When expanding out the product, only the terms $1 \cdot 1 \cdot 1 \cdots 1$ and $(\frac{t_1}{q}) \cdot (\frac{-t_2}{q}) \cdot (\frac{t_3}{q}) \cdots (\frac{t_p}{q})$ should be taken into consideration; the other terms disappear because Legendre symbols sum up to zero, i.e., $\sum_{t \in \mathbb{Z}/(q)} (\frac{t}{q}) = 0$. Therefore, the above expression simplifies to

$$q^{p-1} + \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \sum_{t_1 + \cdots + t_p = 1} \left(\frac{t_1 t_2 t_3 \cdots t_p}{q}\right).$$

Now modulo $p$, the latter sum almost completely vanishes, since the tuples $(t_1, \ldots, t_p)$ satisfying $t_1 + \cdots + t_p = 1$ with not all $t_i$ equal to $p^{-1}$ can be collected in groups of size $p$ by cyclic permutation. Note that $p$ is indeed a multiplicative unit in $\mathbb{Z}/(q)$. We thus obtain

$$N_p \equiv 1 + \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p^{-p}}{q}\right) \equiv 1 + \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \mod p.$$

The last congruence follows from the well-known formula $(\frac{a}{q}) \equiv a^{\frac{q-1}{2}} \mod q$ (which in the case $a = \pm 1$ becomes an exact equality) and the obvious observation that $p^{-p}$ is a square in $\mathbb{Z}/(q)$ if and only if $p$ is a square in $\mathbb{Z}/(q)$.

Comparing our two formulas for $N_p \pmod p$, the reciprocity law follows.

**ACKNOWLEDGMENTS.** I would like to thank the Fund for Scientific Research–Flanders (FWO–Vlaanderen) for its financial support.

**REFERENCES**


**Department of Mathematics, K.U. Leuven, Celestijnenlaan 200B, B-3001 Leuven (Heverlee), Belgium**
wouter.castryck@wis.kuleuven.be

---

**Infinite Divisibility of GCD Matrices**

**Rajendra Bhatia and J. A. Dias da Silva**

In 1876 H. J. S. Smith [8] showed that the determinant of the $n \times n$ matrix $A$ whose entries are given by $a_{ij} = (i, j)$, where $(i, j)$ stands for the greatest common divisor (GCD) of the positive integers $i$ and $j$, has an interesting formula:

$$\det A = \varphi(1) \varphi(2) \cdots \varphi(n).$$

Here $\varphi$ represents the Euler totient function. Such matrices, and their generalisations, have since been studied by several authors. See, for example, the references [5, 7].
Let \( \{x_1, \ldots, x_n\} \) be any set of distinct positive integers. The GCD matrix \( G \) associated with this set is the \( n \times n \) matrix whose entries are \( g_{ij} = (x_i, x_j) \). One striking property of this matrix is that it is infinitely divisible, which, by definition, means that for every nonnegative real number \( r \), the matrix \( g_{ij}^r \) is positive semidefinite. A proof of this fact was given by K. Bourque and S. Ligh [4], and is reproduced in the article [1] where several other examples of infinitely divisible matrices are discussed. In this note we present a simple proof that derives this property of GCD matrices from the positive semidefiniteness of the closely related min matrices.

Let \( \lambda_1, \ldots, \lambda_n \) be nonnegative real numbers. The min matrix \( M \) associated with them is the matrix with entries \( m_{ij} = \lambda_i \land \lambda_j = \min(\lambda_i, \lambda_j) \). It is very easy to see that this matrix is positive semidefinite. One proof of this is indicated in Exercise 18, p. 401 of [6]. Another simple proof, which also shows \( M \) is infinitely divisible, is presented in [1].

If \( A = [a_{ij}] \) and \( B = [b_{ij}] \) are any two \( n \times n \) matrices, we denote by \( A \odot B \) their Hadamard product, or the entrywise product \( [a_{ij} \cdot b_{ij}] \). If \( a_{ij} \geq 0 \) for all \( i, j \), and \( r \) is any nonnegative real number, we denote by \( A^r \) the Hadamard power \( [a_{ij}^r] \). If \( A \) and \( B \) are positive semidefinite, then by a well-known theorem of Schur, the product \( A \odot B \) is positive semidefinite, and so are the powers \( A^m \) for \( m = 1, 2, \ldots \).

Now suppose \( x_1, \ldots, x_n \) are (distinct) positive integers. Let \( p_1, \ldots, p_k \) be prime numbers such that

\[
x_i = p_1^{m_{i1}} p_2^{m_{i2}} \cdots p_k^{m_{ik}}, \quad 1 \leq i \leq n.
\]

Then we have

\[
(x_i, x_j) = p_1^{m_{ij}^1} p_2^{m_{ij}^2} \cdots p_k^{m_{ij}^k}.
\]

For \( 1 \leq \ell \leq k \), let \( P_\ell \) be the matrix whose \( i, j \) entry is equal to \( p_\ell^{m_{i\ell}^j} \). Then the GCD matrix \( G \) with entries \( g_{ij} = (x_i, x_j) \) can be expressed as a Hadamard product

\[
G = P_1 \odot P_2 \odot \cdots \odot P_k.
\]

If we show that each of the matrices \( P_\ell \) is infinitely divisible, then by Schur’s theorem \( G \) will also be infinitely divisible.

Suppose \( A = [a_{ij}] \) is any matrix with nonnegative entries and \( q \) is any real number greater than 1. Let \( E \) be the matrix that has all its entries equal to 1. Then the matrix \( [q^{a_{ij}}] \) can be represented by the series

\[
E + (\log q)A + \frac{(\log q)^2}{2!} A^2 + \frac{(\log q)^3}{3!} A^3 + \cdots.
\]

If \( A \) is positive semidefinite, then each of these summands, and hence their sum, is positive semidefinite.

This observation, together with the fact that min matrices are positive semidefinite, shows that for each \( r \geq 0 \) and each \( \ell \) satisfying \( 1 \leq \ell \leq k \) the matrix

\[
P_\ell^r = \left[ p_\ell^{r(m_{i\ell}^j)} \right]
\]

is positive semidefinite. In other words, \( P_\ell \) is infinitely divisible as we claimed.
Closely related to the GCD matrix is the Hadamard reciprocal of the LCM matrix. Let $\ell_{ij}$ be the least common multiple of the positive integers $x_i$ and $x_j$. Since

$$\frac{1}{\ell_{ij}} = \frac{(x_i, x_j)}{x_i x_j},$$

the matrix $L$ whose $i, j$ entry is $1/\ell_{ij}$ can be expressed as $XG_X$, where $X$ is the diagonal matrix whose diagonal entries are the positive numbers $1/x_i$, $1 \leq i \leq n$. Hence the infinite divisibility of $G$ implies the same property for $L$.

Infinitely divisible matrices arise in several different contexts, and are discussed in [1], [2], and [3].

REFERENCES


Indian Statistical Institute, New Delhi - 110 016, India
rbh@isid.ac.in

Department of Mathematics, University of Lisbon, 1749-016, Lisbon, Portugal
japsilva@fc.ul.pt

Borsuk-Ulam Implies Brouwer: A Direct Construction Revisited

Alexey Yu. Volovikov

1. INTRODUCTION. In the MONTHLY article [3] Su showed by a direct construction that the Borsuk-Ulam theorem implies the Brouwer fixed point theorem. Su used a cubical ball in his proof. In [4] the author using a simple construction for a Euclidean ball showed that the multi-valued generalization of the Borsuk-Ulam theorem implies the multi-valued generalization of the Brouwer theorem, in particular the Kakutani theorem.

The purpose of this note is to present a very simple and short proof by a direct construction that the Schauder fixed point theorem follows from the generalization of the Borsuk-Ulam theorem for Banach spaces due to B. Gel’man [1]. In the finite-dimensional case it turns into the proof that the Borsuk-Ulam theorem implies the Brouwer theorem. In Section 4, a class of similar constructions is developed and in Section 5 we show that Su’s construction (considered for an arbitrary ball) can be used in this argument as well.

We refer the reader to the paper of Su [3] for historical and other comments.