Analytic Number Theory
Lecture 5

Mariusz Mirek
Rutgers University

Padova, March 26, 2025.

Supported by the NSF grant DMS-2154712,
and the CAREER grant DMS-2236493.

Congruences

Definition

Let $m \in \mathbb{Z}_+$. If $a, b \in \mathbb{Z}$ are such that $a - b$ is divisible by m, then we say that a and b are congruent modulo m, and write

$$a \equiv b \pmod{m}.$$

Fact

Congruence modulo $m \in \mathbb{Z}_+$ is an equivalence relation, which means that for all $a, b, c \in \mathbb{Z}$ we have

(i) Reflexivity: $a \equiv a \pmod{m}$;

(ii) Symmetry: if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$;

(iii) Transitivity: if $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Notation

- The equivalence class of $a \in \mathbb{Z}$ under this relation is called the congruence class of a modulo m, and written $a + m\mathbb{Z}$.
- Thus, $a + m\mathbb{Z}$ is the set of all integers b such that $b \equiv a \pmod{m}$, that is, the set of all integers of the form $a + mx$ for some $x \in \mathbb{Z}$.
- If $(a + m\mathbb{Z}) \cap (b + m\mathbb{Z}) \neq \emptyset$, then $a + m\mathbb{Z} = b + m\mathbb{Z}$. We denote by $\mathbb{Z}/m\mathbb{Z}$ the set of all congruence classes modulo m.
- A congruence class modulo m is also called a residue class modulo m.

Congruences

- By the division algorithm, we can write every $a \in \mathbb{Z}$ in the form $a = mq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r \leq m - 1$. Then $a \equiv r \pmod{m}$, and r is called the least nonnegative residue of a modulo m.
- If $a \equiv 0 \pmod{m}$ and $|a| < m$, then $a = 0$, since 0 is the only integral multiple of m in the open interval $(-m, m)$. This implies that if $a \equiv b \pmod{m}$ and $|a - b| < m$, then $a = b$.
- In particular, if $r_1, r_2 \in \{0, 1, \ldots, m-1\}$ and if $a \equiv r_1 \pmod{m}$ and $a \equiv r_2 \pmod{m}$, then $r_1 = r_2$. Thus, every integer belongs to a unique congruence class of the form $r + m\mathbb{Z}$, where $0 \leq r \leq m - 1$, and so

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}.$$

- The integers $0, 1, \ldots, m - 1$ are pairwise incongruent modulo m. A set of integers $R = \{r_1, \ldots, r_m\}$ is called a complete set of residues modulo m if $r_1, \ldots, r_m$ are pairwise incongruent modulo m and every integer x is congruent modulo m to some integer $r_i \in R$.

Simple properties of the congruances

Proposition (Exercise)

Let $m \in \mathbb{Z}_+$ and $x, y \in \mathbb{Z}$, if $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$, then

- $a_1 x + b_1 y \equiv a_2 x + b_2 y \pmod{m}$ *and* $a_1 b_1 \equiv a_2 b_2 \pmod{m}$.
- $a_1^n \equiv a_2^n \pmod{m}$ *for every* $n \in \mathbb{Z}_+$.
- $f(a_1) \equiv f(a_2) \pmod{m}$ *for every polynomial* f *with integer coefficients.*

Moreover, we have

- $a_1 \equiv a_2 \pmod{m}$ *iff* $a_1 z \equiv a_2 z \pmod{mz}$ *for any integer* $z \neq 0$.
- *If* $a_1 z \equiv a_2 z \pmod{m}$ *and* $d = \gcd(z, m)$, *then* $a_1 \equiv a_2 \pmod{m/d}$.
- *If* $a_1 \equiv a_2 \pmod{m}$ *and* $d \mid a_1$ *and* $d \mid m$, *then* $d \mid a_2$.
- *If* $a_1 \equiv a_2 \pmod{m}$, *then one has* $\gcd(a_1, m) = \gcd(a_2, m)$.
- *If* $a_1 \equiv a_2 \pmod{n}$ *and* $\gcd(m, n) = 1$, *then* $a_1 \equiv a_2 \pmod{mn}$.
- $a_1 \equiv a_2 \pmod{m}$ *iff* $a_1 + m\mathbb{Z} = a_2 + m\mathbb{Z}$.
- *The integers* $a_1, a_2 \in \mathbb{Z}$ *are in the same residue class modulo* m *iff* $a_1 \equiv a_2 \pmod{m}$.
- *The* m *residue classes* $0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}$ *are disjoint and their union is* $\mathbb{Z}$.

Integer ring $\mathbb{Z}/m\mathbb{Z}$ modulo m

Definition

Addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$ are defined by

$$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z},$$
$$(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = ab + m\mathbb{Z}.$$

By the previous proposition, the sum and product of congruence classes modulo m are well-defined.

Theorem

For every integer $m \geq 2$, the set $\mathbb{Z}/m\mathbb{Z} = (\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ of congruence classes modulo m is a commutative ring with additive identity $0 + m\mathbb{Z}$ and multiplicative identity $1 + m\mathbb{Z}$.

- *Depending on how explicit we want to be we will abbreviate $a + m\mathbb{Z}$ to*

$$[a]_m \quad \text{or} \quad a \pmod{m} \quad \text{or} \quad a.$$

- *We will write*

$$\mathbb{Z}/m\mathbb{Z} := \{0, 1, \ldots, m - 1\}.$$

Linear congruences

Theorem

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$ and let $d = \gcd(a, m)$. The congruence

$$ax \equiv b \pmod{m} \qquad (*)$$

has a solution if and only if $d \mid b$.

- *If $d \mid b$, then the congruence (*) has exactly d solutions in integers that are pairwise incongruent modulo m.*
- *In particular, if $(a, m) = 1$, then for every integer b the congruence (*) has a unique solution modulo m.*

Proof.

- If congruence (*) has a solution then there exist $x, y \in \mathbb{Z}$ such that

$$ax - b = my \qquad \Longleftrightarrow \qquad b = ax - my$$

  Thus $d = \gcd(a, m) \mid b$.
- If $d = \gcd(a, m) \mid b$, then by the GCD theorem there are $x_1, x_2 \in \mathbb{Z}$ such that $ax_1 + mx_2 = d$. Multiplying both sides by b/d and taking $x = x_1 b/d$ and $y = -x_2 b/d$ we obtain that $ax - my = b$ as desired.

Proof

- If x, u are solutions of (*), then

$$a(u-x) \equiv au - ax \equiv b - b \equiv 0 \pmod{m}$$

  and so for some $z \in \mathbb{Z}$ we have $a(u-x) = mz$.
- If $d = \gcd(a, m)$, then $\gcd(a/d, m/d) = 1$ and

$$\left(\frac{a}{d}\right)(u-x) = \left(\frac{m}{d}\right)z.$$

- By Euclid's lemma m/d divides $u - x$, and so

$$u = x + \frac{im}{d} \quad \text{for some} \quad i \in \mathbb{Z},$$

  that is,

$$u \equiv x \pmod{m/d}.$$

- Moreover, every integer u of this form is a solution of (*). An integer u congruent to x modulo m/d is congruent to $x + im/d$ modulo m for some integer $i \in \{0, 1, \ldots, d-1\}$, and the d integers $x + im/d$ with $i \in \{0, 1, \ldots, d-1\}$ are pairwise incongruent modulo m.
- Thus, the congruence (*) has exactly d pairwise incongruent solutions. This completes the proof. □

$\mathbb{Z}/p\mathbb{Z}$ is a field modulo a prime number p

Theorem

If $p \in \mathbb{P}$ is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof.

- If $a \in \mathbb{Z}/p\mathbb{Z}$ and $a \neq 0$, then a is an integer not divisible by p.
- Thus $\gcd(a, p) = 1$ and by the previous theorem, there exists $x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{p}$.
- This implies that $ax = 1$ in $\mathbb{Z}/p\mathbb{Z}$, and so a is invertible.
- Thus, $\mathbb{Z}/p\mathbb{Z}$ is a field.

This completes the proof. □

Lemma

Let $p \in \mathbb{P}$ be a prime number. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

Proof.

- If $x \equiv \pm 1 \pmod{p}$, then $x^2 \equiv 1 \pmod{p}$.
- Conversely, if $x^2 \equiv 1 \pmod{p}$, then p divides $x^2 - 1 = (x-1)(x+1)$, and so p must divide $x - 1$ or $x + 1$.

This completes the proof. □

Wilson's theorem

Theorem (Wilson)

If $p \in \mathbb{P}$ is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof.

- This is true for $p = 2$ and $p = 3$, since $1! \equiv -1 \pmod{2}$ and $2! \equiv -1 \pmod{3}$. Let $p \in \mathbb{P}$ be such that $p \geq 5$.
- By the previous theorem, to each integer $a \in \mathbb{Z}/p\mathbb{Z}$ there is a unique integer $a^{-1} \in \mathbb{Z}/p\mathbb{Z}$ such that $aa^{-1} \equiv 1 \pmod{p}$.
- By the previous lemma, $a = a^{-1}$ if and only if $a = 1$ or $a = p-1$.
- Therefore, the $p-3$ numbers in the set $\{2, 3, \ldots, p-2\}$ can be partitioned into $(p-3)/2$ pairs of integers $\{a_i, a_i^{-1}\}$ such that $a_i a_i^{-1} \equiv 1 \pmod{p}$ for $i \in [(p-3)/2]$. Then

$$\begin{aligned}(p-1)! &\equiv 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \\ &\equiv (p-1) \prod_{i=1}^{(p-3)/2} a_i a_i^{-1} \equiv p-1 \equiv -1 \pmod{p}.\end{aligned}$$

This completes the proof. □

Useful result

Theorem

Let $m, d \in \mathbb{Z}_+$ be such that $d \mid m$. If $\gcd(a, d) = 1$ for some $a \in \mathbb{Z}$, then there exists $b \in \mathbb{Z}$ such that $b \equiv a \pmod{d}$ and $\gcd(b, m) = 1$.

Proof.

- Let $m = \prod_{i \in [k]} p_i^{r_i}$ and $d = \prod_{i \in [k]} p_i^{s_i}$, where $r_i \geq 1$ and $0 \leq s_i \leq r_i$ for $i \in [k]$. Let n be the product of the prime powers that divide m but not d. Then $n = \prod_{\substack{i \in [k] \\ s_i = 0}} p_i^{r_i}$ and $\gcd(n, d) = 1$.
- By the existence of solutions for linear congruences there is $x \in \mathbb{Z}$ such that $dx \equiv 1 - a \pmod{n}$. Then $b = a + dx \equiv 1 \pmod{n}$ and $\gcd(b, n) = 1$.
- Also,
$$b \equiv a \pmod{d}.$$
- If $\gcd(b, m) \neq 1$, there exists a prime $p \in \mathbb{P}$ that divides both b and m. However, p does not divide n since $\gcd(b, n) = 1$. It follows that $p \mid d$, and so p divides $b - dx = a$, which is impossible since $(a, d) = 1$. Therefore, $\gcd(b, m) = 1$.

Group of units in $\mathbb{Z}/m\mathbb{Z}$

- A congruence class modulo m is called relatively prime to m if some (and, consequently, every) integer in the class is relatively prime to m.
- An integer $a \in \mathbb{Z}$ is called invertible modulo m or a unit modulo m if there exists $x \in \mathbb{Z}$ such that

$$ax \equiv 1 \pmod{m}.$$

- By the theorem on the existence of solutions for linear congruences $a \in \mathbb{Z}$ is invertible modulo m if and only if a is relatively prime to m.
- Moreover, if a is invertible and $ax \equiv 1 \pmod{m}$, then x is unique modulo m. The congruence class $a + m\mathbb{Z}$ is called invertible and denoted by $(a + m\mathbb{Z})^{-1} = a^{-1} + m\mathbb{Z}$ if there exists a congruence class $x + m\mathbb{Z}$ such that $(a + m\mathbb{Z})(x + m\mathbb{Z}) = 1 + m\mathbb{Z}$.
- The invertible congruence classes are the units in the ring $\mathbb{Z}/m\mathbb{Z}$. We denote the group of units in $\mathbb{Z}/m\mathbb{Z}$ by $(\mathbb{Z}/m\mathbb{Z})^\times$.
- Identifying $\mathbb{Z}/m\mathbb{Z}$ with the set $\{0, 1, \ldots, m-1\}$ we can write

$$(\mathbb{Z}/m\mathbb{Z})^\times := \{a \in \mathbb{Z}/m\mathbb{Z} : \gcd(a, m) = 1\},$$

and it is immediate that $\#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(m)$.

Important result

Theorem

Let $m, n \in \mathbb{Z}_+$ and $(m, n) = 1$. For every $c \in \mathbb{Z}$ there exist unique integers $a, b \in \mathbb{Z}$ such that $0 \leq a \leq n-1$ and $0 \leq b \leq m-1$ and

$$c \equiv ma + nb \pmod{mn}. \qquad (*)$$

Moreover, $(c, mn) = 1$ if and only if $(a, n) = (b, m) = 1$ in equation (*).

Proof.

- If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $ma_1 + nb_1 \equiv ma_2 + nb_2 \pmod{mn}$, then

$$ma_1 \equiv ma_1 + nb_1 \equiv ma_2 + nb_2 \equiv ma_2 \pmod{n}.$$

- Thus $a_1 \equiv a_2 \pmod{n}$, since $(m, n) = 1$, giving $a_1 = a_2$. Similarly, $b_1 = b_2$. Hence the mn integers $ma + nb$ are pairwise incongruent modulo mn. Since there are exactly mn distinct congruence classes modulo mn, the congruence (*) has a unique solution for every $c \in \mathbb{Z}$.
- Let $c \equiv ma + nb \pmod{mn}$. Since $(m, n) = 1$, we have

$$(c, m) = (ma + nb, m) = (nb, m) = (b, m),$$
$$(c, n) = (ma + nb, n) = (ma, n) = (a, n).$$

- So $(c, mn) = 1 \iff (c, m) = (c, n) = 1 \iff (b, m) = (a, n) = 1.$ □

Chinise reminder theorem

Theorem (Chinise reminder theorem)

Let $m_1, \ldots, m_k \in \mathbb{Z}_+$ be pairwise relatively prime. For any $a_1, \ldots, a_k \in \mathbb{Z}$ there is $a \in \mathbb{Z}$ such that $a \equiv a_i \pmod{m_i}$ for all $i \in [k]$. If $b \in \mathbb{Z}$ is also a solution, then $a \equiv b \pmod{m_1 \cdots m_k}$.

Proof.

- Let $M = \prod_{i \in [k]} m_i$ and $M_i = M/m_i$ for $i \in [k]$.
- Since $(m_i, m_j) = 1$ whenever $i \neq j$, we have $(m_i, M_i) = 1$ for $i \in [k]$.
- In particular, $M_i \pmod{m_i}$ is invertible modulo m_i and there is $n_i \in \mathbb{Z}$ such that $n_i M_i \equiv 1 \pmod{m_i}$.
- Set $a = \sum_{i \in [k]} a_i n_i M_i$. Since $m_j \mid M_i$ for $i \neq j$, we obtain that

$$a \equiv \sum_{i=1}^{k} a_i n_i M_i \equiv a_j n_j M_j \equiv a_j \pmod{m_j},$$

  implying that a satisfies the desired congruence equations.
- If there is another solution $b \in \mathbb{Z}$ such that $b \equiv a_i \pmod{m_i}$ for all $i \in [k]$, then $a \equiv b \pmod{m_1 \cdots m_k}$, since $m_1, \ldots, m_k \in \mathbb{Z}_+$ are pairwise coprime. This completes the proof. □

Ring isomorphism

Theorem

Let $m_1, \ldots, m_k \in \mathbb{Z}_+$ be pairwise relatively prime. The map

$$\psi : \mathbb{Z}/m_1 \cdots m_k\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

given by

$$\psi(a \pmod{m_1 \cdots m_k}) = (a \pmod{m_1}, \ldots, a \pmod{m_k})$$

is a ring isomorphism.

Proof.

- One easily checks that ψ is a homomorphism of rings.
- To see that ψ is injective, let $a \in \mathbb{Z}$ so that $\psi(a \pmod{m_1 \cdots m_k}) = 0$.
- In particular, $a \equiv 0 \pmod{m_i}$ for each $i \in [k]$, so that $m_i \mid a$ for all $i \in [k]$. Since $(m_i, m_j) = 1$ for $i \neq j$, we conclude that $m_1 \cdots m_k \mid a$, so that $a \equiv 0 \pmod{m_1 \cdots m_k}$.
- The fact that ψ is surjective is then an immediate consequence of the Chinese remainder theorem.

Applications of the Chinise reminder theorem

Theorem

Let $m = p_1^{r_1} \cdots p_k^{r_k} \in \mathbb{Z}_+$. Let f be a polynomial with integral coefficients. The congruence $f(x) \equiv 0 \pmod{m}$ is solvable if and only if the congruences $f(x) \equiv 0 \pmod{p_i^{r_i}}$ are solvable for all $i \in [k]$.

Proof.

- If $f(x) \equiv 0 \pmod{m}$ has a solution in integers, then there exists $a \in \mathbb{Z}$ such that $m \mid f(a)$. Since $p_i^{r_i} \mid m$, it follows that $p_i^{r_i} \mid f(a)$, and so the congruences $f(x) \equiv 0 \pmod{p_i^{r_i}}$ are solvable for $i \in [k]$.
- Conversely, suppose that the congruences $f(x) \equiv 0 \pmod{p_i^{r_i}}$ are solvable for $i \in [k]$. Then for each $i \in [k]$ there exists $a_i \in \mathbb{Z}$ such that

$$f(a_i) \equiv 0 \pmod{p_i^{r_i}}$$

  Since the prime powers $p_1^{r_1}, \ldots, p_k^{r_k}$ are pairwise relatively prime, the Chinese remainder theorem tells us that there exists $a \in \mathbb{Z}$ such that $a \equiv a_i \pmod{p_i^{r_i}}$ for all $i \in [k]$. Then $f(a) \equiv f(a_i) \equiv 0 \pmod{p_i^{r_i}}$ for all $i \in [k]$. Since $f(a)$ is divisible by each of the prime powers $p_i^{r_i}$, it is also divisible by their product m, and so $f(a) \equiv 0 \pmod{m}$.

This completes the proof. □

Lagrange's theorem

Theorem (Lagrange's theorem)

If $\mathbb{G}$ is a finite group and $\mathbb{H}$ is a subgroup of $\mathbb{G}$, then $|\mathbb{H}|$ divides $|\mathbb{G}|$.

Proof.

- Let $\mathbb{G}$ be a group, written multiplicatively, and let $\emptyset \neq X \subseteq \mathbb{G}$. For every $a \in \mathbb{G}$ we define the set $aX = \{ax : x \in X\}$.
- The map $f : X \to aX$ defined by $f(x) = ax$ is a bijection, and so $|X| = |aX|$ for all $a \in \mathbb{G}$. If $\mathbb{H}$ is a subgroup of $\mathbb{G}$, then $a\mathbb{H}$ is called a coset of $\mathbb{H}$. Let $a\mathbb{H}$ and $b\mathbb{H}$ be cosets of the subgroup $\mathbb{H}$. We will show that the cosets of a subgroup $\mathbb{H}$ are either disjoint or equal.
- Indeed, if $a\mathbb{H} \cap b\mathbb{H} \neq \emptyset$, then there exist $x, y \in \mathbb{H}$ such that $ax = by$. If $z \in a\mathbb{H}$, then $z = ah$ for some $h \in \mathbb{H}$ and $z = ah = axx^{-1}h = byx^{-1}h$, but $yx^{-1}h \in \mathbb{H}$, since $\mathbb{H}$ is a subgroup. Thus $a\mathbb{H} \subseteq b\mathbb{H}$. By symmetry we also have that $b\mathbb{H} \subseteq a\mathbb{H}$ and consequently $a\mathbb{H} = b\mathbb{H}$.
- Since every element of $\mathbb{G}$ belongs to some coset of $\mathbb{H}$ (for example, $a \in a\mathbb{H}$ for all $a \in \mathbb{G}$), it follows that the cosets of $\mathbb{H}$ partition $\mathbb{G}$. We denote the set of cosets by $\mathbb{G}/\mathbb{H}$. If $\mathbb{G}$ is a finite group, then $\mathbb{H}$ and $\mathbb{G}/\mathbb{H}$ are finite, and $|\mathbb{G}| = |\mathbb{H}||\mathbb{G}/\mathbb{H}|$.
- In particular, we see that $|\mathbb{H}|$ divides $|\mathbb{G}|$ as desired. □

Basic group theory

- Let $\mathbb{G}$ be a group, written multiplicatively, and let $\mathbb{H} = \{a^k : k \in \mathbb{Z}\}$ for some $a \in \mathbb{G}$. Then $1 = a^0 \in \mathbb{H} \subseteq \mathbb{G}$. Since $a^k a^l = a^{k+l}$ for all $k, l \in \mathbb{Z}$, it follows that $\mathbb{H}$ is a subgroup of $\mathbb{G}$. This subgroup is called the cyclic subgroup generated by a, and written $\mathbb{H} = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.
- Cyclic subgroups are abelian. The group $\mathbb{G}$ is cyclic if there exists an element $a \in \mathbb{G}$ such that $\mathbb{G} = \langle a \rangle$. In this case, the element a is called a generator of $\mathbb{G}$. For example, the group $(\mathbb{Z}/7\mathbb{Z})^\times = \langle 3 + 7\mathbb{Z} \rangle$.
- If $a^k \neq a^l$ for all integers $k \neq l$, then the cyclic subgroup $\langle a \rangle$ is infinite.
- If there exist integers k and l such that $k < l$ and $a^k = a^l$, then $a^{l-k} = 1$. Let d be the smallest positive integer such that $a^d = 1$. Then the group elements $1, a, a^2, \ldots, a^{d-1}$ are distinct. By the division algorithm, for any $n \in \mathbb{Z}$ there exist $q, r \in \mathbb{Z}$ such that $n = dq + r$ and $0 \leq r \leq d - 1$. Since $a^n = a^{dq+r} = \left(a^d\right)^q a^r = a^r$, it follows that

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{a^r : 0 \leq r \leq d - 1\},$$

  and the cyclic subgroup generated by a has order d.
- Moreover, $a^k = a^l$ if and only if $k \equiv l \pmod{d}$.
- Let $\mathbb{G}$ be a group. We define the order of $a \in \mathbb{G}$ as the cardinality of the cyclic subgroup generated by a and write $\mathrm{ord}_{\mathbb{G}}(a) = |\langle a \rangle|$.
- If $\mathbb{G} = (\mathbb{Z}/m\mathbb{Z})^\times$ we will abbreviate $\mathrm{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times}(a)$ to $\mathrm{ord}_m(a)$.

Euler's theorem and Fermat's little theorem

Theorem

Let $\mathbb{G}$ be a finite group, and $a \in \mathbb{G}$. Then $\operatorname{ord}_{\mathbb{G}}(a) = |\langle a \rangle|$ divides $|\mathbb{G}|$.

Proof.

By Lagrange's theorem $|\langle a \rangle|$ divides $|\mathbb{G}|$, since $\langle a \rangle$ is the subgroup of $\mathbb{G}$. □

Theorem (Euler's theorem)

Let $m \in \mathbb{Z}_+$ and $a \in \mathbb{Z}$ be such that $(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof.

- We apply the previous theorem to $\mathbb{G} = (\mathbb{Z}/m\mathbb{Z})^\times$, then $|\mathbb{G}| = \varphi(m)$.
- By the previous theorem, $d = \operatorname{ord}_{\mathbb{G}}(a) = |\langle a \rangle|$ divides $\varphi(m)$, and so

$$a^{\varphi(m)} \equiv \left(a^d\right)^{\varphi(m)/d} \equiv 1 \pmod{m}.$$

This completes the proof of Euler's theorem. □

Theorem (Fermat's little theorem)

Let $p \in \mathbb{P}$ be a prime number. If the integer $a \in \mathbb{Z}$ is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$, which follows from Euler's theorem applied to $m = p$.

Subgroups of cyclic groups

Theorem

Let $\mathbb{G}$ be a cyclic group of order m, and let $\mathbb{H}$ be a subgroup of $\mathbb{G}$. If a is a generator of $\mathbb{G}$, then there exists a unique divisor d of m such that $\mathbb{H}$ is the cyclic subgroup generated by a^d, and $\mathbb{H}$ has order m/d.

Proof.

- Let $\mathbb{H}$ be a subgroup of $\mathbb{G}$. If $\mathbb{H} = \langle 1 \rangle$, then $\mathbb{H}$ is cyclic and we are done. We can assume that $\mathbb{H} \neq \langle 1 \rangle$ and take $a^d \in \mathbb{H}$ with the smallest $d \in \mathbb{Z}_+$ such that $a^d \neq 1$. Our aim is to prove that $\mathbb{H} = \langle a^d \rangle$ and $d \mid m$.
- Obviously $\langle a^d \rangle \subseteq \mathbb{H}$. For the converse, take $b \in \mathbb{H}$, since $\mathbb{H}$ is a subgroup of $\mathbb{G} = \langle a \rangle$, then $b = a^n$ for some $n \in [m-1]$.
- By the division algorithm we have that $n = dq + r$ for some $q, r \in \mathbb{N}$ such that $0 \leq r < d$.
- Thus $b = a^n = \left(a^d\right)^q a^r$, hence $a^r = a^n a^{-dq} \in \mathbb{H}$, since $a^n \in \mathbb{H}$ and $a^{-dq} \in \mathbb{H}$ and $\mathbb{H}$ is a subgroup.
- If $0 < r < d$, then $a^r \in \mathbb{H}$, which contradicts the minimality of d. Thus we must have $r = 0$ and consequently $b = a^{dq} \in \langle a^d \rangle$, giving $\mathbb{H} \subseteq \langle a^d \rangle$. This shows that $\mathbb{H} = \langle a^d \rangle$ and by the Lagrange theorem $d \mid m$.

This completes the proof of the theorem. □

Subgroups of cyclic groups

Theorem

Let $\mathbb{G}$ be a cyclic group of order m, and let a be a generator of $\mathbb{G}$. For every $k \in \mathbb{Z}$, the cyclic subgroup generated by a^k has order m/d, where $d = (m,k)$, and $\langle a^k \rangle = \langle a^d \rangle$. In particular, $\mathbb{G}$ has exactly $\varphi(m)$ generators.

Proof.

- Since $d = (k,m)$, there exist integers x and y such that $d = kx + my$.
- Then
$$a^d = a^{kx+my} = \left(a^k\right)^x \left(a^m\right)^y = \left(a^k\right)^x$$
and so $a^d \in \langle a^k \rangle$ and $\langle a^d \rangle \subseteq \langle a^k \rangle$.
- Since $d \mid k$, there exists $z \in \mathbb{Z}$ such that $k = dz$. Then
$$a^k = \left(a^d\right)^z$$
and so $a^k \in \langle a^d \rangle$ and $\langle a^k \rangle \subseteq \langle a^d \rangle$.
- Hence, $\langle a^k \rangle = \langle a^d \rangle$ and a^k has order m/d.
- In particular, a^k generates $\mathbb{G}$ if and only if $d = 1$ if and only if $(m,k) = 1$, and so $\mathbb{G}$ has exactly $\varphi(m)$ generators.

This completes the proof of the theorem. □

Primitive roots

Definition of order (revised)

- Let $m \in \mathbb{Z}_+$ be such that $m > 1$, and $a \in \mathbb{Z}$ such that $(a, m) = 1$.
- The order of a modulo m, denoted by $\mathrm{ord}_m(a)$, is the smallest positive integer d such that $a^d \equiv 1 \pmod{m}$. We know that $\mathrm{ord}_m(a) \mid \varphi(m)$.
- The order of a modulo m is also called the exponent of a modulo m, and is sometimes denoted by $\exp_m(a) = \mathrm{ord}_m(a)$.

Definition of primitive roots

- The integer a is called a primitive root modulo m if a has order $\varphi(m)$.
- In this case, the $\varphi(m)$ integers $1, a, a^2, \ldots, a^{\varphi(m)-1}$ are relatively prime to m and are pairwise incongruent modulo m.
- In other words, they form a reduced residue system modulo m.

Examples

- If $m = 7$, then $\mathrm{ord}_7(2) = 3$, thus 2 is not a primitive root modulo 7, but $\mathrm{ord}_7(3) = 6$ thus 3 is a primitive root modulo 7.
- No number in $(\mathbb{Z}/8\mathbb{Z})^\times$ is a primitive root modulo 8.

Examples

- For example, if $m = 7$ and $a = 2$, then $\mathrm{ord}_7(2) = 3$, since
$$\begin{aligned} 2^0 &\equiv 1 \pmod 7, \\ 2^1 &\equiv 2 \pmod 7, \\ 2^2 &\equiv 4 \pmod 7, \\ 2^3 &\equiv 1 \pmod 7. \end{aligned}$$
- If $m = 7$ and $a = 3$, then $\mathrm{ord}_7(3) = 6$, since
$$\begin{aligned} 3^0 &\equiv 1 \pmod 7, \\ 3^1 &\equiv 3 \pmod 7, \\ 3^2 &\equiv 2 \pmod 7, \\ 3^3 &\equiv 6 \pmod 7, \\ 3^4 &\equiv 4 \pmod 7, \\ 3^5 &\equiv 5 \pmod 7, \\ 3^6 &\equiv 1 \pmod 7. \end{aligned}$$
- For $m = 8$ we also have
$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8.$$

Division algorithm for polynomials

Theorem (Exercise!)

Let $\mathbb{F}$ be a field. If $f(x)$ and $d(x)$ are polynomials in $\mathbb{F}[x]$ and if $d(x) \neq 0$, then there exist unique polynomials $q(x)$ and $r(x)$ such that

$$f(x) = d(x)q(x) + r(x),$$

and

- *either $r(x) = 0$;*
- *or the degree of $r(x)$ is strictly smaller than the degree of $d(x)$.*

Theorem (Exercise!)

Let $f(x) \in \mathbb{F}[x]$ be such that $f(x) \neq 0$, and let $N_0(f)$ denote the number of distinct zeros of $f(x)$ in $\mathbb{F}$. Then $N_0(f)$ does not exceed the degree of $f(x)$, that is,

$$N_0(f) \leq \deg(f).$$

Subgroups of the multiplicative group of a field

Theorem

Every finite subgroup of the multiplicative group of a field is cyclic.

Proof.

- Let $\mathbb{F}$ be a field and let $\mathbb{F}^\times := \mathbb{F} \setminus \{0\}$ be its multiplicative group.
- Let $\mathbb{G}$ be a finite subgroup of $\mathbb{F}^\times$ and assume that $|\mathbb{G}| = m$.
- If $a \in \mathbb{G}$, then $\mathrm{ord}_{\mathbb{G}}(a)$ is a divisor of m. For every divisor d of m, let

$$\psi(d) := |\{b \in \mathbb{G} : \mathrm{ord}_{\mathbb{G}}(b) = d\}|.$$

- If $\psi(d) \neq 0$, then there exists an element $a \in \mathbb{G}$ of order d, and every element of the cyclic subgroup $\langle a \rangle$ generated by a satisfies $a^d = 1$.
- By the previous theorem, the polynomial

$$f(x) = x^d - 1 \in \mathbb{F}[x],$$

  has at most d zeros. Hence, every zero of $f(x)$ must belong to the cyclic subgroup $\langle a \rangle$, otherwise we would have more than d zeros for $f(x)$, which is impossible.
- In particular, every element of $\mathbb{G}$ of order d must belong to $\langle a \rangle$.

For any prime $p \in \mathbb{P}$ primitive roots $\pmod p$ exist

- We know that a cyclic group of order d has exactly $\varphi(d)$ generators. Therefore, $\psi(d) = 0$ or $\psi(d) = \varphi(d)$ for every divisor d of m.
- Since every element of $\mathbb{G}$ has order d for some divisor d of m, we have

$$\sum_{d|m} \psi(d) = m.$$

- Also we know that

$$\sum_{d|m} \varphi(d) = m,$$

  and so $\psi(d) = \varphi(d)$ for every divisor d of m, since $\psi(d) \leq \varphi(d)$.
- In particular, $\psi(m) = \varphi(m) \geq 1$, and so $\mathbb{G}$ is a cyclic group of order m.

This completes the proof of the theorem. □

Theorem

For every prime $p \in \mathbb{P}$, the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$ is cyclic. This group has $\varphi(p-1)$ generators. Equivalently, for every prime $p \in \mathbb{P}$, there exist $\varphi(p-1)$ pairwise incongruent primitive roots modulo p.

Proof.

This follows from the previous theorem, since $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$. □

Examples

- By the structure theorem of subgroups in cyclic groups, if g is a primitive root modulo p, then g^k is a primitive root iff $(k, p-1) = 1$.
- For example, for $p = 13$ there are $\varphi(12) = 4$ integers k such that $0 \leq k \leq 11$ and $(k, 12) = 1$, namely, $k = 1, 5, 7, 11$, and so the four pairwise incongruent primitive roots modulo 13 are

$$\begin{aligned} 2^1 &\equiv 2 \pmod{13}, \\ 2^5 &\equiv 6 \pmod{13}, \\ 2^7 &\equiv 11 \pmod{13}, \\ 2^{11} &\equiv 7 \pmod{13}. \end{aligned}$$

- The following table lists the primitive roots for the first six primes.

p	$\varphi(p-1)$	primitive roots
2	1	1
3	1	2
5	2	2,3
7	2	3,5
11	4	2, 6, 7, 8
13	4	2, 6, 7, 11

Primitive roots of composite moduli for $m = 2$ or $m = 4$

Theorem

There exists a primitive root modulo $m = 2^k$ if and only if $m = 2$ or $m = 4$.

Proof.

- We note that 1 is a primitive root modulo 2, and 3 is a primitive root modulo 4. For $k \geq 3$ we prove that there is no primitive root modulo 2^k.
- Since $\varphi\left(2^k\right) = 2^{k-1}$, it suffices to show by induction on $k \geq 3$, that

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \quad \text{for any odd} \quad a \in \mathbb{Z}_+ \qquad (*)$$

- If $k = 3$, then $m = 8$ and $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$, thus the base case follows. Let $k \geq 3$, and suppose that (*) is true.
- Then $a^{2^{k-2}} - 1$ is divisible by 2^k. Since $a \in \mathbb{Z}_+$ is odd, it follows that $a^{2^{k-2}} + 1$ is even. Therefore,

$$a^{2^{k-1}} - 1 = \left(a^{2^{k-2}} - 1\right)\left(a^{2^{k-2}} + 1\right)$$

  is divisible by 2^{k+1}, and so $a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$.

This completes the induction and the proof of theorem. □

Primitive roots to composite moduli

Theorem

Let $m \in \mathbb{Z}_+$ be not a power of 2. If m has a primitive root, then $m = p^k$ or $2p^k$, where $p \in \mathbb{P}$ is an odd prime and $k \in \mathbb{Z}_+$.

Proof.

- Let $a, m \in \mathbb{Z}$ be such that $(a, m) = 1$ and $m \geq 3$. Suppose that

$$m = m_1 m_2, \quad \text{where} \quad (m_1, m_2) = 1 \quad \text{and} \quad m_1 \geq 3, m_2 \geq 3.$$

- Then $(a, m_1) = (a, m_2) = 1$. Since $\varphi(m)$ is even for $m \geq 3$, then

$$n = \frac{\varphi(m)}{2} = \frac{\varphi(m_1)\,\varphi(m_2)}{2} \in \mathbb{Z}_+.$$

- Consequently, by Euler's theorem, we have

$$a^{\varphi(m_1)} \equiv 1 \pmod{m_1}$$

and so

$$a^n = \left(a^{\varphi(m_1)}\right)^{\varphi(m_2)/2} \equiv 1 \pmod{m_1}.$$

Proof

- Similarly,
$$a^n = \left(a^{\varphi(m_2)}\right)^{\varphi(m_1)/2} \equiv 1 \pmod{m_2}.$$
- Since $(m_1, m_2) = 1$ and $m = m_1 m_2$, we have
$$a^n \equiv 1 \pmod{m}$$
and so the order of a modulo m is strictly smaller than $\varphi(m)$.
- Consequently, if we can factor $m = m_1 m_2$, then there does not exist a primitive root modulo m.
- In particular, if m is divisible by two distinct odd primes, then m does not have a primitive root.
- Similarly, if $m = 2^l p^k$, where $l \geq 2$, then m does not have a primitive root.
- Therefore, the only moduli $m \neq 2^l$ for which primitive roots can exist are of the form $m = p^k$ or $m = 2p^k$ for some odd prime p.

This completes the proof of the theorem. □

Exponential increase in the order

Theorem

Let $p \in \mathbb{P}$ be an odd prime, and let $a \neq \pm 1$ be an integer not divisible by p. Let $d = \operatorname{ord}_p(a)$ and let k_0 be the largest integer so that $a^d \equiv 1 \pmod{p^{k_0}}$. Then

$$\operatorname{ord}_{p^k}(a) = \begin{cases} d & \text{if } 1 \leq k \leq k_0, \\ dp^{k-k_0} & \text{if } k \geq k_0. \end{cases}$$

Proof.

- There exists $u_0 \in \mathbb{Z}$ such that $a^d = 1 + p^{k_0} u_0$ and $(u_0, p) = 1$.
- Let $k \in [k_0]$, and let $v = \operatorname{ord}_{p^k}(a)$. If $a^v \equiv 1 \pmod{p^k}$, then $a^v \equiv 1 \pmod{p}$, and so $d \mid v$. Since $k \in [k_0]$, we have $a^d \equiv 1 \pmod{p^k}$, and so $v \mid d$. It follows that $v = d$ and $\operatorname{ord}_{p^k}(a) = d$ for $k \in [k_0]$ as desired.
- Let $j \in \mathbb{N}$. We shall show that there exists $u_j \in \mathbb{Z}$ such that

$$a^{dp^j} = 1 + p^{j+k_0} u_j \quad \text{and} \quad (u_j, p) = 1 \qquad (*)$$

- The proof is by induction on $j \in \mathbb{N}$. The assertion is true for $j = 0$ by our choice of k_0. Suppose we have (*) for some integer $j \geq 0$. We will show that (*) remains true with $j + 1$ in place of j.

Proof

- By the binomial theorem, there exists $v_j \in \mathbb{N}$ such that

$$a^{dp^{j+1}} = \left(1 + p^{j+k_0} u_j\right)^p = 1 + p^{j+1+k_0} u_j + \sum_{i=2}^{p} \binom{p}{i} p^{i(j+k_0)} u_j^i$$
$$= 1 + p^{j+1+k_0} u_j + p^{j+2+k_0} v_j = 1 + p^{j+1+k_0} \left(u_j + p v_j\right).$$

- Setting $u_{j+1} = u_j + p v_j$ we have $(u_{j+1}, p) = 1$, giving (*) for all $j \in \mathbb{N}$.
- By induction on $k \geq k_0$ we prove the second part of the theorem. The base case for $k = k_0$ follows from the first part. Let $k \geq k_0 + 1$ and $j = k - k_0 \geq 1$ and suppose that $\operatorname{ord}_{p^{k-1}}(a) = dp^{j-1}$.
- Let $v_k = \operatorname{ord}_{p^k}(a)$ and note that

$$a^{v_k} \equiv 1 \pmod{p^k} \quad \Longrightarrow \quad a^{v_k} \equiv 1 \pmod{p^{k-1}}$$

and so dp^{j-1} divides v_k.

- Since

$$a^{dp^{j-1}} = 1 + p^{k-1} u_{j-1} \not\equiv 1 \pmod{p^k}$$

it follows that dp^{j-1} is a proper divisor of v_k. On the other hand,

$$a^{dp^j} = 1 + p^k u_j \equiv 1 \pmod{p^k}$$

and so v_k divides dp^j. It follows that the order of a modulo p^k is exactly $v_k = dp^j = dp^{k-k_0}$. This completes the proof. □

Primitive roots of composite moduli for $m = p^k$ or $m = 2p^k$

Theorem

Let $p \in \mathbb{P}$ be an odd prime.

- *If g is a primitive root modulo p, then either g or $g + p$ is a primitive root modulo p^k for all $k \geq 2$.*
- *If g is a primitive root modulo p^k and $h \in \{g, g + p^k\}$ is odd, then h is a primitive root modulo $2p^k$.*

Proof.

- Let g be a primitive root modulo p. Then $\operatorname{ord}_p(g) = p - 1$.
- Let $k_0 \in \mathbb{Z}_+$ be the largest integer such that p^{k_0} divides $g^{p-1} - 1$.
- By the previous theorem, if $k_0 = 1$, then the order of g modulo p^k is $(p-1)p^{k-1} = \varphi\left(p^k\right)$, and g is a primitive root modulo p^k for all $k \geq 1$.
- If $k_0 \geq 2$, then $g^{p-1} = 1 + p^2 v$ for some $v \in \mathbb{Z}$. By the binomial theorem, we have

$$\begin{aligned}(g+p)^{p-1} &= \sum_{i=0}^{p-1} \binom{p-1}{i} g^{p-1-i} p^i \equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2} \\ &\equiv 1 + p^2 v + g^{p-2}p^2 - g^{p-2}p \pmod{p^2} \\ &\equiv 1 - g^{p-2}p \pmod{p^2} \not\equiv 1 \pmod{p^2}.\end{aligned}$$

Proof

- This proves that $g + p$ is a primitive root modulo p such that

$$(g+p)^{p-1} = 1 + pu_0 \quad \text{and} \quad (u_0, p) = 1.$$

- Therefore, $g + p$ is a primitive root modulo p^k for all $k \in \mathbb{Z}_+$.
- Next we prove that primitive roots exist for all moduli of the form $2p^k$.
- If g is a primitive root modulo p^k, then $g + p^k$ is also a primitive root modulo p^k by the binomial theorem. Since p^k is odd, it follows that one of the two integers g and $g + p^k$ is odd, and the other is even.
- Let $h \in \left\{g, g + p^k\right\}$ be odd. Since $\left(g + p^k, p^k\right) = \left(g, p^k\right) = 1$, it follows that $\left(h, 2p^k\right) = 1$. The order of h modulo $2p^k$ is not less than $\varphi\left(p^k\right)$, which is the order of h modulo p^k, and not greater than $\varphi\left(2p^k\right)$.
- However, since p is an odd prime, we have

$$\varphi\left(2p^k\right) = \varphi\left(p^k\right)$$

and so h has order $\varphi\left(2p^k\right)$ modulo $2p^k$, that is, h is a primitive root modulo $2p^k$. This completes the proof. □

Primitive roots using the group theoretic language

Gathering what has been proven about primitive roots can be subsumed in the following result.

Theorem

If $q \in \{1, 2, 4, p^k, 2p^k\}$, where $p \in \mathbb{P}$ is an odd prime number and $k \in \mathbb{Z}_+$, then the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic. In other words, there exists a primitive root modulo q, that is, $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that $\operatorname{ord}_q(a) = \varphi(q)$.

Remark

- We know that $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is cyclic if and only if $k \in [2]$. For $k = 2$ we can see that all elements have order 2.
- However, there do exist odd integers of order 2^{k-2} in $(\mathbb{Z}/2^k\mathbb{Z})^\times$.

Proposition

For every $k \in \mathbb{Z}_+$, one has that $5^{2^k} \equiv 1 + 3 \cdot 2^{k+2} \pmod{2^{k+4}}$.

Proof.

- The proof is by induction on $k \in \mathbb{Z}_+$.
- For $k = 1$ we have $5^{2^1} = 25 \equiv 1 + 3 \cdot 2^3 \pmod{2^5}$.
- For $k = 2$ we have $5^{2^2} = 625 = 1 + 48 + 576 \equiv 1 + 3 \cdot 2^4 \pmod{2^6}$.

$(\mathbb{Z}/2^k\mathbb{Z})^\times \equiv \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$

- If the theorem holds for $k \in \mathbb{Z}_+$, then there exists $u \in \mathbb{Z}$ such that

$$5^{2^k} = 1 + 3 \cdot 2^{k+2} + 2^{k+4}u = 1 + 2^{k+2}(3 + 4u).$$

- Since $2k + 4 \geq k + 5$, we have

$$5^{2^{k+1}} = \left(5^{2^k}\right)^2 = \left(1 + 2^{k+2}(3 + 4u)\right)^2 \equiv 1 + 2^{k+3}(3 + 4u) \pmod{2^{2k+4}}$$
$$\equiv 1 + 3 \cdot 2^{k+3} \pmod{2^{k+5}} \qquad \text{as desired.} \qquad \square$$

Theorem

If $k \geq 3$, then 5 has order 2^{k-2} modulo 2^k. One can say even more.

- *If $a \equiv 1 \pmod 4$, then there exists a unique integer $i \in \{0, 1, \ldots, 2^{k-2} - 1\}$ such that*

$$a \equiv 5^i \pmod{2^k}.$$

- *If $a \equiv 3 \pmod 4$, then there exists a unique integer $i \in \{0, 1, \ldots, 2^{k-2} - 1\}$ such that*

$$a \equiv -5^i \pmod{2^k}.$$

Proof

- In the case $k = 3$, we observe that 5 has order 2 modulo 8, and

$$\begin{aligned} 1 &\equiv 5^0 \pmod 8, \\ 3 &\equiv -5^1 \pmod 8, \\ 5 &\equiv 5^1 \pmod 8, \\ 7 &\equiv -5^0 \pmod 8. \end{aligned}$$

- Let $k \geq 4$. By the previous proposition, we have

$$\begin{aligned} 5^{2^{k-2}} &\equiv 1 + 3 \cdot 2^k \pmod{2^{k+2}} \\ &\equiv 1 \pmod{2^k}, \end{aligned}$$

and

$$\begin{aligned} 5^{2^{k-3}} &\equiv 1 + 3 \cdot 2^{k-1} \pmod{2^{k+1}} \\ &\equiv 1 + 3 \cdot 2^{k-1} \pmod{2^k} \\ &\not\equiv 1 \pmod{2^k}. \end{aligned}$$

Proof

- Therefore, 5 has order exactly 2^{k-2} modulo 2^k, and so the integers 5^i are pairwise incongruent modulo 2^k for $i \in \{0, 1, \ldots, 2^{k-2} - 1\}$.
- Since $5^i \equiv 1 \pmod 4$ for all $i \in \mathbb{Z}_+$, and since exactly half, that is, 2^{k-2}, of the 2^{k-1} odd numbers between 0 and 2^k are congruent to 1 modulo 4, it follows that the congruence

$$5^i \equiv a \pmod{2^k}$$

  is solvable for every $a \equiv 1 \pmod 4$.
- If $a \equiv 3 \pmod 4$, then $-a \equiv 1 \pmod 4$ and so the congruence

$$-a \equiv 5^i \pmod{2^k} \quad \Longleftrightarrow \quad a \equiv -5^i \pmod{2^k}$$

  is solvable. This completes the proof. □

Remark

- If $k \geq 3$ then the previous theorem can be restated as follows

$$(\mathbb{Z}/2^k\mathbb{Z})^\times = \langle -1 \rangle \times \langle 5 \rangle \equiv \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z},$$

  where $\langle a \rangle$ denotes the cyclic subgroup of $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$ generated by a for $a = -1$ and $a = 5$.