Abelian groups and quadratic residues in weak arithmetic

Emil Jeřábek*

Institute of Mathematics of the Academy of Sciences
Žitná 25, 115 67 Praha 1, Czech Republic, email: jerabek@math.cas.cz

November 5, 2008

Abstract

We investigate the provability of some properties of abelian groups and quadratic residues in variants of bounded arithmetic. Specifically, we show that the structure theorem for finite abelian groups is provable in $S^2_2 + iWPHP(\Sigma^b_1)$, and use it to derive Fermat's little theorem and Euler's criterion for the Legendre symbol in $S^2_2 + iWPHP(PV)$ extended by the pigeonhole principle $PHP(PV)$. We prove the quadratic reciprocity theorem (including the supplementary laws) in the arithmetic theories $T^0_2 + Count_2(PV)$ and $I\Delta_0 + Count_2(\Delta_0)$ with modulo-2 counting principles.

Keywords: bounded arithmetic, abelian group, Fermat's little theorem, quadratic reciprocity, pigeonhole principle
MSC (2000): primary 03F30, 03F20; secondary 11A15, 20K01

1 Introduction

Bounded arithmetic is primarily studied because of its connections to complexity theory, see e.g. Buss [3], Krajíček [13], Cook and Nguyen [6]. However, as with other systems of formal arithmetic, it is also interesting to note which mathematical (typically, number-theoretic or combinatorial) theorems are provable in weak arithmetical theories, or to put it differently, to find as weak a natural theory as possible which proves a given statement (this approach fits into the general "reverse mathematics" scheme of Simpson [20], cf. Nguyen [17]). Examples include the proof of infinitude of prime numbers in $I\Delta_0 + iWPHP(\Delta_0)$ by Paris et al. [19], the proof of Lagrange's four-square theorem in $I\Delta_0 + iWPHP(\Delta_0)$ by Berarducci and Intrigila [2], the proof of the prime number theorem in $I\Delta_0 + \exp$ by Cornaros and Dimitracopoulos [8], or the proof of a discrete version of the Jordan curve theorem in $V^0[2]$ by Nguyen [17].

The first contribution of the present paper is a proof of the *structure theorem for finite abelian groups*—stating that every finite abelian group is isomorphic to a direct sum of cyclic groups (see e.g. Mac Lane and Birkhoff [15])—in the theory $S^2_2 + iWPHP(\Sigma^b_1)$ (a subtheory of Buss' T^2_2), where we represent a finite group by a Σ^b_1-definable binary operation on a bounded

*Supported by grant IAA1019401 of GA AV ČR, and grant 1M0545 of MŠMT ČR.

set of numbers. Our motivating example, and main application, for the structure theorem is *Fermat's little theorem* (*FLT*), stating

$$a^p \equiv a \pmod p$$

for a prime p. FLT was considered in the context of bounded arithmetic by Krajíček and Pudlák [14], who have shown that S^1_2 does not prove FLT if the RSA cryptosystem is secure. (Actually, their argument applies to a weak corollary of FLT stating that multiplication modulo a prime is a torsion group, which is provable using the weak pigeonhole principle.) Jeřábek [10] proved that FLT is in S^1_2 equivalent to the correctness of the Rabin–Miller probabilistic primality testing algorithm. It remains an open problem whether FLT is provable in the bounded arithmetic S_2. Here we derive FLT using the structure theorem for finite abelian groups in the theory $S^2_2 + iWPHP(PV) + PHP(PV)$, which includes the strong pigeonhole principle for polynomial-time functions.

Next to Fermat's little theorem, we consider *Euler's criterion* for quadratic residues stating

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$$

for an odd prime p, where $(a|p)$ is the Legendre symbol. We will show in S^1_2 that Euler's criterion is equivalent to FLT together with a statement ensuring that the quadratic character $a \mapsto a^{(p-1)/2} \bmod p$ is nontrivial. In particular, we obtain a proof of Euler's criterion in $S^2_2 + iWPHP(PV) + PHP(PV)$.

Finally, we will discuss another result on quadratic residues: the *quadratic reciprocity* theorem. Quadratic reciprocity, originally proved by Carl Friedrich Gauss, is one of the most famous theorems of elementary number theory. Apart from Gauss (who gave no less than eight different proofs of the theorem), over 200 proofs of quadratic reciprocity have been published by various authors. As far as bounded arithmetic is concerned, the work of D'Aquino and Macintyre [9] on quadratic forms aims towards proving quadratic reciprocity or at least some of its special cases in S_2, and Cornaros [7] formalized a standard textbook proof of quadratic reciprocity in $I\mathcal{E}^2_*$ (a rather strong theory corresponding to the Grzegorczyk class $\mathcal{E}^2 = \mathit{LinSpace}$). The supplementary laws were proved by Berarducci and Intrigila [2] in $I\Delta_0$ extended with modular counting principles.

Observe that many elementary proofs of quadratic reciprocity (e.g., proofs based on Gauss' lemma or Zolotarev's lemma, and Eisenstein's proof) directly or indirectly involve counting the parity of sets. We will show that a rudimentary counting modulo 2 indeed suffices to prove the theorem. More precisely, we do not even require the existence of modulo-2 counting functions, as we can witness the parity of all sets we need by explicit functions. We only need to assume the *modulo-2 counting principle* Count_2; in detail, we can prove the law of quadratic reciprocity as well as the supplementary laws and multiplicativity of the Legendre symbol in the theories $T^0_2 + \mathit{Count}_2(PV)$ and $I\Delta_0 + \mathit{Count}_2(\Delta_0)$. We also generalize these statements to the Jacobi symbol, and prove the soundness of the standard polynomial-time algorithm for the Jacobi symbol in $S^1_2 + \mathit{Count}_2(PV)$.

2 Preliminaries

We review below basic facts about bounded arithmetic, we refer the reader to Krajíček [13] for more details.

We will work with two kinds of arithmetical systems: theories based on $I\Delta_0$ (introduced by Parikh [18]), and Buss' theories [3]. $I\Delta_0$ is a theory in the basic language of arithmetic $L_{PA} = \langle 0, S, +, \cdot, \leq \rangle$. A formula φ is bounded (or Δ_0) if every quantifier in φ is bounded, i.e., it has one of the forms

$$\exists x \leq t\, \psi(x) := \exists x\, (x \leq t \wedge \psi(x)),$$
$$\forall x \leq t\, \psi(x) := \forall x\, (x \leq t \to \psi(x)),$$

where t is a term not containing the variable x. The axioms of $I\Delta_0$ include the axioms of Robinson's arithmetic Q (which state basic inductive properties of addition, multiplication, and ordering), and the induction schema Δ_0-*IND*:

$$(\varphi\text{-}\mathit{IND}) \qquad \varphi(0) \wedge \forall x\, (\varphi(x) \to \varphi(x+1)) \to \varphi(a).$$

We formulate Buss' theories in the language $L = \langle 0, S, +, \cdot, \leq, \#, |x|, \lfloor x/2^y \rfloor \rangle$, where the intended meaning of the symbols is $|x| = \lceil \log_2(x+1) \rceil$, $x \# y = 2^{|x|\cdot|y|}$. A bounded quantifier is called sharply bounded if its bounding term is of the form $|t|$. A formula is $\Sigma^b_0 = \Pi^b_0$ if all its quantifiers are sharply bounded. A formula is Σ^b_{i+1} (Π^b_{i+1}) if it is constructed from $\Sigma^b_i \cup \Pi^b_i$-formulas by means of conjunctions, disjunctions, sharply bounded quantifiers, and existential (universal, respectively) bounded quantifiers. The set of Boolean combinations of Σ^b_i-formulas is denoted by $\mathcal{B}(\Sigma^b_i)$.

The theory T^i_2 is axiomatized by a finite set *BASIC* of open axioms stating basic properties of the symbols of L, and the schema Σ^b_i-*IND*. If $i > 0$, the theory S^i_2 consists of *BASIC* and the polynomial induction schema Σ^b_i-*PIND*

$$(\varphi\text{-}\mathit{PIND}) \qquad \varphi(0) \wedge \forall x\, (\varphi(\lfloor x/2 \rfloor) \to \varphi(x)) \to \varphi(a).$$

Alternatively, S^i_2 can be axiomatized over *BASIC* by the length induction schema Σ^b_i-*LIND*

$$(\varphi\text{-}\mathit{LIND}) \qquad \varphi(0) \wedge \forall x\, (\varphi(x) \to \varphi(x+1)) \to \varphi(|a|),$$

the length minimization schema Σ^b_i-*LMIN*

$$(\varphi\text{-}\mathit{LMIN}) \qquad \varphi(a) \to \exists b \leq a\, (\varphi(b) \wedge \forall x\, (|x| < |b| \to \neg\varphi(x))),$$

or the analogous length maximization schema Σ^b_i-*LMAX*.

The theory S^i_2 also proves the Σ^b_i-comprehension schema

$$(\varphi\text{-}\mathit{COMP}) \qquad \exists b < a \# 1\, \forall i < |a|\, (i \in b \leftrightarrow \varphi(i)),$$

where we define $i \in x$ iff $\lfloor x/2^i \rfloor$ is odd.

The basic relationship of these theories is given by $T^i_2 \subseteq S^{i+1}_2 \subseteq T^{i+1}_2$. Buss' witnessing theorem implies that S^{i+1}_2 is a $\forall\Sigma^b_{i+1}$-conservative extension of T^i_2.

All these theories can be relativized by introducing an extra unary predicate α in the language. $\Sigma^b_i(\alpha)$ and $\Pi^b_i(\alpha)$ formulas in the expanded language $L(\alpha)$ are defined as above. The theories $S^i_2(\alpha)$ and $T^i_2(\alpha)$ include the (polynomial) induction schema for $\Sigma^b_i(\alpha)$-formulas, but no other axioms about the predicate α.

PV is an equational theory introduced by Cook [5]. Its language contains function symbols for all polynomial-time algorithms, introduced inductively using limited recursion on notation (cf. Cobham [4]). It is axiomatized by defining equations of its function symbols, and a derivation rule similar to *PIND*. We will denote the set of PV-function symbols also by PV. All PV-function have provably total Σ^b_1-definitions in T^0_2 such that T^0_2 proves their defining equations and $\Sigma^b_0(PV)$-*IND* (Jeřábek [11]), furthermore every $\Sigma^b_i(PV)$-formula is equivalent to a Σ^b_i-formula for $i > 0$, hence we will use PV-functions freely in T^0_2 and its extensions.

If f is a definable function (possibly with parameters), the injective weak pigeonhole principle $iWPHP(f)$ is the axiom

$$a > 0 \to \exists x < 2a\, f(x) \geq a \vee \exists x < x' < 2a\, f(x) = f(x').$$

If Γ is a set of functions (or formulas, meaning the functions with Γ-definable graph), then we put $iWPHP(\Gamma) = \{iWPHP(f) \mid f \in \Gamma\}$. The multifunction weak pigeonhole principle $mWPHP(R)$ is the axiom

$$a > 0 \to \exists x < 2a\, \forall y < a\, \neg R(x, y) \vee \exists x < x' < 2a\, \exists y < a\, (R(x, y) \wedge R(x', y)),$$

where R is a definable binary relation. Again, we put $mWPHP(\Gamma) = \{mWPHP(R) \mid R \in \Gamma\}$ for a set Γ of formulas. Note that $mWPHP(\Gamma)$ implies $iWPHP(\Gamma)$. The schema $mWPHP(\Sigma^b_i(\alpha))$ for $i > 0$ is provable in $T^{i+1}_2(\alpha)$ by Maciel et al. [16].

3 Finite abelian groups

Definition 3.1 (in $S^1_2(\alpha)$) A *definable finite abelian group* is a structure $\langle G, +\rangle$, where G is a nonempty subset of an interval $[0, t)$ (which we will denote simply as t), and $+$ is a definable binary operation on G satisfying the usual axioms of abelian groups:

$$x + (y + z) = (x + y) + z,$$
$$x + y = y + x,$$
$$\exists v\, x + v = y.$$

We will denote the group $\langle G, +\rangle$ by just G, if there is no danger of confusion. If Γ is a set of formulas, and G and $+$ are definable by Γ-formulas (with parameters), we say that $\langle G, +\rangle$ is a Γ-definable finite abelian group, or simply Γ *finite abelian group*. Observe that a group is $\Sigma^b_1(\alpha)$ iff it is definable by a nondeterministic circuit with oracle α; we may identify the group with (the number representing) the circuit, hence it makes sense to speak of, e.g., sequences of groups. Notice that G is automatically $\Sigma^b_1(\alpha)$-definable by the formula $\exists y < t\, x + x = y$ if $+$ is $\Sigma^b_1(\alpha)$.

Definition 3.2 (in $S^1_2(\alpha)$) For any positive integer n, $C(n)$ denotes the cyclic group of addition modulo n.

Let $\langle G_i \mid i < k\rangle$ be a sequence of $\Sigma^b_1(\alpha)$ abelian groups such that $G_i \subseteq t_i$ for each $i < k$. The *direct sum* $\bigoplus_{i<k} G_i$ is the $\Sigma^b_1(\alpha)$ group $\langle G, +\rangle$, where

$$G = \{\langle a_i \mid i < k\rangle \mid \forall i < k\, a_i \in G_i\} \subseteq \prod_i t_i,$$

$$\langle a_i \mid i < k\rangle + \langle b_i \mid i < k\rangle = \langle a_i + b_i \mid i < k\rangle.$$

Here, $a = \langle a_i \mid i < k\rangle$ refers to the sequence encoding function $a_i = \lfloor a/\prod_{j<i} t_j\rfloor \bmod t_i$.

Lemma 3.3 *(in $S^1_2(\alpha)$) If G is a $\Sigma^b_1(\alpha)$ finite abelian group, there exists a $\Sigma^b_1(\alpha)$-definable function nx such that $0x = 0$, $1x = x$, $(n + m)x = nx + mx$, $n(x + y) = nx + ny$, $(nm)x = n(mx)$, and $(-n)x = -nx$ for every $x, y \in G$, and integers n, m.*

If $+$ is defined by a $PV(\alpha)$-function, then so is nx for nonnegative n.

Proof: We can define nx for nonnegative n by limited recursion on notation:

$$0x = 0,$$
$$(2n)x = nx + nx,$$
$$(2n + 1)x = (2n)x + x.$$

We put $(-n)x = -nx$. Verification of the properties is then straightforward. □

Recall that a *torsion element* of a group G is an $x \in G$ such that $nx = 0$ for some $n > 0$. A *torsion group* is an abelian group consisting of torsion elements.

Lemma 3.4 *(in $S^1_2(\alpha)$) If x is a torsion element of a $\Sigma^b_1(\alpha)$ finite abelian group, there exists a unique positive integer $o(x)$ (the* order *of x) such that*

$$ax = 0 \quad \textit{iff} \quad o(x) \mid a$$

for every a.

Proof: By $\Sigma^b_1(\alpha)$-*LMIN*, there exists $o(x) > 0$ such that $o(x)x = 0$ of minimal length. Assume that $ax = 0$, and let $d = \gcd(a, o(x))$. By Bézout's lemma, there exist integers u, v such that $d = ua + vo(x)$, hence $dx = 0$. If d is a proper divisor of $o(x)$, then $|d| < |o(x)|$, which contradicts the choice of $o(x)$. Therefore $d = o(x)$, and $o(x) \mid a$. Uniqueness of $o(x)$ is obvious. □

Lemma 3.5 *(in $S^1_2(\alpha) + iWPHP(\Sigma^b_1(\alpha))$) Any $\Sigma^b_1(\alpha)$ finite abelian group is a torsion group.*

Proof: Let $x \in G \subseteq t$. By *iWPHP*, there exist $a < b < 2t$ such that $ax = bx$, hence $(b - a)x = 0$. □

Remark 3.6 Similarly to Lemma 3.5, $S^1_2(\alpha) + iWPHP(\Sigma^b_1(\alpha))$ also proves that any finite structure with a $\Sigma^b_1(\alpha)$-definable associative, commutative, and cancellative binary operation is an abelian group.

Before we turn to the main structure theorem, we prove the simpler decomposition to p-primary components below. It is a consequence of the structure theorem, but we prove it separately because we can formalize the proof in a weaker theory that the structure theorem.

Definition 3.7 (in $S^1_2(\alpha)$) If $\langle G, +\rangle$ is a $\Sigma^b_1(\alpha)$ finite abelian group, and p is a prime, then the *p-primary component of* G is defined by

$$G_p = \{x \in G \mid \exists e\, p^{|e|}x = 0\}.$$

Notice that G_p is a subgroup of G. If G is a torsion group with $o(x) \le t$ for every x, then G_p is $\Sigma^b_1(\alpha)$, as we can bound e by t.

A *p-group* is a $\Sigma^b_1(\alpha)$ finite abelian group $\langle G, +\rangle$ such that $G = G_p$.

Theorem 3.8 *(in $S^1_2(\alpha)+iWPHP(\Sigma^b_1(\alpha))$) Let $\langle G, +\rangle$ be a $\Sigma^b_1(\alpha)$ finite abelian group. There exists a sequence $\langle p_i \mid i < k\rangle$ of pairwise distinct primes, such that the mapping*

$$\varphi \colon \bigoplus_{i<k} G_{p_i} \to G$$

defined by $\varphi(\langle x_i \mid i < k\rangle) = \sum_i x_i$ is an isomorphism. If a prime p is not on the list, then $G_p = 0$.

Proof: Let $G \subseteq t$. By $\Sigma^b_1(\alpha)$-$LMAX$, there exists the maximal k with the property that $k \le |t| + 1$ and there exists a sequence $\langle z_i \mid i < k\rangle$ of nonzero elements of G, and a sequence $\langle p_i \mid i < k\rangle$ of pairwise coprime integers $p_i \le 2t$ such that $p_i z_i = 0$. By $\Sigma^b_1(\alpha)$-$LMIN$, there exists the smallest ℓ such that there exist $\vec z$ and $\vec p$ as above with $\sum_i |p_i| \le \ell$. Fix the witnesses $\vec z$ and $\vec p$.

By the choice of ℓ, all p_i are primes: if $p_i = mn$ is a nontrivial factorization, then either $mz_i = 0$, or $y = mz_i$ is a nonzero element such that $ny = 0$. We can thus replace p_i with m or n, which contradicts the minimality of ℓ. In particular, $p_i = o(z_i)$ for all $i < k$.

Define $f \colon \prod_i p_i \to G$ by $f(\langle a_i \mid i < k\rangle) = \sum_i a_i z_i$. We claim that f is injective. Indeed, let $\sum_i a_i z_i = \sum_i a'_i z_i$, and fix $i < k$. Put $q = \prod_{j\ne i} p_j$. We have $0 = q\sum_j (a'_j - a_j)z_j = q(a'_i - a_i)z_i$, hence $o(z_i) = p_i \mid q(a'_i - a_i)$. However, q is coprime to p_i, thus $p_i \mid a'_i - a_i$. As $0 \le a'_i, a_i < p_i$, this implies $a_i = a'_i$. By $iWPHP(\Sigma^b_1(\alpha))$, we obtain $2^k \le \prod_i p_i < 2t$, hence $k \le |t|$.

Consequently, if $p \ne p_i$ for all i, then $G_p = 0$. Indeed, if $x \ne 0$, and $p^e x = 0$, we can extend $\vec p$ and $\vec z$ by p^e and x (respectively), which contradicts the maximality of k.

Clearly, φ is a group homomorphism. We claim that φ is injective, i.e., $\ker(\varphi) = 0$. Let thus $\sum_i x_i = 0$, $x_i \in G_{p_i}$. Consider $i < k$, and put $q = \prod_{j\ne i} p_j^{|t|}$. We have $0 = q\sum_j x_j = qx_i$, and $p_i^{|t|} x_i = 0$, hence $x_i = 0$, as q and $p_i^{|t|}$ are coprime.

It remains to show that φ is onto. Let thus $x \in G$, and using $\Sigma^b_1(\alpha)$-$LMIN$ find a of minimal length such that $ax \in \mathrm{rng}(\varphi)$. We have $bx \in \mathrm{rng}(\varphi)$ iff $a \mid b$, as in the proof of

Lemma 3.4. If $a = 1$, the proof is finished. Let us assume for contradiction $a > 1$, and choose a prime $p \mid a$. Put $q = \prod_{p_i \neq p} p_i^{|t|}$, and $y = (qa/p)x$. We have $ax = \sum_i x_i$ for some $x_i \in G_{p_i}$, hence

$$py = qax = q \sum_i x_i = \begin{cases} qx_i & p = p_i \text{ for some } i, \\ 0 & \text{otherwise.} \end{cases}$$

If $p = p_i$, we have $py = qx_i \in G_p$, hence also $y \in G_p \subseteq \operatorname{rng}(\varphi)$. If $p \neq p_i$ for all i, then $y \in G_p = 0 \subseteq \operatorname{rng}(\varphi)$. In both cases, we obtain $(qa/p)x \in \operatorname{rng}(\varphi)$, hence $a \mid (qa/p)$. This implies $p \mid q$, which contradicts the definition of q. □

Corollary 3.9 *(in $S^1_2(\alpha) + iWPHP(\Sigma^b_1(\alpha))$) If G is a $\Sigma^b_1(\alpha)$ finite abelian group, then there exists $n > 0$ such that $nG = 0$.*

Proof: Let $n = \prod_i p_i^{|t|}$, where $\vec{p}$ and t is as in Theorem 3.8. Then $nx = 0$ for all $x \in G$. □

Corollary 3.10 *(in $S^1_2(\alpha) + iWPHP(PV(\alpha))$) If $+$ is definable by a $PV(\alpha)$-function, then so is $-$.*

Proof: Under the assumption all instances of $iWPHP(\Sigma^b_1(\alpha))$ used above were actually $iWPHP(PV(\alpha))$. If n is as in Corollary 3.9, then $-x = (n-1)x$ is $PV(\alpha)$ by Lemma 3.3. □

The main result of this section is the structure theorem below.

Theorem 3.11 *(in $S^2_2(\alpha) + iWPHP(\Sigma^b_1(\alpha))$) Let G be a $\Sigma^b_1(\alpha)$ finite abelian group. There exists a sequence of prime powers $P = \langle p_i^{e_i} \mid i < k\rangle$ with $e_i > 0$, and a sequence $\langle x_i \mid i < k\rangle$ of elements of G, such that the $\Sigma^b_1(\alpha)$-function*

$$\varphi\colon \bigoplus_{i<k} C(p_i^{e_i}) \to G$$

defined by

$$\varphi(\langle \alpha_i \mid i < k\rangle) = \sum_{i<k} \alpha_i x_i$$

is a group isomorphism. Moreover, P is unique up to permutation of indices.

Remark 3.12 No claim is being made on uniformity of the $\Sigma^b_1(\alpha)$-isomorphism, as the proof will give no nontrivial estimate on the complexity of finding the sequence $\vec{x}$.

Proof: Existence: let us say that $\langle x_i \mid i < k\rangle$ is an *independent sequence* with exponents $\langle m_i \mid i < k\rangle$ if

$$(*) \qquad \forall i < k\, (x_i \in G \wedge m_i > 1 \wedge m_i x_i = 0) \wedge \forall \vec{\alpha} \in \prod_{i<k} m_i \Big(\sum_{i<k} \alpha_i x_i = 0 \to \vec{\alpha} = \vec{0}\Big).$$

Notice that $(*)$ is a $\mathcal{B}(\Sigma^b_1(\alpha)) \subseteq \Sigma^b_2(\alpha)$-formula, as the quantifier $\forall i < k$ is sharply bounded. If $\vec{x}$ is an independent sequence with exponents $\vec{m}$, then the mapping $\varphi\colon \bigoplus_{i<k} C(m_i) \to G$ defined by

$$\varphi(\langle \alpha_i \mid i < k\rangle) = \sum_{i<k} \alpha_i x_i$$

is easily seen to be a homomorphism, and $\ker(\varphi) = 0$, hence φ is injective. As φ is $\Sigma^b_1(\alpha)$, we can apply $iWPHP(\varphi)$, which implies that $\prod_i m_i \le 2t$, where $G \subseteq t$. In particular,

$$k \le \Bigl|\prod_{i<k} m_i\Bigr| \le |t| + 1.$$

We apply the $\Sigma^b_2(\alpha)$-*LMAX* principle to fix the maximal k such that there exists an independent sequence of length k. Then we apply $\Sigma^b_2(\alpha)$-*LMAX* once more to find an independent sequence $\langle x_i \mid i < k\rangle$ with exponents $\langle m_i \mid i < k\rangle$ such that $|\prod_i m_i|$ is maximal.

Claim 1 *Each m_i is a prime power.*

Proof: Assume for contradiction that m_i is not a prime power. By Claim 2 in [10, Ex. 1.13], we can write $m_i = ab$, where $a, b > 1$ are coprime. By Bézout's lemma, we can choose integers u, v such that $ua + vb = 1$. Put $y = uax_i$, $z = vbx_i$. Clearly, $by = 0 = az$. We will show that $\langle y, z, x_j \mid j \ne i\rangle$ is an independent sequence with exponents $\langle b, a, m_j \mid j \ne i\rangle$, contradicting the definition of k.

Let thus $\alpha < b$, $\beta < a$, $\alpha_j < m_j$ be such that $\alpha y + \beta z + \sum_{j\ne i} \alpha_j x_j = 0$. By the definition of y, z, we have

$$(\alpha ua + \beta vb)x_i + \sum_{j\ne i} \alpha_j x_j = 0,$$

thus the independence of $\vec{x}$ implies that $\alpha_j = 0$ for $j \ne i$, and $m_i \mid \alpha ua + \beta vb$. In particular, $a \mid \beta vb$, and as a is coprime to vb, $a \mid \beta$, hence $\beta = 0$. We can show $\alpha = 0$ by a symmetric argument. □ (Claim 1)

We write $m_i = p_i^{e_i}$, where p_i is prime, and define the mapping φ as above.

Claim 2 *φ is surjective.*

Proof: Assume for contradiction that there exists an element $x \in G$ such that $x \notin \operatorname{rng}(\varphi)$. By Lemma 3.5 and a generalization of Lemma 3.4, there exists an $a > 0$ such that $bx \in \operatorname{rng}(\varphi)$ iff $a \mid b$ for any integer b. As $a > 1$, there is a prime $p \mid a$. If $x' = (a/p)x$, then $bx' \in \operatorname{rng}(\varphi)$ iff $p \mid b$, hence we may simply assume that $a = p$ is prime. Write

$$px = \sum_i \beta_i x_i.$$

If i is such that $p \ne p_i$, then m_i is coprime to p, hence there exists u such that $um_i \equiv -\beta_i \pmod p$. Putting $\beta'_i = \beta_i + um_i$, we have $\beta'_i x_i = \beta_i x_i$, and $p \mid \beta'_i$. We may thus replace β_i with β'_i, and assume that

$$p \ne p_i \to p \mid \beta_i$$

for every i. We have

$$px' := p\Bigl(x - \sum_{p\mid\beta_i} \frac{\beta_i}{p} x_i\Bigr) = \sum_{p\nmid\beta_i} \beta_i x_i,$$

and $x' \notin \operatorname{rng}(\varphi)$, hence we may replace x with x'. This means that we can assume that $\beta_i = 0$ whenever $p \mid \beta_i$; putting our constraints together, we have

$$(**) \qquad \beta_i \neq 0 \to p = p_i \wedge p \nmid \beta_i.$$

We need to distinguish two cases.

Case 1: $px = 0$. We will show that $\langle x, x_i \mid i < k\rangle$ is an independent sequence with exponents $\langle p, m_i \mid i < k\rangle$, contradicting the choice of k. Take $\alpha < p$, $\alpha_i < m_i$ such that $\alpha x + \sum_i \alpha_i x_i = 0$. If $\alpha = 0$, then $\vec{\alpha} = \vec{0}$ by the independence of $\vec{x}$. On the other hand, if $\alpha \neq 0$, then there exists u such that $u\alpha \equiv 1 \pmod p$. Then $x = u\alpha x = -\sum_i u\alpha_i x_i$, which contradicts $x \notin \operatorname{rng}(\varphi)$.

Case 2: $px \neq 0$. We can find i_0 such that $\beta_{i_0} \neq 0$, and $e_{i_0} \geq e_i$ for all i such that $\beta_i \neq 0$. In order to simplify the notation, we assume that $i_0 = 0$. As all i that $\beta_i \neq 0$ have $p = p_i$ by $(**)$, we obtain $p^{e_0+1}x = \sum_i p^{e_0}\beta_i x_i = 0$. We claim that $\langle x, x_i \mid i > 0\rangle$ is an independent sequence with exponents $\langle p^{e_0+1}, m_i \mid i > 0\rangle$. The sequence has length k; as $p^{e_0+1} = pm_0$, the length of $\prod_i m_i$ strictly increases, hence we obtain a contradiction with the choice of $\vec{x}$ and $\vec{m}$. So, take $\alpha < p^{e_0+1}$ and $\alpha_i < m_i$ such that $\alpha x + \sum_{i\neq 0}\alpha_i x_i = 0$. Multiplying the equation by p and expanding px we get

$$\alpha\beta_0 x_0 + \sum_{i\neq 0}(\alpha\beta_i + p\alpha_i)x_i = 0.$$

By the independence of $\vec{x}$, we have $p^{e_0} \mid \alpha\beta_0$. As β_0 is coprime to p by $(**)$, we obtain $p^{e_0} \mid \alpha$, and in particular, $p \mid \alpha$. Using the expression of px in term of $\vec{x}$ once again, we have

$$\frac{\alpha}{p}\beta_0 x_0 + \sum_{i\neq 0}\left(\frac{\alpha}{p}\beta_i + \alpha_i\right)x_i = 0.$$

By the independence of $\vec{x}$, we have $p^{e_0} \mid (\alpha/p)\beta_0$, hence $p^{e_0+1} \mid \alpha$, which implies $\alpha = 0$. Then $\vec{\alpha} = \vec{0}$ by the independence of $\vec{x}$. □ (Claim 2)

We recall that φ is an injective homomorphism, hence the two claims imply that φ is an isomorphism of the form required in the theorem.

Uniqueness: assume that

$$\varphi' \colon \bigoplus_i C({p'_i}^{e'_i}) \simeq G$$

is another $\Sigma^b_1(\alpha)$-isomorphism. Let p^e be any prime power. We have

$$\{x \in C(p_i^{e_i}) \mid p^e x = 0\} = \begin{cases} 0 & p_i \neq p, \\ C(p_i^{e_i}) & p_i = p, e_i \leq e, \\ p_i^{e_i - e}C(p_i^e) \simeq C(p_i^e) & p_i = p, e_i > e. \end{cases}$$

It follows that φ induces a $\Sigma^b_1(\alpha)$-bijection

$$\{x \in G \mid p^e x = 0\} \simeq \bigoplus_{p_i = p} C(p^{\min(e,e_i)}) \approx p^{\lambda(p^e)},$$

where $\lambda(p^e) = \sum_{p_i = p} \min(e, e_i)$. Similarly, φ' induces a bijection of the same set and $p^{\lambda'(p^e)}$, thus $\lambda(p^e) = \lambda'(p^e)$ by $iWPHP(\Sigma^b_1(\alpha))$. However, we have

$$\lambda(p^{e+1}) - \lambda(p^e) = |\{i \mid p_i = p, e_i > e\}|,$$

and similarly for λ', hence

$$|\{i \mid p_i = p, e_i = e\}| = 2\lambda(p^e) - \lambda(p^{e+1}) - \lambda(p^{e-1}) = |\{i \mid p'_i = p, e'_i = e\}|.$$

It follows that $p'_i = p_{\pi(i)}$, $e'_i = e_{\pi(i)}$ for some permutation π. □

We can vary the strength of the weak pigeonhole principle needed to prove the theorem depending on the complexity of the representation of the group. We give two examples.

Corollary 3.13 *The structure theorem 3.11 for $\Sigma^b_1(\alpha)$ finite abelian groups $\langle G, +\rangle$ such that $+$ is given by a $PV(\alpha)$-function is provable in $S^2_2(\alpha) + iWPHP(PV(\alpha))$.*

Proof: If $+$ is $PV(\alpha)$, then all instances of $iWPHP$ used in the proofs of Lemma 3.5 and Theorem 3.11 are instances of $iWPHP(PV(\alpha))$. □

Definition 3.14 (in $S^1_2(\alpha)$) A Γ-*definable finite abelian group with nonabsolute equality* is a structure $\langle G, +, \approx\rangle$, where G is a nonempty Γ-definable subset of some t, $+$ is a Γ-definable ternary relation on G, and $\approx$ is a Γ-definable equivalence relation on G, such that

$$\exists w \in G\, {+}(x, y, w),$$
$$x \approx x' \wedge y \approx y' \wedge {+}(x, y, z) \wedge {+}(x', y', z') \to z \approx z'$$

for all $x, x', y, y', z, z' \in G$, and appropriate versions of the axioms of abelian groups hold, e.g., commutativity is expressed as

$${+}(x, y, z) \wedge {+}(y, x, w) \to z \approx w.$$

Example 3.15 Let $\langle G, +\rangle$ be a $\Sigma^b_1(\alpha)$ finite abelian group, and H its $\Sigma^b_1(\alpha)$ subgroup. We can represent the quotient group G/H as a $\Sigma^b_1(\alpha)$ finite abelian group with nonabsolute equality $\langle G, +, \approx\rangle$, where $x \approx y$ iff $x - y \in H$.

Corollary 3.16 *The structure theorem 3.11 for $\Sigma^b_1(\alpha)$-definable finite abelian groups with nonabsolute equality is provable in $S^2_2(\alpha) + mWPHP(\Sigma^b_1(\alpha))$.*

Proof: The proof of Theorem 3.11 works without change, except that now we need to apply the weak pigeonhole principle to multivalued functions. □

We remind the reader that $S^2_2(\alpha) + iWPHP(\Sigma^b_1(\alpha))$ and $S^2_2(\alpha) + mWPHP(\Sigma^b_1(\alpha))$ are contained in $T^2_2(\alpha)$. On the other hand, the structure theorem implies that a finite vector space over $GF(2)$ encoded by α has a basis, and this statement is not provable in $S^2_2(\alpha)$ [13, Cor. 11.3.5]. Thus, some version of the weak pigeonhole principle is indispensable to prove the structure theorem.

The unique representation of finite abelian groups in Theorem 3.11 in terms of cyclic p-groups is known as the *primary decomposition.* There is also another unique representation of finite abelian groups as sums of cyclic groups, known as *invariant factor decomposition.* We will describe it next, we can prove it easily from Theorem 3.11.

Lemma 3.17 (*in* T^0_2) *Let* $n = \prod_{i<k} n_i$*, where* n_i *are pairwise coprime. Then the mapping*

$$\varphi\colon C(n) \to \bigoplus_{i<k} C(n_i)$$

defined by

$$\varphi(\alpha) = \langle \alpha \bmod n_i \mid i < k\rangle$$

is an isomorphism, and its inverse is poly-time computable.

Proof: Easy, cf. Claim 1 in the proof of [10, Ex. 1.13]. □

Theorem 3.18 (*in* $S^2_2(\alpha) + iWPHP(\Sigma^b_1(\alpha))$) *Let* G *be a* $\Sigma^b_1(\alpha)$ *finite abelian group. There exists a unique sequence* $\langle n_i \mid i < k\rangle$ *of natural numbers* $n_i > 1$ *satisfying* $n_{i+1} \mid n_i$ *for every* $i < k$*, such that there exists a* $\Sigma^b_1(\alpha)$*-definable isomorphism*

$$\varphi\colon \bigoplus_{i<k} C(n_i) \simeq G$$

of the same form as in Theorem 3.11*.*

Proof: Existence: consider the isomorphism

$$\bigoplus_i C(p_i^{e_i}) \simeq G$$

from Theorem 3.11. We can collect powers of the same prime together, put each collection in nonincreasing order, and pad it with trivial factors $p_i^0 = 1$ so that all collections have the same length. We obtain a representation

$$\bigoplus_{i<k, j<\ell} C(p_j^{e_{i,j}}) \simeq G,$$

where p_j are distinct primes, and $e_{i,j} \ge e_{i+1,j}$. Put $n_i = \prod_j p_j^{e_{i,j}}$. Clearly $n_{i+1} \mid n_i$, and we have

$$\bigoplus_i C(n_i) \simeq G$$

using Lemma 3.17.

Uniqueness: let

$$\varphi'\colon \bigoplus_i C(n'_i) \simeq G$$

be another such isomorphism. We may arrange the sequences $\vec{n}$, $\vec{n'}$ to have the same length by padding the shorter one with $\vec{1}$. We denote by $o_p(n)$ the maximal $e \le |n|$ such that $p^e \mid n$. Let p^e be any prime power. As in the proof of Theorem 3.11, we can establish

$$\{x \in G \mid p^e x = 0\} \simeq \bigoplus_i C(\gcd(p^e, n_i)) \approx p^{\sum_i \min(e, o_p(n_i))},$$

and conclude

$$(*) \qquad |\{i \mid o_p(n_i) = e\}| = |\{i \mid o_p(n'_i) = e\}|.$$

We observe that the sequence $o_p(n_i)$ is nonincreasing in i, as $n_{i+1} \mid n_i$. We can thus prove $o_p(n_i) = o_p(n'_i)$ by induction on i, using $(*)$. This implies $n_i = n'_i$. $\square$

Remark 3.19 Theorem 3.18 has also variants for $PV(\alpha)$-groups or groups with nonabsolute equality similar to Corollaries 3.13 and 3.16.

4 Fermat's little theorem and Euler's criterion

Definition 4.1 If f is a definable function (possibly with parameters), then $PHP(f)$ states that f is not a bijection of a onto b for any $a \neq b$, i.e.,

$$a \neq b \to \exists x < a\, f(x) \geq b \vee \exists x < x' < a\, f(x) = f(x') \vee \exists y < b \forall x < a\, f(a) \neq b.$$

If Γ is a set of definable functions, $PHP(\Gamma)$ denotes the schema $\{PHP(f) \mid f \in \Gamma\}$.

Theorem 4.2 *$S^2_2 + iWPHP(PV) + PHP(PV)$ proves Fermat's little theorem:*

$$x^p \equiv x \pmod p$$

for every prime p and integer x.

Proof: Let $G = GF(p)^*$ (i.e., the multiplicative group of units of the finite field $GF(p)$ of residues modulo p). By Corollary 3.13, there exists an isomorphism

$$\varphi\colon \bigoplus_{i<k} C(p_i^{e_i}) \to G$$

defined by a PV-function (as "+" of the group, i.e., modular multiplication, is poly-time). Let $n = \prod_i p_i^{e_i}$. Clearly $nx = 0$ (i.e., $x^n = 1$ in multiplicative notation) for every $x \in G$. As φ induces a bijection of n and $p-1$, we must have $n = p-1$ by *PHP*. $\square$

PHP is a rather strong axiom, but in this case it seems unavoidable. If $GF(p)^*$ is cyclic, it is easy to see that Fermat's little theorem is in $S^2_2 + iWPHP(PV)$ *equivalent* to the instance of $PHP(PV)$ used in the proof of Theorem 4.2. In the absence of *PHP*, we see no reason why $GF(p)^*$ could not be isomorphic to, say, $C(p+1)$, in which case Fermat's little theorem fails spectacularly. In view of this discussion, we conjecture that the answer to the following problem is negative.

Question 4.3 *Is Fermat's little theorem provable in S_2?*

Fermat's little theorem can be strengthened to Euler's criterion. Recall that the *Legendre symbol* is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } p \mid a, \end{cases}$$

for any integer a, and an odd prime p. Euler's criterion states that

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$$

for every such a, p. We are going to characterize the relationship of Euler's criterion to Fermat's little theorem in S^1_2, and in particular, we will show that Euler's criterion is provable in $S^2_2 + iWPHP(PV) + PHP(PV)$.

Berarducci and Intrigila [2] have shown multiplicativity of the Legendre symbol

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

in $I\Delta_0 + iWPHP(\Delta_0)$ (their proof also works in $T^0_2 + iWPHP(PV)$, cf. [12]). We will use a different proof to get multiplicativity under a weaker assumption (cf. Lemma 3.5).

Lemma 4.4 *(in T^0_2)If p is an odd prime such that $GF(p)^*$ is a torsion group, then $(\cdot|p)$ is multiplicative.*

Proof: We make a few observations about multiplication in $GF(p)^*$:

Claim 1

(i) *For any x, there are y, z such that $x = yz$ and $y^{2^k} = 1 = z^m$ for some k and odd m. We have $(z|p) = 1$ and $(x|p) = (y|p)$.*

(ii) *If $y^{2^k} = 1$, then either $y = 1$, or $y^{2^\ell} = -1$ for some $\ell < k$.*

(iii) *If $z^{2^k} = -1$ and $y^{2^{k+1}} = 1$, there exists a such that $z^a = y$.*

(iv) *If $y^{2^k} = -1$, then $(y|p) = 1$ if and only if $\exists z\, z^{2^{k+1}} = -1$.*

Proof: (i): We have $x^n = 1$ for some $n > 0$, and we can write $n = 2^k m$ where m is odd. Pick u, v such that $um + v2^k = 1$, and put $y = x^{um}$ and $z = x^{v2^k}$. Then $x = yz$, and $y^{2^k} = 1$, $z^m = 1$. If $m = 2r + 1$, we have $(z^{r+1})^2 = z$, thus $(z|p) = 1$. It follows that $y = w^2$ iff $x = (wz^{r+1})^2$, and symmetrically $x = w^2$ iff $y = (wz^{-(r+1)})^2$, hence $(y|p) = (x|p)$.

(ii) follows immediately from the fact that the only square roots of 1 are ± 1.

(iii): We show by reverse induction on $\ell \le k + 1$ that $\exists a < 2^{k+1}\, y^{2^\ell} = z^a$. The induction step: we assume $y^{2^{\ell+1}} = z^a$ by the induction hypothesis. We have $(-1)^a = z^{a2^k} = y^{2^{k+\ell+1}} = 1$, hence a is even. Thus $y^{2^\ell} = \pm z^{a/2}$, which equals either $z^{a/2}$ or $z^{a/2+2^k}$. As stated, the proof used Σ^b_1-*LIND*; however, we can clearly construct a explicitly by a PV-function, hence T^0_2 suffices.

(iv): If there exists such a z, then $y = z^a$ for some a by (iii). We have $1 = y^{2^{k+1}} = z^{2^{k+1}a} = (-1)^a$, hence a is even, and $y = (z^{a/2})^2$. On the other hand, if $y = z^2$, then $z^{2^{k+1}} = -1$. □ (Claim 1)

We have $(xx'|p) = (x|p)(x'|p)$ whenever $(x|p) = 1$ or $(x'|p) = 1$, as in the proof of (i). Let thus $(x|p) = (x'|p) = -1$, we want to show $(xx'|p) = 1$. We may assume $x^{2^r} = x'^{2^r} = 1$ for some r by (i). We can fix k, k' such that $x^{2^k} = x'^{2^{k'}} = -1$ by (ii). We must have $k = k'$ by (iv). We obtain $(xx')^{2^k} = 1$, hence $xx' = 1$ or $(xx')^{2^\ell} = -1$ for some $\ell < k$ by (ii), which implies $(xx'|p) = 1$ by (iv). □

Lemma 4.5 (*in* S^1_2) *Let G be a $\Sigma^b_1(\alpha)$ finite abelian group such that $nG = 0$ for some $n > 0$, and p be a prime. If $pG = G$, then $G_p = 0$.*

Proof: Write $n = p^e m$, where $p \nmid m$. Let $x \in G$ be such that $p^k x = 0$ for some k. Using $pG = G$ and $\Sigma^b_1(\alpha)$-*LIND*, there exists $y \in G$ such that $p^e y = x$, thus $mx = ny = 0$. As $\gcd(m, p^k) = 1$, we obtain $x = 0$. □

Theorem 4.6 (*in* S^1_2) *For any odd prime p, Euler's criterion*

$$\forall a \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$$

is equivalent to the conjunction of Fermat's little theorem

$$\forall a\ a^p \equiv a \pmod p$$

and the statement

$$\exists a\ a^{(p-1)/2} \equiv -1 \pmod p.$$

Proof: Right-to-left: if $(a|p) = 1$, there exists a b such that $b^2 = a$, thus $a^{(p-1)/2} = b^{p-1} = 1$. If $(a|p) = -1$, we choose a b such that $b^{(p-1)/2} = -1$; then $(b|p) = -1$, thus $(ab|p) = 1$ by Lemma 4.4, hence $(ab)^{(p-1)/2} = 1$, which implies $a^{(p-1)/2} = -1$.

Left-to-right: FLT is clear. If $G = GF(p)^*$, then $-1 \in G_2 \neq 0$, hence $G^2 \neq G$ by Lemma 4.5, i.e., there exists a square nonresidue a. By Euler's criterion, $a^{(p-1)/2} = -1$. □

Theorem 4.7 *$S^2_2 + iWPHP(PV) + PHP(PV)$ proves Euler's criterion.*

Proof: We have Fermat's little theorem by Theorem 4.2. Fix an isomorphism of $GF(p)^*$ and $\bigoplus_{i<k} C(p_i^{e_i})$ by Corollary 3.13, where p_i are primes. We have $p - 1 = \prod_i p_i^{e_i}$ by *PHP*. As $GF(p)^*$ contains only two square roots of 1, only one of the p_i is 2; assume $p_0 = 2$, and put $e = e_0$. Then $(p-1)/2^e$ is an odd integer, and as $C(2^e)$ is cyclic, there exists a $b \in GF(p)^*$ such that $b^{2^{e-1}} = -1$. We have $b^{(p-1)/2} = (-1)^{(p-1)/2^e} = -1$, hence we obtain Euler's criterion by Theorem 4.6. □

In connection to Fermat's little theorem, it is natural to ask

Question 4.8 *Does $S_2 + PHP(PV)$ (or a similar theory) prove that the multiplicative group of $GF(p)$ is cyclic for every prime p?*

Consider an isomorphism

$$\varphi\colon \bigoplus_{i<k} C(p_i^{e_i}) \simeq G = GF(p)^*$$

as in Theorem 4.2. If $p_i \neq p_j$ for every $i \neq j$, then $G \simeq C(n)$ is cyclic by Lemma 3.17, where $n = \prod_i p_i^{e_i}$. If q is a prime, then elements of $C(n)$ satisfying $qx = 0$ form a cyclic subgroup H of order 1 (if $q \nmid n$) or q (if $q \mid n$, in which case $H = (n/q)C(q)$).

On the other hand, if $p_i = p_j$ for some $i \neq j$, we can put $q = p_i$. The element $a = q^{e_i - 1}$ generates a subgroup isomorphic to $C(q)$ in $C(q^{e_i})$, and similarly there is an element $b \in C(q^{e_j})$ generating a subgroup isomorphic to $C(q)$. Then $\{a, b\}$ generates a subgroup isomorphic to $C(q) \oplus C(q)$, all elements of which satisfy $qx = 0$. Lifting the situation to G using φ, we obtain the following dichotomy.

Lemma 4.9 *(in $S^2_2 + iWPHP(PV)$) Let p be a prime, and let G be the multiplicative group of units in $GF(p)$.*

(i) If G is cyclic, then for every prime q, there exists a PV-surjection of q onto the set $\{x \in G \mid x^q = 1\}$.

(ii) If G is not cyclic, there exists a prime q, and a PV-injection of q^2 to $\{x \in G \mid x^q = 1\}$.

□

The usual proof of cyclicity of $GF(p)^*$ relies on the fact that the degree q polynomial $x^q - 1$ can have only q roots in the field $GF(p)$; the latter is proved by induction on the degree of the polynomial. Unfortunately, the intermediate polynomials needed for the induction are not sparse, hence they are exponentially sized objects, and cannot be used in bounded arithmetic (even extended by pigeonhole principles or counting functions). On the other hand, if we could manage to match the roots against the degree using a different counting argument, there is a good chance that a weak pigeonhole principle would suffice because of the large gap given by Lemma 4.9.

Notice that the same principle can be applied to the relationship of Fermat's little theorem to Euler's criterion: assuming the former, the extra condition $\exists a\; a^{(p-1)/2} \equiv -1 \pmod{p}$ from Theorem 4.6 is equivalent to asking the degree $(p-1)/2$ polynomial $x^{(p-1)/2} - 1$ to have less than $p - 1$ roots in $GF(p)$, hence a solution to the degree-vs-roots problem would also answer the following problem:

Question 4.10 *Does Fermat's little theorem imply Euler's criterion over S_2?*

5 Quadratic reciprocity

In this section we prove the quadratic reciprocity theorem (including the supplementary laws) from the modulo-2 counting principle $Count_2$ (cf. [13]). Our proof is loosely based on Gauss' third proof of reciprocity, however we have streamlined the argument so that it only uses counting modulo 2 instead of bounded sums and products, and we made sure that we can construct explicit functions witnessing the parity of the sets we want to count modulo 2.

The basic form of the modulo-2 counting principle (also called the *equipartition principle* in [2]) states that we cannot partition an odd-length interval $2a + 1 = [0, 2a + 1)$ into two-element blocks. We can weaken the principle by representing the partition in a more explicit way. We do so by requiring a function f which assigns to each element of $2a+1$ its partner in its block. Such a function f defines a partition into blocks of size at most two if and only if f is an involution (i.e., $f \circ f = \mathrm{id}$), and the partition has no blocks of size one iff f has no fixpoint. We thus state the counting principle as "every involution on $2a+1$ contains a fixpoint":

Definition 5.1 If f is a function (possibly with parameters), $Count_2(f)$ is the axiom

$$\exists x \leq 2a\, (f(x) > 2a \vee f(f(x)) \neq x \vee f(x) = x).$$

If Γ is a set of definable functions, we define the schema $Count_2(\Gamma) = \{Count_2(f) \mid f \in \Gamma\}$.

Notice that $Count_2(\Delta_0)$ is in $I\Delta_0$ equivalent to the original version of the mod-2 counting (equipartition) principle: given a Δ_0 equivalence relation with two-element blocks, we can easily define the neighbourhood function f by a Δ_0-formula. We will, however, also use the principle for PV-functions in T^0_2, and in this context our version of the principle appears to be genuinely weaker.

Similar mod-4 and mod-8 counting principles were employed by Berarducci and Intrigila [2] to prove the two supplementary laws. Note also that $I\Delta_0 + Count_2(\Delta_0)$ is contained in the two-sorted theory $V^0[2]$.

Definition 5.2 If p is an odd prime and $p \nmid a$, we put

$$\left[\frac{a}{p}\right] = \begin{cases} 0, & a \equiv \square \pmod{p}, \\ 1, & a \not\equiv \square \pmod{p}, \end{cases}$$

so that $(a|p) = (-1)^{[a|p]}$. Unless stated otherwise, all functions are assumed to be defined by PV-functions (i.e., circuits) when we work over T^0_2, and Δ_0-definable when we work over $I\Delta_0$. Residues modulo p are usually taken from $P = [-(p-1)/2, (p-1)/2]$. We also put $P^+ = [1, (p-1)/2]$, $P^- = [-(p-1)/2, 1]$, and $P^+_0 = P^+ \cup \{0\}$. We treat P and friends as sets of residues rather than integers, so that, e.g., the formula $ax \in P^+$ means $(ax \bmod p) \in [1, (p-1)/2]$. We also use x^{-1} to refer to multiplicative inverse modulo p.

We begin with a version of Gauss' Lemma.

Lemma 5.3 *(in T^0_2 or $I\Delta_0$) Let p be an odd prime, and $p \nmid a$. There exists an involution on $P^- \cup \{x \in P^+ \mid ax \in P^+\}$ with $[a|p]$ fixpoints.*

Proof: We define

$$f(x) = \begin{cases} -x, & (x, ax \in P^+ \wedge x^{-1} \in P^-) \vee (x, ax \in P^- \wedge x^{-1} \in P^+), \\ x^{-1}, & x, x^{-1} \in P^-, \\ a^{-1}x^{-1}, & ax, x^{-1} \in P^+. \end{cases}$$

It is easy to see that the three conditions define a partition of $P^- \cup \{x \in P^+ \mid ax \in P^+\}$, and f is an involution on each part. f has no fixpoints in the first part, and one ($x = -1$) in the second part. A fixpoint in the third part is an x such that x^{-1} is a positive square root of a, which is unique if it exists. In total, f has one fixpoint if $[a|p] = 1$, and two if $[a|p] = 0$. In the latter case, we modify f so that the original fixpoints are mapped to each other. $\square$

Definition 5.4 If $X \subseteq t$, and $Y \subseteq s$, we use $X \mathbin{\dot\cup} Y$ to denote disjoint union: if X and Y are disjoint, we may take $X \mathbin{\dot\cup} Y = X \cup Y$; in general, we put

$$X \mathbin{\dot\cup} Y := X \cup \{t + y \mid y \in Y\} \subseteq t + s.$$

If $f\colon X \to Z$ and $g\colon Y \to Z$, then $f \mathbin{\dot\cup} g\colon X \mathbin{\dot\cup} Y \to Z$ is defined in the obvious way.

Lemma 5.5 *(in T^0_2 or $I\Delta_0$) If p and q are distinct odd primes, there exists an involution on $(p+3)(q+3)/4 - 4$ with $[p|q] + [q|p]$ fixpoints.*

Proof: Let $f(x) = \langle x, \lfloor qx/p \rfloor \rangle$. Then f is a bijection

$$f\colon \{x \in P^+ \mid qx \in P^+\} \approx \{\langle x, y\rangle \in P^+_0 \times Q^+_0 \mid 0 < qx - py < p/2\},$$

with left projection as its inverse. Symmetrically, there is an invertible bijection

$$g\colon \{y \in Q^+ \mid py \in Q^+\} \approx \{\langle x, y\rangle \in P^+_0 \times Q^+_0 \mid -q/2 < qx - py < 0\}.$$

By Lemma 5.3, there exists an involution h on

$$(P^- \mathbin{\dot\cup} Q^-) \mathbin{\dot\cup} \{x \in P^+ \mid qx \in P^+\} \mathbin{\dot\cup} \{y \in Q^+ \mid py \in Q^+\}$$

with $[p|q] + [q|p]$ fixpoints, thus $i = (\mathrm{id} \mathbin{\dot\cup} f \mathbin{\dot\cup} g) \circ h \circ (\mathrm{id} \mathbin{\dot\cup} f \mathbin{\dot\cup} g)^{-1}$ is an involution on

$$(P^- \mathbin{\dot\cup} Q^-) \mathbin{\dot\cup} \big\{\langle x, y\rangle \in (P^+_0 \times Q^+_0) \smallsetminus \{\langle 0, 0\rangle\} \mid -q/2 < qx - py < p/2\big\}$$

with $[p|q] + [q|p]$ fixpoints. As

$$q\left(\frac{p-1}{2} - x\right) - p\left(\frac{q-1}{2} - y\right) = \frac{p-q}{2} - (qx - py),$$

the function $j(\langle x, y\rangle) = \langle (p-1)/2 - x, (q-1)/2 - y\rangle$ is an involutive bijection

$$j\colon \{\langle x, y\rangle \in P^+_0 \times Q^+_0 \mid qx - py < -q/2\} \approx \{\langle x, y\rangle \in P^+_0 \times Q^+_0 \mid p/2 < qx - py\}.$$

Therefore $i \mathbin{\dot\cup} j$ is an involution on

$$P^- \mathbin{\dot\cup} Q^- \mathbin{\dot\cup} \big((P^+_0 \times Q^+_0) \smallsetminus \{\langle 0, 0\rangle\}\big) \approx \frac{p-1}{2} + \frac{q-1}{2} + \frac{p+1}{2}\frac{q+1}{2} - 1 = \frac{(p+3)(q+3)}{4} - 4$$

with $[p|q] + [q|p]$ fixpoints. $\square$

Lemma 5.6 *(in T^0_2 or $I\Delta_0$) Let p be an odd prime, and $p \nmid a, b$. There exists an involution on $2(p-1) \dot\cup \{x \in P^+ \mid abx \in P^-\}$ with $[a|p] + [b|p]$ fixpoints.*

Proof: By Lemma 5.3, there exist involutions on

$$P^- \dot\cup \{x \in P^+ \mid a^{-1}x \in P^+\}$$

and

$$P^- \dot\cup \{x \in P^+ \mid bx \in P^+\} \approx P^+ \dot\cup \{x \in P^- \mid bx \in P^-\}$$

with $[a^{-1}|p]$ and $[b|p]$ fixpoints, respectively. Their union f is an involution on

$$\begin{aligned}&(P^+ \cup P^-) \dot\cup \{x \mid x, a^{-1}x \in P^+ \vee x, bx \in P^-\} = \\ &\qquad (p-1) \dot\cup \{x \mid a^{-1}x \in P^+, bx \in P^-\} \dot\cup \{x \mid x, a^{-1}x, bx \in P^+ \vee x, a^{-1}x, bx \in P^-\}.\end{aligned}$$

The function $x \mapsto -x$ is an involutive bijection between the disjoint sets

$$\{x \in P^+ \mid a^{-1}x \in P^- \vee bx \in P^-\} \approx \{x \in P^- \mid a^{-1}x \in P^+ \vee bx \in P^+\},$$

and its union with f is thus an involution on

$$(p-1) \dot\cup \{x \mid a^{-1}x \in P^+, bx \in P^-\} \dot\cup (P^+ \cup P^-) = 2(p-1) \dot\cup \{x \mid a^{-1}x \in P^+, bx \in P^-\}.$$

We may lift it using the function $x \mapsto a^{-1}x$, which is an invertible bijection

$$\{x \mid a^{-1}x \in P^+, bx \in P^-\} \approx \{x \in P^+ \mid abx \in P^-\},$$

to obtain an involution on

$$2(p-1) \dot\cup \{x \in P^+ \mid abx \in P^-\}.$$

The number of fixpoints is $[a^{-1}|p] + [b|p] = [a|p] + [b|p]$, as obviously $(a^{-1}|p) = (a|p)$. $\square$

Theorem 5.7 *$T^0_2 + Count_2(PV)$ and $I\Delta_0 + Count_2(\Delta_0)$ prove the law of quadratic reciprocity*

(1) $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4},$$

the supplementary laws

(2) $$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

(3) $$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

and multiplicativity of the Legendre symbol

(4) $$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),$$

where p, q are distinct odd primes, and a, b are integers.

Proof: (1) follows from Lemma 5.5, as $(p+3)(q+3)/4 - 4 \equiv (p-1)(q-1)/4 \pmod 2$.

(2) is an immediate consequence of Lemma 5.3 for $a = -1$, as $\{x \in P^+ \mid -x \in P^+\} = \varnothing$.

(3): By Lemma 5.3, there exists an involution with $[2|p]$ fixpoints on

$$P^- \cup \{x \in P^+ \mid 2x \in P^+\} \approx \frac{p-1}{2} + \left\lfloor \frac{p}{4} \right\rfloor = p - 1 - \left\lceil \frac{p-1}{4} \right\rceil,$$

thus

$$\left[\frac{2}{p}\right] \equiv \left\lceil \frac{p-1}{4} \right\rceil \equiv \left\{\begin{matrix} 0, & p \equiv \pm 1 \pmod 8 \\ 1, & p \equiv \pm 3 \pmod 8 \end{matrix}\right\} \equiv \frac{(p^2-1)}{8} \pmod 2.$$

(4): The identity holds trivially if p divides a or b, thus assume $p \nmid a, b$. By Lemmas 5.3 and 5.6, there exists an involution on $3(p-1)$ with $[a|p] + [b|p] + [ab|p]$ fixpoints, thus $[a|p] + [b|p] \equiv [ab|p] \pmod 2$. □

We remark that the proof of Lagrange's four-square theorem in $I\Delta_0 + iWPHP(I\Delta_0)$ by Berarducci and Intrigila [2] only used multiplicativity of the Legendre symbol (apart from $I\Delta_0$). Consequently, Lagrange's four-square theorem is also provable in $I\Delta_0 + Count_2(\Delta_0)$.

Recall that the *Jacobi symbol* $(a|n)$ is defined for any integer a and an odd natural number n by

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right),$$

where

$$n = \prod_i p_i$$

is a prime factorization of n. We can introduce it in bounded arithmetic as follows.

We assume that we have fixed an efficient sequence coding function such that

$$|w| = O\Big(\mathrm{lh}(w) + \sum_{i<\mathrm{lh}(w)} |(w)_i|\Big)$$

for any sequence w. In particular, there is an L_{PA}-term $s(n)$ such that $w \le s(n)$ for every sequence w such that $(w)_i > 1$ for every $i < \mathrm{lh}(w)$, and $n = \prod_{i<\mathrm{lh}(w)} (w)_i$. (Recall that bounded products of natural numbers are Δ_0-definable in $I\Delta_0$ by Berarducci and D'Aquino [1].) Then an easy Δ_0-induction on n shows that

$$\exists p \le s(n) \left(Seq(p) \wedge \forall i < \mathrm{lh}(p)\, Prime((p)_i) \wedge \prod_{i<\mathrm{lh}(p)} (p)_i = n \right),$$

and furthermore p is unique up to permutation of indices. Then we can define the Jacobi symbol by the Δ_0-formula

$$\begin{aligned} \left(\frac{a}{n}\right) = \varepsilon \Leftrightarrow \exists p, w \le s(n) \Bigg(& Seq(p) \wedge Seq(w) \wedge \mathrm{lh}(p) = \mathrm{lh}(w) \\ & \wedge \forall i < \mathrm{lh}(p) \left(Prime((p)_i) \wedge (w)_i = \left(\frac{a}{(p)_i}\right) \right) \wedge n = \prod_{i<\mathrm{lh}(p)} (p)_i \wedge \varepsilon = \prod_{i<\mathrm{lh}(w)} (w)_i \Bigg). \end{aligned}$$

Note that the product $\prod_{i<\mathrm{lh}(w)}(w)_i$ may involve negative integers; however, it has logarithmic length, hence it can be easily evaluated by counting the number of minus signs in w. It readily follows that $I\Delta_0$ proves the existence and uniqueness of $(a|n)$.

In the case of S^1_2, we proceed in a similar way. Prime factorization of natural numbers is provable in S^1_2 by Jeřábek [10]. Given a sequence p of primes such that $n = \prod_i (p)_i$, we can define the sequence w such that $(w)_i = (a|(p)_i)$ using Σ^b_1-comprehension, as the Legendre symbol is $\mathcal{B}(\Sigma^b_1)$-definable. Then it is easy to see that the above formula gives a provably total Σ^b_2-definition of the Jacobi symbol in S^1_2.

Theorem 5.8 *The Jacobi symbol has a provably total Σ^b_2-definition in S^1_2, and a Δ_0-definition in $I\Delta_0$. For any integers a, b, and odd positive m, n, $S^1_2 + Count_2(PV)$ and $I\Delta_0 + Count_2(\Delta_0)$ prove*

$$\begin{aligned}
a \equiv b \pmod{n} \to \left(\frac{a}{n}\right) &= \left(\frac{b}{n}\right), \\
\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) &= \left(\frac{ab}{n}\right), \\
\left(\frac{a}{n}\right)\left(\frac{a}{m}\right) &= \left(\frac{a}{nm}\right), \\
\gcd(a, n) \neq 1 \leftrightarrow \left(\frac{a}{n}\right) &= 0, \\
\left(\frac{n}{m}\right) &= \left(\frac{m}{n}\right)(-1)^{(n-1)(m-1)/4}, \\
\left(\frac{-1}{n}\right) &= (-1)^{(n-1)/2}, \\
\left(\frac{2}{n}\right) &= (-1)^{(n^2-1)/8}, \\
n \equiv m \pmod{4a} \to \left(\frac{a}{n}\right) &= \left(\frac{a}{m}\right).
\end{aligned}$$

Proof: We will show the reciprocity law, the other properties can be proved easily using a similar strategy. If $\gcd(n, m) \neq 1$ then $(n|m) = (m|n) = 0$, hence we may assume $\gcd(n, m) = 1$. Pick a sequence p of primes such that $n = \prod_i (p)_i$.

Assume first that $m = q$ is prime. Using Σ^b_1-comprehension (in the case of S^1_2) or Δ_0-comprehension (in the case of $I\Delta_0$), we find sequences e and w such that $(e)_i = ((p)_i|q)$, $(w)_i = (q|(p)_i)$. Using Theorem 5.7, we have

$$\left(\frac{n}{q}\right)\left(\frac{q}{n}\right) = \prod_i (e)_i \prod_i (w)_i = \prod_i (-1)^{\frac{(q-1)((p)_i-1)}{4}} = (-1)^{\frac{q-1}{2}\sum_i \frac{(p)_i-1}{2}} = (-1)^{\frac{q-1}{2}\frac{n-1}{2}},$$

as $\sum_{i<k} \frac{1}{2}((p)_i - 1) \equiv \frac{1}{2}\big(\prod_{i<k}(p)_i - 1\big) \pmod 2$ by induction on k.

In general, we fix a sequence q of primes such that $m = \prod_j (q)_j$. As above, we find a sequence w such that $(w)_j = (n|(q)_j)$. In the case of $I\Delta_0$, we find a sequence e such that $(e)_j = ((q)_j|n)$ in the same way. In the case of S^1_2, we cannot do it directly, as $((q)_j|n)$ is only

```
   input: integer a, odd positive b
1  r ← 1
2  if a < 0 then:
3      a ← −a
4      r ← −r if b ≡ −1 (mod 4)
5  while a > 0 do:
6      while a is even do:
7          a ← a/2
8          r ← −r if b ≡ ±3 (mod 8)
9      if a < b then:
10         ⟨a, b⟩ ← ⟨b, a⟩
11         r ← −r if a ≡ b ≡ −1 (mod 4)
12     a ← a − b
13 if b > 1 then output 0 else output r
```

Figure 1: An algorithm for the Jacobi symbol

Σ^b_2. However, we can use Σ^b_1-comprehension to find a sequence s of length $\mathrm{lh}(p)\,\mathrm{lh}(q)$ such that $(s)_{i,j} = ((q)_j|(p)_i)$, and then $(e)_j = \prod_i (s)_{i,j}$ is constructible by a PV-function from s. Then we compute

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_j (w)_j \prod_j (e)_j = \prod_j (-1)^{\frac{(n-1)((q)_j-1)}{4}} = (-1)^{\frac{n-1}{2}\sum_j \frac{(q)_j-1}{2}} = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$$

as before. □

Theorem 5.9 *S^1_2 + $Count_2(PV)$ proves that the Jacobi symbol is polynomial-time computable.*

Proof: Consider a PV-function formalizing the standard algorithm for computing $(a|b)$ (see Figure 1). As two odd numbers are subtracted on line 12, a is even on line 5 in every but possibly the first iteration of the outer loop, in which case the division on line 7 is executed at least once. It follows that the total number of iterations is bounded by $|a| + |b|$, and the algorithm is polynomial-time.

Let $\langle a_i, b_i, r_i \mid i \le k\rangle$ be the sequence of values of a, b, and r during the execution of the algorithm. We find a prime factorization of $\prod_i b_i$, and use it to compute a sequence $p = \langle p_{i,j} \mid i < k, j < d(i)\rangle$ of primes such that $b_i = \prod_{j<d(i)} p_{i,j}$ for every i. Using Σ^b_1-comprehension, there is a sequence $w = \langle w_{i,j} \mid i < k, j < d(i)\rangle$ such that $w_{i,j} = (a_i|p_{i,j})$. Then we can compute the sequence $v = \langle v_i \mid i < k\rangle$ by $v_i = \prod_{j<d(i)} w_{i,j}$, so that $v_i = (a_i|b_i)$. Put $e = (a|b)$. Armed with v, we can prove $e = r_i v_i$ by induction on $i \le k$ using Theorem 5.8, which implies that the algorithm gives the correct output. □

Acknowledgement

I would like to thank Phuong Nguyen and Alan Woods for useful suggestions and comments.

References

[1] Alessandro Berarducci and Paola D'Aquino, Δ_0-*complexity of the relation* $y = \prod_{i \le n} F(i)$, Annals of Pure and Applied Logic 75 (1995), no. 1–2, pp. 49–56.

[2] Alessandro Berarducci and Benedetto Intrigila, *Combinatorial principles in elementary number theory*, Annals of Pure and Applied Logic 55 (1991), no. 1, pp. 35–50.

[3] Samuel R. Buss, *Bounded arithmetic*, Bibliopolis, Naples, 1986, revision of 1985 Princeton University Ph.D. thesis.

[4] Alan Cobham, *The intrinsic computational difficulty of functions*, in: Proceedings of the 2nd International Congress of Logic, Methodology and Philosophy of Science (Y. Bar-Hillel, ed.), North–Holland, 1965, pp. 24–30.

[5] Stephen A. Cook, *Feasibly constructive proofs and the propositional calculus*, in: Proceedings of the 7th Annual ACM Symposium on Theory of Computing, 1975, pp. 83–97.

[6] Stephen A. Cook and Phuong Nguyen, *Logical foundations of proof complexity*, book in preparation, `http://www.cs.toronto.edu/~sacook/homepage/book/`.

[7] Charalambos Cornaros, *On Grzegorczyk induction*, Annals of Pure and Applied Logic 74 (1995), no. 1, pp. 1–21.

[8] Charalambos Cornaros and Costas Dimitracopoulos, *The prime number theorem and fragments of* PA, Archive for Mathematical Logic 33 (1994), no. 4, pp. 265–281.

[9] Paola D'Aquino and Angus Macintyre, *Quadratic forms in models of* $I\Delta_0 + \Omega_1$*. I*, Annals of Pure and Applied Logic 148 (2007), pp. 31–48.

[10] Emil Jeřábek, *Dual weak pigeonhole principle, Boolean complexity, and derandomization*, Annals of Pure and Applied Logic 129 (2004), pp. 1–37.

[11] ———, *The strength of sharply bounded induction*, Mathematical Logic Quarterly 52 (2006), no. 6, pp. 613–624.

[12] ———, *On independence of variants of the weak pigeonhole principle*, Journal of Logic and Computation 17 (2007), no. 3, pp. 587–604.

[13] Jan Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications vol. 60, Cambridge University Press, 1995.

[14] Jan Krajíček and Pavel Pudlák, *Some consequences of cryptographical conjectures for* S^1_2 *and EF*, Information and Computation 140 (1998), no. 1, pp. 82–94.

[15] Saunders Mac Lane and Garrett Birkhoff, *Algebra*, third ed., American Mathematical Society, Providence, 1999.

[16] Alexis Maciel, Toniann Pitassi, and Alan R. Woods, *A new proof of the weak pigeonhole principle*, Journal of Computer and System Sciences 64 (2002), no. 4, pp. 843–872.

[17] Phuong Nguyen, *Bounded reverse mathematics*, Ph.D. thesis, University of Toronto, 2008.

[18] Rohit Parikh, *Existence and feasibility in arithmetic*, Journal of Symbolic Logic 36 (1971), no. 3, pp. 494–508.

[19] Jeff B. Paris, Alex J. Wilkie, and Alan R. Woods, *Provability of the pigeonhole principle and the existence of infinitely many primes*, Journal of Symbolic Logic 53 (1988), no. 4, pp. 1235–1244.

[20] Stephen G. Simpson, *Subsystems of second order arithmetic*, Perspectives in Mathematical Logic, Springer, Berlin, 1999.