Circular sets of prime numbers and $p$-extensions of the rationals

by Alexander Schmidt

Abstract: Let $p$ be an odd prime number and let $S$ be a finite set of prime numbers congruent to 1 modulo $p$. We prove that the group $G_S(\mathbb{Q})(p)$ has cohomological dimension 2 if the linking diagram attached to $S$ and $p$ satisfies a certain technical condition, and we show that $G_S(\mathbb{Q})(p)$ is a duality group in these cases. Furthermore, we investigate the decomposition behaviour of primes in the extension $\mathbb{Q}_S(p)/\mathbb{Q}$ and we relate the cohomology of $G_S(\mathbb{Q})(p)$ to the étale cohomology of the scheme $\text{Spec}(\mathbb{Z}) - S$. Finally, we calculate the dualizing module.

1 Introduction

Let $k$ be a number field, $p$ a prime number and $S$ a finite set of places of $k$. The pro-$p$-group $G_S(k)(p) = G(k_S(p)/k)$, i.e. the Galois group of the maximal $p$-extension of $k$ which is unramified outside $S$, contains valuable information on the arithmetic of the number field $k$. If all places dividing $p$ are in $S$, then we have some structural knowledge on $G_S(k)(p)$, in particular, it is of cohomological dimension less or equal to 2 (if $p = 2$ one has to require that $S$ contains no real place, [Sc3]), and it is often a so-called duality group, see [NSW], X, §7. Furthermore, the cohomology of $G_S(k)(p)$ coincides with the étale cohomology of the arithmetic curve $\text{Spec}(\mathcal{O}_k) - S$ in this case.

In the opposite case, when $S$ contains no prime dividing $p$, only little is known. By a famous theorem of Golod and Šafarevič, $G_S(k)(p)$ may be infinite. A conjecture due to Fontaine and Mazur [FM] asserts that $G_S(k)(p)$ has no infinite quotient which is an analytic pro-$p$-group. So far, nothing was known on the cohomological dimension of $G_S(k)(p)$ and on the relation between its cohomology and the étale cohomology of the scheme $\text{Spec}(\mathcal{O}_k) - S$.

Recently, J. Labute [La] showed that pro-$p$-groups with a certain kind of relation structure have cohomological dimension 2. By a result of H. Koch [Ko], $G_S(\mathbb{Q})(p)$ has such a relation structure if the set of prime numbers $S$ satisfies a certain technical condition. In this way, Labute obtained first examples of pairs $(p, S)$ with $p \notin S$ and $\text{cd} G_S(\mathbb{Q})(p) = 2$, e.g. $p = 3$, $S = \{7, 19, 61, 163\}$.

The objective of this paper is to use arithmetic methods in order to extend Labute’s result. First of all, we weaken the condition on $S$ which implies cohomological dimension 2 (and strict cohomological dimension 3!) and we show that $G_S(\mathbb{Q})(p)$ is a duality group in these cases. Furthermore, we investigate the decomposition behaviour of primes in the extension $\mathbb{Q}_S(p)/\mathbb{Q}$ and we relate the cohomology of $G_S(\mathbb{Q})(p)$ to the étale cohomology of the scheme $\text{Spec}(\mathbb{Z}) - S$. Finally, we calculate the dualizing module.
2 Statement of results

Let \( p \) be an odd prime number, \( S \) a finite set of prime numbers not containing \( p \) and \( G_S(p) = G_S(\mathbb{Q})(p) \) the Galois group of the maximal \( p \)-extension \( \mathbb{Q}_S(p) \) of \( \mathbb{Q} \) which is unramified outside \( S \). Besides \( p \), only prime numbers congruent to 1 modulo \( p \) can ramify in a \( p \)-extension of \( \mathbb{Q} \), and we assume that all primes in \( S \) have this property. Then \( G_S(p) \) is a pro-\( p \)-group with \( n \) generators and \( n \) relations, where \( n = \#S \) (see lemma 3.1).

Inspired by some analogies between knots and prime numbers (cf. [Mo]), J. Labute [La] introduced the notion of the linking diagram \( \Gamma(S)(p) \) attached to \( p \) and \( S \) and showed that \( cd G_S(p) = 2 \) if \( \Gamma(S)(p) \) is a ‘non-singular circuit’.

Roughly speaking, this means that there is an ordering \( S = \{q_1, q_2, \ldots, q_n\} \) such that \( q_1q_2\cdots q_nq_1 \) is a circuit in \( \Gamma(S)(p) \) (plus two technical conditions, see section 7 for the definition).

We generalize Labute’s result by showing

**Theorem 2.1.** Let \( p \) be an odd prime number and let \( S \) be a finite set of prime numbers congruent to 1 modulo \( p \). Assume there exists a subset \( T \subset S \) such that the following conditions are satisfied.

(i) \( \Gamma(T)(p) \) is a non-singular circuit.

(ii) For each \( q \in S \setminus T \) there exists a directed path in \( \Gamma(S)(p) \) starting in \( q \) and ending with a prime in \( T \).

Then \( cd G_S(p) = 2 \).

**Remarks.**

1. Condition (ii) of Theorem 2.1 can be weakened, see section 7.

2. Given \( p \), one can construct examples of sets \( S \) of arbitrary cardinality \( \#S \geq 4 \) with \( cd G_S(p) = 2 \).

**Example.** For \( p = 3 \) and \( S = \{7, 13, 19, 61, 163\} \), the linking diagram has the following shape

![Linking Diagram](image)

The linking diagram associated to the subset \( T = \{7, 19, 61, 163\} \) is a non-singular circuit, and we obtain \( cd G_S(3) = 2 \) in this case.

The proof of Theorem 2.1 uses arithmetic properties of \( G_S(p) \) in order to enlarge the set of prime numbers \( S \) without changing the cohomological dimension of \( G_S(p) \). In particular, we show
Theorem 2.2. Let $p$ be an odd prime number and let $S$ be a finite set of prime numbers congruent to 1 modulo $p$. Assume that $G_S(p) \neq 1$ and $cd G_S(p) \leq 2$. Then the following holds.

(i) $cd G_S(p) = 2$ and $scd G_S(p) = 3$.

(ii) $G_S(p)$ is a pro-$p$ duality group (of dimension 2).

(iii) For all $\ell \in S$, $Q_S(p)$ realizes the maximal $p$-extension of $Q_\ell$, i.e. (after choosing a prime above $\ell$ in $\overline{Q}$), the image of the natural inclusion $Q_S(p) \hookrightarrow Q_\ell(p)$ is dense.

(iv) The scheme $X = \text{Spec} \mathbb{Z} - S$ is a $K(\pi,1)$ for $p$ and the étale topology, i.e. for any $p$-primary $G_S(p)$-module $M$, considered as a locally constant étale sheaf on $X$, the natural homomorphism

$$H^i(G_S(p), M) \rightarrow H^i_{et}(X, M)$$

is an isomorphism for all $i$.

Remarks. 1. If $S$ consists of a single prime number, then $G_S(p)$ is finite, hence $\# S \geq 2$ is necessary for the theorem. At the moment, we do not know examples of cardinality 2 or 3.

2. The property asserted in Theorem 2.2 (iv) implies that the natural morphism of pro-spaces

$$X_{et}(p) \longrightarrow K(G_S(p), 1)$$

from the pro-$p$-completion of the étale homotopy type $X_{et}$ of $X$ (see [AM]) to the $K(\pi,1)$-pro-space attached to the pro-$p$-group $G_S(p)$ is a weak equivalence. Since $G_S(p)$ is the fundamental group of $X_{et}(p)$, this justifies the notion ‘$K(\pi,1)$ for $p$ and the étale topology’. If $S$ contains the prime number $p$, this property always holds (cf. [Sc2]).

We can enlarge the set of prime numbers $S$ by the following

Theorem 2.3. Let $p$ be an odd prime number and let $S$ be a finite set of prime numbers congruent to 1 modulo $p$. Assume that $cd G_S(p) = 2$. Let $\ell \notin S$ be another prime number congruent to 1 modulo $p$ which does not split completely in the extension $Q_S(p)/\mathbb{Q}$. Then $cd G_{S \cup \{\ell\}}(p) = 2$.

3 Comparison with étale cohomology

In this section we show that cohomological dimension 2 implies the $K(\pi,1)$-property.

Lemma 3.1. Let $p$ be an odd prime number and let $S$ be a finite set of prime numbers congruent to 1 modulo $p$. Then

$$\dim_{\mathbb{Z}} H^i(G_S(p), \mathbb{Z}/p\mathbb{Z}) = \begin{cases} 1 & \text{if } i = 0 \\ \# S & \text{if } i = 1 \\ \# S & \text{if } i = 2. \end{cases}$$
Proof. The statement for $H^0$ is obvious. [NSW], Theorem 8.7.11 implies the statement on $H^1$ and yields the inequality

$$\dim_{\mathbb{F}_p} H^2(G_S(p), \mathbb{Z}/p\mathbb{Z}) \leq \#S.$$ 

The abelian pro-$p$-group $G_S(p)^{ab}$ has $\#S$ generators. There is only one $\mathbb{Z}_p$-extension of $\mathbb{Q}$, namely the cyclotomic $\mathbb{Z}_p$-extension, which is ramified at $p$. Since $p$ is not in $S$, $G_S(p)^{ab}$ is finite, which implies that $G_S(p)$ must have at least as many relations as generators. By [NSW], Corollary 3.9.5, the relation rank of $G_S(p)$ is $\dim_{\mathbb{F}_p} H^2(G_S(p), \mathbb{Z}/p\mathbb{Z})$, which yields the remaining inequality for $H^2$.

**Proposition 3.2.** Let $p$ be an odd prime number and let $S$ be a finite set of prime numbers congruent to 1 modulo $p$. If $cd G_S(p) \leq 2$, then the scheme $X = \text{Spec}(\mathbb{Z}) - S$ is a $K(\pi, 1)$ for $p$ and the étale topology, i.e. for any discrete $p$-primary $G_S(p)$-module $M$, considered as locally constant étale sheaf on $X$, the natural homomorphism

$$H^i(G_S(p), M) \to H^i_{\text{et}}(X, M)$$

is an isomorphism for all $i$.

Proof. Let $L/k$ be a finite subextension of $k$ in $k_S(p)$. We denote the normalization of $X$ in $L$ by $X_L$. Then $H^i_{\text{et}}(X_L, \mathbb{Z}/p\mathbb{Z}) = 0$ for $i > 3$ ([Ma], §3, Proposition C). Since flat and étale cohomology coincide for finite étale group schemes ([Mi], III, Theorem 3.9), the flat duality theorem of Artin-Mazur ([Mi2], III Theorem 3.1) implies

$$H^1_{\text{et}}(X_L, \mathbb{Z}/p\mathbb{Z}) = H^3_{\text{et}}(X_L, \mathbb{Z}/p\mathbb{Z}) \cong H^0_{\text{fl}}(X_L, \mathbb{Z}/p\mathbb{Z}),$$

since a $p$-extension of $\mathbb{Q}$ cannot contain a primitive $p$-th root of unity. Let $\tilde{X}$ be the universal (pro-)-$p$-covering of $X$. We consider the Hochschild-Serre spectral sequence

$$E^{pq}_2 = H^p(G_S(p), H^q_{\text{et}}(\tilde{X}, \mathbb{Z}/p\mathbb{Z})) \Rightarrow H^{p+q}_{\text{et}}(X, \mathbb{Z}/p\mathbb{Z}).$$

Étale cohomology commutes with inverse limits of schemes if the transition maps are affine (see [AGV], VII, 5.8). Therefore we have $H^i_{\text{et}}(\tilde{X}, \mathbb{Z}/p\mathbb{Z}) = 0$ for $i \geq 3$, and for $i = 1$ by definition. Hence $E^{0q}_2 = 0$ unless $i = 0, 2$. Using the assumption $cd G_S(p) \leq 2$, the spectral sequence implies isomorphisms $H^{i}(G_S(p), \mathbb{Z}/p\mathbb{Z}) \cong H^{i}_{\text{et}}(\tilde{X}, \mathbb{Z}/p\mathbb{Z})$ for $i = 0, 1$ and a short exact sequence

$$0 \to H^{2}(G_S(p), \mathbb{Z}/p\mathbb{Z}) \to H^{2}_{\text{et}}(X, \mathbb{Z}/p\mathbb{Z}) \to H^{2}_{\text{et}}(\tilde{X}, \mathbb{Z}/p\mathbb{Z})G_{S}(p) \to 0.$$

Let $\bar{X} = \text{Spec}(\mathbb{Z})$. By the flat duality theorem of Artin-Mazur, we have an isomorphism $H^{2}_{\text{et}}(\bar{X}, \mathbb{Z}/p\mathbb{Z}) \cong H^{1}_{\text{fl}}(\bar{X}, \mathbb{Z}/p\mathbb{Z})$. The flat Kummer sequence $0 \to \mu_p \to \mathbb{G}_m \to \mathbb{G}_m \to 0$, together with $H^{1}_{\text{fl}}(\bar{X}, \mathbb{G}_m)/p = 0 = H^{1}(\bar{X}, \mathbb{G}_m)$ implies $H^{2}_{\text{et}}(\bar{X}, \mathbb{Z}/p\mathbb{Z}) = 0$. Furthermore, $H^{2}_{\text{et}}(\bar{X}, \mathbb{Z}/p\mathbb{Z}) \cong H^{0}_{\text{fl}}(\bar{X}, \mathbb{Z}/p\mathbb{Z}) = 0$. Considering the étale excision sequence for the pair $(\bar{X}, X)$, we obtain an isomorphism

$$H^{2}_{\text{et}}(X, \mathbb{Z}/p\mathbb{Z}) \cong \bigoplus_{i \in S} H^{2}_{\text{et}}(\text{Spec}(\mathbb{Z}), \mathbb{Z}/p\mathbb{Z}).$$
The local duality theorem ([Mi2], II, Theorem 1.8) implies

$$H^1_c(\text{Spec}(\mathbb{Z}_\ell), \mathbb{Z}/p\mathbb{Z}) \cong \text{Hom}_{\text{Spec}(\mathbb{Z}_\ell)}(\mathbb{Z}/p\mathbb{Z}, G_m)^\vee.$$ 

All primes $\ell \in S$ are congruent to 1 modulo $p$ by assumption, hence $\mathbb{Z}_\ell$ contains a primitive $p$-th root of unity for $\ell \in S$, and we obtain $\dim_{\mathbb{F}_p} H^2_c(X, \mathbb{Z}/p\mathbb{Z}) = |S|$. Now Lemma 3.1 implies that $\phi$ is an isomorphism. We therefore obtain

$$H^2_c(X, \mathbb{Z}/p\mathbb{Z})^{G_S(p)} = 0.$$ 

Since $G_S(p)$ is a pro-$p$-group, this implies ([NSW], Corollary 1.7.4) that

$$H^2_c(\hat{X}, \mathbb{Z}/p\mathbb{Z}) = 0.$$ 

We conclude that the Hochschild-Serre spectral sequence degenerates to a series of isomorphisms

$$H^i(G_S(p), \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\sim} H^i_c(X, \mathbb{Z}/p\mathbb{Z}), \quad i \geq 0.$$ 

If $M$ is a finite $p$-primary $G_S(p)$-module, it has a composition series with graded pieces isomorphic to $\mathbb{Z}/p\mathbb{Z}$ with trivial $G_S(p)$-action ([NSW], Corollary 1.7.4), and the statement of the proposition for $M$ follows from that for $\mathbb{Z}/p\mathbb{Z}$ and from the five-lemma. An arbitrary discrete $p$-primary $G_S(p)$-module is the filtered inductive limit of finite $p$-primary $G_S(p)$-modules, and the statement of the proposition follows since group cohomology ([NSW], Proposition 1.5.1) and étale cohomology ([AGV], VII, 3.3) commute with filtered inductive limits. 

4 Proof of Theorem 2.2

In this section we prove Theorem 2.2. Let $p$ be an odd prime number and let $S$ be a finite set of prime numbers congruent to 1 modulo $p$. Assume that $G_S(p) \neq 1$ and $cd G_S(p) \leq 2$.

Let $U \subset G_S(p)$ be an open subgroup. The abelianization $U^{ab}$ of $U$ is a finitely generated abelian pro-$p$-group. If $U^{ab}$ were infinite, it would have a quotient isomorphic to $\mathbb{Z}_p^\infty$, which corresponds to a $\mathbb{Z}_p$-extension $K_{\infty}$ of the number field $K = Q_S(p)^et$ inside $Q_S(p)$. By [NSW], Theorem 10.3.20 (ii), a $\mathbb{Z}_p$-extension of a number field is ramified at at least one prime dividing $p$. This contradicts $K_{\infty} \subset Q_S(p)$ and we conclude that $U^{ab}$ is finite.

In particular, $G_S(p)^{ab}$ is finite. Hence $G_S(p)$ is not free, and we obtain $cd G_S(p) = 2$. This shows the first part of assertion (i) of Theorem 2.2 and assertion (iv) follows from Proposition 3.2.

By Lemma 3.1, we know that for each prime number $\ell \in S$, the group $G_{S \setminus \{\ell\}}(\ell)$ is a proper quotient of $G_S(p)$, hence each $\ell \in S$ is ramified in the extension $Q_S(p)/\mathbb{Q}$. Let $G_\ell(Q_S(p)/\mathbb{Q})$ denote the decomposition group of $\ell$ in $G_S(p)$ with respect to some prolongation of $\ell$ to $Q_S(p)$. As a subgroup of $G_S(p)$, $G_\ell(Q_S(p)/\mathbb{Q})$ has cohomological dimension less or equal to 2. We have a natural surjection $G(Q_\ell(p)/\mathbb{Q}) \twoheadrightarrow G_\ell(Q_S(p)/\mathbb{Q})$. By [NSW], Theorem 7.5.2, $G(Q_\ell(p)/\mathbb{Q})$ is the pro-$p$-group on two generators $\sigma, \tau$ subject to the relation $\sigma \tau \sigma^{-1} = \tau^p$. $\tau$ is a generator of the inertia group and $\sigma$ is a Frobenius lift.
Therefore, $G(\mathbb{Q}_p(p) / \mathbb{Q}_p)$ has only three quotients of cohomological dimension less or equal to 2: itself, the trivial group and the Galois group of the maximal unramified $p$-extension of $\mathbb{Q}_p$. Since $\ell$ is ramified in the extension $\mathbb{Q}_p(\ell)/\mathbb{Q}_p$, the map $G(\mathbb{Q}_p(\ell)/\mathbb{Q}_p) \to G(\mathbb{Q}_p(\ell)/\mathbb{Q}_p)$ is an isomorphism, and hence $\mathbb{Q}_p(\ell)$ realizes the maximal $p$-extension of $\mathbb{Q}_p$. This shows statement (iii) of Theorem 2.2.

Next we show the second part of statement (i). By [NSW], Proposition 3.3.3, we have $scd G_S(p) \in \{2, 3\}$. Assume that $scd G = 2$. We consider the $G_S(p)$-module

$$D_2(\mathbb{Z}) = \lim_{\mathcal{U}} U^{ab},$$

where the limit runs over all open normal subgroups $U \triangleleft G_S(p)$ and for $V \subset U$ the transition map is the transfer $\text{Ver}: U^{ab} \to V^{ab}$, i.e. the dual of the corestriction map $\text{cor}: H^2(V, \mathbb{Z}) \to H^2(U, \mathbb{Z})$ (see [NSW], I, §5). By [NSW], Theorem 3.6.4 (iv), we obtain $G_S(p)^{ab} = D_2(\mathbb{Z})^{G_S(p)}$. On the other hand, $U^{ab}$ is finite for all $U$ and the group theoretical version of the Principal Ideal Theorem (see [Ne], VI, Theorem 7.6) implies $D_2(\mathbb{Z}) = 0$. Hence $G_S(p)^{ab} = 0$ which implies $G_S(p) = 1$ producing a contradiction. Hence $scd G_S(p) = 3$ showing the remaining assertion of Theorem 2.2, (i).

It remains to show that $G_S(p)$ is a duality group. By [NSW], Theorem 3.4.6, it suffices to show that the terms

$$D_i(G_S(p), \mathbb{Z}/p\mathbb{Z}) = \lim_{\mathcal{U}} H^i(U, \mathbb{Z}/p\mathbb{Z})$$

are trivial for $i = 0, 1$. Here $U$ runs through the open subgroups of $G_S(p)$, $\lor$ denotes the Pontryagin dual and the transition maps are the duals of the corestriction maps. For $i = 0$, and $V \not\subsetneq U$, the transition map

$$\text{cor}^\lor: \mathbb{Z}/p\mathbb{Z} = H^0(V, \mathbb{Z}/p\mathbb{Z})^\lor \to H^0(U, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$$

is multiplication by $(U : V)$, hence zero. Since $G_S(p)$ is infinite, we obtain $D_0(G_S(p), \mathbb{Z}/p\mathbb{Z}) = 0$. Furthermore,

$$D_1(G_S(p), \mathbb{Z}/p\mathbb{Z}) = \lim_{\mathcal{U}} U^{ab}/p = 0$$

by the Principal Ideal Theorem. This finishes the proof of Theorem 2.2.

5 The dualizing module

Having seen that $G_S(p)$ is a duality group under certain conditions, it is interesting to calculate its dualizing module. The aim of this section is to prove

**Theorem 5.1.** Let $p$ be an odd prime number and let $S$ be a finite set of prime numbers congruent to 1 modulo $p$. Assume that $cd G_S(p) = 2$. Then we have a natural isomorphism

$$D \cong \text{tor}_p(C_S(\mathbb{Q}_S(p)))$$

between the dualizing module $D$ of $G_S(p)$ and the $p$-torsion submodule of the $S$-adèlic class group of $\mathbb{Q}_S(p)$. There is a natural short exact sequence

$$0 \to \bigoplus_{\ell \in S} \text{Ind}_{G_S(p)}^{G_S(\ell)} \mu_{p^\infty}(\mathbb{Q}_\ell(p)) \to D \to E_S(\mathbb{Q}_S(p)) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0,$$
in which \( G_\ell \) is the decomposition group of \( \ell \) in \( G_S(p) \) and \( E_S(\mathbb{Q}_S(p)) \) is the group of \( S \)-units of the field \( \mathbb{Q}_S(p) \).

Working in a more general situation, let \( S \) be a non-empty set of primes of a number field \( k \). We recall some well-known facts from class field theory and we give some modifications for which we do not know a good reference.

By \( k_S \) we denote the maximal extension of \( k \) which is unramified outside \( S \) and we denote \( G(k_S/k) \) by \( G_S(k) \). For an intermediate field \( k \subset K \subset k_S \), let \( C_S(K) \) denote the \( S \)-idéle class group of \( K \). If \( S \) contains the set \( S_\infty \) of archimedean primes of \( k \), then the pair \( (G_S(k),C_S(k_S)) \) is a class formation, see [NSW], Proposition 8.3.8. This remains true for arbitrary non-empty \( S \), as can be seen as follows: We have the class formation

\[
(G_S(k), C_{S:S_\infty}(k_S)).
\]

Since \( k_S \) is closed under unramified extensions, the Principal Ideal Theorem implies \( Cl(k_S) = 0 \). Therefore we obtain the exact sequence

\[
0 \to \bigoplus_{v \in S_\infty \setminus S(k)} \text{Ind}_{G_S(k)}^{k_v} C_{S:S_\infty}(k_S) \to C_{S:S_\infty}(k_S) \to C_S(k_S) \to 0.
\]

Since the left term is a cohomologically trivial \( G_S(k) \)-module, we obtain that \( (G_S(k), C_S(k_S)) \) is a class formation. Finally, if \( p \) is a prime number, then also \( (G_S(k)(p), C_S(k_S(p))) \) is a class formation.

**Remark:** An advantage of considering the class formation \( (G_S(k)(p), C_S(k_S(p))) \) for sets \( S \) of primes which do not contain \( S_\infty \) is that we get rid of ‘redundancy at infinity’. A technical disadvantage is the absence of a reasonable Hausdorff topology on the groups \( C_S(K) \) for finite subextensions \( K \) of \( k \) in \( k_S \).

Next we calculate the module

\[
D_2(\mathbb{Z}_p) = \lim_{\to \atop U,n} H^2(U, \mathbb{Z}/p^n \mathbb{Z})^\vee,
\]

where \( n \) runs through all natural numbers, \( U \) runs through all open subgroups of \( G_S(k)(p) \) and \( \vee \) is the Pontryagin dual. If \( cd G_S(p) = 2 \), then \( D_2(\mathbb{Z}_p) \) is the dualizing module \( D \) of \( G_S(k)(p) \).

**Theorem 5.2.** Let \( k \) be a number field, \( p \) an odd prime number and \( S \) a finite non-empty set of non-archimedean primes of \( k \) such that the norm \( N(p) \) of \( p \) is congruent to 1 modulo \( p \) for all \( p \in S \). Assume that the scheme \( X = \text{Spec} \mathcal{O}_k - S \) is a \( K(\pi,1) \) for \( p \) and the étale topology and that \( k_S(p) \) realizes the maximal \( p \)-extension \( k_\pi(p) \) of \( k_\pi \) for all \( \pi \in S \). Then \( G_S(p) \) is a pro-\( p \)-duality group of dimension 2 with dualizing module

\[
D \cong \text{tor}_p(C_S(k_S(p))).
\]

**Remarks.** 1. In view of Theorem 2.2, Theorem 5.2 shows Theorem 5.1.
2. In the case when \( S \) contains all primes dividing \( p \), a similar result has been proven in [NSW], X, §5.
Proof of Theorem 5.2. We consider the schemes $\bar{X} = \text{Spec}(O_K)$ and $X = \bar{X} - S$ and we denote the natural embedding by $j : X \to \bar{X}$. As in the proof of Proposition 3.2, the flat duality theorem of Artin-Mazur implies

$$H^2_{\text{fl}}(X, \mathbb{Z}/p\mathbb{Z}) \cong H^0_{\mu}(X, \mu_p)^\vee,$$

and the group on the right vanishes since $k_p$ contains a primitive $p$-th root of unity for all $p \in S$. The $K(\pi, 1)$-property yields $cd G_{S}(k)(p) \leq 2$. Since $k_S(p)$ realizes the maximal $p$-extension $k_p(p)$ of $k_p$ for all $p \in S$, the inertia groups of these primes are of cohomological dimension 2 and we obtain $cd G_S(p) = 2$.

Next we consider, for some $n \in \mathbb{N}$, the constant sheaf $\mathbb{Z}/p^n\mathbb{Z}$ on $X$. The duality theorem of Artin-Verdier shows an isomorphism

$$H^i(\bar{X}, j_i(\mathbb{Z}/p^n\mathbb{Z})) = H^i_X(X, \mathbb{Z}/p^n\mathbb{Z}) \cong \text{Ext}^3_{\mathbb{X}}((\mathbb{Z}/p^n\mathbb{Z}, G_m))^\vee.$$

For $p \in S$, a standard calculation (see, e.g., [Mi2], II, Proposition 1.1) shows

$$H^i_p(\bar{X}, j_i(\mathbb{Z}/p^n\mathbb{Z}) \cong H^{i-1}(k_p, \mathbb{Z}/p^n\mathbb{Z}),$$

where $k_p$ is (depending on the readers preference) the henselization or the completion of $k$ at $p$. The excision sequence for the pair $(\bar{X}, X)$ and the sheaf $j_!(\mathbb{Z}/p^n\mathbb{Z})$ therefore implies a long exact sequence

$$(*) \quad \cdots \to H^i(\bar{X}, \mathbb{Z}/p^n\mathbb{Z}) \to \bigoplus_{p \in S} H^i(k_p, \mathbb{Z}/p^n\mathbb{Z}) \to \text{Ext}^2_{\mathbb{X}}((\mathbb{Z}/p^n\mathbb{Z}, G_m))^\vee \to \cdots$$

The local duality theorem ([NSW], Theorem 7.2.6) yields isomorphisms

$$H^i(k_p, \mathbb{Z}/p^n\mathbb{Z})^\vee \cong H^{2-i}(k_p, \mu_{p^n})$$

for all $i \in \mathbb{Z}$. Furthermore,

$$\text{Ext}^0_{\mathbb{X}}(\mathbb{Z}/p^n\mathbb{Z}, G_m) = H^0(k, \mu_{p^n}).$$

We denote by $E_S(k)$ and $Cl_S(k)$ the group of $S$-units and the $S$-ideal class group of $k$, respectively. By $Br(X)$, we denote the Brauer group of $X$. The short exact sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \to 0$ together with

$$\text{Ext}^i_X(\mathbb{Z}, G_m) = H^i_{\text{et}}(X, G_m) = \begin{cases} E_S(k) & \text{for } i = 0 \\ Cl_S(k) & \text{for } i = 1 \\ Br(X) & \text{for } i = 2 \end{cases}$$

and the Hasse principle for the Brauer group implies exact sequences

$$0 \to E_S(k)/p^n \to \text{Ext}^1_X(\mathbb{Z}/p^n\mathbb{Z}, G_m) \to p^n Cl_S(k) \to 0$$

and

$$0 \to Cl_S(k)/p^n \to \text{Ext}^2_X(\mathbb{Z}/p^n\mathbb{Z}, G_m) \to \bigoplus_{p \in S} p^n Br(k_p).$$

The same holds, if we replace $X$ by its normalization $X_K$ in a finite extension $K$ of $k$ in $k_S(p)$. Now we go to the limit over all such $K$. Since $k_S(p)$ realizes the maximal $p$-extension of $k_p$ for all $p \in S$, we have

$$\lim_{K} \bigoplus_{p \in S(K)} H^i(K_p, \mathbb{Z}/p^n\mathbb{Z})^\vee = \lim_{K} \bigoplus_{p \in S(K)} H^i(K_p, \mu_{p^n}) = 0$$
for $i \geq 1$ and
\[
\lim_{K} \bigoplus_{p \in S(K)} p^i \text{Br}(K_p) = 0.
\]

The Principal Ideal Theorem implies $Cl_S(k_S(p))/p = 0$ and since this group is a torsion group, its $p$-torsion part is trivial. Going to the limit over the exact sequences $(\ast)$ for all $X_K$, we obtain $D_i(\mathbb{Z}/p\mathbb{Z}) = 0$ for $i = 0, 1$, hence $G_S(k(p))$ is a duality group of dimension 2. Furthermore, we obtain the exact sequence
\[
0 \to \text{tor}_p(E_S(k_S(p))) \to \bigoplus_{p \in S} \text{Ind}_{G_S(k(p))} G_p \text{tor}_p(k_p(p)^\times) \to D \to E_S(k_S(p)) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0.
\]

Let $U \subset G_S(k(p))$ be an open subgroup and put $K = k_S(p)^U$. The invariant map
\[
\text{inv}_K : H^2(U, C_S(k_S(p))) \to \mathbb{Q}/\mathbb{Z}
\]
induces a pairing
\[
\text{Hom}_U(\mathbb{Z}/p^n\mathbb{Z}, C_S(k_S(p))) \times H^2(U, \mathbb{Z}/p^n\mathbb{Z}) \to H^2(U, C_S(K)) \to \mathbb{Q}/\mathbb{Z},
\]
and therefore a compatible system of maps
\[
p^n C_S(K) \to H^2(U, \mathbb{Z}/p^n\mathbb{Z})^U
\]
for all $U$ and $n$. In the limit, we obtain a natural map
\[
\phi : \text{tor}_p(C_S(k_S(p))) \to D.
\]

By our assumptions, the idele group $J_S(k_S(p))$ is $p$-divisible. We therefore obtain the exact sequence
\[
0 \to \text{tor}_p(E_S(k_S(p))) \to \bigoplus_{p \in S} \text{Ind}_{G_S(k(p))} G_p \text{tor}_p(k_p(p)^\times) \to \\
\text{tor}_p(C_S(k_S(p))) \to E_S(k_S(p)) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0
\]
which, via the just constructed map $\phi$, compares to the similar sequence with $D$ above. Hence $\phi$ is an isomorphism by the five lemma.

Finally, without any assumptions on $G_S(k(p))$, we calculate the $G_S(k(p))$-module $D_2(\mathbb{Z}_p)$ as a quotient of $\text{tor}_p(C_S(k_S(p)))$ by a subgroup of universal norms. We therefore can interpret Theorem 5.2 as a vanishing statement on universal norms.

Let us fix some notation. If $G$ is a profinite group and if $M$ is a $G$-module, we denote by $p^\infty M$ the submodule of elements annihilated by $p^n$. By $N_G(M) \subset M^G$ we denote the subgroup of universal norms, i.e.
\[
N_G(M) = \bigcap_U N_{G/U}(M^U),
\]
where $U$ runs through the open normal subgroups of $G$ and $N_{G/U}(M^U) \subset M^G$ is the image of the norm map
\[
N : M^U \to M^G, \quad m \mapsto \sum_{\sigma \in G/U} \sigma m.
\]
Proposition 5.3. Let $S$ be a non-empty finite set of non-archimedean primes of $k$ and let $p$ be an odd prime number such that $S$ contains no prime dividing $p$. Then

$$D_2(G_S(k)(p), \mathbb{Z}_p) \cong \lim_{K \to K_n} p^nC_S(K)/N_{G(k_S(p)/K)}(p^nC_S(K)),$$

where $n$ runs through all natural numbers and $K$ runs through all finite subextensions of $k$ in $k_S(p)$.

Proof. We want to use Poitou’s duality theorem ([Sc2], Theorem 1). But the class module $C_S(k_S(p))$ is not level-compact and we cannot apply the theorem directly. Instead, we consider the level-compact class formation

$$(G_S(k)(p), C^0_{S\cup S_\infty}(k_S(p))),$$

where $C^0_{S\cup S_\infty}(k_S(p))$ is the subgroup of idèle classes of norm 1. By [Sc2], Theorem 1, we have for all natural numbers $n$ and all finite subextensions $K$ of $k$ in $k_S(p)$ a natural isomorphism

$$H^2(G_S(K)(p), \mathbb{Z}/p^n\mathbb{Z})^\vee \cong \hat{H}^0(G_S(K)(p), p^nC^0_{S\cup S_\infty}(k_S(p))),$$

where $\hat{H}^0$ is Tate-cohomology in dimension 0 (cf. [Sc2]). The exact sequence

$$0 \to \bigoplus_{v \in S_\infty(K)} K_v^\times \to C^p_{S\cup S_\infty}(K) \to C_S(K) \to 0$$

and the fact that $K_v^\times$ is $p$-divisible for archimedean $v$, implies for all $n$ and all finite subextensions $K$ of $k$ in $k_S(p)$ an exact sequence of finite abelian groups

$$0 \to \bigoplus_{v \in S_\infty(K)} \mu_{p^n}(K_v) \to p^nC^p_{S\cup S_\infty}(K) \to p^nC_S(K) \to 0.$$

[Sc2], Proposition 7 therefore implies isomorphisms

$$\hat{H}^0(G_S(K)(p), p^nC^p_{S\cup S_\infty}(k_S(p))) \cong \hat{H}^0(G_S(K)(p), p^nC_S(k_S(p)))$$

for all $n$ and $K$. Furthermore, the exact sequence

$$0 \to p^nC^0_{S\cup S_\infty}(K) \to C^p_{S\cup S_\infty}(K) \xrightarrow{\sim} \mathbb{R}_p^\times \to 0$$

shows $p^nC^0_{S\cup S_\infty}(K) = p^nC^p_{S\cup S_\infty}(K)$ for all $n$ and all finite subextensions $K$ of $k$ in $k_S(p)$. Finally, [Sc2], Lemma 5 yields isomorphisms

$$\hat{H}^0(G_S(K)(p), p^nC_S(k_S(p))) \cong p^nC_S(K)/N_{G(k_S(p)/K)}(p^nC_S(K)).$$

Going to the limit over all $n$ and $K$, we obtain the statement of the Proposition. \(\square\)
6 Going up

The aim of this section is to prove Theorem 2.3. We start with the following lemma.

Lemma 6.1. Let \( \ell \neq p \) be prime numbers. Let \( \mathbb{Q}_\ell^h \) be the henselization of \( \mathbb{Q} \) at \( \ell \) and let \( K \) be an algebraic extension of \( \mathbb{Q}_\ell^h \) containing the maximal unramified \( p \)-extension \( (\mathbb{Q}_\ell^h)^{nr,p} \) of \( \mathbb{Q}_\ell^h \). Let \( Y = \text{Spec}(\mathcal{O}_K) \), and denote the closed point of \( Y \) by \( y \). Then the local étale cohomology group \( H^i_y(Y, \mathbb{Z}/p\mathbb{Z}) \) vanishes for \( i \neq 2 \) and we have a natural isomorphism

\[
H^2_y(Y, \mathbb{Z}/p\mathbb{Z}) \cong H^1(G(K(p)/K), \mathbb{Z}/p\mathbb{Z}).
\]

Proof. Since \( K \) contains \( (\mathbb{Q}_\ell^h)^{nr,p} \), we have \( H^2_y(Y, \mathbb{Z}/p\mathbb{Z}) = 0 \) for \( i > 0 \). The excision sequence shows \( H^0_y(Y, \mathbb{Z}/p\mathbb{Z}) = 0 \) for \( i = 0 \), and \( H^1_y(Y, \mathbb{Z}/p\mathbb{Z}) \cong H^{i-1}(G(K/K), \mathbb{Z}/p\mathbb{Z}) \) for \( i \geq 2 \). By [NSW], Proposition 7.5.7, we have

\[
H^{i-1}(G(K/K), \mathbb{Z}/p\mathbb{Z}) = H^{i-1}(G(K(p)/K), \mathbb{Z}/p\mathbb{Z})
\]

But \( G(K(p)/K) \) is a free pro-\( p \)-group (either trivial or isomorphic to \( \mathbb{Z}_p \)). This concludes the proof.

Let \( k \) be a number field and let \( S \) be finite set of primes of \( k \). For a (possibly infinite) algebraic extension \( K \) of \( k \) we denote by \( S(K) \) the set of prolongations of primes in \( S \) to \( K \). Now assume that \( M/K/k \) is a tower of pro-\( p \) Galois extensions. We denote the inertia group of a prime \( p \in S(K) \) in the extension \( M/K \) by \( T_p(M/K) \). For \( i \geq 0 \) we write

\[
\bigoplus'_{p \in S(K)} H^i(T_p(M/K), \mathbb{Z}/p\mathbb{Z}) \cong \lim_{k' \subset K \text{ finite}} \bigoplus_{p \in S(k')} H^i(T_p(M/k'), \mathbb{Z}/p\mathbb{Z}),
\]

where the limit on the right hand side runs through all finite subextensions \( k' \) of \( k \) in \( K \). The \( G(K/k) \)-module \( \bigoplus'_{p \in S(k)} H^i(T_p(M/K), \mathbb{Z}/p\mathbb{Z}) \) is the maximal discrete submodule of the product \( \prod_{p \in S(k)} H^i(T_p(M/K), \mathbb{Z}/p\mathbb{Z}) \).

Proposition 6.2. Let \( p \) be an odd prime number and let \( S \) be a finite set of prime numbers congruent to 1 modulo \( p \) such that \( \text{cd} \ G_S(p) = 2 \). Let \( \ell \notin S \) be another prime number congruent to 1 modulo \( p \) which does not split completely in the extension \( \mathbb{Q}_S(p)/\mathbb{Q} \). Then, for any prime \( p \) dividing \( \ell \) in \( \mathbb{Q}_S(p) \), the inertia group of \( p \) in the extension \( \mathbb{Q}_{S \cup \{\ell\}}(p)/\mathbb{Q}_S(p) \) is infinite cyclic. Furthermore, \( H^i(G(\mathbb{Q}_{S \cup \{\ell\}}(p)/\mathbb{Q}_S(p)), \mathbb{Z}/p\mathbb{Z}) = 0 \) for \( i \geq 2 \). For \( i = 1 \) we have a natural isomorphism

\[
H^1(G(\mathbb{Q}_{S \cup \{\ell\}}(p)/\mathbb{Q}_S(p)), \mathbb{Z}/p\mathbb{Z}) \cong \bigoplus_{p \in S_l(\mathbb{Q}_S(p))} H^1(T_p(\mathbb{Q}_{S \cup \{\ell\}}(p))/\mathbb{Q}_S(p), \mathbb{Z}/p\mathbb{Z}),
\]

where \( S_l(\mathbb{Q}_S(p)) \) denotes the set of primes of \( \mathbb{Q}_S(p) \) dividing \( \ell \). In particular, \( G(\mathbb{Q}_{S \cup \{\ell\}}(p)/\mathbb{Q}_S(p)) \) is a free pro-\( p \)-group.
Proof. Since ℓ does not split completely in \( \mathbb{Q}_\ell(p)/\mathbb{Q} \) and since \( cdG_S(p) = 2 \), the decomposition group of ℓ in \( \mathbb{Q}_\ell(p)/\mathbb{Q} \) is a non-trivial and torsion-free quotient of \( \mathbb{Z}_p \cong G(\mathbb{Q}_\ell^\text{et}/\mathbb{Q}_\ell) \). Therefore \( \mathbb{Q}_\ell(p) \) realizes the maximal unramified \( p \)-extension of \( \mathbb{Q}_\ell \). We consider the scheme \( X = \text{Spec}(\mathbb{Z}) - S \) and its universal \( p \)-covering \( \tilde{X} \) whose field of functions is \( \mathbb{Q}_\ell(p) \). Let \( Y \) be the subscheme of \( \tilde{X} \) obtained by removing all primes of residue characteristic \( \ell \). We consider the étale excision sequence for the pair \((\tilde{X}, Y)\). By Theorem 3.2, we have \( H^i_{\text{et}}(\tilde{X}, \mathbb{Z}/p\mathbb{Z}) = 0 \) for \( i > 0 \), which implies isomorphisms

\[
H^i_{\text{et}}(Y, \mathbb{Z}/p\mathbb{Z}) \sim \bigoplus_{p|\ell} H^{i+1}_{\text{et}}(Y^h_p, \mathbb{Z}/p\mathbb{Z})
\]

for \( i \geq 1 \). By Lemma 6.1, we obtain \( H^i_{\text{et}}(Y, \mathbb{Z}/p\mathbb{Z}) = 0 \) for \( i \geq 2 \). The universal \( p \)-covering \( \tilde{Y} \) of \( Y \) has \( \mathbb{Q}_{S \cup \{\ell\}}(p) \) as its function field, and the Hochschild-Serre spectral sequence for \( \tilde{Y}/Y \) yields an inclusion

\[
H^2(G(\mathbb{Q}_{S \cup \{\ell\}}(p)/\mathbb{Q}_S(p)), \mathbb{Z}/p\mathbb{Z}) \hookrightarrow H^2_{\text{et}}(Y, \mathbb{Z}/p\mathbb{Z}) = 0.
\]

Hence \( G(\mathbb{Q}_{S \cup \{\ell\}}(p)/\mathbb{Q}_S(p)) \) is a free pro-\( p \)-group and for \( H^1 \) we obtain

\[
H^1(G(\mathbb{Q}_{S \cup \{\ell\}}(p)/\mathbb{Q}_S(p)), \mathbb{Z}/p\mathbb{Z}) \sim H^1_{\text{et}}(Y, \mathbb{Z}/p\mathbb{Z}) \cong \bigoplus_{p \in S(\mathbb{Q}_S(p))} H^1(G(\mathbb{Q}_S(p)_p(\mathbb{Q}_S(p)), \mathbb{Z}/p\mathbb{Z}).
\]

This shows that each \( p \mid \ell \) ramifies in \( \mathbb{Q}_{S \cup \{\ell\}}(p)/\mathbb{Q}_S(p) \), and since the Galois group is free, \( \mathbb{Q}_{S \cup \{\ell\}}(p) \) realizes the maximal \( p \)-extension of \( \mathbb{Q}_S(p)_p \). In particular,

\[
H^1(G(\mathbb{Q}_S(p)_p(\mathbb{Q}_S(p)), \mathbb{Z}/p\mathbb{Z}) \cong H^1(T_p(\mathbb{Q}_{S \cup \{\ell\}}(p)/\mathbb{Q}_S(p)), \mathbb{Z}/p\mathbb{Z})
\]

for all \( p \mid \ell \), which finishes the proof.

Let us mention in passing that the above calculations imply the validity of the following arithmetic form of Riemann’s existence theorem.

**Theorem 6.3.** Let \( p \) be an odd prime number and let \( S \) be a finite set of prime numbers congruent to 1 modulo \( p \) such that \( cdG_S(p) = 2 \). Let \( T \supset S \) be another set of prime numbers congruent to 1 modulo \( p \). Assume that all \( \ell \in T \setminus S \) do not split completely in the extension \( \mathbb{Q}_S(p)/\mathbb{Q} \). Then the inertia groups in \( \mathbb{Q}_T(p)/\mathbb{Q}_S(p) \) of all primes \( p \in T \setminus S(\mathbb{Q}_S(p)) \) are infinite cyclic and the natural homomorphism

\[
\phi : \bigstar_{p \in T \setminus S(\mathbb{Q}_S(p))} T_p(\mathbb{Q}_T(p)/\mathbb{Q}_S(p)) \longrightarrow G(\mathbb{Q}_T(p)/\mathbb{Q}_S(p))
\]

is an isomorphism.

**Remark:** A similar theorem holds in the case that \( S \) contains \( p \), see [NSW], Theorem 10.5.1.

**Proof.** By Proposition 6.2 and by the calculation of the cohomology of a free product ([NSW], 4.3.10 and 4.1.4), \( \phi \) is a homomorphism between free pro-\( p \)-groups which induces an isomorphism on mod \( p \) cohomology. Therefore \( \phi \) is an isomorphism.
Proof of theorem 2.3. We consider the Hochschild-Serre spectral sequence

\[ E_2^{ij} = H^i(G_S(p), H^j(G_{Q_{S \cup \{ \ell \}}}(p)/Q_S(p)), \mathbb{Z}/p\mathbb{Z}) \Rightarrow H^{i+j}(G_{Q_{S \cup \{ \ell \}}}(p), \mathbb{Z}/p\mathbb{Z}). \]

By Proposition 6.2, we have \( E_2^{ij} = 0 \) for \( j \geq 2 \) and

\[ H^1(G_{Q_{S \cup \{ \ell \}}}(p)/Q_S(p)), \mathbb{Z}/p\mathbb{Z}) \cong \bigoplus_{p|\ell} H^1(T_p(Q_{S \cup \{ \ell \}}(p)/Q_S(p)), \mathbb{Z}/p\mathbb{Z}) \]

\[ \cong \Ind_{G_S(p)}^{G_{\ell}} H^1(T_\ell(Q_{S \cup \{ \ell \}}(p)/Q_S(p)), \mathbb{Z}/p\mathbb{Z}), \]

where \( G_\ell \cong \mathbb{Z}_p \) is the decomposition group of \( \ell \) in \( G_S(p) \). We obtain \( E_2^{1,1} = 0 \) for \( i \geq 2 \). By assumption, \( cd G_S(p) = 2 \), hence \( E_2^{0,j} = 0 \) for \( j \geq 3 \). This implies \( H^1(G_{Q_{S \cup \{ \ell \}}}(p), \mathbb{Z}/p\mathbb{Z}) = 0 \), and hence \( cd G_{Q_{S \cup \{ \ell \}}}(p) \leq 2 \). Finally, the decomposition group of \( \ell \) in \( G_{Q_{S \cup \{ \ell \}}}(p) \) is full, i.e. of cohomological dimension 2. Therefore, \( cd G_{Q_{S \cup \{ \ell \}}}(p) = 2 \).

We obtain the following

**Corollary 6.4.** Let \( p \) be an odd prime number and let \( S \) be a finite set of prime numbers congruent to 1 modulo \( p \). Let \( \ell \notin S \) be another prime number congruent to 1 modulo \( p \). Assume that there exists a prime number \( q \in S \) such that the order of \( \ell \) in \( \mathbb{Z}/q\mathbb{Z} \) is divisible by \( p \) (e.g. \( \ell \) is not a \( p \)-th power modulo \( q \)). Then \( cd G_S(p) = 2 \) implies \( cd G_{Q_{S \cup \{ \ell \}}}(p) = 2 \).

**Proof.** Let \( K_q \) be the maximal subextension of \( p \)-power degree in \( \mathbb{Q}(\mu_q)/\mathbb{Q} \). Then \( K_q \) is a non-trivial finite subextension of \( \mathbb{Q} \) in \( Q_S(p) \) and \( \ell \) does not split completely in \( K_q/\mathbb{Q} \). Hence the result follows from Theorem 2.3. \( \square \)

**Remark.** One can sharpen Corollary 6.4 by finding weaker conditions on a prime \( \ell \) not to split completely in \( Q_S(p) \).

### 7 Proof of Theorem 2.1

In this section we prove Theorem 2.1. We start by recalling the notion of the linking diagram attached to \( S \) and \( p \) from [La]. Let \( p \) be an odd prime number and let \( S \) be a finite set of prime numbers congruent to 1 modulo \( p \). Let \( \Gamma(S)(p) \) be the directed graph with vertices the primes of \( S \) and edges the pairs \( (r, s) \in S \times S \) with \( r \) not a \( p \)-th power modulo \( s \). We now define a function \( \ell \) on the set of pairs of distinct primes of \( S \) with values in \( \mathbb{Z}/p\mathbb{Z} \) by first choosing a primitive root \( g_s \) modulo \( s \) for each \( s \in S \). Let \( \ell_{rs} = \ell(r, s) \) be the image in \( \mathbb{Z}/p\mathbb{Z} \) of any integer \( c \) satisfying

\[ r \equiv g_s^{-c} \mod s. \]

The residue class \( \ell_{rs} \) is well-defined since \( c \) is unique modulo \( s - 1 \) and \( p \mid s - 1 \).

Note that \( (r, s) \) is an edge of \( \Gamma(S)(p) \) if and only if \( \ell_{rs} \neq 0 \). We call \( \ell_{rs} \) the linking number of the pair \( (r, s) \). This number depends on the choice of primitive roots, if \( g \) is another primitive root modulo \( s \) and \( g_s \equiv g^a \mod s \), then the linking number attached to \( (r, s) \) would be multiplied by \( a \) if \( g \) were used instead of \( g_s \). The directed graph \( \Gamma(S)(p) \) together with \( \ell \) is called the linking diagram attached to \( S \) and \( p \).
Definition 7.1. We call a finite set $S$ of prime numbers congruent to 1 modulo $p$ strictly circular with respect to $p$ (and $\Gamma(S)(p)$ a non-singular circuit), if there exists an ordering $S = \{q_1, \ldots, q_n\}$ of the primes in $S$ such that the following conditions hold.

(a) The vertices $q_1, \ldots, q_n$ of $\Gamma(S)(p)$ form a circuit $q_1q_2 \cdots q_nq_1$.

(b) If $i, j$ are both odd, then $q_iq_j$ is not an edge of $\Gamma(S)(p)$.

(c) If we put $\ell_{ij} = \ell(q_i, q_j)$, then

$$\ell_{12}\ell_{23} \cdots \ell_{n-1,n}\ell_{n1} \neq \ell_{1n}\ell_{21} \cdots \ell_{n,n-1}.$$

Note that condition (b) implies that $n$ is even $\geq 4$ and that (c) is satisfied if there is an edge $q_iq_j$ of the circuit $q_1q_2 \cdots q_nq_1$ such that $q_jq_i$ is not an edge of $\Gamma(S)(p)$. Condition (c) is independent of the choice of primitive roots since the condition can be written in the form

$$\frac{\ell_{1n}}{\ell_{n-1,n}}\frac{\ell_{21}}{\ell_{n1}} \cdots \frac{\ell_{n,n-1}}{\ell_{n-2,n-1}} \neq 1,$$

where each ratio in the product is independent of the choice of primitive roots.

If $p$ is an odd prime number and if $S = \{q_1, \ldots, q_n\}$ is a finite set of prime numbers congruent to 1 modulo $p$, then, by a result of Koch [Ko], the group $G_S(p) = F/R$, where $F$ is a free pro-$p$-group on generators $x_1, \ldots, x_n$ and $R$ is the minimal normal subgroup in $F$ on generators $r_1, \ldots, r_n$, where

$$r_i \equiv x_i^{q_i-1}\prod_{j \neq i}[x_i, x_j]^{\ell_{ij}} \mod F_3.$$

Here $F_3$ is the third step of the lower $p$-central series of $F$ and the $\ell_{ij}$ are the linking numbers for some choice of primitive roots. If $S$ is strictly circular, Labute ([La], Theorem 1.6) shows that $G_S(p)$ is a so-called ‘mild’ pro-$p$-group, and, in particular, is of cohomological dimension 2 ([La], Theorem 1.2).

Proof of Theorem 2.1. By [La], Theorem 1.6, we have $cd G_T(p) = 2$. By assumption, we find a series of subsets

$$T = T_0 \subset T_1 \subset \cdots \subset T_r = S,$$

such that for all $i \geq 1$, the set $T_i \setminus T_{i-1}$ consists of a single prime number $q$ congruent to 1 modulo $p$ and there exists a prime number $q' \in T_{i-1}$ with $q$ not a $p$-th power modulo $q'$. An inductive application of Corollary 6.4 yields the result.

Remark. Labute also proved some variants of his group theoretic result [La], Theorem 1.6. The same proof as above shows corresponding variants of Theorem 2.1, by replacing condition (i) by other conditions on the subset $T$ as they are described in [La], §3.

A straightforward applications of Čebotarev’s density theorem shows that, given $\Gamma(S)(p)$, a prime number $q$ congruent to 1 modulo $p$ can be found with the additional edges of $\Gamma(S \cup \{q\})(p)$ arbitrarily prescribed (cf. [La], Proposition 6.1). We therefore obtain the following corollaries.

---

14
Corollary 7.2. Let \( p \) be an odd prime number and let \( S \) be a finite set of prime numbers congruent to 1 modulo \( p \), containing a strictly circular subset \( T \subset S \). Then there exists a prime number \( q \) congruent to 1 modulo \( p \) with
\[
\text{cd} G_{S \cup \{q\}}(p) = 2.
\]

Corollary 7.3. Let \( p \) be an odd prime number and let \( S \) be a finite set of prime numbers congruent to 1 modulo \( p \). Then we find a finite set \( T \) of prime numbers congruent to 1 modulo \( p \) such that
\[
\text{cd} G_{S \cup T}(p) = 2.
\]

References


