Mersenne primes and class field theory

Jansen, B.J.H.

Chapter 10

Mersenne primes in arithmetic progressions

We know that there exist at least 47 Mersenne primes, and it is a conjecture that there are infinitely many. Dirichlet's theorem says for each $a, b \in \mathbb{Z}_{>0}$ with a and b relatively prime there are infinitely many primes p such that $p \equiv a \bmod b$ (see [11, Chapter 8, §7, Corollary 7.3]). Since there are no Mersenne primes that are 1 modulo 4, Dirichlet's theorem is not true if we replace primes by Mersenne primes. However for the exponents of Mersenne primes one might wonder if for each $a, b \in \mathbb{Z}_{>0}$ with a and b relatively prime there are infinitely many primes p with $p \equiv a \bmod b$ such that $2^p - 1$ is prime.

In this chapter we will speculate on Mersenne primes in arithmetic progression and reformulate these speculations in terms of Artin symbols (see Theorem 10.6 below). With this reformulation we prepare ourselves for the next chapter, where we will speculate on Frobenius symbols of Mersenne primes and generalise Theorem 10.6 (see Theorem 11.7 below).

Exponents in arithmetic progressions

Let $\mathcal{E}_{2012}$ be the set of currently known exponents p such that 2^p-1 is a Mersenne prime, i.e.

$$\begin{aligned}\mathcal{E}_{2012} \;=\; \{&2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281,\\ &3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243,\\ &110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221,\\ &3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457,\\ &32582657, 37156667, 42643801, 43112609\}.\end{aligned}$$

In the table below we see the frequency of the last digit of $p \in \mathcal{E}_{2012}\backslash\{2, 5\}$.

i	1	3	7	9
$\#\{p \in \mathcal{E}_{2012} : p \equiv\ i \bmod 10\}$	11	11	14	9

The following table shows the frequency of $p \in \mathcal{E}_{2012}\backslash\{3\}$ in residue classes modulo 3.

i	1	2
$\#\{p \in \mathcal{E}_{2012} : p \equiv i \bmod 3\}$	23	23

The last table shows the frequency of $p \in \mathcal{E}_{2012}\backslash\{3,5\}$ in residue classes modulo 15.

i	1	2	4	7	8	11	13	14
$\#\{p \in \mathcal{E}_{2012} : p \equiv i \bmod 15\}$	6	7	4	8	5	5	5	5

The distribution of the exponents over the different residue classes modulo 10, 3 and 15, make it reasonable to expect that for every $a, b \in \mathbb{Z}_{>0}$ with a and b relatively prime there are infinitely many exponents $p \equiv a \bmod b$ such that $2^p - 1$ is prime. In this chapter we will reformulate this expectation in two ways using Artin symbols.

Artin symbols of Mersenne primes

Let L be a finite abelian extension of $\mathbb{Q}$.

Definition 10.1. *We define* Mer_L *to be the set of all* $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ *such that there are infinitely many Mersenne primes* M *with* $\sigma = ((M), L/\mathbb{Q})$.

Examples. From Definition 10.1 it is clear that Mer_L is empty if and only if there are only finitely many Mersenne primes. We have $\mathrm{Mer}_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}/\mathbb{Q})$ if there are infinitely Mersenne primes. Let $n \in \mathbb{Z}_{>0}$ and let ζ_{2^n} be a primitive 2^n-th root of unity. If there are infinitely many Mersenne primes then the set $\mathrm{Mer}_{\mathbb{Q}(\zeta_{2^n})}$ contains precisely the automorphism induced by complex conjugation.

Next we define the set $W_L \subset \mathrm{Gal}(L/\mathbb{Q})$, which one should think of as the smallest subset of $\mathrm{Gal}(L/\mathbb{Q})$ that we know that contains Mer_L. Let n_L be the conductor of $L/\mathbb{Q}$ and let $n_{L,\mathrm{odd}} \in \mathbb{Z}_{>0}$ be the largest odd integer that divides n_L. Denote by d_L the multiplicative order of $(2 \bmod n_{L,\mathrm{odd}})$ in the group $(\mathbb{Z}/n_{L,\mathrm{odd}}\mathbb{Z})^*$. In order to make the Artin symbols in the next definition well-defined, we note that from Lemma 10.9 we get: if $q \in \mathbb{Z}_{>0}$, $q \geq \mathrm{ord}_2(n_L)$ and $\gcd(q, d_L) = 1$ then $\gcd(2^q - 1, n_L) = 1$.

Definition 10.2. *We define* W_L *to be the set of all Artin symbols* $((2^q-1), L/\mathbb{Q})$ *with* $q \in \mathbb{Z}_{>0}$, $q \geq \mathrm{ord}_2(n_L)$ *and* $\gcd(q, d_L) = 1$.

Proposition 10.3. *We have* $\mathrm{Mer}_L \subset W_L$.

We prove Proposition 10.3 in the last section of this chapter.

Examples. We have $W_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}/\mathbb{Q})$. For $n \in \mathbb{Z}_{>0}$ let ζ_n be a primitive n-th root of unity. Then for $k \in \mathbb{Z}_{>0}$ the set $W_{\mathbb{Q}(\zeta_{2^k})}$ contains only the automorphism induced by complex conjugation.

Suppose $n = 2^{10}-1$. Define $L = \mathbb{Q}(\zeta_n+\zeta_n^{-1})$. Then one easily sees $n_L = (n)$, $d_L = 10$ and $W_L = \{\sigma_1, \sigma_7, \sigma_{127}, \sigma_{511}\}$, where $\sigma_i : \zeta_n + \zeta_n^{-1} \mapsto \zeta_n^i + \zeta_n^{-i}$. The

table below is similar to the first table of this chapter, but from an Artin symbol point of view.

i	1	3	7	9
$\#\{p \in \mathcal{E}_{2012} : (2^p-1, L/\mathbb{Q}) = \sigma_{2^i-1}\}$	11	11	14	9

There are $\varphi(2^{10}-1) = 600$ different Artin symbols of non-ramified primes in $L/\mathbb{Q}$, but only four different Artin symbols come from Mersenne primes.

The following theorem, which we prove in the last section of this chapter, suggests that one may reasonably conjecture $\mathrm{Mer}_L = W_L$.

Theorem 10.4. *The following two statements are equivalent:*

(i) *For every $a, b \in \mathbb{Z}_{>0}$ relatively prime there are infinitely many integers $p \equiv a \bmod b$ such that $2^p - 1$ is a Mersenne prime.*

(ii) *For each finite abelian extension L of $\mathbb{Q}$ we have $\mathrm{Mer}_L = W_L$.*

Profinite groups

In this section we define the notion of a profinite group (and set and ring) and we will give some examples which will be applied in the next section.

A topological group G is a set together with a group structure and a topological structure such that the multiplication map $G \times G \to G$, defined by $(g_1, g_2) \mapsto g_1 g_2$, and inverse map $G \to G$, defined by $g \mapsto g^{-1}$, are continuous. A topological ring R is a set together with a ring structure and a topological structure such that the multiplication map $R \times R \to R$, defined by $(r_1, r_2) \mapsto r_1 r_2$, and addition map $R \times R \to R$, defined by $(r_1, r_2) \mapsto r_1 + r_2$, are continuous. Every finite group (or set or ring) is a topological group (or set or ring) if we give the finite group (or set or ring) the discrete topology.

Next we need the notion of a directed partially ordered set. This is a set I with a partial order $\geq$ such that for every $i, j \in I$ there is an element $k \in I$ such that $k \geq i$ and $k \geq j$.

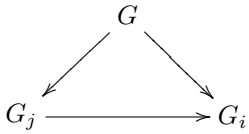
Now we can define a projective system. Let I be a partially ordered set. A projective system of groups (or sets or rings) is a collection of groups (or sets or rings) G_i for $i \in I$ with a group (or set or ring) homomorphism $f_i^j : G_j \to G_i$ for all $i, j \in I$ with $j \geq i$ such that $f_i^j \circ f_j^k = f_i^k$ for $k \geq j \geq i$ and f_i^i is the identity on G_i.

A projective system has a projective limit, namely

$$G = \varprojlim_i G_i = \{(\alpha_i)_{i \in I} \in \prod_{i \in I} G_i : \text{for all } i, j \in I \text{ with } j \geq i \text{ we have } f_i^j(\alpha_j) = \alpha_i\}.$$

We put a topology on G: we give G_i the discrete topology, $\prod_{i \in I} G_i$ the product topology and $\varprojlim_i G_i$ the subspace topology. We call G a profinite group (or set or ring) if G is a topological group (or set or ring) which is isomorphic (as a

topological group (or set or ring)) to a projective limit of finite groups (or sets or rings). For each $i \in I$ we have a projection map $G \to G_i$ such that for all $j \geq i$ the diagram



commutes.

Next we describe two examples of projective limits that we use below. Let $\mathbb{N}$ be the set of positive integers, which we partially order by divisibility. The collection of rings $\mathbb{Z}/n\mathbb{Z}$ (with $n \in \mathbb{N}$) and the maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $(a \bmod n) \mapsto (a \bmod m)$ for $n, m \in \mathbb{N}$ with $m \mid n$, is a projective system. We denote the projective limit $\varprojlim_{n\in\mathbb{N}}(\mathbb{Z}/n\mathbb{Z})$ by $\hat{\mathbb{Z}}$. Let $\mathbb{Z}_2$ be the projective limit of the rings $(\mathbb{Z}/2^i\mathbb{Z})$, where i runs over the positive integers. Let $\mathbb{Z}_{\text{odd}}$ be the projective limit of the rings $(\mathbb{Z}/n_{\text{odd}}\mathbb{Z})$, where n_{odd} runs over the odd positive integers. Write $n \in \mathbb{Z}_{>0}$ as $2^i \cdot n_{\text{odd}}$, where $i \in \mathbb{Z}_{\geq 0}$ and n_{odd} is an odd positive integer. By the Chinese remainder theorem the map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/n_{\text{odd}}\mathbb{Z}$ defined by $(a \bmod n) \mapsto (a \bmod 2^i, a \bmod n_{\text{odd}})$ is a ring isomorphism. This isomorphism induces an isomorphism between the profinite rings $\hat{\mathbb{Z}}$ and $\mathbb{Z}_2 \times \mathbb{Z}_{\text{odd}}$. We denote the group of units of $\hat{\mathbb{Z}}$ by $\hat{\mathbb{Z}}^*$. Note that $\hat{\mathbb{Z}}^*$ is a profinite group.

We have an action of $\hat{\mathbb{Z}}^*$ on the set G as follows. For $i \in I$ and $x \in \hat{\mathbb{Z}}^*$ let $e_i(x) \in \mathbb{Z}$ be such that for $n = n(i)$, the order of G_i, we have $x_n = (e_i(x) \bmod n)$. For $g \in G$ and $x \in \hat{\mathbb{Z}}^*$ let $g^x = (g_i^{e_i(x)})$. This action $\hat{\mathbb{Z}}^* \times G \to G$ is continuous (see [19, Chapter 1, §5, Proposition 1.5.3]).

Let I be the set of finite abelian extensions of $\mathbb{Q}$ inside a chosen algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. The collection of groups $\mathrm{Gal}(L/\mathbb{Q})$ (with $L \in I$) and the restriction maps $\mathrm{Gal}(L'/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ for $L \subset L'$ is a projective system. We denote the projective limit $\varprojlim_{L\in I} \mathrm{Gal}(L/\mathbb{Q})$ by $G_{\mathbb{Q}}^{\text{ab}}$.

The group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. Now from the Kronecker-Weber Theorem it follows that $G_{\mathbb{Q}}^{\text{ab}} = \varprojlim_{n\in\mathbb{Z}_{>0}} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \hat{\mathbb{Z}}^*$.

A profinite reformulation

In this section we will reformulate Theorem 10.4(ii) in terms of projective limits.

Proposition 10.5. *Let L, L' be finite abelian extensions of $\mathbb{Q}$. Suppose $L \subset L'$. Then the restriction map $\mathrm{Gal}(L'/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ induces surjective maps $\mathrm{Mer}_{L'} \to \mathrm{Mer}_L$ and $W_{L'} \to W_L$.*

Proposition 10.5 will be proved in the next section. Now we can define Mer_{ab} and W_{ab} to be the projective limit of all Mer_L and W_L respectively, where $L \subset \overline{\mathbb{Q}}$ runs over all finite abelian extensions of $\mathbb{Q}$. The inclusions $\mathrm{Mer}_L \subset$

$W_L \subset \mathrm{Gal}(L/\mathbb{Q})$ yield the inclusions $\mathrm{Mer}_{\mathrm{ab}} \subset W_{\mathrm{ab}} \subset G_{\mathbb{Q}}^{\mathrm{ab}}$. Now we can extend Theorem 10.4.

Theorem 10.6. *The following three statements are equivalent:*

(i) *For every $a, b \in \mathbb{Z}_{>0}$ relatively prime there are infinitely many integers $p \equiv a \bmod b$ such that $2^p - 1$ is a Mersenne prime.*

(ii) *For each finite abelian extension L of $\mathbb{Q}$ we have $\mathrm{Mer}_L = W_L$.*

(iii) *We have $\mathrm{Mer}_{\mathrm{ab}} = W_{\mathrm{ab}}$.*

A proof of Theorem 10.6 can be found in the next section.

Next we describe W_{ab} by means of class field theory. Let the notation be as above. That is, L is an abelian extension of $\mathbb{Q}$ with conductor n_L, and d_L is the multiplicative order of $(2 \bmod n_{L,\mathrm{odd}})$ in the group $(\mathbb{Z}/n_{L,\mathrm{odd}}\mathbb{Z})^*$. Let $x \in \mathbb{Z}_{>0}$ such that $\gcd(x, d_L) = 1$. Then Lemma 10.9 implies $\gcd(2^x - 1, n_L) = 1$. Hence we have a well-defined map

$$\tau_{d_L} : (\mathbb{Z}/d_L\mathbb{Z})^* \to \mathrm{Gal}(L/\mathbb{Q})$$

defined by

$$u \bmod d_L \mapsto ((2^x - 1), L/\mathbb{Q}),$$

where $x \in \mathbb{Z}_{>0}$ is such that $x \equiv u \bmod d_L$ and $x \geq \mathrm{ord}_2(n_L)$. Let $m_L \in \mathbb{Z}_{>0}$ be the smallest divisor of d_L such that τ_{d_L} factors via the natural map $r : (\mathbb{Z}/d_L\mathbb{Z})^* \to (\mathbb{Z}/m_L\mathbb{Z})^*$. Define $\tau_L : (\mathbb{Z}/m_L\mathbb{Z})^* \to \mathrm{Gal}(L/\mathbb{Q})$ by $\tau_{d_L} = \tau_L \circ r$. Note that the image of τ_L is W_L.

Proposition 10.7. *The maps τ_L induce a map τ_{ab} from $\hat{\mathbb{Z}}^*$ to $G_{\mathbb{Q}}^{\mathrm{ab}}$. Moreover τ_{ab} is continuous.*

We prove Proposition 10.7 in the next section.

Now we describe the image of τ_{ab} more explicitly. We recall that we can identify $\hat{\mathbb{Z}}^*$ with $\mathbb{Z}_2^* \times \mathbb{Z}_{\mathrm{odd}}^*$ and $G_{\mathbb{Q}}^{\mathrm{ab}}$ with $\hat{\mathbb{Z}}^*$. For $g \in \mathbb{Z}_{\mathrm{odd}}^*$ and $x \in \hat{\mathbb{Z}}^*$ recall the definition of g^x (see previous section).

Theorem 10.8. *We have $\tau_{\mathrm{ab}}(\hat{\mathbb{Z}}^*) = W_{\mathrm{ab}}$. By identifying $G_{\mathbb{Q}}^{\mathrm{ab}}$ with $\mathbb{Z}_2^* \times \mathbb{Z}_{\mathrm{odd}}^*$, the set W_{ab} can be described as*

$$\{-1\} \times \{2^x - 1 : x \in \hat{\mathbb{Z}}^*\} \subset \mathbb{Z}_2^* \times \mathbb{Z}_{\mathrm{odd}}^*.$$

Furthermore the map τ_{ab} is injective.

We prove Theorem 10.8 in the next section.

Justifying the reformulations

In this section we prove Proposition 10.3, Theorem 10.4, Proposition 10.5, Theorem 10.6, Proposition 10.7, and Theorem 10.8.

Proof of Proposition 10.3. Suppose $\sigma \in \mathrm{Mer}_L$. Recall that n_L is the conductor of $L/\mathbb{Q}$. Recall the definition of $n_{L,\mathrm{odd}}$ and d_L (see just below Definition 10.1). By assumption there are infinitely many Mersenne primes $M_p = 2^p - 1$ with $\sigma = ((M_p), L/\mathbb{Q})$, so we can choose one M_p such that $p \geq \mathrm{ord}_2(n_L)$, $\gcd(p, d_L) = 1$. The definition of W_L implies $((M_p), L/\mathbb{Q}) = \sigma \in W_L$. Therefore Mer_L is a subset of W_L. □

Proof of Proposition 10.5. Let $\sigma \in \mathrm{Mer}_L$. Then there exist infinitely many Mersenne primes M with $\sigma = ((M), L/\mathbb{Q})$. Since there are only finitely many $\tau \in \mathrm{Gal}(L'/\mathbb{Q})$ with $\tau|_L = \sigma$, the consistency property (see Proposition 5.4) implies that there exists $\tau \in \mathrm{Gal}(L'/\mathbb{Q})$ with $\tau|_L = \sigma$ such that there are infinitely many Mersenne primes M with $\tau = ((M), L'/\mathbb{Q})$. Hence the restriction map $\mathrm{Mer}_{L'} \to \mathrm{Mer}_L$ is surjective.

Since $L \subset L'$, the Kronecker-Weber Theorem implies $n_L \mid n_{L'}$. Therefore we have $n_{L,\mathrm{odd}} \mid n_{L',\mathrm{odd}}$, so $d_L \mid d_{L'}$. Now the consistency property implies that the map $W_{L'} \to W_L$ is well defined and surjective. □

Proof of Theorem 10.6. (ii)⇒(iii). Direct from the definition of $\mathrm{Mer}_{\mathrm{ab}}$ and W_{ab} as projective limits.

(iii)⇒(ii). For each finite abelian extension L and L' of $\mathbb{Q}$ we have a surjective restriction map $f_L : G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathrm{Gal}(L/\mathbb{Q})$. Proposition 10.5 implies that the restriction maps $W_L \to W_{L'}$ and $\mathrm{Mer}_L \to \mathrm{Mer}_{L'}$ are also surjective. By assumption $W_{\mathrm{ab}} = \mathrm{Mer}_{\mathrm{ab}}$, so

$$W_L = f_L(W_{\mathrm{ab}}) = f_L(\mathrm{Mer}_{\mathrm{ab}}) = \mathrm{Mer}_L.$$

The first and the third equality follow from [19, Chapter 1, §1, Proposition 1.1.6].

(ii)⇒(i). Fix $b \in \mathbb{Z}_{>0}$. Let L be the cyclotomic extension obtained by adjoining a root of unity if order $2^b - 1$ to $\mathbb{Q}$. Then L has conductor $(2^b - 1)$. The multiplicative order of $(2 \bmod 2^b - 1)$ is b. By assumption $\mathrm{Mer}_L = W_L$, so for each $a \in \mathbb{Z}_{>0}$ with $\gcd(a, b) = 1$ the element $((2^a - 1), L/\mathbb{Q})$ is contained in Mer_L. By definition of Mer_L this means: there are infinitely many Mersenne primes $M_q = 2^q - 1$ with $((M_q), L/\mathbb{Q}) = ((2^a - 1), L/\mathbb{Q})$. Note that $((M_q), L/\mathbb{Q}) = ((2^a - 1), L/\mathbb{Q})$ implies $M_q \equiv 2^a - 1 \bmod 2^b - 1$. The congruence $M_q \equiv 2^a - 1 \bmod 2^b - 1$ implies $q \equiv a \bmod b$. Hence for each $a \in \mathbb{Z}_{>0}$ with $\gcd(a, b) = 1$ there are infinitely many exponents $q \in \mathbb{Z}_{>0}$ with $q \equiv a \bmod b$ such that $2^q - 1$ is prime.

(i)⇒(ii). Let L be a finite abelian extension of $\mathbb{Q}$. Let $n \in \mathbb{Z}_{>0}$ be the conductor of $L/\mathbb{Q}$. By Kronecker-Weber the cyclotomic field $L' = \mathbb{Q}(\zeta_n)$ contains L. We recall the definition of $d_{L'}$. Write n as $2^i \cdot n_{\mathrm{odd}}$ where $i \in \mathbb{Z}_{\geq 0}$ and $n_{\mathrm{odd}} \in \mathbb{Z}_{>0}$ odd. Then $d_{L'}$ is the order of $(2 \bmod n_{\mathrm{odd}})$ in the group

$(\mathbb{Z}/n_{\text{odd}}\mathbb{Z})^*$. By assumption (see (i)): for each $a \in \mathbb{Z}_{>0}$ with $\gcd(a, d_{L'}) = 1$ there are infinitely many exponents $p \in \mathbb{Z}_{>0}$ with $p \equiv a \bmod d_{L'}$ such that $2^p - 1$ is prime. Hence for each $a \in \mathbb{Z}_{>0}$ with $\gcd(a, d_{L'}) = 1$ there exists $p \in \mathbb{Z}_{>0}$ with $p \equiv a \bmod d_{L'}$ and $p \geq \text{ord}_2(n)$ such that $((2^p - 1), L'/\mathbb{Q})$ is an element of $\text{Mer}_{L'}$, so $\text{Mer}_{L'} = W_{L'}$. Using the surjective maps $W_{L'} \to W_L$ and $\text{Mer}_{L'} \to \text{Mer}_L$ (see Proposition 10.5) we conclude that $\text{Mer}_L = W_L$. □

Proof of Theorem 10.4. This follows directly from Theorem 10.6. □

Lemma 10.9. *Let $n, d, x \in \mathbb{Z}_{>0}$ and let $\mathfrak{f}$ be an ideal of the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\sqrt[n]{2})$. If we have $\sqrt[n]{2}^d \equiv 1 \bmod \mathfrak{f}$ and $\gcd(d, x) = 1$, then we have $(\sqrt[n]{2}^x - 1) + \mathfrak{f} = \mathcal{O}$.*

Proof. Let $\mathfrak{d} = (\sqrt[n]{2}^x - 1) + \mathfrak{f}$ be an ideal of $\mathcal{O}$. Then we have $\sqrt[n]{2}^d \equiv 1 \bmod \mathfrak{d}$ and $\sqrt[n]{2}^x \equiv 1 \bmod \mathfrak{d}$. Since $\gcd(d, x) = 1$, there exist $a, b \in \mathbb{Z}$ such that $ad + bx = 1$. Therefore we get $1 \equiv (\sqrt[n]{2}^d)^a \cdot (\sqrt[n]{2}^x)^b \equiv \sqrt[n]{2}^{ad+bx} \equiv \sqrt[n]{2} \bmod \mathfrak{d}$. Hence $\sqrt[n]{2} - 1 \in \mathfrak{d}$. Note that $\sqrt[n]{2} - 1$ is a root of $f = (y + 1)^n - 2$. Since f has constant term -1, we see that $\sqrt[n]{2} - 1$ is a unit of $\mathcal{O}$. Hence we have $\mathfrak{d} = \mathcal{O}$. □

Let $A \subset \mathbb{Z}$ and let $n \in \mathbb{Z}_{>0}$. Note that we have the natural map $A \to \mathbb{Z}/n\mathbb{Z}$. Let X be a set. We call a map $f : A \to X$ periodic modulo n if there exists a map $\bar{f} : \mathbb{Z}/n\mathbb{Z} \to X$ such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & X \\ & \searrow \quad \nearrow_{\bar{f}} & \\ & \mathbb{Z}/n\mathbb{Z} & \end{array}$$

commutes.

Lemma 10.10. *Let $g, n, m \in \mathbb{Z}_{>0}$. Let $A = \{x \in \mathbb{Z} : \gcd(x, nm) = 1 \text{ and } x \geq g\}$. Suppose $f : A \to X$ is periodic modulo n and modulo m. Then f is periodic modulo $\gcd(n, m)$.*

Proof. Let $c = \gcd(n, m)$. Let $x, y \in A$ such that $x \equiv y \bmod c$. Since $x \equiv y \bmod c$, there exists $z \in \mathbb{Z}$ such that $z \equiv x \bmod n$ and $z \equiv y \bmod m$. Indeed, solve the congruence modulo every highest prime power dividing $\text{lcm}(n, m)$ and apply the Chinese remainder Theorem. Clearly we have $\gcd(z, nm) = 1$. Let $h \in \mathbb{Z}_{>0}$ be such that $z' = z + nm \cdot h \geq g$. Then z' is an element of A and we have $z' \equiv x \bmod n$ and $z' \equiv y \bmod m$. Therefore we get $f(x) = f(z') = f(y)$. Hence f is periodic modulo c. □

Lemma 10.11. *Let L and L' be finite abelian extensions of $\mathbb{Q}$ such that $L \subset L'$. Then m_L divides $m_{L'}$ and the diagram*

$$\begin{array}{ccccc} \hat{\mathbb{Z}}^* & \longrightarrow & (\mathbb{Z}/m_{L'}\mathbb{Z})^* & \xrightarrow{\tau_{L'}} & \text{Gal}(L'/\mathbb{Q}) \\ \downarrow \text{id} & & \downarrow & & \downarrow \text{res} \\ \hat{\mathbb{Z}}^* & \longrightarrow & (\mathbb{Z}/m_L\mathbb{Z})^* & \xrightarrow{\tau_L} & \text{Gal}(L/\mathbb{Q}) \end{array}$$

commutes.

Proof. Set $n = m_L \cdot m_{L'}$ and $g = \mathrm{ord}_2(n_L)$. Let $A = \{x \in \mathbb{Z} : \gcd(x, n) = 1 \text{ and } x \geq g\}$. Let $r : A \to (\mathbb{Z}/m_L\mathbb{Z})^*$ and $r' : A \to (\mathbb{Z}/m'_L\mathbb{Z})^*$ be the natural maps. Note that $\tau_L \circ r$ is periodic modulo m_L. By the consistency property we have $\tau_L \circ r = \mathrm{res} \circ \tau_{L'} \circ r'$, so $\tau_L \circ r$ is periodic modulo m'_L. Hence by Lemma 10.10 the map $\tau_L \circ r$ is periodic modulo $\gcd(m_L, m_{L'})$. The definition of m_L (see just above Proposition 10.7) implies $m_L = \gcd(m_L, m_{L'})$. Hence m_L divides m'_L. Therefore we have a natural the map $(\mathbb{Z}/m'_L\mathbb{Z})^* \to (\mathbb{Z}/m_L\mathbb{Z})^*$. Hence by definition of $\hat{\mathbb{Z}}^*$ the left square of the diagram in Lemma 10.11 commutes (see the diagram in the section on profinite groups). The consistency property implies that the right square of the diagram in Lemma 10.11 commutes. □

Proof of Proposition 10.7. Lemma 10.11 implies that the maps τ_L induce a map $\hat{\mathbb{Z}}^*$ to $G_{\mathbb{Q}}^{\mathrm{ab}}$. Let r_L be the restriction map $G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathrm{Gal}(L/\mathbb{Q})$. The map $r_L \circ \tau_{\mathrm{ab}}$ factors via the continuous maps $\hat{\mathbb{Z}}^* \to (\mathbb{Z}/m_L\mathbb{Z})^*$ and τ_L. Therefore $r_L \circ \tau_{\mathrm{ab}}$ is continuous. Hence we can conclude that τ_{ab} is continuous (see [19, Chapter 1, §1, Proposition 1.1.6(d)]). □

Proof of Theorem 10.8. The condition $x \geq \mathrm{ord}_2(n_L)$ in the definition of the maps τ_L implies that the projection of W_{ab} (seen as a subset of $\mathbb{Z}_2^* \times \mathbb{Z}_{\mathrm{odd}}^*$) on the first coordinate equals $\{-1\}$. Now the definition of g^x implies $W_{\mathrm{ab}} = \{-1\} \times \{2^x - 1 : x \in \hat{\mathbb{Z}}^*\}$.

Let $(a_m)_m, (b_m)_m \in \hat{\mathbb{Z}}^*$. Suppose $(a_m)_m \neq (b_m)_m$. Then there is an integer $m \in \mathbb{N}$ such that $a_m \neq b_m$. Let $L = \mathbb{Q}(\zeta_{2^m-1})$, so $m_L = m$. Then $((2^{a_m} - 1), L/\mathbb{Q}) \neq ((2^{b_m} - 1), L/\mathbb{Q})$, which yields $\tau_{\mathrm{ab}}(a) \neq \tau_{\mathrm{ab}}(b)$. Hence the map τ_{ab} is injective. □