|_\mathbb{m} = \frac{|b_{D_m(b,c)}|_\mathbb{m}}{(K, |b_{D_m(b,c)}|_\mathbb{m})}
\]

we get that \((K, |b_{D_m(b,c)}|_\mathbb{m}) = 1\). Furthermore

\[
\frac{|b|_\mathbb{m}}{D_m(b,c)} = |\langle b \rangle_\mathbb{m} \cap \langle c \rangle_\mathbb{m}| = \frac{|c|_\mathbb{m}}{D_m(c,b)} \quad \Rightarrow \quad D_m(b,c) \left( \frac{|b|_\mathbb{m}}{|b|_\mathbb{m}, |c|_\mathbb{m}} \right) = D_m(b,c) \left( \frac{|c|_\mathbb{m}}{|b|_\mathbb{m}, |c|_\mathbb{m}} \right)
\]

\(^\dagger\)The theorem was conjectured by the author, and the presented proof is a modified version of the first draft provided by Prof. Mihály Szalay, which appeared in the author’s master’s thesis [21].
Proof. Letting one of the solutions be denoted as 

\[ x \]

For any 

\[ 3 \]

Solvability

\[ d \]

According to Lemma 2.1, for 

\[ u := |b|_m, \ v := |c|_m \]

the following factorization is possible

\[ |b|_m = u_1u_2, \ |c|_m = v_1v_2, \ w = w_1w_2 \mid (|b|_m, |c|_m) = u_2v_1 \]

\[ w_1 \mid v_1 \mid u_1, \ w_2 \mid u_2 \mid v_2, \ 1 = (u_1, u_2) = (v_1, v_2) = (u_1, u_2) = (u_2, v_1). \]

Then these properties hold

\[ |b^{u_2}|_m = \frac{|b|_m}{(u_2, |b|_m)} = u_1, \ |c^{v_1}|_m = \frac{|c|_m}{(v_1, |c|_m)} = v_2, \ (|b^{u_2}|_m, |c^{v_1}|_m) = 1 \]

\[ D_m(b, c) = \frac{w|b|_m}{(|b|_m, |c|_m)} = \frac{u_1u_2}{u_2v_1} = \frac{v_1}{w_1}, \ D_m(c, b) = \frac{|c|_m}{|b|_m} = \frac{w_1}{u_1}, \ D_m(b, c) = \frac{u_1u_2}{w_1v_1} = \frac{u_2v_1}{w} \in \mathbb{N}. \]

Defining 

\[ d := b^{u_2}|c^{v_1} \mod m \]

we have by Proposition 2.7 the required order

\[ |d|_m = u_1v_2 = \frac{u_1u_2v_1v_2}{u_2v_1} = \frac{|b|_m|c|_m}{(|b|_m, |c|_m)} = [|b|_m, |c|_m]. \]

Lastly, we need an exponent \( E \in \mathbb{N} \) such that \( d^E \equiv a \pmod{m} \). First define

\[ M := \frac{u_1v_2}{u_1u_2} \Rightarrow d^M \equiv (b^{D_m(b, c)}v_2(c^{D_m(c, b)})u_1 \equiv (b^{D_m(b, c)}v_2+Ku_1 \pmod{m}). \]

Now observe that \( (v_2 + Ku_1, |b^{D_m(b, c)}|_m) = 1 \) where \( |b^{D_m(b, c)}|_m = u_2v_1/w \) from above, since \( \frac{u_2v_1}{w} \mid v_1 \mid u_1 \mid Ku_1 \) but \( (v_1/w, v_2) = 1 \) and \( \frac{u_2v_1}{w} \mid u_2 \mid v_2 \) but \( (u_2/w, Ku_1) = 1 \) since as we saw above \( 1 = (K, |b^{D_m(b, c)}|_m) = (K, u_2v_1/w) \). So there must exist an inverse \( N \in \mathbb{N} \) such that \( (v_2 + Ku_1)N \equiv 1 \pmod{|b^{D_m(b, c)}|_m} \). Furthermore, by the assumption of the theorem, there exists an \( I \in \mathbb{N} \) such that \( (b^{D_m(b, c)})^I \equiv a \pmod{m} \).

Multiplying the above exponents \( E := MNI \), we may now conclude that \( a \in (d)_m \) since

\[ d^E = d^MNI \equiv (b^{D_m(b, c)}v_2+Ku_1NI \equiv (b^{D_m(b, c)})^I \equiv a \pmod{m}. \]

\[ \Box \]

3 Solvability

Proposition 3.1. For any \( m \in \mathbb{N}, a \in \mathbb{Z}_m, k \in \mathbb{N} \), if the equation \( x^k \equiv a \pmod{m} \) is solvable for \( x \in \mathbb{Z}_m \) then necessarily

\[ a^{φ(m)/2} \in_m E_m. \]

Proof. Letting one of the solutions be denoted as \( x_0 \) we have

\[ a^{φ(m)/2} \equiv (x_0^k)^{φ(m)/2} \equiv (x_0^{φ(m)})^{k/φ(m)} \in_m E_m. \]

\[ \Box \]
Theorem 3.1. (Generalization of Euler’s Criterion) For any \( m \in \mathbb{N} \), \( a \in \mathbb{R}_m \), \( k \in \mathbb{N} \) the equation \( x^k \equiv a \pmod{m} \) is solvable for \( x \in \mathbb{Z}_m \) if and only if

\[
\frac{\omega_m(a)}{a^k \omega_m(a)} \in_m E_m.
\]

Proof. Let \( b \in \mathbb{R}_m \) be such that \( \exists \text{ind}_b^m a \) and \( |b|_m = \omega_m(a) \). Then by Proposition 2.6

\[
\frac{\omega_m(a)}{a^k \omega_m(a)} \in_m E_m \iff (k, |b|_m) \mid \text{ind}_b^m a.
\]

If \( (k, |b|_m) \mid \text{ind}_b^m a \) holds, then there exists some \( 1 \leq l \leq |b|_m \) for which \( kl \equiv \text{ind}_b^m a \pmod{|b|_m} \). Therefore

\[
b^{kl} \equiv b^{\text{ind}_b^m a} \pmod{m} \Rightarrow (b^l)^k \equiv a \pmod{m}
\]

implying that \( b^l \) is a solution of the equation. Conversely, suppose that \( x_0 \) is a solution, and denote \( e := a^{[a]_m} \pmod{m} \), \( c := x_0^{[e]_m} \pmod{m} \). Then \( c \) must be a regular solution, since

\[
c^k \equiv (x_0)^k e \equiv a \cdot a^{[a]_m} \equiv a \pmod{m}
\]

\[
c \cdot c^{[c]_m} \equiv e \cdot c^{[e]_m} \equiv x_0 e(x_0 e)^{[e]_m} \equiv x_0 e(x_0^k)^{[e]_m} \equiv x_0 e \equiv c \pmod{m}.
\]

We now show that \( |c|_m \mid |b|_m \). Supposing indirectly that \( |c|_m \nmid |b|_m \) we have \( |c|_m < |b|_m \) by the definition of \( \omega_m(a) = |b|_m \). We also know by Theorem 2.3 that there exists some \( d \in \mathbb{R}_m \) such that \( \exists \text{ind}_d^m a \) and \( |d|_m = [|b|_m, |c|_m] \). Then \( |c|_m \mid |b|_m \) implies that \( |d|_m > |b|_m \) which contradicts our original selection of \( b \). So we must have that \( |c|_m \mid |b|_m \) implying

\[
\frac{\omega_m(a)}{a^{(k, |b|_m)}} \equiv a^{(k, |b|_m)} \equiv (c^k)^{[|b|_m]/(|c|_m)} \equiv (c^{[c]_m})^{[|b|_m]/(|c|_m)} \equiv e \pmod{m}.
\]

4 Concluding remarks

A generalization of Euler’s Criterion was presented in Theorem 3.1, while the lack of a cyclical generator (primitive root) in general, was circumvented via Theorem 2.3. The criterion

\[
\frac{\omega_m(a)}{a^k \omega_m(a)} \in_m E_m
\]

in its current form is theoretical. For its practical verification, the calculation of \( \omega_m(a) \) must be made efficient. Likely the examination of the mapping \( m \mapsto \omega_m(a) \) is a worthwhile direction for future investigations, since \( \omega_m(a) = \varphi(m) \) when \( (a, m) = 1 \) and a primitive root is known to exist modulo \( m \).

This paper was inspired by the following solution devised by the author as a freshman, upon accidentally employing Euler’s Theorem when \( (a, m) \neq 1 \) and seeing that \( a^{\varphi(m)} \pmod{m} \) is idempotent (Theorem 2.1). This problem can nevertheless be solved in a more elementary way also.

Problem 4.1. Define a sequence of numbers \( (a_n) \) recursively as

\[
a_0 := 1, \quad a_n := 42 a_{n-1} \quad (n \in \mathbb{N}).
\]

What are the last two digits of \( a_{100} \)?
Solution. Let us first calculate the order and idempotent number for the last few terms, where each modulus is implied by the previous order. We descend in modulus until reaching the term $a_{97}$ congruent to zero – this must necessarily occur since $|a|_m \leq \varphi(m) < m$.

\[
a_{100} = 42^{a_{99}}, \quad |42|_{100} = 20, \quad 42^{20} \equiv 76 \pmod{100}
\]

\[
a_{99} = 42^{a_{98}}, \quad |42|_{20} = 4, \quad 42^4 \equiv 16 \pmod{20}
\]

\[
a_{98} = 42^{a_{97}}, \quad |42|_{4} = 2, \quad 42^2 \equiv 0 \pmod{4}.
\]

We reach zero with $a_{97} \equiv 0 \pmod{2}$ since $2 \mid 42 \mid a_{97}$, implying $a_{97} = 2i$, $i \in \mathbb{N}$. Now working backwards

\[
a_{98} = 42^{2i} \equiv 0 \pmod{4} \implies a_{98} = 4j, \ j \in \mathbb{N}
\]

\[
a_{99} = 42^{4j} \equiv 16 \pmod{20} \implies a_{99} = 20k + 16, \ k \in \mathbb{N}
\]

we finally arrive at the answer

\[
a_{100} = 42^{20k+16} \equiv 76 \cdot 42^{16} \equiv 76 \cdot 56 \equiv 56 \pmod{100}.
\]

Acknowledgements

The author is grateful to Prof. Mihály Szalay for providing the first draft of the proof of Theorem 2.3 and for his careful review of this paper, as well as for that of Prof. András Sárközy. The author is also indebted to the referees for their valuable suggestions for citations.

References


