===== **RESEARCH ARTICLES** =====

# Number-Theory Renormalization of Vacuum Energy

## M. G. Ivanov[1*], V. A. Dudchenko[2**], and V. V. Naumov[1***]

*[1]Moscow Institute of Physics and Technology,
Institutskiy Pereulok 9, Dolgoprudny, 141701, Russia*

*[2]Vernadsky Institute of Geochemistry and Analytical Chemistry
of the Russian Academy of Sciences, Kosygina 19, Moscow, 117975, Russia*

**Abstract**—For QFT on a lattice of dimension $d \geqslant 3$, the vacuum energy (both bosonic and fermionic) is zero if the Hamiltonian is a function of the square of the momentum, and the calculation of the vacuum energy is performed in the ring of residue classes modulo $N$. This fact is related to a problem from number theory about the number of ways to represent a number as a sum of $d$ squares in the ring of residue classes modulo $N$.

## 1. INTRODUCTION

In most models of quantum field theory (QFT), the problem of renormalization of the vacuum energy [1] arises. We assume that the problem may be related to the uncritical use of real numbers and operations on them in QFT. The possibility of using other numerical systems in QFT was raised in the monograph [2], in which $p$-adic numbers from the methods of number theory were transferred to mathematical physics. The role of number theory in physics was discussed in the paper [3].

We are considering QFT on the lattice. But we do not consider the transition from a continuous space to a lattice using difference schemes. Instead, we build a theory on a lattice using arithmetic operations in the ring $\mathbb{Z}(N)$ of residue classes modulo $N$, assuming that such arithmetic is native for this lattice. In this approach the renormalization of the vacuum energy occurs naturally for a wide class of models under consideration.

Initially, the problem was set (M.I.) to study the vacuum energy for the dispersion relation $E(\mathbf{p}) = \sqrt{\mathbf{p}^2 + m^2}$ with different definitions of square root in the ring $\mathbb{Z}(N)$. Numerical calculation (V.N.) showed that regardless of the method used to define the lattice analogue of the positive branch of the square root, the vacuum energy is zero at any $N$ with the dimension of the space $d \geqslant 3$. After that, the multiplicities of various values of $\mathbf{p}^2$ in the ring $\mathbb{Z}(N)$ were numerically calculated depending on $N$ and the dimension of the space $d$ (V.N.), it turned out that all multiplicities are divisible by $N$, for arbitrary $N$ if $d \geqslant 3$, and also if $N = 2^n$ and $d \geqslant 2$. This means that all multiplicities of different values of $\mathbf{p}^2$ are zero modulo $N$, and all values of $\mathbf{p}^2 \in \mathbb{Z}(N)$ contribute zero to the vacuum energy. The corresponding theorem is formulated and proved in this paper.

*E-mail: `ivanov.mg@mipt.ru`
**E-mail: `dudchenko.va@phystech.edu`
***E-mail: `naumov.vv@phystech.edu`

## 2. THEOREM ON NUMBER-THEORY RENORMALIZATION

We consider a bosonic quantum field theory on a lattice $\mathbb{Z}^d(N)$ with a Hamiltonian of the form

$$\hat{H}_b = \sum_{\mathbf{p}\in\mathbb{Z}^d(N),\,\mathbf{p}^2\in D} E(\mathbf{p}^2)\left(2\hat{b}^\dagger_\mathbf{p}\hat{b}_\mathbf{p} + 1\right), \tag{2.1}$$

$$\mathbf{p}^2 = \sum_{k=1}^d p_k^2 \in \mathbb{Z}(N), \quad E : D \to \mathbb{Z}(N), \quad D \subset \mathbb{Z}(N), \quad [\hat{b}_{\mathbf{p_1}}, \hat{b}^\dagger_{\mathbf{p_2}}] = \delta_{\mathbf{p_1 p_2}}\,\hat{1}.$$

We believe permissible $\mathbf{p} \in \mathbb{Z}^d(N)$ iff $\mathbf{p}^2 \in D$.

Hereafter $\mathbb{Z}(N)$ is the ring of residue classes modulo $N$. Usually we will use a representation of the form $\mathbb{Z}(N) = \{0, 1, 2, \ldots, N-1\}$.

We will need the operation of *division with remainder*:

$$a \mod N \text{ is the remainder of the division of } a \text{ by } N. \tag{2.2}$$

For example

$$7 \mod 5 = 2, \quad -3 \mod 5 = 2.$$

We will also need *congruence modulo $N$*:

$$a \equiv b \,(\mathrm{mod}\, N) \;\Leftrightarrow\; a \mod N = b \mod N \text{ means } a \text{ and } b \text{ are congruent modulo } N. \tag{2.3}$$

These operations are useful in constructing a proof by mathematical induction with different values of $N$. In the formulating of the results (with a fixed $N$), we can avoid division with remainder and congruence, simply assuming that all operations are performed in the ring $\mathbb{Z}(N)$.

The vacuum energy is the sum of the zero oscillation energies for all permissible values of the momentum and has the form

$$\mathcal{E}_{vac\,b} = \mathcal{E} = \sum_{\mathbf{p}\in\mathbb{Z}^d(N),\,\mathbf{p}^2\in D} E(\mathbf{p}^2) \in \mathbb{Z}(N).$$

Let us also consider a fermionic quantum field theory on the lattice $\mathbb{Z}^d(N)$ with a Hamiltonian of the form

$$\hat{H}_f = \sum_{\mathbf{p}\in\mathbb{Z}^d(N),\,\mathbf{p}^2\in D} E(\mathbf{p}^2)\left(\hat{a}^\dagger_{\mathbf{p}+}\hat{a}_{\mathbf{p}+} - \hat{a}^\dagger_{\mathbf{p}-}\hat{a}_{\mathbf{p}-}\right), \tag{2.4}$$

$$\mathbf{p}^2 = \sum_{k=1}^d p_k^2 \in \mathbb{Z}(N), \quad E : D \to \mathbb{Z}(N), \quad D \subset \mathbb{Z}(N), \quad [\hat{a}_{\mathbf{p_1}\sigma_1}, \hat{a}^\dagger_{\mathbf{p_2}\sigma_2}]_+ = \delta_{\mathbf{p_1 p_2}}\,\delta_{\sigma_1\sigma_2}\,\hat{1}.$$

The vacuum energy is the sum of the negative energies of all the fermions of the Dirac Sea (for all permissible values of momentum) and has the form

$$\mathcal{E}_{vac\,f} = -\mathcal{E} = -\sum_{\mathbf{p}\in\mathbb{Z}^d(N),\,\mathbf{p}^2\in D} E(\mathbf{p}^2) \in \mathbb{Z}(N). \tag{2.5}$$

For both bosons and fermions, we have limited ourselves to the case of one polarization, the case of an arbitrary number of polarizations can be considered completely similarly.

Since $\mathbf{p}^2 \in \mathbb{Z}(N)$, the value of $\mathcal{E}$ can be calculated as follows

$$\mathcal{E} = \sum_{k\in D\subset\mathbb{Z}(N)} c(k)\,E(k) \in \mathbb{Z}(N). \tag{2.6}$$

The multiplicity $c(k)$ is

$$c(k) = c_{Nd}(k) = \left(\text{the number of nodes } \mathbf{p} \text{ of the lattice } \mathbb{Z}^d(N) \text{ such that } \mathbf{p}^2 \equiv k \,(\mathrm{mod}\, N)\right). \tag{2.7}$$

**Theorem.** *For an arbitrary $N$ with $d \geqslant 3$, and for $N = 2^n$ with $d \geqslant 2$*

$$\forall k \in \mathbb{Z}(N) \quad c_{Nd}(k) \equiv 0 \ (\mathrm{mod} \ N). \tag{2.8}$$

The proof of the Theorem is given in the Appendix.

Note that if the theorem is proved for some $N$ and $d$, then for a given $N$ for all $d_1 > d$, the theorem also holds.

### 2.1. The Overview of the Theorem Proof

The proof of the Theorem is given in the Appendices A−G.

The Appendices A−D (V.D.) prove the Theorem for $N = p^m$, where $p$ is an odd prime number. These Appendices use the generating functions of the form (B.1)

$$f_N^d(\tau) = \sum_{k \in \mathbb{Z}(N)} c_{Nd}(k) \, \tau^k$$

and the Legendre symbol (A.2). The formalism used is convenient for arithmetic in the field $\mathbb{Z}(p)$, where $p$ is an odd prime number.

The Appendix A contains the derivation of the properties of quadratic congruences.

The Appendix B contains the derivation of the properties of generating functions.

The Appendix C contains the proof of the Theorem and derivation of the generating functions in the case $N = p$.

The Appendix D contains the proof by induction $(N = p^{m-1} \to N = p^m)$ of the Theorem and derivation of the generating functions in the case $N = p^m$.

The Appendices E−G (V.N.) prove the Theorem for an arbitrary $N$ if the Theorem is proven for odd prime $N$. The idea of the proof is induction transition from the cases $N = M$ and $N = K$ to the case $N = MK$ $(N = M, N = K \to N = MK)$.

The Appendix E contains the definitions of sets and functions used in the proof.

The Appendix F contains the simple Lemmas, which descibe the properties of multiplicities under different transformations of lattices: increasing and decrasing of the size of momentum lattice, stretching and shift of lattice, summation and substraction of lattices, etc.

The Appendix G contains the proof itself.

The Appendix G.1 contains the proof by induction $(N = p^{m-2}, N = p^{m-1} \to N = p^m)$ of the Theorem in the case $N = p^m$, where $p$ is odd prime number. (It partially reproduces the result of the Appendix C by the other method.)

The Appendix G.2 contains the proof by induction $(N = 2^{m-3}, N = 2^{m-2}, N = 2^{m-1} \to N = 2^m)$ of the Theorem in the case $N = 2^m$.

The Appendix G.3 contains the proof by induction $(N = \prod_{i=1}^{n-1} p_i^{m_i} \to N = \prod_{i=1}^{n} p_i^{m_i}, p_i$ are prime$)$ of the Theorem for composite $N$, which is not power of prime.

## 2.2. The Applications of the Theorem

When the conditions of the Theorem hold (for an arbitrary $N$ at $d \geqslant 3$, and for $N = 2^n$ at $d \geqslant 2$) for an arbitrary function $E : D \to \mathbb{Z}(N)$ the vacuum energy calculated in the ring of residue classes $\mathbb{Z}(N)$ is zero:

$$\mathcal{E} \equiv 0 \, (\mathrm{mod}\, N). \tag{2.9}$$

The Hamiltonians (2.1) and (2.4), for which the vacuum energy renormalization is obtained, look like Hamiltonians for free fields. However, they can be considered as diagonalized Hamiltonians of the theory with interaction. In this case, the function $E(\mathbf{p}^2)$ can be of arbitrary form, for example: $\mathbf{p}^2$ (field of non-relativistic particles), $\sqrt{\mathbf{p}^2 + m^2}$ (the field of relativistic particles), or even $(\mathbf{p}^2)^2$. If the theory is invariant with respect to shifts, then the momentum $\mathbf{p}$ will number possible excitations. If in the limit of large $N$ the theory becomes isotropic, the excitation energy can depend only on $\mathbf{p}^2$. Thus, vacuum energy renormalization takes place for a wide class of physically meaningful Hamiltonians.

More general Hamiltonian with zero vacuum energy in field $\mathbb{Z}(N)$ has the form

$$\hat{H}_g = \sum_{\mathbf{p} \in \mathbb{Z}^d(N), \mathbf{p}^2 \in D} \hat{h}_{\mathbf{p}}, \qquad d \geqslant 3 \text{ or } d = 2,\ N = 2^2, \tag{2.10}$$

$$[\hat{h}_{\mathbf{p}_1}, \hat{h}_{\mathbf{p}_2}] = 0, \quad \mathbf{p}_1, \mathbf{p}_2 \in \mathbb{Z}^d(N),$$

where the spectra of Hamiltonians $\hat{h}_{\mathbf{p}}$ has the form

$$E : (\mathbf{p}^2, \sigma) \mapsto E(\mathbf{p}^2, \sigma) \in \mathbb{Z}(N), \tag{2.11}$$

$\sigma \in \Sigma(k)$ is multi-index, which numerates energy levels for fixed $\mathbf{p}^2 = k \in D \subset \mathbb{Z}(N)$. To define vacuum energy field one has to choose an arbitrary linear order in the ring $\mathbb{Z}(N)$.

$$\mathcal{E}_{vac} = \sum_{k \in D \subset \mathbb{Z}(N)} c(k) \sum_{\sigma_0 \in \Sigma_0(k) \subset \Sigma(k)} E(k, \sigma_0) \equiv 0 \, (\mathrm{mod}\, N), \tag{2.12}$$

where $\Sigma_0(k)$ is defined by following condition

$$E(k, \sigma_0)|_{\sigma_0 \in \Sigma_0(k)} = \min_{\sigma \in \Sigma(k)} E(k, \sigma), \text{ or } E(k, \sigma_0)|_{\sigma_0 \in \Sigma_0(k)} < 0.$$

The Hamiltonians of the form (2.10) describe a wide range of interacting lattice QFTs.

## 3. CONCLUSION

In comparison with the standard lattice QFT, what is new in our approach is that not only the momentum components, but also the energy run through discrete values on the finite lattice, and both the momentum projections and the energy are considered as elements of the ring of residue classes $\mathbb{Z}(N)$. This automatically implies that spatial coordinates and time take values on the inverse lattice $\Delta x \cdot \mathbb{Z}(N)$ ($x \sim x + \Delta x \cdot N$). The quantity that we call the momentum (the spatial shift generator on the lattice) in physics is often called *quasi-momentum* (the quasi-momentum coincides with the momentum in the continuous limit). Similarly, the quantity that we call energy (the generator of the time shift on the lattice) can be called *quasi-energy*.

If we assume that «Time is that which is measured by a clock.» [4], then in our model the clock is such that the time is given by a finite number of $q$-nary digits. The time by this clock is discrete and cyclic. After the clock counts down the maximum possible time for a given number of digits, the countdown begins from the beginning.

Since on a three-dimensional lattice, the quasi-energy of the vacuum is renormalized to zero for an arbitrary lattice size, the question arises whether it is possible to use the limit transition $N \to \infty$ to move from the lattice QFT to the QFT in continuous space. Is it possible to transfer the constructed number-theoretic renormalization to the continuous case? There are reasons to believe that such transfer is possible. In the series of papers [5–7], the representation of the coordinate and momentum using a sequence of digits in an arbitrary number system was considered. Renormalization on the lattice was described as a change in the representation of $\mathbb{Z}(N)$: the transition from the representation of

$\{0, 1, \ldots, N-1\}$ to the representation of $\{-n, -n+1, \ldots, 0, 1, \ldots, N-n-1\}$. This lattice renormalization gives natural generalizations for the continuous limit at which the non-renormalized series passes into the renormalized one. The simplest of such generalizations (on a lattice it works only for $q = 2$) is

$$x = \sum_{s=-\infty}^{+\infty} \mathbf{d}(s, x)\, q^s \quad \longrightarrow \quad x' = \frac{1}{q-1} \sum_{s=-\infty}^{+\infty} [\mathbf{d}(s-1, x) - \mathbf{d}(s, x)]\, q^s.$$

Here $\mathbf{d}(s, x)$ is the digit in the position $s$ of the number $x$ in the $q$-nary number system. The digit is assumed to be a periodic function of $x$

$$\mathbf{d}(s, x) = \mathbf{d}(s, x + q^{s+1}).$$

The non-renormalized series for $x$ for some numeral systems may diverge for negative numbers (if numbers from the set $\{0, 1, \ldots, q-1\}$ are used) or for positive numbers (if numbers from the set $\{0, -1, \ldots, -q+1\}$ are used) or for all numbers (if a set of digits not containing $0$ is used). The renormalized series converges in all these cases.

We are not yet ready to analytically calculate the individual digits of the $q$-nary expansion of integrals for vacuum energy, for this reason we started with the study of finite lattices.

The fact that the quasi-energy of the vacuum turned out to be zero for any lattice size, as well as the fact that the number-theoretic renormalization was previously determined not only for the finite lattice, but also on the real line, seems to be a weighty argument in favor of the physical meaningfulness of the transition to the continuous limit $N \to \infty$.

The direct calculation of the number-theoretic renormalization in the continuous case may be facilitated by the previously found [5, 6] integral representation of real numbers and number-theoretic renormalizations in such a representation:

$$x = \int_{s=-\infty}^{+\infty} \mathbf{d}(s, x)\, q^s\, ds \quad \longrightarrow \quad x' = \frac{1}{q-1} \int_{s=-\infty}^{+\infty} [\mathbf{d}(s-1, x) - \mathbf{d}(s, x)]\, q^s\, ds.$$

Here the digit position $s$ runs through all real (including fractional) values

$$\mathbf{d}(s, x) = \mathbf{d}(0, x \cdot q^{-s}).$$

The other form of number-theoretic renormalization for the integral representation is obtained by integration by parts with omission of boundary terms:

$$x = \int_{s=-\infty}^{+\infty} \mathbf{d}(s, x)\, q^s\, ds \quad \longrightarrow \quad x'' = -\frac{1}{\ln q} \int_{s=-\infty}^{+\infty} \frac{d(\mathbf{d}(s, x))}{ds}\, q^s\, ds.$$

The function $\mathbf{d}(s, x)$ experiences jumps (it is piecewise constant between jumps), so the derivative $\frac{d(\mathbf{d}(s,x))}{ds}$ is understood in the sense of generalized functions.

The integral representation of real numbers is overdetermined (it is enough to know any series of values of $\mathbf{d}(s, x)$ with a unit step of $s$), but there are no special scales in the integral representation (in the representation in the form of a series of $s \in \mathbb{Z}$, scales of the form $q^s$ are special).

Above we discussed the possibility of switching from $\mathbb{Z}(N)$ to real numbers, however, we should also consider the possibility of switching to $p$-adic numbers [2]. If the lattice size is set as $N = p^m$, then at $m \to \infty$ the vacuum energy tends to zero in the $p$-adic sense. This point of view on the renormalization of vacuum energy also needs further investigation.

The problems under study are also interesting from a number-theoretic point of view. In the course of the research, one of us (V.N.) formulated and numerically tested the following hypothesis:

*1) For arbitrary integers $m \geqslant 0$ and $N \geqslant 1$, the number of ways in which an arbitrary element $X$ of the ring $\mathbb{Z}(N)$ is represented as the sum of $d$ terms of degree $m$*

$$X \equiv x_1^m + \cdots + x_d^m \pmod{N}$$

*is always a multiple of N if $d \geqslant m + 1$.*

*2) If $d < m + 1$, then there is such a N, and such a $X \in \mathbb{Z}(N)$, that the number of ways in which X is represented as the sum of d terms of degree m is not divisible by N.*

The hypothesis is obvious for $m = 0$ and $m = 1$. For $m = 2$, the hypothesis follows from the Theorem in this paper. For higher degrees, the hypothesis has so far been tested numerically (V.N.).

The first statement of the hypothesis is verified numerically for all cases

- $m \leqslant 8$, $N \leqslant 1000$;

- $m \leqslant 35$, $N \leqslant 300$;

- $m \leqslant 100$, $N \leqslant 37$.

The second statement of the hypothesis is verified for all $m \leqslant 100$.

# APPENDIX

*Appendix*

## A, QUADRATIC CONGRUENCES

### 1. Quadratic Congruences to Prime Modulus

Simplest quadratic congruence

$$x^2 \equiv 0 \pmod{p}$$

in field $\mathbb{Z}(p)$ means that square root of 0 is uniquely defined in $\mathbb{Z}(p)$.

Quadratic congruence

$$x^2 \equiv a \pmod{p}, \qquad \text{in case } a \not\equiv 0 \pmod{p} \tag{A.1}$$

has solutions for some $a \in \mathbb{Z}(p)$, and such $a$ is said to be a quadratic residue. Note that the trivial case $a = 0$ is generally excluded from set of quadratic residues $\mathrm{Res}(p) = \{1, r, s, \dots\}$, which are congruent to integers

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

The number of quadratic residues is exactly $\frac{p-1}{2}$ because if we take different $x_1$ and $x_2$

$$x_1^2 \equiv x_2^2 \equiv a \not\equiv 0 \pmod{p},$$

then, since $\mathbb{Z}(p)$ is field, we have

$$(x_1/x_2)^2 \equiv 1 \pmod{p} \quad \Rightarrow \quad x_1 = \pm x_2.$$

If the congruence (A.1) does not have a solution, then $a$ is said to be a quadratic nonresidue.

The Legendre symbol is defined for integers $a \in \mathbb{Z}$:

$$\chi(a) \overset{\text{def}}{=} \left(\frac{a}{p}\right)_L \overset{\text{def}}{=} \begin{cases} 0 & \text{if } a \text{ is divisible by } p, \\ 1 & \text{if } a \text{ is quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is quadratic nonresidue.} \end{cases} \tag{A.2}$$

Legendre symbol is group theoretical character and we denote it like $\chi(a)$ for $p$ fixed. From Fermat's and Legendre theorems it follows that

$$\forall a: \qquad \chi(a) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{A.3}$$

Using this congruence one can simply evaluate Legendre symbol of $-1$ by formula

$$\chi(-1) = (-1)^{\frac{p-1}{2}}.$$

Also characters' sum over all elements of $\mathbb{Z}(p)$ is equal to 0:

$$\sum_a \chi(a) = 0. \tag{A.4}$$

Hence (in one dimension and $N = p$) the multiplicity (2.7) as number of solutions of congruence (A.1) is of the form

$$c(k) = 1 + \chi(k), \quad k \in \mathbb{Z}(p).$$

## 2. Quadratic Congruence to $p^m$ Modulus

We can consider all solutions $x$ of congruence with parameter $a$

$$x^2 \equiv a \,(\mathrm{mod}\ p^m), \quad x,\, a \in \mathbb{Z}(p^m). \tag{A.5}$$

Any solution of (A.5) will be also the solution of similar congruence with less by 1 power of $p$:

$$\text{if } \acute{x} : \ \acute{x}^2 \equiv a \,(\mathrm{mod}\ p^m) \text{ then } \Rightarrow \acute{x}^2 \equiv a \,(\mathrm{mod}\ p^{m-1}) \Rightarrow \cdots \Rightarrow \acute{x}^2 \equiv a \,(\mathrm{mod}\ p^1). \tag{A.6}$$

Notation of $x$ expansion in powers of $p^\alpha$ and digits $x_\alpha$ looks like:

$$\begin{aligned} x &= x_0 + x_1\, p + x_2\, p^2 + \cdots + x_\alpha p^\alpha + \cdots + x_{m-1}\, p^{m-1}, \quad x_\alpha \in \mathbb{Z}(p); \\ a &= a_0 + a_1\, p + a_2\, p^2 + \cdots + a_\alpha p^\alpha + \cdots + a_{m-1}\, p^{m-1}, \quad a_\alpha \in \mathbb{Z}(p). \end{aligned} \tag{A.7}$$

First we explain the case when $a$ is relatively prime to $p$.

*For $a$ with digit $a_0 \neq 0$.* The greatest common divisor of $a$ and $p$ in this case is 1

$$(a, p) = 1.$$

From (A.6) and (A.7) one can immediately find congruence for digit $x_0$

$$x_0^2 \equiv a_0 \,(\mathrm{mod}\ p^1), \tag{A.8}$$

it looks like (A.1). If $a_0$ is a quadratic nonresidue there are no solutions of (A.5). So one-dimensional multiplicity for $N = p^m$

$$c(a) = 0 \quad \text{if } (a, p) = 1 \text{ and digit } a_0 \notin \mathrm{Res}(p).$$

We go further with $a_0$ as quadratic residue, so $x_0 = \pm\sqrt{a_0} \in \mathbb{Z}(p)$. From (A.6) and (A.7) from next $p^2$-modulo congruence $x^2 \equiv a \,(\mathrm{mod}\ p^2)$ we get

$$x_0^2 + 2x_0 x_1 p + \cancel{x_2\, p^2} \equiv a_0 + a_1 p \,(\mathrm{mod}\ p^2) \tag{A.9}$$

as linear congruence with respect to unknown $x_1$

$$2x_0 x_1\, p \equiv a_0 - x_0^2 + a_1 p \,(\mathrm{mod}\ p^2),$$

one can reduce this right side by $p$ due to (A.8). Then

$$2x_0\, x_1 \equiv a_1 + \frac{a_0 - x_0^2}{p} \,(\mathrm{mod}\ p).$$

In field $\mathbb{Z}(p)$ since $2x_0 \neq 0$ we have inverse element $(2x_0)^{-1} \in \mathbb{Z}(p)$. Digit $x_1$ is uniquely defined:

$$x_1 \equiv \left(a_1 + \frac{a_0 - x_0^2}{p}\right)(2x_0)^{-1} \,(\mathrm{mod}\ p).$$

From next $p^3$-modulo congruence $x^2 \equiv a \,(\mathrm{mod}\ p^3)$ we get linear congruence with unknown $x_2$

$$\begin{aligned} (x_0 + x_1\, p)^2 + 2(x_0 + \cancel{x_1 p})x_2\, p^2 &\equiv a_0 + a_1 p + a_2\, p^2 \,(\mathrm{mod}\ p^3) \quad \Rightarrow \\ 2x_0\, x_2\, p^2 &\equiv a_0 + a_1 p - (x_0 + x_1\, p)^2 + a_2 p^2 \,(\mathrm{mod}\ p^3), \end{aligned}$$

whose right side has common factor $p^2$ due to (A.9). So at this step one can find $x_2$ uniquely:

$$x_2 \equiv \left( a_2 + \frac{a_0 + a_1 p - (x_0 + x_1 p)^2}{p^2} \right) (2x_0)^{-1} \pmod{p}.$$

All digits $x_\alpha$ are found sequentially step by step. Let us consider arbitrary step of finding $x_\alpha$ from $p^{\alpha+1}$-modulo congruence $x^2 \equiv a \pmod{p^{\alpha+1}}$.

$$([x_0 + x_1 p + \cdots] + x_\alpha p^\alpha)^2 \equiv [a_0 + a_1 p + \cdots] + a_\alpha p^\alpha \pmod{p^{\alpha+1}};$$
$$[x_0 + \cdots]^2 + 2[x_0 + \diagup]x_\alpha p^\alpha \equiv [a_0 + a_1 p + \cdots] + a_\alpha p^\alpha \pmod{p^{\alpha+1}};$$
$$2x_0 x_\alpha p^\alpha \equiv [a_0 + \cdots] - [x_0 + \cdots]^2 + a_\alpha p^\alpha \pmod{p^{\alpha+1}}.$$

We have $x_\alpha \in \mathbb{Z}(p)$ uniquely as

$$x_\alpha \equiv \left( a_\alpha + \frac{[a_0 + \cdots] - [x_0 + \cdots]^2}{p^\alpha} \right) (2x_0)^{-1} \pmod{p},$$

when $x_0$ is fixed with its sign, then solution $x$ is calculated uniquely.

Thus multiplicities in one dimension

$$c_{p^m}(a) = c_p(a_0) = 1 + \chi(a_0) \quad \text{if digit } a_0 \neq 0, \tag{A.10}$$

and we obtain this property of multiplicities for arbitrary $n < m$

$$c_{p^m}(a) = c_{p^n}(a \mod p^n) \quad \text{if digit } a_0 \neq 0. \tag{A.11}$$

*For a with $a_0 = 0$ and $a_1 \neq 0$.* From $p^2$-modulo congruence $x^2 \equiv a \pmod{p^2}$ we get

$$(x_0 + x_1 p + x_2 p^2 + \cdots)^2 \equiv a_1 p \pmod{p^2}.$$

and anyway no solutions for $x_1$. So if $a_1 \neq 0$ than $c_{p^m}(a) = 0$, i.e.

$$c_{p^m}(\xi p^1) = 0, \quad \xi \in \mathbb{Z}(p^{m-1}) \setminus \{0\}.$$

*For a with $a_0 = a_1 = \cdots = a_{2\lambda} = 0$ and $a_{2\lambda+1} \neq 0$, $\lambda \geqslant 0$.* We put the lowest non-zero digit in $x$ as $x_\alpha \neq 0$. Then congruence (A.5) takes the form

$$(x_\alpha \cdot p^\alpha + \cdots)^2 \equiv (a_{2\lambda+1} + \cdots)p^{2\lambda+1} \pmod{p^m},$$

$$(x_\alpha + \cdots)^2 p^{2\alpha} \equiv (a_{2\lambda+1} + \cdots)p^{2\lambda+1} \pmod{p^m}.$$

Anyway no solutions exist and multiplicity

$$c_{p^m}(\xi p^{2\lambda+1}) = 0, \quad \text{where } \xi \in \mathbb{Z}(p^{m-2\lambda-1}) \setminus \{0\}, \, \lambda \geqslant 0. \tag{A.12}$$

*For a with $a_0 = a_1 = 0$ and $a_2 \neq 0$.* From $p^2$-modulo congruence $x^2 \equiv a \pmod{p^2}$ we get

$$(x_0 + x_1 p + x_2 p^2 + \cdots)^2 \equiv 0 \pmod{p^2}.$$

Simply $x_0 = 0$ and from $p^3$-modulo congruence $x^2 \equiv a \pmod{p^3}$ we get ordinary quadratic congruence for $x_1$

$$(x_1 p + x_2 p^2 + \cdots)^2 \equiv a_2 p^2 \pmod{p^3} \Rightarrow x_1^2 \equiv a_2 \pmod{p},$$

with some solutions if $\sqrt{a_2}$ exists. But now starting equation is not (A.5), because of power descending by 2 units

$$(x_1 p + x_2 p^2 + \cdots + x_{m-1} p^{m-1})^2 \equiv a_2 p^2 + \cdots + a_{m-1} p^{m-1} \pmod{p^m}$$

$$\Rightarrow (x_1 + x_2 p^1 + \cdots + x_{m-1} p^{m-2})^2 \equiv a_2 + \cdots + x_{m-3} p^{m-1} \pmod{p^{m-2}},$$

thus obviously last digit $x_{m-1}$ can take arbitrary values from $\mathbb{Z}(p)$. Therefore multiplicities as number of solutions of (A.5) are greater by $p$

$$c_{p^m}(a) = \left( 1 + \chi(a_2) \right) p \quad \text{if digit } a_2 \neq 0,$$

i.e.

$$c_{p^m}(\xi p^2) = \left( 1 + \chi(\xi \mod p) \right) p, \quad \text{where } \xi \in \mathbb{Z}(p^{m-2}) \setminus \{0\}.$$

*For a with $a_0 = a_1 = \cdots = a_{2\lambda-1} = 0$ and $a_{2\lambda} \neq 0$, $2\lambda < m$.*

$$(x_\alpha + \cdots)^2 p^{2\alpha} \equiv (a_{2\lambda} + \cdots)p^{2\lambda} \pmod{p^m}, \quad x_\alpha \neq 0.$$

The solutions exist only when $\alpha = \lambda$. We obtain

$$(x_\lambda + \cdots + \underline{x_{m-1}p^{m-1-\lambda}})^2 \equiv a_{2\lambda} + \cdots \pmod{p^{m-2\lambda}}, \tag{A.13}$$

and we have the similar case as (A.10) (when $a$ is relatively prime to $p$).

In solution $x$ we see that the lowest $\alpha$ digits are zero and the highest $\alpha$ digits one can take arbitrarily. And between them $m - 2\alpha$ digits are calculated step by step from linear congruences.

Therefore multiplicities as number of solutions of (A.5) are greater by $p^\alpha$

$$c_{p^m}(a) = \big(1 + \chi(a_{2\alpha})\big)p^\alpha, \quad \text{if digits } a_0 = \cdots = a_{2\alpha-1} = 0, a_{2\alpha} \neq 0 \text{ and } 2\alpha < m. \tag{A.14}$$

And for arbitrary $n < m$

$$c_{p^m}(a) = c_{p^n}(a \mod p^n) \quad \text{if digit } a_{2\alpha} \neq 0 \text{ and } 2\alpha \leqslant n < m. \tag{A.15}$$

In section D we'll investigate similarity of generating functions in $d = 1$ using this relation.

*For $a = 0$ with $a_0 = \cdots = a_{m-1} = 0$.* We denote the lowest non-zero digit in $x$ by index $\alpha$.

$$(x_\alpha p^\alpha + \cdots)^2 = (x_\alpha + \cdots + x_{m-1}p^{m-1-\alpha})^2\, p^{2\alpha} \equiv 0 \pmod{p^m}. \tag{A.16}$$

We have solutions here if

$$2\alpha \geqslant m,$$

so the lowest value of index $\alpha$ is $\lfloor \frac{m+1}{2} \rfloor$. The number of arbitrary digits is $\lfloor \frac{m}{2} \rfloor$. So multiplicity is $c_{p^m}(0) = p^{\lfloor \frac{m}{2} \rfloor}$. We get all-for-one in formulæ

$$c_{p^m}(a) = \begin{cases} p^{\lfloor \frac{m}{2} \rfloor} & \text{if } a = 0, \\ \big(1 + \chi(a_{2\lambda})\big)p^\lambda & \text{if } a \text{ is divisible by } p^{2\lambda}, \text{ i.e. } (a, p^m) = p^{2\lambda}, \text{ and } \lambda \geqslant 0, \\ 0 & \text{if } a \text{ is divisible by } p^{2\lambda+1}, \text{ i.e. } (a, p^m) = p^{2\lambda+1}, \lambda \geqslant 0. \end{cases} \tag{A.17}$$

*Appendix*

## B. GENERATING FUNCTIONS FOR MULTIPLICITIES

We define the polynomial of $\tau$

$$f_N^d(\tau) = \sum_{k \in \mathbb{Z}(N)} c_{Nd}(k)\, \tau^k \tag{B.1}$$

as a generating function for multiplicities $c_{N\,d}(k)$ of $E(k)$ on the lattice $\mathbb{Z}^d(N)$. For one-dimensional generating function we skip the upper index $d = 1$, i.e. $f_N(\tau) \stackrel{\text{def}}{=} f_N^1(\tau)$. And $f_0(\tau) \stackrel{\text{def}}{=} 1$.

We use brackets [1] to extract multiplicity $c_{N\,d}(k)$ from generating function:

$$\left\langle \tau^k \mid f_N^d(\tau) \right\rangle = c_{N\,d}(k). \tag{B.2}$$

We treat $\tau$ as a formal variable with the equivalence relation:

$$\tau^N = 1, \tag{B.3}$$

i.e. the powers of $\tau$ in (B.1) can be considered as elements of $\mathbb{Z}(N)$. The multiplication with relation (B.3) we denote as $f \circ g$. Hereafter $\tau^N$ is equivalent to unity in reduction of similar terms so that $\tau^{k+N} = \tau^k$:

$$\left( \sum_{p_1 \in \mathbb{Z}(N)} \tau^{p_1^2} \right)^d = \sum_{p_1 \in \mathbb{Z}(N)} \cdots \sum_{p_d \in \mathbb{Z}(N)} \tau^{p_1^2} \circ \cdots \circ \tau^{p_d^2} = \sum_{\mathbf{p} \in \mathbb{Z}^d(N)} \tau^{\mathbf{p}^2},$$

---

[1] $\left\langle \tau^k \mid f_N(\tau) \right\rangle = \frac{1}{N} \sum_{l=1}^{N} \tau(l)^* f_N(\tau(l))$, where $\tau(l)$ are roots of unity in $\mathbb{C}$ given by $\tau(l) = e^{2\pi i\, l/N}$.

hence in case $d > 1$ the generating function can be represented as a $d$ times product of one-dimensional generating functions:

$$f_N^d(\tau) = \left( f_N(\tau) \right)^d. \tag{B.4}$$

The introduced equivalence (B.3) doesn't violate the commutativity and distributivity of multiplication. Thereby, we reduce our investigation of multiplicities (2.7) to problems of polynomial algebra and arithmetic of quadratic forms [8, 9].

One can assume that variable $\tau$ takes values in the set of complex $N$th roots of unity:

$$\tau \in \{ \tau(l) = e^{2\pi i \frac{l}{N}}, l \in \mathbb{Z}(N) \}.$$

In such a representation we find multiplicities $c_{Nd}(k)$ as coefficients of discrete Fourier expansion of the function $f_N^d(\tau(l))$ on the lattice $\mathbb{Z}(N)$.

**Polynomial $\phi_N(\tau)$.** We define the polynomial $\phi_N(\tau)$ with all coefficients equal to 1:

$$\phi_N(\tau) = \sum_{k \in \mathbb{Z}(N)} \tau^k = 1 + \tau + \tau^2 + \cdots + \tau^{N-1}. \tag{B.5}$$

Here $\phi_N(\tau) \not\equiv \frac{1-\tau^N}{1-\tau}$ because due to (B.3) the value 1 of variable $\tau$ is possible value.

If $\tau$ runs over complex roots of unity then

$$\phi_N(\tau) = \begin{cases} N & \text{if } \tau = 1, \\ 0 & \text{otherwise.} \end{cases}$$

From this point of view $\phi_N(\tau)$ is the lattice analogue of the delta function

$$\phi_N\big(\tau(l)\big) = \begin{cases} N & \text{if } l = 0, \\ 0 & \text{otherwise.} \end{cases}$$

For any $k \in \mathbb{Z}(N)$ we have

$$\tau^k \circ \phi_N (\tau) = 1 \cdot \phi_N(\tau), \tag{B.6}$$

hence

$$\phi_N \circ \phi_N = \left( \sum_{k=0}^{N-1} \tau^k \right) \circ \phi_N = N \cdot \phi_N \tag{B.7}$$

and consequently

$$\phi_N \circ (N - \phi_N) = 0, \tag{B.8}$$

$$(N - \phi_N)^2 = N(N - \phi_N),$$
$$(N - \phi_N)^m = N^{m-1}(N - \phi_N).$$

*Appendix*

## C. CASE $N = p$, $p \neq 2$

Now $p$ is prime odd number and we put $N = p$ hereafter in section C. During intermediate calculations we sometimes skip the index $p$ (or $N$).

For the one-dimensional case we can derive the explicit expression for the multiplicities $c_{N1}(k) = c_N(k)$ in terms of quadratic congruences [10].

**Polynomial** $g_p(\tau)$ **.** Coefficients $c_p(k)$ take values 0 or 2, or 1 (square root of 0); and the generating function is

$$f_p(\tau) = 1 + 2\tau + 2\tau^r + 2\tau^s + \cdots = 1 + \sum_{r \in \mathrm{Res}(p)} 2\tau^r,$$

where powers $\tau$ with nonresidues $\tilde{r}, \tilde{s}, ..$ disappeared from $f_p(\tau)$ because of its null coefficients (multiplicities).

Next we introduce the polynomial $g_p(\tau)$ using the character $\chi(k)$ (defined in section A):

$$g_p(\tau) = \sum_{k \in \mathbb{Z}(p)} \chi(k) \cdot \tau^k. \tag{C.1}$$

So, the generating function for multiplicities in the one-dimensional case is the sum of polynomials $g_p(\tau)$ and $\phi_p(\tau)$:

$$f_p(\tau) = 1 + \sum_{r \in \mathrm{Res}(p)} 2\tau^r = \phi_p(\tau) + g_p(\tau). \tag{C.2}$$

And multiplicities in $d = 1$ are given by explicit formula:

$$\text{in } d = 1 \quad c_{p1}(k) = 1 + \chi(k).$$

### 1. Properties of Polynomials $g_p$ and $\phi_p$ in Multiplication

Due to (B.7) we have

$$\phi_p \circ \phi_p = p \cdot \phi_p \quad \text{and} \quad \phi_p{}^m = p^{m-1} \cdot \phi_p,$$
$$(p - \phi_p) \circ \phi_p = 0, \tag{C.3}$$

and we get

$$\phi_p \circ g_p = 0, \tag{C.4}$$

because of (B.6) and (A.4)

$$\phi_p \circ \left( \sum_{a=0}^{p-1} \chi(a)\,\tau^a \right) = \phi_p \circ \left( \underbrace{\sum_{a=0}^{p-1} \chi(a)}_{0} \right) = 0.$$

**Proposition for $g_p^2$.** The explicit result for $g_p^2$ is:

$$g_p \circ g_p = (-1)^{\frac{p-1}{2}} \left( p - \phi_p \right). \tag{C.5}$$

*Proof.* Writing out $g_p^2$ as a double sum and remembering about (B.3), we will make a transition at fixed $a$ from summation variable $b$ to the new summation variable $t$ by simple rule $b \equiv a \cdot t \pmod{p}$, since $\mathbb{Z}(p)$ is field. In third line, we split the sum over $t$ into two parts.

$$g_p \circ g_p\,(\tau) = \left( \sum_a \chi(a)\tau^a \right) \circ \left( \sum_b \chi(b)\tau^b \right) = \sum_{a,b=1}^{p-1} \chi(a)\chi(b)\tau^{a+b} =$$

$$= \sum_{a,t=1}^{p-1} \chi(a)\chi(at)\tau^{a+at} = \sum_{t=1}^{p-1}\sum_{a=1}^{p-1} \overset{1}{\cancel{\chi^2(a)}}\chi(t)\tau^{a(1+t)} =$$

$$= \chi(t)\big|_{t=p-1} \sum_{a=1}^{p-1} \tau^{a \cdot 0} + \sum_{t=1}^{p-2} \chi(t) \sum_{a=1}^{p-1} \tau^{a(1+t)} = \chi(-1)\sum_{a=1}^{p-1} 1 + \sum_{t \neq -1} \chi(t) \sum_{a=1}^{p-1} \tau^a =$$

$$= \chi(-1)(p-1) + \Big(0 - \chi(-1)\Big) \cdot \big(-1 + \phi_p(\tau)\big) = \chi(-1)\left( p - \phi_p(\tau) \right).$$

$$\square$$

As a consequence of (C.3), (C.4), (C.5) we have the equation for arbitrary powers $m$ and $n$

$$\phi_p{}^m \circ g_p{}^n = 0, \tag{C.6}$$

then we obtain

$$(\phi_p + g_p)^m = \phi_p{}^m + g_p{}^m. \tag{C.7}$$

And from (C.5)

$$g_p \circ g_p \circ g_p = (-1)^{\frac{p-1}{2}} \cdot p \cdot g_p. \tag{C.8}$$

Arbitrary power $m$:

$$g_p{}^m = (-1)^{\frac{p-1}{2}\lfloor \frac{m}{2} \rfloor} \begin{cases} p^{\lfloor \frac{m}{2} \rfloor} \cdot g_p & \text{if odd } m, \\ p^{\frac{m}{2}-1}(p - \phi_p) & \text{if even } m. \end{cases} \tag{C.9}$$

### 2. Multiplicities in $d = 2$

From generation function (C.2) we have in two-dimensional case due to (C.7)

$$f_p^2(\tau) = f_p \circ f_p = \phi_p \circ \phi_p + g_p \circ g_p.$$

Now we have mathematical expression for $f_p^2$ for any prime odd $p$:

$$f_p^2 = p \cdot \phi_p + (-1)^{\frac{p-1}{2}} (p - \phi_p), \tag{C.10}$$

in explicit polynomial form we have

$$f_p^2(\tau) = \begin{cases} (2p - 1) \cdot \tau^0 + (p - 1) \cdot \tau^1 + \cdots + (p - 1) \cdot \tau^{p-1} & \text{if even } \frac{p-1}{2}, \\ 1 \cdot \tau^0 + (p + 1) \cdot \tau^1 + \cdots + (p + 1) \cdot \tau^{p-1} & \text{if odd } \frac{p-1}{2}. \end{cases} \tag{C.11}$$

So polynomial coefficient from $f_p^2$ is congruent with $\pm 1$ and multiplicity is congruent as

$$\text{in } d = 2 \quad c_{p\,2}(k) \equiv -\chi(-1) \pmod{p}, \quad k \in \mathbb{Z}(p). \tag{C.12}$$

### 3. Multiplicities in $d = 3$

Using (C.7) and (C.9) for $f_p^3$ we have

$$f_p^3 = f_p \circ f_p \circ f_p = \phi_p^3 + g_p^3 = p^2 \phi_p + (-1)^{\frac{p-1}{2}} p\, g_p.$$

In the expression above one can take the common factor $p$ out of brackets. So each coefficient in polynomial above is divisible by $p$ and we have

$$c_{p\,3}(k) \equiv 0 \pmod{p}.$$

And for $d > 3$ formula

$$c_{p\,d}(k) \equiv 0 \pmod{p}$$

is obvious due to factorization (B.4). We proved the proposition of the Theorem in case $N = p$.

*Appendix*

## D. CASE $N = p^m$, $p \neq 2$

**Cyclotomic Polynomials** $\Phi_n(\tau)$. In this section $N = p^m$, $p$ is prime odd and $m \in \mathbb{N}$, $m > 1$. The equivalence relation (B.3) now is

$$\tau^{p^m} = 1.$$

In addition to $\phi_N(\tau)$ as sum of all powers in (B.5) we introduce cyclotomic polynomials for $N = p^m$:

$$\Phi_p(\tau) = 1 + \tau + \tau^2 + \cdots + \tau^{p-1} = \phi_p(\tau),$$

$$\Phi_{p^2}(\tau) = \Phi_p(\tau^p) = 1 + \tau^p + \tau^{2p} + \tau^{3p} + \cdots + \tau^{(p-1)p} = \phi_p(\tau^p),$$

$$\Phi_{p^3}(\tau) = \Phi_p(\tau^{p^2}) = 1 + \tau^{p^2} + \tau^{2p^2} + \tau^{3p^2} + \cdots + \tau^{(p-1)p^2} = \phi_p(\tau^{p^2}), \tag{D.1}$$

$$\vdots$$

$$\Phi_{p^m}(\tau) = \Phi_p(\tau^{p^{m-1}}) = 1 + \tau^{p^{m-1}} + \tau^{2p^{m-1}} + \tau^{3p^{m-1}} + \cdots + \tau^{(p-1)p^{m-1}} = \phi_p(\tau^{p^{m-1}}).$$

One can easily derive that the product of cyclotomic polynomials of successive powers of $p$ is the sum of all powers of $\tau$ in $\phi_N(\tau)$:

$$\phi_{p^m} = \Phi_p \cdot \Phi_{p^2} \cdots \Phi_{p^m}.$$

We have similar to (C.3) equalities

$$\tau^{p^{m-1}} \circ \Phi_{p^m} = \Phi_{p^m},$$

$$\Phi_{p^m} \circ \Phi_{p^m} = p \cdot \Phi_{p^m}, \tag{D.2}$$

$$(p - \Phi_{p^m}) \circ \Phi_{p^m} = 0.$$

And polynomials with modified argument $\tau^{p^{m-1}}$

$$\Phi_{p^m}(\tau) \circ g_p(\tau^{p^{m-1}}) = \phi_p(\tau^{p^{m-1}}) \circ g_p(\tau^{p^{m-1}}) = 0, \tag{D.3}$$

$$\left(\phi_p(\tau^{p^{m-1}}) + g_p(\tau^{p^{m-1}})\right)^n = \phi_p(\tau^{p^{m-1}})^n + g_p(\tau^{p^{m-1}})^n. \tag{D.4}$$

### 1. Similarity of Successive Generating Functions in $d = 1$

**Proposition.** The recurrent formula for $f_{p^m}(\tau) = \mathcal{F}\left(f_{p^{m-1}}(\tau)\right)$ is

$$f_{p^m}(\tau) = \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) + (-1)^{\frac{p-1}{2}\lfloor\frac{m}{2}\rfloor} \cdot \left(g_p(\tau^{p^{m-1}})\right)^m, \tag{D.5}$$

or via (C.9)

$$f_{p^m}(\tau) = \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) + \begin{cases} p^{\lfloor\frac{m}{2}\rfloor} \cdot g_p(\tau^{p^{m-1}}) & \text{if odd } m, \\ p^{\frac{m}{2}-1}\left(p - \Phi_{p^m}(\tau)\right) & \text{if even } m. \end{cases} \tag{D.6}$$

**The Proof for $f_{p^m}$ Recurrent Formula.** For example, if we take $k = 1 \in \mathbb{Z}(p^m)$ then from (A.10) in $d = 1$ it follows that $c_{p^m}(1) = c_p(1)$. Using notation with brackets (B.2) we write

$$\left\langle \tau^1 \mid f_{p^m}(\tau) \right\rangle = \left\langle \tau^1 \mid f_p(\tau) \right\rangle = 1 + \chi(1) = 2.$$

To generalize this relation we use (A.11) for non divisible by $p$ arbitrary $k \in \mathbb{Z}(p^m)$ and the equality of $\tau^k$ coefficients $c_{p^m}(k)$ in $f_{p^m}(\tau)$ and $c_{p^{m-1}}(k \mod p^{m-1})$ in $f_{p^{m-1}}(\tau)$ is clear. Using cyclotomic polynomials (D.1) we can write this similarity relation

$$\left\langle \tau^k \mid f_{p^m}(\tau) \right\rangle = \left\langle \tau^k \mid \Phi_{p^m}(\tau) \circ f_{p^{m-1}}(\tau) \right\rangle = \left\langle \tau^k \mid \Phi_{p^m} \cdots \Phi_{p^2} \cdot f_p \right\rangle \quad \text{if } k \not\equiv 0 \pmod p. \tag{D.7}$$

NB. In fact, the largest power of $\Phi_{p^m}$ polynomial is $(p-1)p^{m-1}$ and the largest power of $f_{p^{m-1}}$ polynomial is $p^{m-1}-1$ and power of their product is

$$(p-1)p^{m-1} + p^{m-1} - 1 = p^m - 1,$$

there is no need to use here $\circ$ product.

We can obtain formula more general than (D.7). Due to (A.15) $c_{p^m}(a) = c_{p^{m-1}}(a \mod p^{m-1})$ and then

$$\left\langle \tau^k \mid f_{p^m}(\tau) \right\rangle = \left\langle \tau^k \mid \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) \right\rangle \quad \text{if } k \not\equiv 0 \pmod{p^{m-1}}. \tag{D.8}$$

We will consider odd $m$ and even separately.

**For Odd** $m = 2\mu + 1$, $\mu \in \mathbb{N}$. For example, if we take $k = 0 \in \mathbb{Z}(p^m)$ then

$$\left\langle \tau^0 \mid f_{p^m}(\tau) \right\rangle = p^\mu \qquad \text{and} \qquad \left\langle \tau^0 \mid \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) \right\rangle = p^\mu.$$

For $k = p^{2\mu} \in \mathbb{Z}(p^m)$

$$\left\langle \tau^{p^{2\mu}} \mid f_{p^m}(\tau) \right\rangle = c_{p^m}(1 \cdot p^{2\mu}) = (1 + \chi(1))\, p^\mu,$$

$$\left\langle \tau^{p^{2\mu}} \mid \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) \right\rangle = \left\langle \tau^{p^{2\mu}} \mid (1 + \tau^{p^{2\mu}} + \cdots) \cdot (p^\mu + 2\tau + \cdots) \right\rangle = p^\mu,$$

so in general case when $k \equiv 0 \pmod{p^{m-1}}$

$$\left\langle \tau^k \mid f_{p^m}(\tau) \right\rangle = \left\langle \tau^k \mid \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) \right\rangle + \chi(\kappa)\, p^\mu, \qquad \text{where } k = \kappa \cdot p^{m-1} \in \mathbb{Z}(p^m). \tag{D.9}$$

Relations (D.8) and (D.11) give for odd $m$

$$f_{p^m}(\tau) = \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) + p^\mu \sum_{\kappa=0}^{p-1} \chi(\kappa)\tau^{\kappa\, p^{m-1}} = \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) + p^{\lfloor \frac{m}{2} \rfloor} \cdot g_p(\tau^{p^{m-1}}). \tag{D.10}$$

**For Even** $m = 2\mu$, $\mu \in \mathbb{N}$. If we take $k = 0 \in \mathbb{Z}(p^m)$ then due to (A.17)

$$\left\langle \tau^0 \mid f_{p^m}(\tau) \right\rangle = p^\mu \qquad \text{and} \qquad \left\langle \tau^0 \mid \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) \right\rangle = p^{\mu-1}.$$

For $k = p^{2\mu} \in \mathbb{Z}(p^m)$

$$\left\langle \tau^{p^{m-1}} \mid f_{p^m}(\tau) \right\rangle = 0,$$

$$\left\langle \tau^{p^{m-1}} \mid \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) \right\rangle = \left\langle \tau^{p^{2\mu-1}} \mid (1 + \tau^{p^{2\mu-1}} + \cdots) \cdot (p^{\mu-1} + 2\tau + \cdots) \right\rangle = p^{\mu-1},$$

so in general case when $k \equiv 0 \pmod{p^{m-1}}$

$$\left\langle \tau^k \mid f_{p^m}(\tau) \right\rangle = \left\langle \tau^k \mid \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) \right\rangle + p^\mu \cdot \delta_{\kappa 0} - p^{\mu-1} \cdot 1, \quad \text{where } k = \kappa \cdot p^{m-1} \in \mathbb{Z}(p^m). \tag{D.11}$$

We obtain

$$\text{for } m = 2\mu: \quad f_{p^m}(\tau) = \Phi_{p^m}(\tau) \cdot f_{p^{m-1}}(\tau) + p^{\frac{m}{2}-1}\big(p - \Phi_{p^m}(\tau)\big). \tag{D.12}$$

### 2. Multiplicities in $d = 2$

In two-dimensional case due to (D.4) from one-dimensional (D.5) we have

$$\begin{aligned}
f_{p^m}^2 = f_{p^m} \circ f_{p^m} &= \left(\Phi_{p^m} \circ f_{p^{m-1}}\right)^2 + \left(g_p(\tau^{p^{m-1}})\right)^{2m} \\
&= p \cdot \Phi_{p^m} \cdot f_{p^{m-1}}^2 + \left((-1)^{\frac{p-1}{2}} \cdot (p - \Phi_{p^m})\right)^m \\
&= p \cdot \Phi_{p^m} \cdot f_{p^{m-1}}^2 + (-1)^{\frac{p-1}{2} m} \cdot p^{m-1} \cdot (p - \Phi_{p^m}).
\end{aligned} \tag{D.13}$$

### 3. Multiplicities in $d = 3$

In three-dimensional case

$$f_{p^m}^3 = f_{p^m} \circ f_{p^m} \circ f_{p^m} = \left(\Phi_{p^m} \circ f_{p^{m-1}}\right)^3 + (-1)^{\frac{p-1}{2}\lfloor\frac{m}{2}\rfloor m}\left(g_p(\tau^{p^{m-1}})\right)^{3m}$$

$$= p^2 \cdot \Phi_{p^m} \cdot f_{p^{m-1}}^3 + (-1)^{\frac{p-1}{2}\lfloor\frac{m}{2}\rfloor m}\left((-1)^{\frac{p-1}{2}} p \cdot g_p(\tau^{p^{m-1}})\right)^m \qquad \text{(D.14)}$$

$$= p^2 \cdot \Phi_{p^m} \cdot f_{p^{m-1}}^3 + (\pm)\, p^m \left(g_p(\tau^{p^{m-1}})\right)^m,$$

where the sign $\pm$ equals $(-1)$ if $\quad -p \equiv m \equiv 1 \pmod 4 \quad$ and $(+1)$ otherwise.

It is clear that if $f_{p^{m-1}}^3$ is divisible by $p^{m-1}$ than $f_{p^m}^3$ is also divisible by $p^m$. In section C the Theorem is proved for $N = p^1$ and hence by induction we proved the Theorem for $N = p^m$.

*Appendix*

## E. DEFINITIONS FOR PROOF-2

### 1. d-Dimensional Integer Space

Let us consider the $d$-dimensional space $\mathbb{Z}^d$ of integer vectors

$$\boldsymbol{\xi} = (\xi_1, \xi_2, ..., \xi_d), \quad \xi_i \in \mathbb{Z}.$$

In the figures, the elements of space $\mathbb{Z}^d$ is represented by cells of unit size in all coordinates.

Let L be some finite subset of $\mathbb{Z}^d$

$$\mathrm{L} \subset \mathbb{Z}^d, \quad |\mathrm{L}| \in \mathbb{N},$$

where $|\mathrm{L}|$ is the number of elements in L.

Notation

$$n \cdot \mathrm{L} + \mathbf{a} = \{n \cdot \boldsymbol{\xi} + \mathbf{a} | \boldsymbol{\xi} \in \mathrm{L}\},$$

where $n \in \mathbb{N}$, $\mathbf{a} \in \mathbb{Z}^d$, is used for the set L stretched by factor $n$ and shifted by the vector $\mathbf{a}$. That is, the points of this set are obtained from the points of the set L by multiplying all coordinates by $n$ and shifting by vectors $\mathbf{a}$:

$$\xi_i \to n\xi_i + a_i.$$

The notation $\mathrm{L} + \mathbf{a}$ is equivalent to $1 \cdot \mathrm{L} + \mathbf{a}$.

The notation $n \cdot \mathrm{L}$ is equivalent to $n \cdot \mathrm{L} + \mathbf{0}$, where $\mathbf{0}$ is the null vector in $\mathbb{Z}^d$.

### 2. Sets of Integers

**Definition E.1.** $\mathbb{Z}(\alpha)$ *is the set of integers from* $0$ *to* $\alpha - 1$, *i.e.*

$$\mathbb{Z}(\alpha) = \{0, 1, 2, \ldots, \alpha - 1\}.$$

**Definition E.2.** $n\mathbb{Z}(\alpha) + a$ *is the set of all numbers from* $\mathbb{Z}(\alpha)$, *multiplied by* $n$ *and shifted by* $a$, *i.e.*

$$n\mathbb{Z}(\alpha) + a = \{a, n + a, 2n + a, \ldots, (\alpha - 1)n + a\}.$$

The notation $\mathbb{Z}(\alpha) + a$ is equivalent to $1\mathbb{Z}(\alpha) + a$.

The notation $n\mathbb{Z}(\alpha)$ is equivalent to $n\mathbb{Z}(\alpha) + 0$.

### 3. Lattices

Let us introduce the notation for the $b$-dimensional lattice $\underbrace{N \times N \times \ldots \times N}_{b}$.

**Definition E.3.** $\text{lattice}^b(N)$ *for $a \leqslant d$ is the set of $\boldsymbol{\xi} \in \mathbb{Z}^d$ such that $\xi_1, \ldots, \xi_b \in \mathbb{Z}(N)$, and $\xi_{b+1} = \cdots = \xi_d = 0$.*

**Definition E.4.** $\text{lattice}^b_{i_1 \ldots i_b}(N)$ *for $b \leqslant d$ is the set of $\boldsymbol{\xi} \in \mathbb{Z}^d$ such that $\xi_{i_1}, \ldots, \xi_{i_b} \in \mathbb{Z}(N)$, and $\xi_j = 0$ if $j \notin \{i_1, \ldots, i_b\}$.*

For example, if $d = 6$, then $\text{lattice}^3_{2,3,5}(N)$ is the set of $\boldsymbol{\xi} \in \mathbb{Z}^6$ such that $\xi_2, \xi_3, \xi_5 \in \mathbb{Z}(\alpha)$, and $\xi_1 = \xi_4 = \xi_6 = 0$.

### 4. Functions

**Definition E.5.** $\text{ncells}(\text{L}, \alpha, k)$ *("the number of cells") is the number of cells $\boldsymbol{\xi} \in \text{L} \subset \mathbb{Z}^d$, such that*

$$\sum_{i=1}^{d} \xi_i^2 \equiv k \pmod{\alpha}.$$

In terms of ncells the multiplicity function $c_{Nd}$ (2.7) has the following form

$$c_{Nd}(k) = \text{ncells}(\text{lattice}^d(N), N, k).$$

**Definition E.6.** *The logical function $\text{zrf}(\text{L}, \alpha, \beta)$ ("zerofy") is equal to "true" if*

$$\forall k \in \mathbb{Z}(\alpha) \quad \text{ncells}(\text{L}, \alpha, k) \equiv 0 \pmod{\beta},$$

*otherwise it is "false".*

The notation $\text{zrf}(\text{L}, \alpha, \beta)$ is equivalent to $\text{zrf}(\text{L}, \alpha, \beta) = true$.

The parameter $\alpha$ of the functions ncells and zrf is called the *momentum ring parameter*, and $\beta$ is called the *energy ring parameter*.

In terms of fumction zrf the theorem (2.8) has the following form

$$d \geqslant 3 \text{ or } (d \geqslant 2, N = 2^n) \implies \text{zrf}(\text{lattice}^d(N), N, N).$$

*Appendix*

### F. LEMMAS

To simplify the proof we introduce several simple lemmas. For obvious lemmas, the proofs are skipped.

**Lemma F.1** (on increasing of the momentum ring parameter)**.**

$$\text{ncells}(\text{L}, \alpha, k) = \sum_{j=0}^{n-1} \text{ncells}(\text{L}, n\alpha, k + j\alpha). \tag{F.1}$$

*Proof.* The number $k \in \mathbb{Z}(\alpha)$ corresponds to the numbers $k$, $k + \alpha$, $k + 2\alpha$, $k + 3\alpha$, ... , $k + (n-1)\alpha$ in $\mathbb{Z}(n\alpha)$. To go from modulus $n\alpha$ to modulus $\alpha$, one needs to sum the corresponding numbers of cells. $\square$

**Lemma F.2** (on decreasing of the momentum ring parameter)**.**

$$\text{zrf}(\text{L}, n\alpha, \beta) \implies \text{zrf}(\text{L}, \alpha, \beta).$$

**Lemma F.3** (on decreasing of the energy ring parameter).
$$\mathrm{zrf}(\mathrm{L}, \alpha, n\beta) \;\Rightarrow\; \mathrm{zrf}(\mathrm{L}, \alpha, \beta).$$

**Lemma F.4** (on lattice stretching).
$$\mathrm{zrf}(\mathrm{L}, \alpha, \beta) \;\Rightarrow\; \mathrm{zrf}(n \cdot \mathrm{L}, n^2\alpha, \beta).$$

**Lemma F.5** (on lattice shift).
$$\mathrm{ncells}(n \cdot \mathrm{L} + n\alpha\mathbf{a}, n^2\alpha, k) = \mathrm{ncells}(n \cdot \mathrm{L}, n^2\alpha, k).$$

*Proof.* Let $\xi_i$ be the coordinates of a cell in the set L. $n\xi_i$ are the coordinates of a cell in the set $n \cdot \mathrm{L}$. When shifted by the vector $n\alpha\mathbf{a}$, the coordinates of the cells of the set $n \cdot \mathrm{L}$ are shifted by the corresponding components of this vector:
$$(n\xi_1, n\xi_2, n\xi_3, \ldots) \to (n\xi_1 + n\alpha a_1, n\xi_2 + n\alpha a_2, n\xi_3 + n\alpha a_3, \ldots).$$
The sum of the squares of the coordinates changes as follows:
$$(n\xi_1)^2 + (n\xi_2)^2 + (n\xi_3)^2 + \ldots \to (n\xi_1 + n\alpha a_1)^2 + (n\xi_2 + n\alpha a_2)^2 + (n\xi_3 + n\alpha a_3)^2 + \ldots.$$
Increment of the sum of squares:
$$(n\xi_1 + n\alpha a_1)^2 + (n\xi_2 + n\alpha a_2)^2 + (n\xi_3 + n\alpha a_3)^2 + \ldots - (n\xi_1)^2 - (n\xi_2)^2 - (n\xi_3)^2 - \ldots$$
$$= 2n^2\alpha a_1\xi_1 + n^2\alpha^2 a_1^2 + 2n^2\alpha a_2\xi_2 + n^2\alpha^2 a_2^2 + 2n^2\alpha a_3\xi_3 + n^2\alpha^2 a_3^2 + \ldots$$
$$= n^2\alpha(2a_1\xi_1 + \alpha a_1^2 + 2a_2\xi_2 + \alpha a_2^2 + 2a_3\xi_3 + \alpha a_3^2 + \ldots) \equiv 0 \pmod{n^2\alpha}.$$
Therefore
$$\mathrm{ncells}(n \cdot \mathrm{L} + n\alpha\mathbf{a}, n^2\alpha, k) = \mathrm{ncells}(n \cdot \mathrm{L}, n^2\alpha, k).$$
$\square$

**Lemma F.6** (on sum of lattices).
$$\mathrm{L}_1 \cap \mathrm{L}_2 = \varnothing, \; \mathrm{zrf}(\mathrm{L}_1, \alpha, \beta), \mathrm{zrf}(\mathrm{L}_2, \alpha, \beta) \;\Rightarrow\; \mathrm{zrf}(\mathrm{L}_1 \cup \mathrm{L}_2, \alpha, \beta).$$

**Lemma F.7** (on subtraction of lattices).
$$\mathrm{L}_1 \cap \mathrm{L}_2 = \varnothing, \; \mathrm{zrf}(\mathrm{L}_1 \cup \mathrm{L}_2, \alpha, \beta), \mathrm{zrf}(\mathrm{L}_2, \alpha, \beta) \;\Rightarrow\; \mathrm{zrf}(\mathrm{L}_1, \alpha, \beta).$$

**Lemma F.8** (on multiple lattices).
*Let $\mathrm{L}_i \cap \mathrm{L}_j = \varnothing$ if $i \neq j$, and $\mathrm{ncells}(\mathrm{L}_i, \alpha, k) = \mathrm{ncells}(\mathrm{L}_j, \alpha, k)$. Then*
$$\mathrm{zrf}(\mathrm{L}_1, \alpha, \beta) \;\Rightarrow\; \mathrm{zrf}\Big(\bigcup_{j=1}^{n} \mathrm{L}_j, \alpha, n\beta\Big).$$

**Lemma F.9** (on periodicity).
*Let*
$$\forall k \in \mathbb{Z}(P\alpha) \; \mathrm{ncells}(\mathrm{L}, P\alpha, k \oplus P) = \mathrm{ncells}(\mathrm{L}, P\alpha, k),$$
*where $\oplus$ is addition in the ring $\mathbb{Z}(P\alpha)$. Then*
$$\mathrm{zrf}(\mathrm{L}, P, \alpha\beta) \;\Rightarrow\; \mathrm{zrf}(\mathrm{L}, P\alpha, \beta).$$

*Proof.* By Lemma F.1 (on increasing of the momentum ring parameter) and taking into account the periodicity of $\mathrm{ncells}(\mathrm{L}, P\alpha, k)$,
$$\mathrm{ncells}(\mathrm{L}, P, k) = \sum_{j=0}^{\alpha-1} \mathrm{ncells}(\mathrm{L}, P\alpha, k + jP) = \alpha \cdot \mathrm{ncells}(\mathrm{L}, P\alpha, k),$$
$$\frac{\mathrm{ncells}(\mathrm{L}, P, k)}{\alpha} = \mathrm{ncells}(\mathrm{L}, P\alpha, k).$$
If $\mathrm{ncells}(\mathrm{L}, P, k)$ is a multiple of $\alpha\beta$, then $\mathrm{ncells}(\mathrm{L}, P\alpha, k)$ is a multiple of $\beta$. $\square$

**Lemma F.10** (on permutation of remainders). *Let $\alpha$ and $n$ be coprime, $A$ be the set of the remainders of the division of elements $n\mathbb{Z}(\alpha) + a$ by $\alpha$. Then $A = \mathbb{Z}(\alpha)$.*

## G. PROOF-2

Theorem on number-theory renormalization (2.8) formulated in terms of the function zrf: for $d \geqslant 3$ and any natural $N$, as well as for $d = 2$ and $N = 2^m, m \in \mathbb{N}$

$$\text{zrf}(\text{lattice}^d(N), N, N). \tag{G.1}$$

The theorem is obvious in the trivial case $N = 1$, easily verified for $N = 2$, and proved in the Appendix C for odd primes $N$. It remains to prove the theorem for composite $N$.

We will prove the theorem separately for each of the following 3 cases of composite $N$:

- $N$ is a power of an odd prime $p$,

- $N$ is a power of 2,

- $N$ is not a prime power.

### 1. Powers of Odd Primes

Let us prove the theorem (G.1) for the $m$-th power of an odd prime $p$:

$$N = p^m. \tag{G.2}$$

Unless otherwise specifically stated, we will assume that $d = 3$.

We will prove by induction, assuming that the hypothesis is true for $p^{m-1}$ and for $p^{m-2}$:

$$\text{zrf}(\text{lattice}^d(p^{m-1}), p^{m-1}, p^{m-1}), \tag{G.3}$$

$$\text{zrf}(\text{lattice}^d(p^{m-2}), p^{m-2}, p^{m-2}). \tag{G.4}$$

The basis of the induction is the proven above validity of the hypothesis for $d = 3$ for $m = 0, 1$, i.e. for $N = 1$ and $N = p$:

$$\text{zrf}(\text{lattice}^d(1), 1, 1), \tag{G.5}$$

$$\text{zrf}(\text{lattice}^d(p), p, p). \tag{G.6}$$

Divide the lattice$^d(N)$ (Fig. 1) into 2 parts: $p \cdot \text{lattice}^d(p^{m-1})$ and $\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1})$.

The first part ($p \cdot \text{lattice}^d(p^{m-1})$) consists of all cells of lattice$^d(N)$ such that each of their coordinates $\xi_i$ is a multiple of $p$ (Fig. 2).

The second part ($\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1})$) consists of all other cells of lattice$^d(N)$, i.e. those with at least one of their coordinates $\xi_i$ is not a multiple of $p$ (Fig. 3).

Similarly, we divide the lattice$^d(p^{m-1})$ into 2 parts: $p \cdot \text{lattice}^d(p^{m-2})$ and $\text{lattice}^d(p^{m-1}) - p \cdot \text{lattice}^d(p^{m-2})$. (Fig. 1)
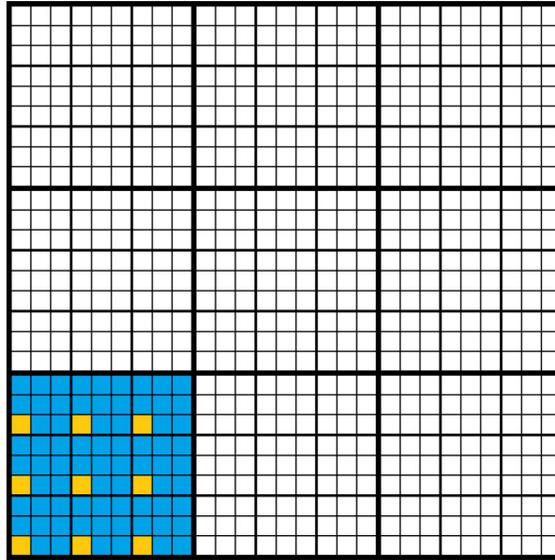
**Fig. 1.** 2-dimensional $\mathrm{lattice}^2(N)$ (the section of $\mathrm{lattice}^3(N)$). The origin is in the lower left corner. Here is an example $N = 3^3 = 27$. $\mathrm{lattice}^2(p^{m-1})$ (orange and blue cells) divided into parts $p \cdot \mathrm{lattice}^2(p^{m-2})$ (orange cells) and $\mathrm{lattice}^2(p^{m-1}) - p \cdot \mathrm{lattice}^2(p^{m-2})$ (blue cells).

We will prove zerofying for each of the 2 parts of $\mathrm{lattice}^d(N)$ separately:

$$\mathrm{zrf}(p \cdot \mathrm{lattice}^d(p^{m-1}), N, N), \tag{G.7}$$

$$\mathrm{zrf}(\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1}), N, N), \tag{G.8}$$

and then, by Lemma F.6 (on sum of lattices), zerofying will be proved for the entire $\mathrm{lattice}^d(N)$ (G.1).
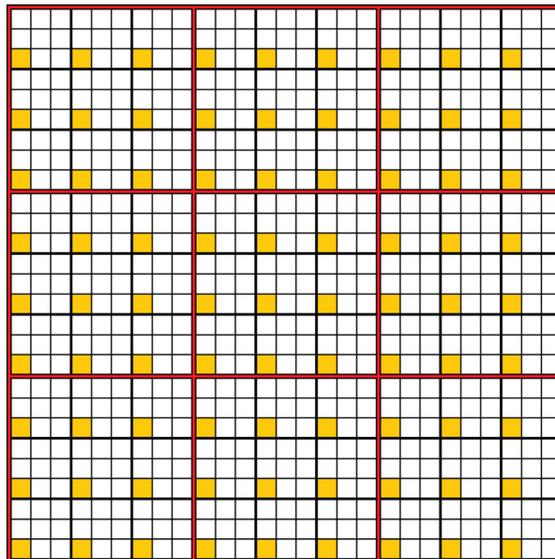


**Fig. 2.** The first part $(p \cdot \mathrm{lattice}^2(p^{m-1}))$ of $\mathrm{lattice}^2(N)$ (orange cells). The red frames show the partition of $p \cdot \mathrm{lattice}^2(p^{m-1})$ into sets $p \cdot \mathrm{lattice}^2(p^{m-2}) + p^{m-1}\mathbf{a}$, where $\mathbf{a} \in \mathrm{lattice}^2(p)$.

**The first part of the lattice.** Since the set $p \cdot \mathrm{lattice}^d(p^{m-2})$ is $\mathrm{lattice}^d(p^{m-2})$ stretched by $p$ times, by virtue of the hypothesis for $p^{m-2}$ (G.4), Lemma F.4 (on lattice stretching) and the fact that $N = p^m$

(G.2)

$$\mathrm{zrf}(p \cdot \mathrm{lattice}^d(p^{m-2}), N, p^{m-2}). \tag{G.9}$$

Note that the set $p \cdot \mathrm{lattice}^d(p^{m-1})$ can be divided into $p^d$ subsets $p \cdot \mathrm{lattice}^d(p^{m-2}) + p^{m-1}\mathbf{a}$, where $\mathbf{a} \in \mathrm{lattice}^d(p)$. One of these subsets is $p \cdot \mathrm{lattice}^d(p^{m-2})$, and the rest are obtained from $p \cdot \mathrm{lattice}^d(p^{m-2})$ by such a shift of all its cells, that each coordinate difference is a multiple of $p^{m-1}$ (Fig. 2).

Since $p^{m-1}$ and the coordinates of all cells from $p \cdot \mathrm{lattice}^d(p^{m-2})$ are divisible by $p$, by Lemma F.5 (on lattice shift) for each set $p \cdot \mathrm{lattice}^d(p^{m-2}) + p^{m-1}\mathbf{a}$ the value of $\mathrm{ncells}(p \cdot \mathrm{lattice}^d(p^{m-2}) + p^{m-1}\mathbf{a}, N, k)$ does not depend on $\mathbf{a}$. Therefore, since one of the sets $p \cdot \mathrm{lattice}^d(p^{m-2}) + p^{m-1}\mathbf{a}$ is the set $p \cdot \mathrm{lattice}^d(p^{m-2})$, and there are $p^d$ such sets, due to (G.9) and Lemma F.8 (on multiple lattices)

$$\mathrm{zrf}(p \cdot \mathrm{lattice}^d(p^{m-1}), N, p^{m+d-2}). \tag{G.10}$$

Hence, taking into account that $N = p^m$ (G.2), if $d \geqslant 2$, by Lemma F.3 (on decreasing of the energy ring parameter)

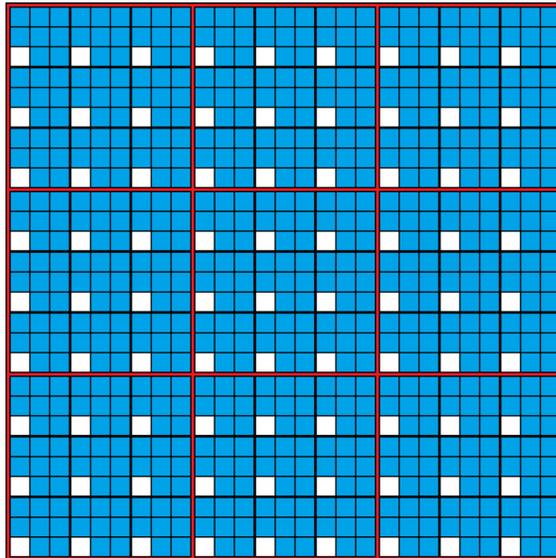$$\mathrm{zrf}(p \cdot \mathrm{lattice}^d(p^{m-1}), N, N). \tag{G.11}$$



**Fig. 3.** The second part $(\mathrm{lattice}^2(N) - p \cdot \mathrm{lattice}^2(p^{m-1}))$ of the $\mathrm{lattice}^2(N)$ (blue cells). The red frames show the partition of $\mathrm{lattice}^2(N) - p \cdot \mathrm{lattice}^2(p^{m-1})$ into sets $[\mathrm{lattice}^2(p^{m-1}) - p \cdot \mathrm{lattice}^2(p^{m-2})] + p^{m-1}\mathbf{a}$, where $\mathbf{a} \in \mathrm{lattice}^2(p)$.

**The second part of the lattice.** From (G.9) and by Lemma F.2 (on decreasing of the momentum ring parameter) it follows that

$$\mathrm{zrf}(p \cdot \mathrm{lattice}^d(p^{m-2}), p^{m-1}, p^{m-2}). \tag{G.12}$$

From the validity of the hypothesis for $p^{m-1}$ (G.3) and by virtue of the Lemma F.3 (on decreasing of the energy ring parameter), it follows that

$$\mathrm{zrf}(\mathrm{lattice}^d(p^{m-1}), p^{m-1}, p^{m-2}). \tag{G.13}$$

Due to (G.12), (G.13) and Lemma F.7 (on subtraction of lattices)

$$\mathrm{zrf}(\mathrm{lattice}^d(p^{m-1}) - p \cdot \mathrm{lattice}^d(p^{m-2}), p^{m-1}, p^{m-2}). \tag{G.14}$$

Now we divide the set $\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1})$ into subsets $[\mathrm{lattice}^d(p^{m-1}) - p \cdot \mathrm{lattice}^d(p^{m-2})] + p^{m-1}\mathbf{a}$, where $\mathbf{a} \in \mathrm{lattice}^d(p)$ (Fig. 3) in the same way as the set $p \cdot \mathrm{lattice}^d(p^{m-1})$ was divided into sets $p \cdot \mathrm{lattice}^d(p^{m-2}) + p^{m-1}\mathbf{a}$, where $\mathbf{a} \in \mathrm{lattice}^d(p)$.

Similarly, by Lemma F.5 (on lattice shift), for each of these sets the values of $\mathrm{ncells}([\mathrm{lattice}^d(p^{m-1}) - p \cdot \mathrm{lattice}^d(p^{m-2})] + p^{m-1}\mathbf{a}, p^{m-1}, k)$ does not depend on $\mathbf{a}$. Therefore, since one of these sets is $\mathrm{lattice}^d(p^{m-1}) - p \cdot \mathrm{lattice}^d(p^{m-2})$, and there are $p^d$ such sets, due to (G.14) and Lemma F.8 (on multiple lattices)

$$\mathrm{zrf}(\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1}), p^{m-1}, p^{m+d-2}). \tag{G.15}$$

For $d \geqslant 3$, if we succeed in applying Lemma F.9 (on periodicity), then, taking into account that $N = p^m$ (G.2), zeroing for the second part of the lattice (G.8) will be proven. For $d = 2$ a separate consideration is required.

Now we divide the set $\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1})$ into disjoint sets of the form

$$p^{m-1} \cdot lattice(p) + (\nu_1, \xi_2, \xi_3, \ldots),$$
$$p^{m-1} \cdot lattice_2(p) + (\xi_1, \nu_2, \xi_3, \ldots),$$
$$p^{m-1} \cdot lattice_3(p) + (\xi_1, \xi_2, \nu_3, \ldots),$$
$$\ldots$$

$$\nu_i \in \mathbb{Z}(p^{m-1}), \quad \nu_i \mod p \neq 0.$$

with $p$ cells in each set (Fig. 4) as follows. Let's take an arbitrary cell $\boldsymbol{\xi}$ from $\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1})$, take from its $d$ coordinates the first not multiple of $p$ (according to the definition of this set, at least one of the coordinates is not a multiple of $p$), and then we will shift this coordinate by multiples of $p^{m-1}$. Collect the resulting $p$ cells into a set. Regardless of which point of this set we start from, we will collect the same set. So, the partition of $\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1})$ into subsets is unique.

Suppose we have selected a cell $\boldsymbol{\xi}$, and $\xi_1$ is the first coordinate not a multiple of $p$. We will shift $\xi_1$ by multiples of $p^{m-1}$. We get the set $p^{m-1} \cdot lattice(p) + (\nu_1, \xi_2, \xi_3, \ldots)$. The elements of the set has the form

$$(\xi_1, \xi_2, \xi_3, \ldots) = (\nu_1 + kp^{m-1}, \xi_2, \xi_3, \ldots), \tag{G.16}$$

where $k \in \mathbb{Z}(p), \nu_1 \in \mathbb{Z}(p^{m-1}), \nu_i \mod p \neq 0$.

The sum of squares of the coordinates (G.16) of cells from this set is

$$(\nu_1 + kp^{m-1})^2 + \xi_2^2 + \xi_3^2 + \ldots = k^2 p^{2m-2} + 2kp^{m-1}\nu_1 + \nu_1^2 + \xi_2^2 + \xi_3^2 + \ldots. \tag{G.17}$$
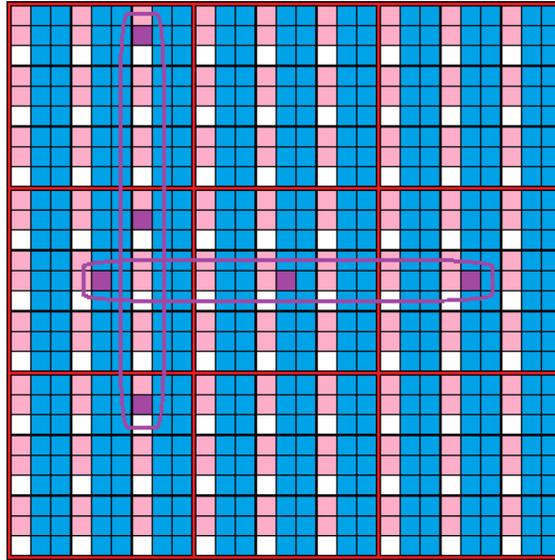
**Fig. 4.** Cells of the the the set $\text{lattice}^2(N) - p \cdot \text{lattice}^2(p^{m-1})$ whose first coordinate is not a multiple of $p$ are shown in blue. The pink color shows those cells of this set, for which the first coordinate is a multiple of $p$, and the second coordinate is not a multiple of $p$. (Note: a 3-dimensional set also has cells whose first two coordinates are not a multiple of $p$, and the third coordinate is a multiple of $p$). Purple color shows examples of sets $p^{m-1} \cdot \text{lattice}(p) + (\nu_1, \xi_2)$ (arranged horizontally) and $p^{m-1} \cdot \text{lattice}_2(p) + (\xi_1, \nu_2)$ (arranged vertically).

Consider the sum (G.17) modulo $N$. If $m \geqslant 2$, then $p^{2m-2}$ is a multiple of $N = p^m$, so the term $k^2 p^{2m-2}$ can be dropped:

$$(2kp^{m-1}\nu_1 + \nu_1^2 + \xi_2^2 + \xi_3^2 + \ldots) \mod N. \tag{G.18}$$

Consider the the remainder of the division of the term $2kp^{m-1}\nu_1$ by $N$ (the other terms of (G.18) are constant):

$$2kp^{m-1}\nu_1 \mod N = p^{m-1}(2k\nu_1 \mod p). \tag{G.19}$$

Since $\nu_i \mod p \neq 0$ and $p$ are odd primes, $2\nu_1$ and $p$ are coprime. Therefore, by Lemma F.10 (on permutation of remainders), the set of possible values of $2k\nu_1 \mod p$ coincides with $\mathbb{Z}(p)$. Therefore, the set of possible values (G.19) is the same as $p^{m-1}\mathbb{Z}(p)$.

Therefore, for the set $p^{m-1} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots)$ the function $\text{ncells}(p^{m-1} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots), N, k)$ is periodic in $k$ with period $p^{m-1}$:

$$\text{ncells}(p^{m-1} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots), N, k \oplus p^{m-1})$$
$$= \text{ncells}(p^{m-1} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots), N, k). \tag{G.20}$$

The function (G.20) takes the values 0 and 1, and it takes the values 1 only for $k - (\nu_1^2 + \xi_2^2 + \xi_3^2 + \ldots) \in p^{m-1}\mathbb{Z}(p)$.

Since the set $\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1})$ consists entirely of such disjoint sets with property (G.20), and for union of disjoint sets, these functions add up, then for the entire set $\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1})$ this function is periodic in $k$ with period $p^{m-1}$, that is

$$\text{ncells}(\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1}), N, k \oplus p^{m-1})$$
$$= \text{ncells}(\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1}), N, k). \tag{G.21}$$

Hence, by virtue of (G.15) and Lemma F.9 (on periodicity)

$$\text{zrf}(\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1}), N, p^{m+d-3}). \tag{G.22}$$

If $d \geqslant 3$, then, taking into account that $N = p^m$ (G.2), by virtue of Lemma F.3 (on decreasing of the energy ring parameter) it follows from (G.22) that

$$\mathrm{zrf}(\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1}), N, N). \tag{G.23}$$

Thus, applying Lemma F.6 (on sum of lattices) to (G.11) and (G.23) we have proved the theorem for $N = p^m, d \geqslant 3$

$$\mathrm{zrf}(\mathrm{lattice}^d(N), N, N).$$

### 2. Proof for $d \geqslant 2$, $N = 2^m$

If we apply the proof for powers of primes for the case $d = 2$, $p = 2$, then it turns out that the proof for the first part of the lattice works, but the proof for the second part of the lattice is valid up to the formula (G.15) before the assumptions $p \neq 2$ and $d \geqslant 3$ are used. A closer look shows that for $d = p = 2$ we need to retreat to the formula (G.10).

Now, as an induction hypothesis, we take the validity of the hypothesis not for the previous two powers $(m - 1, m - 2)$, but for three $(m - 1, m - 2, m - 3)$:

$$\mathrm{zrf}(\mathrm{lattice}^d(p^{m-1}), p^{m-1}, p^{m-1}), \tag{G.24}$$

$$\mathrm{zrf}(\mathrm{lattice}^d(p^{m-2}), p^{m-2}, p^{m-2}), \tag{G.25}$$

$$\mathrm{zrf}(\mathrm{lattice}^d(p^{m-3}), p^{m-3}, p^{m-3}). \tag{G.26}$$

Here $d = p = 2$, but we do not substitute 2 for these parameters for the convenience of comparison with the previously analyzed cases.

Since we now use the hypothesis for the previous three powers as the induction hypothesis, we can use the proof using the previous two powers by substituting $p^{m-1}$ instead of $N$ (that is, lowering the required powers of $p$ by 1). For $d \geqslant 2$ from (G.10) by reducing the powers of $p$ by 1 it follows

$$\mathrm{zrf}(p \cdot \mathrm{lattice}^d(p^{m-2}), p^{m-1}, p^{m-1}). \tag{G.27}$$

From the validity of the hypothesis for $p^{m-1}$ (G.24), due to (G.27) and the Lemma F.7 (on subtraction of lattices)

$$\mathrm{zrf}(\mathrm{lattice}^d(p^{m-1}) - p \cdot \mathrm{lattice}^d(p^{m-2}), p^{m-1}, p^{m-1}). \tag{G.28}$$

In the same way as (G.15) was obtained from (G.14), we obtain (G.29) from (G.24).

Divide the set $\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1})$ into subsets $[\mathrm{lattice}^d(p^{m-1}) - p \cdot \mathrm{lattice}^d(p^{m-2})] + p^{m-1}\mathbf{a}$, where $\mathbf{a} \in \mathrm{lattice}^d(p)$ (Fig. 3).

Similarly, by Lemma F.5 (on lattice shift), for each of these sets the values of $\mathrm{ncells}([\mathrm{lattice}^d(p^{m-1}) - p \cdot \mathrm{lattice}^d(p^{m-2})] + p^{m-1}\mathbf{a}, p^{m-1}, k)$ does not depend on $\mathbf{a}$. Therefore, since one of these sets is $\mathrm{lattice}^d(p^{m-1}) - p \cdot \mathrm{lattice}^d(p^{m-2})$, and there are $p^d$ such sets, due to (G.28) and Lemma F.8 (on multiple lattices)

$$\mathrm{zrf}(\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1}), p^{m-1}, p^{m+d-1}). \tag{G.29}$$

Now (similarly to derivation of (G.15)) we need to apply the F.9 Lemma (on periodicity) to increase the momentum ring parameter by decrease the energy ring parameter.

For $p = 2$, the set of possible values (G.19) no longer coincides with $p^{m-1}\mathbb{Z}(p)$, which was based on the fact that $2\nu_1$ and $p$ are coprime, but this is not true for the case $p = 2$.

Therefore, for $p = 2$ we will divide into sets of $p$ cells not the set $\mathrm{lattice}^d(N) - p \cdot \mathrm{lattice}^d(p^{m-1})$ as a whole, but each of the $p^d$ subsets $[\mathrm{lattice}^d(p^{m-1}) - p \cdot \mathrm{lattice}^d(p^{m-2})] + p^{m-1}\mathbf{a}$, where $\mathbf{a} \in \mathrm{lattice}^d(p)$. So, the coordinate in each of the resulting sets will be shifted by a value that is a multiple of $p^{m-2}$, not $p^{m-1}$.

The set $\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1})$ is divided into disjoint sets of the form

$$p^{m-2} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots),$$

$$p^{m-2} \cdot \text{lattice}_2(p) + (\xi_1, \nu_2, \xi_3, \ldots),$$

$$p^{m-2} \cdot \text{lattice}_3(p) + (\xi_1, \xi_2, \nu_3, \ldots),$$

$$\ldots$$

$$\nu_i \in \mathbb{Z}(p^{m-2}) + p^{m-1}\mathbb{Z}(p), \qquad \nu_i \mod p \neq 0.$$

with $p = 2$ cells in each.

This partition is performed as follows. Take an arbitrary cell $\boldsymbol{\xi}$ from $\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1})$, select from its $d$ coordinates the first non-multiple of $p$ (according to the definition of this set, at least one of the coordinates is not a multiple of $p$), and then we will shift this coordinate by multiples of $p^{m-2}$, so as not to go beyond a specific set $[\text{lattice}^d(p^{m-1}) - p \cdot \text{lattice}^d(p^{m-2})] + p^{m-1}\mathbf{a}$ (Fig. 5). Collect the resulting $p$ cells into a set. Regardless of which point of this set we start from, we will collect the same set, that is, such a partition of $\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1})$ into subsets is unique.
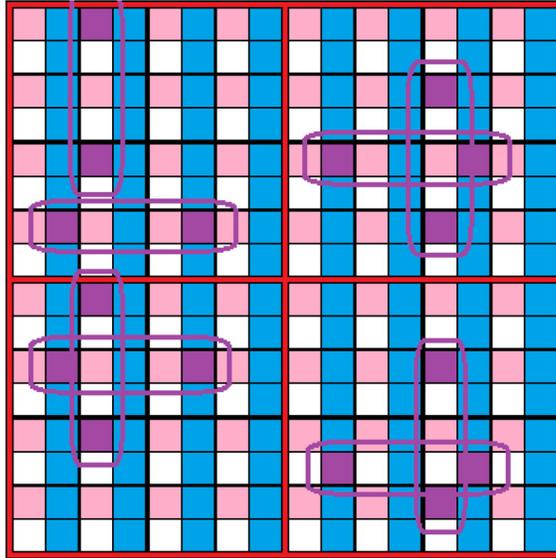


**Fig. 5.** Cells of the $\text{lattice}^2(N) - p \cdot \text{lattice}^2(p^{m-1})$ with first coordinate is not a multiple of $p$ are shown in blue. The pink color shows those cells of this set, for which the first coordinate is a multiple of $p$, and the second coordinate is not a multiple of $p$. (Note: a 3-dimensional set also has cells whose first two coordinates are not a multiple of $p$, and the third coordinate is a multiple of $p$). The set $\text{lattice}^2(N) - p \cdot \text{lattice}^2(p^{m-1})$ is divided into sets $[\text{lattice}^2(p^{m-1}) - p \cdot \text{lattice}^2(p^{m-2})] + p^{m-1}\mathbf{a}$, where $\mathbf{a} \in \text{lattice}^2(p)$ (shown using red frames), each of of which is divided into sets $p^{m-2} \cdot \text{lattice}(p) + (\nu_1, \xi_2)$ (arranged horizontally) and $p^{m-2} \cdot \text{lattice}_2(p) + (\xi_1, \nu_2)$ (arranged vertically) examples of which are shown in purple. Here $N = 2^4 = 16$.

Suppose we have selected a cell $\boldsymbol{\xi}$, and the first coordinate not a multiple of $p$ is $\xi_1$. We will shift $\xi_1$ by multiples of $p^{m-2}$. We get the set $p^{m-2} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots)$ from the cells

$$(\xi_1, \xi_2, \xi_3, \ldots) = (\nu_1 + kp^{m-2}, \xi_2, \xi_3, \ldots), \tag{G.30}$$

where $k \in \mathbb{Z}(p)$, $\nu_1 \in \mathbb{Z}(p^{m-2}) + p^{m-1}\mathbb{Z}(p)$, $\nu_1 \mod p \neq 0$.

The sum of squares of the coordinates (G.30) of cells from this set is

$$(\nu_1 + kp^{m-2})^2 + \xi_2^2 + \xi_3^2 + \ldots = k^2 p^{2m-4} + 2kp^{m-2}\nu_1 + \nu_1^2 + \xi_2^2 + \xi_3^2 + \ldots. \tag{G.31}$$

Consider this sum of squares modulo $N$. If $m \geqslant 4$, then $p^{2m-4}$ is a multiple of $N$, and the term $k^2 p^{2m-4}$ can be dropped:

$$(2kp^{m-2}\nu_1 + \nu_1^2 + \xi_2^2 + \xi_3^2 + \ldots) \mod N. \tag{G.32}$$

Due to the fact that it is possible to pass from the expression (G.31) to the expression (G.32) only when $m \geqslant 4$, for $p = 2$ we have to choose as induction basis not $m = 0, 1, 2$, but $m = 1, 2, 3$.

Taking into account that $p = 2$, so $\nu_1 = 1$ (since $\nu_1 \mod p \neq 0$), we rewrite (G.32) as

$$(kp^{m-1} + 1 + \xi_2^2 + \xi_3^2 + \ldots) \mod N. \tag{G.33}$$

Consider the remainder of the division of the term $2kp^{m-1}\nu_1$ by $N$ (the other terms of (G.33) are constant):

$$kp^{m-1} \in p^{m-1}\mathbb{Z}(p). \tag{G.34}$$

Therefore, for the set $p^{m-2} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots)$ the function $\text{ncells}(p^{m-2} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots), N, k)$ is periodic in $k$ with period $p^{m-1}$:

$$\text{ncells}(p^{m-2} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots), N, k \oplus p^{m-1})$$
$$= \text{ncells}(p^{m-2} \cdot \text{lattice}(p) + (\nu_1, \xi_2, \xi_3, \ldots), N, k). \tag{G.35}$$

Since the set $\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1})$ consists entirely of such disjoint sets, for each of which this function is periodic with period $p^{m-1}$, and for union of disjoint sets, these functions add up, then for the entire set $\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1})$ this function is periodic in $k$ with period $p^{m-1}$, that is

$$\text{ncells}(\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1}), N, k \oplus p^{m-1})$$
$$= \text{ncells}(\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1}), N, k). \tag{G.36}$$

Further, similarly to the statement (G.22) we obtain

$$\text{zrf}(\text{lattice}^d(N) - p \cdot \text{lattice}^d(p^{m-1}), N, N). \tag{G.37}$$

The induction base ($N = 2, 4, 8$) is verified numerically.

**a. Values** $c_{Nd}(k) = \text{ncells}(\text{lattice}^d(N), N, k)$ **for** $d = 1, 2$, $N = 2, 4, 8$.

| | $k$ | 0 | 1 |
|---|---|---|---|
| $c_{2,1}(k) = \text{ncells}(\text{lattice}^1(2), 2, k)$ | | 1 | 1 |
| $c_{2,2}(k) = \text{ncells}(\text{lattice}^2(2), 2, k)$ | | 2 | 2 |

| | $k$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| $c_{4,1}(k) = \text{ncells}(\text{lattice}^1(4), 4, k)$ | | 2 | 2 | 0 | 0 |
| $c_{4,2}(k) = \text{ncells}(\text{lattice}^2(4), 4, k)$ | | 4 | 8 | 4 | 0 |

| | $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| $c_{8,1}(k) = \text{ncells}(\text{lattice}^1(8), 8, k)$ | | 2 | 4 | 0 | 0 | 2 | 0 | 0 | 0 |
| $c_{8,2}(k) = \text{ncells}(\text{lattice}^2(8), 8, k)$ | | 8 | 16 | 16 | 0 | 8 | 16 | 0 | 0 |

### 3. Composite Numbers that are not Prime Powers

A composite number $N$ can be represented as a product of powers of unequal primes $p_i$ (if $i \neq j$, then $p_i \neq p_j$):

$$N = \prod_{i=1}^{n} p_i^{m_i}. \tag{G.38}$$

Denote

$$M = \prod_{i=1}^{n-1} p_i^{m_i}, \tag{G.39}$$

$$K = p_n^{m_n}. \tag{G.40}$$

That is

$$N = MK. \tag{G.41}$$

$M$ and $K$ are coprime.

We will prove by induction. As a step of induction, we deduce the validity of the hypothesis for $N$ from its validity for $M$ and $K$:

$$\mathrm{zrf}(\mathrm{lattice}^d(M), M, M), \ \mathrm{zrf}(\mathrm{lattice}^d(K), K, K) \ \Rightarrow \ \mathrm{zrf}(\mathrm{lattice}^d(N), N, N). \tag{G.42}$$

As the basis of the induction, we take the validity of the hypothesis for $p_1^{m_1}$:

$$\mathrm{zrf}(\mathrm{lattice}^d(p_1^{m_1}), p_1^{m_1}, p_1^{m_1}). \tag{G.43}$$

Since $p_1^{m_1}$ and $K$ are powers of primes, for $d = 3$ the base of induction has already been proved and $\mathrm{zrf}(\mathrm{lattice}^d(K), K, K)$ is proved.

Represent the lattice $\mathrm{lattice}^d(N)$ as $K^d$ pairwise disjoint lattices $K \cdot \mathrm{lattice}^d(M) + \mathbf{a}$, where $\mathbf{a} \in \mathrm{lattice}^d(K)$ (Fig. 6).

We prove that for each lattice $K \cdot \mathrm{lattice}^d(M) + \mathbf{a}$

$$\mathrm{zrf}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, N, N) \tag{G.44}$$

after which, by Lemma F.6 (on sum of lattices), it will be proved that

$$\mathrm{zrf}(\mathrm{lattice}^d(N), N, N). \tag{G.45}$$

Each lattice coordinate $\mathrm{lattice}^d(M)$ runs through all values in $\mathbb{Z}(M)$. By Lemma F.10 (on permutation of remainders), each coordinate of the lattice $K \cdot \mathrm{lattice}^d(M) + \mathbf{a}$ modulo $M$ also runs through all values in $\mathbb{Z}(M)$. That is, the lattices $\mathrm{lattice}^d(M)$ and $K \cdot \mathrm{lattice}^d(M) + \mathbf{a}$ consist of the same cells if their coordinates are taken modulo $M$. Therefore, the validity of the hypothesis for $M$ (G.42) implies

$$\mathrm{zrf}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, M, M). \tag{G.46}$$

Consider two cells in $K \cdot \mathrm{lattice}^d(M) + \mathbf{a}$:

$$K\boldsymbol{\xi} + \mathbf{a},$$

$$K\boldsymbol{\xi}' + \mathbf{a},$$

where $\boldsymbol{\xi}, \boldsymbol{\xi}' \in \mathrm{lattice}^d(M)$. The difference of the sums of squares of their coordinates:

$$(K\xi_1 + a_1)^2 + (K\xi_2 + a_2)^2 + \ldots - (K\xi_1' + a_1)^2 - (K\xi_2' + a_2)^2 - \ldots \tag{G.47}$$
$$= K^2(\xi_1^2 + \xi_2^2 + \ldots - \xi_1'^2 - \xi_2'^2 - \ldots) + 2K((\xi_1 - \xi_1')a_1 + (\xi_2 - \xi_2')a_2 + \ldots).$$

So, the difference between the sums of squared coordinates of two cells from $K \cdot \mathrm{lattice}^d(M) + \mathbf{a}$ is a multiple of $K$.

Compare the functions $\mathrm{ncells}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, M, z)$ and $\mathrm{ncells}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, N, y)$.

Each $z \in \mathbb{Z}(M)$ corresponds to $K$ different values of $y \in \mathbb{Z}(N)$ such that $z = y \mod M$.

Let $\mathrm{ncells}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, M, z_0) = 0$, then $\mathrm{ncells}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, N, y_0) = 0$ for all $z_0 = y_0 \mod M$.

Let $\mathrm{ncells}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, M, z_1) \neq 0$, then there exists a non-empty subset of the lattice $K \cdot \mathrm{lattice}^d(M) + \mathbf{a}$ such that for each of its cells the sum of squared coordinates modulo $M$ is equal to $k_1$. That is, in this subset, the sums of squares of cell coordinates differ from each other by multiples of $M$. But we came to the conclusion that these quantities are multiples of $K$ as well. Therefore, they are multiples of the least common multiple of $M$ and $K$. Since $M$ and $K$ are coprime, these quantities are multiples of $N = MK$ (G.41). Since $y_1 \in \mathbb{Z}(N)$, among all $K$ distinct $y_1 \equiv z_1 \mod M$ there is one value $\tilde{y}_1$ for which

$$\mathrm{ncells}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, N, \tilde{y}_1) = \mathrm{ncells}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, M, z_1), \tag{G.48}$$

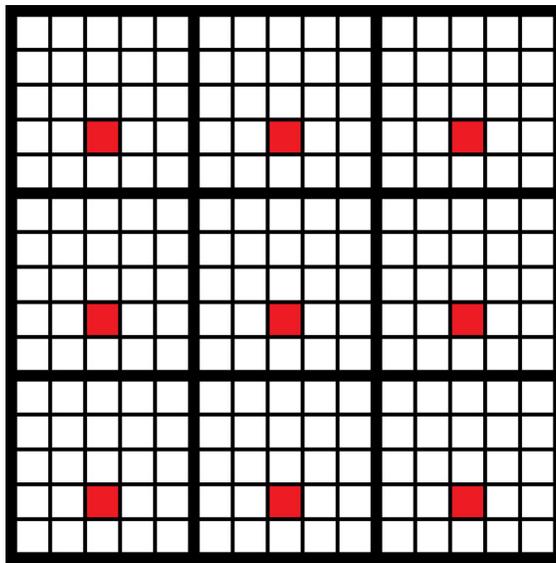for the remaining $y_1 \neq \tilde{y}_1$ we get $\mathrm{ncells}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, N, y_1) = 0$.



**Fig. 6.** The lattice $\mathrm{lattice}^2(N)$. The example $N = 15$, $M = 3$, $K = 5$. The cells highlighted form the set $K \cdot \mathrm{lattice}^2(M) + \mathbf{a}$, where $\mathbf{a} \in \mathrm{lattice}^2(K)$.

Therefore, due to (G.46)

$$\mathrm{zrf}(K \cdot \mathrm{lattice}^d(M) + \mathbf{a}, N, M), \tag{G.49}$$

using the lemma F.6 (on sum of lattices) we obtain

$$\mathrm{zrf}(\mathrm{lattice}^d(N), N, M). \tag{G.50}$$

By permutation of $M$ and $K$, we similarly prove that

$$\mathrm{zrf}(M \cdot \mathrm{lattice}^d(K) + \mathbf{a}, N, K), \quad \mathbf{a} \in \mathrm{lattice}^d(M), \tag{G.51}$$

using the lemma F.6 (on sum of lattices) we obtain

$$\mathrm{zrf}(lattice^d(N), N, K). \tag{G.52}$$

Since $M$ and $K$ are coprime and $N = MK$ (G.41), their least common multiple is equal to $N$, so by (G.50) and (G.52) lattice $\mathrm{lattice}^d(N)$ is zerofied modulo $N$:

$$\mathrm{zrf}(\mathrm{lattice}^d(N), N, N). \tag{G.53}$$

## ACKNOWLEDGEMENTS

## CONFLICT OF INTEREST

The authors of this work declare that they have no conflicts of interest.

## REFERENCES

1. J. C. Collins, *Renormalization* (Cambridge Univ. Press, 1984).
2. V. S. Vladimirov, I. V. Volovich and E. I. Zelenov, *p-Adic Analysis and Mathematical Physics* (World Scientific, Singapore, 1994).
3. I. V. Volovich, "Number theory as the ultimate physical theory," *p*-Adic Num. Ultrametr. Anal. Appl. **2**, 77−87 (2010).
4. H. Bondi, *Assumption and Myth in Physical Theory* (Cambridge Univ. Press, 1967).
5. M. G. Ivanov, "Binary representation of coordinate and momentum in quantum mechanics," Theor. Math. Phys. **196** (1), 1002−1017 (2018).
6. M. G. Ivanov and A. Yu. Polushkin, "Ternary and binary representation of coordinate and momentum in quantum mechanics," AIP Conf. Proceed. **2362**, 040002 (2021).
7. M. G. Ivanov and A. Yu. Polushkin, "Digital representation of continuous observables in Quantum Mechanics," [arXiv:2301.09348 [quant-ph]], (2023), accepted in Theor. Math. Phys..
8. V. V. Dotsenko, *Arithmetic of Quadratic Forms*, [in Russian] (MCCME, Moscow, 2015).
9. N. A. Vavilov, "The computer as a new reality of mathematics. II. The Waring problem," [in Russian], In: *Computer Tools in Education* (2020).
10. I. M. Vinogradov, *Elements of Number Theory*, [in Russian] (Nauka, Moscow (1965); English transl. Dover Publications, 2016).
11. I. R. Shafarevich and Z. I. Borevich, *Number Theory*, [in Russian] (Nauka, Moscow (1985); English transl. Elsevier Science, 1986).