Appendix A

Tabular overview of notation and terminology

The following two tables contain all pieces of notation and terminology that appear in this memoir. We start with a rather short list of notations based on mathematical symbols in Table A.1, which would be hard to find in the much longer Table A.2, the entries of which are listed in alphabetical order (placing Latin letters before Greek letters, lowercase letters before their capital counterparts, and letters in standard font before calligraphic letters, which are in turn placed before Fraktur letters).

notation	page	additional comments
$\{0,1\}^{<\infty}$	91	the set of all finite bit strings
$\circledast$	20	a certain $\mathbb{Q}$-bilinear product over $\mathbb{Q}[x_n : n \in \mathbb{N}^+]$, originally defined by Wei and Xu, such that $\mathrm{CT}(\psi_1 \otimes \psi_2) = \mathrm{CT}(\psi_1) \circledast \mathrm{CT}(\psi_2)$
$\bigotimes_{j\in I} g_j$	15	defined when each g_j is a function $X_j \to X_j$; it is the function on $\prod_{j\in I} X_j$ given by component-wise application of the g_j
gg'	23	composition of the functions g and g' (first g, then g'); synonymous: $g' \circ g$
$\langle g_1, \ldots, g_n \rangle$	32	if $g_1, \ldots, g_n$ are elements of a group G, this denotes the subgroup of G generated by the g_j
$G = H \ltimes N$	24	expresses that G is the (internal) semidirect product of H and N
$\lvert G_1 : G_2 \rvert$	19	the index of the subgroup G_2 in G_1
$G_1 \wr G_2$	8	imprimitive permutational wreath product
$H \leq G$	32	short for "H is a subgroup of G"
$\mathfrak{X} \sim \mathfrak{X}'$	64	shorthand for $\mathrm{SF}(\mathfrak{X}) = \mathrm{SF}(\mathfrak{X}')$
$\mathcal{P} \wedge \mathcal{Q}$	49	the infimum (coarsest common refinement) of the partitions $\mathcal{P}$ and $\mathcal{Q}$; if these are arithmetic partitions, then $\mathcal{P} \wedge \mathcal{Q}$ can be obtained as the arithmetic partition spanned by the concatenation of any choices of spanning congruence sequences for $\mathcal{P}$ and $\mathcal{Q}$
x^g	23	if x is an argument of the function g, this may denote the function value $g(x)$, especially in conjunction with the composition notation gg'
$\bigotimes_{j\in I} \Gamma_j$	15	the digraph tensor product of the Γ_j
$\vec{\nu} \diamond \vec{\nu}'$	57	the concatenation of $\vec{\nu}$ and $\vec{\nu}'$

Table A.1. Notations based on mathematical symbols.

notation/ terminology	page	additional comments
a	15	a variable denoting the linear coefficient of the affine map $A : x \mapsto ax + b$ of $\mathbb{Z}/m\mathbb{Z}$
α	11	a variable used to denote the modulus of an (in)congruence
$\alpha_{i,j}$	61	used in Section 3.4 and Section 5.2.3; the modulus of the j-th spanning congruence of $\mathcal{P}_i$
$\bar{\alpha}_j$	75	(used in the example in Section 4.2); the modulus of the j-th spanning congruence of $\mathcal{Q}_{0,0}$
A	15	a variable denoting an affine map of a group (mostly $\mathbb{Z}/m\mathbb{Z}$)
$\mathrm{AC}(\mathcal{P})$	12	arithmetic complexity of $\mathcal{P}$
admissible indexing function	40	none
admissible input	91	none
admissible output	91	none
affine function (between groups)	226	none
affine map (of a group)	23	none
a_i	3	defined for $i \in \{0, 1, \ldots, d-1\}$; an element of $\mathbb{F}_q$ associated with f; $f(x) = a_i x^{r_i}$ for all $x \in C_i$
A_i	8	defined for each $i \in \{0, 1, \ldots, d-1\}$ such that $a_i \neq 0$; it is the unique affine map of $\mathbb{Z}/s\mathbb{Z}$ corresponding to $f_{\restriction C_i} : C_i \to C_{\bar{f}(i)}$ under identifying $C_i, C_{\bar{f}(i)}$ with $\mathbb{Z}/s\mathbb{Z}$ via $\iota_i, \iota_{\bar{f}(i)}$, and it is given by the formula $A_i(x) = r_i x + \frac{e_i + r_i i - \bar{f}(i)}{d}$
$\mathcal{A}_i$	45	the affine map $A_{i_0} A_{i_1} \cdots A_{i_{\ell-1}}$ of $\mathbb{Z}/s\mathbb{Z}$
$\mathcal{A}_{i,h}$	54	used in Section 3.3; defined for $i \in \mathrm{per}(\bar{f}) \setminus \{d\}$ and $h \in \mathbb{N}_0$; it is defined as $A_{i-h} A_{i-h+1} \cdots A_{i-1}$, an affine map of $\mathbb{Z}/s\mathbb{Z}$
algorithmic problem	91	none
$\bar{\mathcal{A}}_{i,p}$	118	used in Sections 5.2.1 and 5.3.3; it is the reduction $\mathcal{A}_i \bmod p^{v_p(s)}$, an affine map of $\mathbb{Z}/p^{v_p(s)}\mathbb{Z}$
$\mathcal{A}'_i$	122	the affine permutation $\mathcal{A}_i \bmod s'_i$ of $\mathbb{Z}/s'_i\mathbb{Z}$
$\mathrm{aord}(x)$	34	additive order of $x \in \mathbb{Z}/m\mathbb{Z}$ (m must be clear from context)

arc	1	none
(arithmetic) complexity	12	none
arithmetic partition	11	none
$\mathrm{Aut}(G)$	33	the automorphism group of the group G
b	15	a variable denoting the constant coefficient of the affine map $A : x \mapsto ax + b$ of $\mathbb{Z}/m\mathbb{Z}$; also used more generally for the value at 1_G of an affine map of the group G
$\mathfrak{b}$	11	variable used to denote the right-hand side of a congruence or incongruence
$\mathfrak{b}_{i,j}$	61	used in Section 3.4 and Section 5.2.3; the right-hand side of the j-th spanning congruence of $\mathcal{P}_i$
$\bar{\mathfrak{b}}_j$	75	(used in the example in Section 4.2); the right-hand side of the j-th spanning congruence of $\mathcal{Q}_{0,0}$
B	27	variable denoting a block of a (usually arithmetic) partition; cf. the notation $B_{\vec{r}}$ introduced after Problem 2.3.7
$\mathcal{B}_i$	60	used in Section 3.4; the function that maps $x \in C_i$ to the unique $\mathcal{P}_i$-block containing x
$\mathcal{B}(\mathcal{P}, \vec{v})$	12	the block of the arithmetic partition $\mathcal{P}$ associated with the logical sign tuple $\vec{v}$
B_m	12	m-th Bell number
bit operation	89	none
blow-up function	83	none
bounded Las Vegas dual complexity	92	none
bounded query complexity	92	none
bracelet	10	none
bracelet graph	10	none
BU_m	83	m-blow-up function; the unique $\mathbb{Q}$-algebra endomorphism of $\mathbb{Q}[x_n : n \in \mathbb{N}^+]$ such that $\mathrm{BU}_m(x_n) = x_{mn}$ for all $n \in \mathbb{N}^+$
C	3	the index d subgroup of $\mathbb{F}_q^*$
C^C	8	the transformation semigroup of all functions $C \to C$
child	17	synonym: successor
C_i	3	a certain subset of $\mathbb{F}_q$ defined for $i \in \{0, 1, \ldots, d\}$; namely, $C_i := \omega^i C$ if $i \in \{0, 1, \ldots, d-1\}$, and $C_d := \{0_{\mathbb{F}_q}\}$

$\mathcal{C}_{\text{class}}$	91	a classical complexity (i.e., bit operation count); used for denoting the first entry of $\vec{\mathcal{C}}^{(\text{qry})}$ or $\vec{\mathcal{C}}^{(\text{LV})}$
$\mathcal{C}_{\text{conv}}$	92	a conversion complexity (i.e., count of conversions from bits to qubits and vice versa); used for denoting the third entry of $\vec{\mathcal{C}}^{(\text{LV})}$
$\mathcal{C}_{\text{fact}}$	91	a count of (integer) factorization queries; used for denoting the second entry of $\vec{\mathcal{C}}^{(\text{qry})}$
$\mathcal{C}_{\text{fdl}}$	91	a count of (finite) field discrete logarithm queries; used for denoting the fourth entry of $\vec{\mathcal{C}}^{(\text{qry})}$
$\mathcal{C}_{\text{mdl}}$	91	a count of modular discrete logarithm queries; used for denoting the third entry of $\vec{\mathcal{C}}^{(\text{qry})}$
$\mathcal{C}_{\text{mord}}$	91	a count of modular multiplicative order queries; used for denoting the fifth entry of $\vec{\mathcal{C}}^{(\text{qry})}$
$\mathcal{C}_{\text{prt}}$	91	a count of primitive root queries; used for denoting the sixth entry of $\vec{\mathcal{C}}^{(\text{qry})}$
$\mathcal{C}_{\text{quant}}$	92	a quantum complexity (i.e., count of elementary quantum gates); used for denoting the second entry of $\vec{\mathcal{C}}^{(\text{LV})}$
$\vec{\mathcal{C}}^{(\text{LV})}$	92	variable denoting a Las Vegas dual complexity, which is itself a triple of component complexities of different kinds
$\vec{\mathcal{C}}^{(\text{qry})}$	91	variable denoting a query complexity, which is itself a 6-tuple of component complexities of different kinds
$\mathfrak{C}_{i,L}$	198	the set of all $l \in \{1, 2, \ldots, L\}$ such that l is a multiple of ℓ (the $\bar{f}$-cycle length of i) and $\gcd(s, \bar{\alpha}_{i,l} - 1) \mid \bar{\beta}_{i,l}$; these are just those $l \in \{1, 2, \ldots, L\}$ for which $\eta_{i,l}(x)$ is well defined and characterizes, for $x \in C_i$, when $f^l(x) = x$
classical complexity	89	none
complexity (of a partition)	12	none
composition (of algorithmic problems)	93	none
conj(x)	23	the conjugation by $x \in G$ on the group G, i.e., the automorphism $y \mapsto x^{-1}yx$ of G
connected component (of a functional graph)	1	none
consistent (system of m-CCs)	26	none

continued fractions coefficient	99	none
convergent	99	none
conversion complexity	90	none
coset-wise affine function	226	same as coset-wise affine function in the narrow sense
coset-wise affine function in the narrow sense	226	none
coset-wise affine function in the wide sense	226	none
CRL-list	7	short for "cycle representatives and lengths list"
CT(ψ)	3	the cycle type of ψ
cycle type	2	none
cyclic sequence associated with $\vec{x}$	9	none
cyclic sequence	9	none
cyclotomic mapping	4	none
d	3	an index of f
$\mathfrak{d}$	42	a variable denoting a divisor
$\mathfrak{d}_{i,p,\vec{u}}$	124	shorthand for $\prod_{\mathfrak{p}\in\mathfrak{P}_{i,p,\vec{u}}} \mathfrak{p}^{\nu_{\mathfrak{p}}(l_{i,\vec{u}})}$, which is the same as $\prod_{\mathfrak{p}\in\mathfrak{P}_{i,p,\vec{u}}} \mathfrak{p}^{\nu_{\mathfrak{p}}(l_{i,p,\vec{u}_p})}$ and always divides $l_{i,p,\vec{u}_p}$
$\mathfrak{D}$	86	a variable denoting a compact description of a finite directed rooted tree isomorphism type with respect to a fixed recursive tree description list
dihedral sequence	10	none
directed rooted tree	2	we assume that all arcs are oriented toward the root

discrete logarithm (in a group)	103	none
discrete dynamical system	1	none
distribution number	28	none
dual algorithm	88	none
dual digraph	17	none
dual model	88	none
e	20	used for exponents (degrees) of variables in cycle types; needs to be distinguished from the notation e_i
e_i	8	defined for those $i \in \{0, 1, \ldots, d-1\}$ such that $a_i \neq 0$; it is the discrete logarithm of a_i with base ω, i.e., $a_i = \omega^{e_i}$
E	17	variable denoting the edge (arc) set of a digraph
E^{-1}	17	the inverse relation of E
$E(\vec{v}, J)$	28	a certain conjunction of divisiblity conditions
equivalent labeled arithmetic partitions	221	none
equivalent sequences of labeled arithmetic partitions	222	none
equivalent systems of m-CCs	26	none
Expand(Δ)	63	the "expanded version" of the finite edge-weighted directed rooted tree Δ
f	3	a generalized cyclotomic mapping of $\mathbb{F}_q$
f_{per}	46	the restriction of f to $\bigcup_{i \in \mathrm{per}(\bar{f})} C_i$
$\bar{f}$	8	the function on $\{0, 1, \ldots, d\}$ induced by f, defined implicitly via $f(C_i) \subseteq C_{\bar{f}(i)}$
$\overline{f_{\mathrm{per}}}$	46	the induced function of f_{per}, which is equal to $\bar{f}_{\vert \mathrm{per}(\bar{f})}$
$\mathfrak{f}$	31	a variable denoting a fixed point; in Proposition 2.3.6 and discussions based on it, this is a specifically defined fixed point of an affine map of a finite cyclic group
$\mathfrak{f}_i$	146	the unique periodic point of $\mathcal{A}_i \bmod s_i''$
$\mathfrak{f}_{i,p}$	120	defined whenever $\mathcal{A}_{i,p}$ has a fixed point; a certain fixed point of $\mathcal{A}_{i,p}$, given by the formula in Proposition 2.3.6

$\mathcal{F}$	231	a set of generalized cyclotomic mappings over a common finite field
$\mathbb{F}_q$	1	the finite field of size q
finite dynamical system	1	none
functional graph	1	none
g	1	a function $X \to X$
G	23	variable denoting an abstract group
$\mathcal{G}$	230	a set of functions $X \to X$
generalized cyclotomic mapping	3	none
$\mathrm{Good}_{\vec{r}}(\mathcal{I})$	40	the set of all $\mathcal{I}$-good tuples (associated with $\vec{r}$ or, rather, with the cycle length tuple $(l_j(\vec{r}))_{j=1,2,\ldots,n}$) for the $\vec{r}$-admissible indexing function $\mathcal{I}$
good tuple	40	none
$g_{\mid Y}$	7	the restriction of g to the subset $Y \subseteq X$
h_i	51	defined for $i \in \{0, 1, \ldots, d-1\}$; if i is $\bar{f}$-transient, then $h_i = \mathrm{ht}(\mathrm{Tree}_{\Gamma_{\bar{f}}}(i))$; if i is $\bar{f}$-periodic, then $h_i = \infty$
$h'_{i,k}$	134	defined when $i < d$ is $\bar{f}$-periodic and $k \in \mathbb{Z}$; it is the smallest positive integer h' such that $\gcd(\prod_{t=0}^{h'-1} \alpha_{i_{k-h'+t}}, s) = \gcd(\prod_{t=0}^{h'-2} \alpha_{i_{k-h'+t}}, s)$; one has $H_i = \max\{h'_{i,k} : k = 0, 1, \ldots, \ell - 1\}$
$\mathfrak{h}(x)$	52	a certain technical parameter from Section 3.3; when $x \in C_i$ for an $\bar{f}$-periodic $i < d$, then our understanding of $\mathrm{Tree}_{\Gamma_f}(x)$ is gained by recursion on $\mathfrak{h}(x)$ (after dealing with $\bar{f}$-transient indices i and $i = d$ first)
H_i	52	the maximum height of the rooted trees in Γ_{per} above f-periodic vertices in one of the cosets C_{i_t} for $t \in \mathbb{Z}$
$\bar{H}$	165	the maximum tree height in $\Gamma_{\bar{f}}$
$\mathcal{H}_i$	66	defined for $i < d$ if $\bar{f}$ is a permutation; it is the common tree height above f-periodic vertices in C_i; we note that $H_i = \max_{t \in \mathbb{Z}} \mathcal{H}_{i_t}$
$\mathfrak{S}$	135	shorthand for $\max\{H_i : i \in \mathrm{per}(\bar{f}) \setminus \{d\}\}$
height	18	attribute of a finite directed rooted tree, denoting the maximum length of a directed path in it

$\mathrm{ht}(\Delta)$	18	the height of Δ
hyperkernel	23	none
i	3	an index that can range over $\{0, 1, \ldots, d\}$
i_t	45	a notation defined for $i \in \mathrm{per}(\bar{f})$ and $t \in \mathbb{Z}$; shorthand for $(\bar{f}_{\lvert \mathrm{per}(\bar{f})})^t(i)$; in particular, $(i_0, i_1, \ldots, i_{\ell-1})$ is the $\bar{f}$-cycle of $i = i_0$
i'	52	shorthand for i_{-1}
$\mathfrak{i}$	180	a variable denoting an injective function
I	15	a variable denoting an index set
I_i	61	used in Section 3.4; the set of those $j \in \{1, 2, \ldots, m_i\}$ for which the truth value of $x \equiv \mathfrak{b}_{i,j} \pmod{\mathfrak{a}_{i,j}}$ is constant along the $\mathcal{A}_i$-cycle of r_i modulo s
$\mathcal{I}$	40	variable denoting an $\vec{r}$-admissible indexing function (for some $\vec{r}$)
$\mathcal{I}_i$	124	a certain function $\mathfrak{P}_i' \to \mathfrak{P}_i$; if $\mathcal{I}_{i,\vec{\mathfrak{u}}}(\mathfrak{p})$ only has one distinct value for $\vec{\mathfrak{u}} \in \overline{Y}_i$, then $\mathcal{I}_i(\mathfrak{p})$ is that value, otherwise $\mathcal{I}_i(\mathfrak{p})$ is the unique value distinct from $\mathfrak{p}$ which $\mathcal{I}_{i,\vec{\mathfrak{u}}}(\mathfrak{p})$ assumes
$\mathcal{I}_{i,\vec{\mathfrak{u}}}$	122	a certain $\vec{r}_i(\vec{\mathfrak{u}})$-admissible indexing function, extended such that its domain of definition is $\mathfrak{P}_i'$
$\mathfrak{T}$	18	variable denoting an isomorphism type of finite directed rooted trees (either edge-weighted or not, depending on the context)
$\mathfrak{T}^+$	49	the rooted tree isomorphism type obtained by attaching a single copy of $\mathfrak{T}$ to a new root
$\mathfrak{T}_i$	82	(used in Section 4.3) shorthand for $\mathrm{Tree}_{\Gamma_{\bar{f}}}(i)$
$\mathcal{I}$-good tuple	40	none
induced by f	8	attribute referring to the function $\bar{f}$
$\mathrm{im}(g)$	49	the image (synonymously, range) of the function g
infimum (of partitions)	49	none
$\mathrm{inv}_n(u)$	29	the multiplicative inverse modulo n of $u \in \mathbb{Z}$ with $\gcd(u, n) = 1$
isomorphism of vertex-labeled digraphs	9	none

isomorphism of finite edge-weighted directed rooted trees	63	none
iterated pre-image	2	none
J	28	variable denoting an index set
$J_+(\vec{\nu})$	27	the set of indices j such that the j-th entry of $\vec{\nu}$ is $\emptyset$
$J_-(\vec{\nu})$	27	the set of indices j such that the j-th entry of $\vec{\nu}$ is $\neg$
$\ker^{(k)}(\varphi)$	19	defined for $k \in \mathbb{N}_0$ and a group endomorphism φ of G; it is the normal subgroup $\{x \in G : \varphi^k(x) = 1_G\}$ of G
$\mathcal{J}_{i,p,k}$	123	one of up to five subintervals of the range for u_p such that $\nu_p(l_{i,p,\vec{u}_p})$ is given by a simple formula in u_p whenever u_p lies in a fixed $\mathcal{J}_{i,p,k}$
$\mathcal{J}'_{i,p,k}$	123	a subinterval of $\mathcal{J}_{i,p,k}$ such that $\mathcal{I}_{i,\vec{\bar{u}}}(p) = p$ if and only if $u_p \in \bigcup_{k=1}^{\mathfrak{m}_{i,p}} \mathcal{J}'_{i,p,k}$
k_p	124	(in Section 5.2.1) the p-labeled entry of $\vec{k}$ (an element of $\mathbb{Z}/l_{i,\vec{\bar{u}}}\mathbb{Z}$)
$\vec{k}$	124	(in Section 5.2.1) variable denoting an $\mathcal{I}_{i,\vec{\bar{u}}}$-good tuple
k'_p	125	(in Section 5.2.1) the p-labeled entry of $\vec{k'}$ (an element of $\mathbb{Z}/(l_{i,p,\vec{u}_p}/\mathfrak{d}_{i,p,\vec{\bar{u}}})\mathbb{Z}$)
$\vec{k'}$	125	a tuple, ranging over $\prod_{\mathfrak{p}\in\mathfrak{P}_i} \mathbb{Z}/(l_{i,p,\vec{u}_p}/\mathfrak{d}_{i,p,\vec{\bar{u}}})\mathbb{Z}$, which for a fixed $\vec{\bar{u}} \in \bar{Y}_i$ serves as the parameter (argument) of a certain bijective parametrization of $\mathrm{Good}_{\vec{r}_i(\vec{\bar{u}})}(\mathcal{I}_{i,\vec{\bar{u}}})$, the set of good tuples for the $\vec{r}_i(\vec{\bar{u}})$-admissible indexing function $\mathcal{I}_{i,\vec{\bar{u}}}$
$K'_{i,\vec{\bar{u}}}$	125	the set $\prod_{\mathfrak{p}\in\mathfrak{P}_i} \mathbb{Z}/(l_{i,p,\vec{u}_p}/\mathfrak{d}_{i,p,\vec{\bar{u}}})\mathbb{Z}$, from which $\vec{k'}$ stems
l	7	a cycle length of f or g
l_{bit}	172	a bit length
$l_{i,j}$	61	used in Section 3.4 and Section 5.2.3; the cycle length of r'_i under $\mathcal{A}_i$ modulo $\mathfrak{a}_{i,j}$
$l_{i,\vec{\bar{u}}}$	122	the cycle length $\mathrm{lcm}\{l_{i,p,\vec{u}_p} : p \in \mathfrak{P}_i\}$ of $\bigotimes_{p\in\mathfrak{P}_i} \mathcal{A}_{i,p}$ associated with $\vec{\bar{u}}$
$l_{i,p,\vec{u}_p}$	122	the "component cycle length" $\mathrm{proj}_2(\mathrm{par}'_{i,p}(\vec{u}_p))$
ℓ	45	variable denoting a cycle length of $\bar{f}$, as opposed to a cycle length of f, which is denoted by l instead; if $i \in \{0, 1, \ldots, d\}$ has been fixed, then ℓ is *always* the $\bar{f}$-cycle length of i

$\mathfrak{l}$	146	shorthand for $\log_\omega(r)$, where $r \in \mathbb{F}_q$ is an f-periodic point representing a connected component of Γ_f
$\mathfrak{l}_{i,j}$	61	used in Section 3.4 and Section 5.2.3; it denotes the affine discrete logarithm value $\log_{\mathcal{A}_i}^{(\mathfrak{a}_{i,j})}(r_i, \mathfrak{b}_{i,j})$
L	197	used in Section 5.3.3, denoting a maximal cycle length
L_i	125	the smallest non-negative integer such that $\gcd(\overline{\alpha}_i^{L_i}, s) = \prod_{p \mid \gcd(\overline{\alpha}_i, s)} p^{\kappa_p}$, used in the formula for the unique periodic point of $\mathcal{A}_i \bmod (s/s_i')$
$\mathfrak{L}$	7	variable denoting a CRL-list
$\overline{\mathfrak{L}}$	45	a CRL-list of $\bar{f}$
$\mathfrak{L}^{(1)}$	39	the set of first entries of pairs in the CRL-list $\mathfrak{L}$
$\mathfrak{L}_i$	46	a CRL-list of the restriction of f to $\bigcup_{t=0}^{\ell-1} C_{i_t}$
$\mathfrak{L}_i'$	45	a CRL-list of $\mathcal{A}_i$
$\mathfrak{L}_{i,p}'$	118	a CRL-list of $\overline{\mathcal{A}}_{i,p}$ in which all specified cycle lengths are fully factored; for the precise definition, see Table 5.2
$\mathfrak{L}_i''$	122	a CRL-list of $\mathcal{A}_i'$
$\mathfrak{L}(p^v, a)$	33	a certain CRL-list of the automorphism μ_a of $\mathbb{Z}/p^v\mathbb{Z}$, defined in Table 2.1 and (for $p > 2$) depending on a choice of primitive root $\mathfrak{r}$ modulo p^v
$\mathfrak{L}(p^v, a, b)$	37	a certain CRL-list of the affine permutation $x \mapsto ax + b$ of $\mathbb{Z}/p^v\mathbb{Z}$, defined in Table 2.2 and (for $p > 2$) depending on a choice of primitive root $\mathfrak{r}$ modulo p^v
$\mathfrak{L}$	91	variable denoting an algorithmic problem
$\mathfrak{L}_{\text{in}}$	91	the set of admissible inputs for the algorithmic problem $\mathfrak{L}$; formally, this is the domain of definition of the function $\mathfrak{L}$
$\mathfrak{L}\mathfrak{L}'$	93	the composition of the algorithmic problems $\mathfrak{L}$ and $\mathfrak{L}'$ (first $\mathfrak{L}$, then $\mathfrak{L}'$); synonymous notation: $\mathfrak{L}' \circ \mathfrak{L}$
$\mathfrak{L}' \circ \mathfrak{L}$	93	see $\mathfrak{L}\mathfrak{L}'$
lab	220	variable denoting a labeling function (i.e., the second entry of a labeled arithmetic partition)
lab_i	220	a certain labeling function for the arithmetic partition $\mathcal{P}^{(i)}$, used in two slightly different meanings (see also the paragraph before Definition 6.2.1)
Lab	222	variable denoting a labeling function (like lab)
labeled arithmetic partition	220	none
Las Vegas algorithm	88	none

Layer_h	116	the set of those $i \in \{0, 1, \ldots, d-1\}$ for which $h_i = h$
left-regular representation	23	none
$\log_a^{(m)}(x)$	41	the discrete logarithm modulo m of x with base a
$\log_A^{(m)}(x, y)$	41	an "affine discrete logarithm", formally defined at the beginning of Section 2.4
$\log_x(y)$	103	if x and y are elements of a group G, this denotes the discrete logarithm of y with base x (defined to be ∞ if y is not a power of x)
m	1	a positive integer; used as a general modulus
m_i	50	defined for $i \in \{0, 1, \ldots, d-1\}$; it denotes the length of a fixed spanning s-congruence sequence of $\mathcal{P}_i$
$\bar{m}_i$	220	length of the standard spanning congruence sequence for $\mathcal{P}^{(i)}$; in the notation of Section 3.4, one has $\bar{m}_i = m_i - \lvert I_i \rvert$
m_p	104	the so-called p-part of $m \in \mathbb{N}^+$; defined as $p^{\nu_p(m)}$
$m_{p'}$	103	the so-called p'-part of $m \in \mathbb{N}^+$; defined as $m/p^{\nu_p(m)}$
m'	31	the product of all prime powers $p^{\nu_p(m)}$, where p does *not* divide a certain other integer that is clear from context (usually the linear coefficient of a certain affine map of $\mathbb{Z}/m\mathbb{Z}$, whereas on page 101, it is the integer 2); not to be confused with the notation i'
m''	31	the quotient m/m'
$\mathfrak{m}$	173	variable denoting a count of isomorphism types of connected components of a functional graph
$\mathfrak{m}_i$	203	a function, used in the proof of Theorem 5.3.3.4, which encodes the block sizes of $\mathcal{W}_{i,L}$
$\mathfrak{m}_{i,p}$	123	the number of intervals $\mathcal{J}_{i,p,k}$ $(k = 1, 2, \ldots, \mathfrak{m}_{i,p})$
M	48	variable denoting a subset of a universal set (usually $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{F}_q$)
M^c	28	the complement set of M (in its respective universal set)
m-CC	11	short for "m-congruential condition"
m-(in)congruence	11	an (in)congruence whose modulus divides m
merging (of sorted arrays)	95	none
$\mathrm{minperl}(\vec{x})$	172	minimal period length of the finite sequence $\vec{x}$
Monte Carlo algorithm	98	none

$\mathrm{mpe}(m)$	22	the maximum prime exponent of m, i.e., $\mathrm{mpe}(m) = \max_p \nu_p(m)$
multiple of a rooted tree isomorphism type	49	none
n_i	53	the length of a fixed spanning s-congruence sequence for $\mathcal{R}_i$
$\bar{n}_i$	165	used in the proof of Lemma 5.3.2.2 (2); it denotes the unique $n \in \mathcal{N}$ such that $\mathfrak{T}_n = \mathrm{Tree}_{\Gamma_f}(x)$ for each $x \in C_i$
$\bar{n}_{i,k}$	168	used in the proof of Lemma 5.3.2.2 (4); it denotes the unique $n \in \mathcal{N}$ such that $\mathrm{Expand}(\mathfrak{T}_{i,k}) = \mathfrak{T}_n$ (i.e., $i \in S_{n,\mathrm{trans}}$ and $\mathrm{ht}(\mathfrak{T}_n) = k$)
$n'_i(\vec{v})$	148	a special notation used in Section 5.2.3; it denotes the unique $n \in \mathcal{N}$ such that $\vec{v}^+ \in S_{i,n}$
$\mathfrak{n}_p$	120	used in Section 5.2.1; it denotes the number of distinct prime divisors of $p-1$
$\mathcal{N}$	131	used in Sections 5.2.2 and 5.3.2; it denotes an initial segment of $\mathbb{N}_0$, consisting of those n for which the compact tree description $\mathfrak{D}_n$ has been defined (at the respective point in the algorithm in question)
$\mathfrak{N}$	174	variable denoting a tree necklace list
$\mathbb{N}^+$	3	the set of positive integers
$\mathbb{N}_0$	1	the set of non-negative integers
necklace	9	none
necklace graph	9	none
$\mathrm{nil}(\varphi)$	23	the hyperkernel of φ
$\mathcal{O}_{i,L}$	196	defined for $\bar{f}$-periodic $i \in \{0,1,\ldots,d-1\}$ and $L \in \mathbb{N}^+$; it is the set of all logical sign tuples $\diamond_{t=0}^{H_i+L-1} \vec{o}'_t \in \{\emptyset, \neg\}^{n_{i_0}+n_{i_{-1}}+\cdots+n_{i_{-H_i-L+1}}}$ such that the associated block $\mathcal{B}(\mathcal{Q}_{i,H_i+L-1}, \diamond_{t=0}^{H_i+L-1} \vec{o}'_t \diamond \vec{\xi}_{i,H_i})$ of $\mathcal{Q}_{i,H_i+L-1}$ consisting of f-periodic points is non-empty
$\mathrm{ord}(x)$	32	the order of the group element $x \in G$; the group G must be clear from context; for elements of $\mathbb{Z}/m\mathbb{Z}$, this always denotes the multiplicative order (hence is only well defined if x is a unit modulo m) – see also the notation aord
$\mathrm{ord}_n(x)$	104	the multiplicative order of x modulo n
p	15	variable denoting a prime, not necessarily the prime base of q; using p as a summation index implies that only prime indices satisfying the explicitly stated constraints should be used

$\mathfrak{p}$	123	variable used to denote a general element of $\mathfrak{P}'_i$ (to be distinguished from p used for elements of $\mathfrak{P}_i$)
$\mathfrak{p}_{p,k}$	120	the k-th prime divisor of $p-1$ (in a fixed factorization)
$P(T)$	85	a polynomial in the variable T
$\mathcal{P}$	11	variable denoting a partition, usually an arithmetic one
$\mathcal{P}_i$	11	a certain arithmetic partition of $C_i \cong \mathbb{Z}/s\mathbb{Z}$, defined in Section 3.3, which "controls" the trees above vertices in C_i
$\mathcal{P}^{(i)}$	61	used in Section 3.4 and Section 5.2.3; a certain arithmetic partition that encodes (part of) the cyclic sequence of rooted tree isomorphism types that represents the connected component of Γ_f containing r'_i
$\mathcal{P}'_i$	50	shorthand for $\mathfrak{P}'(\mathcal{P}_i, A_i)$
$\mathcal{P}_{i,h}$	56	a certain arithmetic partition of C_i such that for $x \in C_i$ with $\mathfrak{h}(x) = h$, the isomorphism type $\mathrm{Tree}_{\Gamma_f}(x)$ only depends on the $\mathcal{P}_{i,h}$-block in which x is contained
$\mathfrak{P}$	11	an operator, used in the notation $\mathfrak{P}(x \equiv \mathfrak{b}_k \pmod{\mathfrak{a}_k} : k = 1, 2, \ldots, K)$, which denotes the arithmetic partition of $\mathbb{Z}/m\mathbb{Z}$ (for implicitly clear $m \in \mathbb{N}^+$) spanned by those m-congruences
$\mathfrak{P}_i$	118	the set of all primes $p \mid s$ such that $p \nmid \overline{\alpha}_i$ (i.e., such that $\mathcal{A}_{i,p}$ is a permutation of $\mathbb{Z}/p^{v_p(s)}\mathbb{Z}$)
$\mathfrak{P}_{i,p,\vec{u}}$	124	the pre-image set $\mathcal{I}^{-1}_{i,\vec{u}}(\{p\})$
$\mathfrak{P}'_i$	122	the extended domain of definition $\mathfrak{P}_i \cup \pi(\prod_{p \in \mathfrak{P}_i}(p-1))$ of $\mathcal{I}_{i,\vec{u}}$
$\mathfrak{P}(\Theta(x))$	55	the arithmetic partition of $\mathbb{Z}/m\mathbb{Z}$ spanned by the non-negated versions of the m-CCs in $\Theta(x)$
$\mathfrak{P}'(\mathcal{P}, A)$	27	defined when $\mathcal{P}$ is an arithmetic partition of $\mathbb{Z}/m\mathbb{Z}$ with a fixed spanning congruence sequence and A is an affine map of $\mathbb{Z}/m\mathbb{Z}$; it is a certain arithmetic partition of $\mathbb{Z}/m\mathbb{Z}$ such that the intersection size $\lvert A^{-1}(\{x\}) \cap B\rvert$, where $B = \mathcal{B}(\mathcal{P}, \vec{v})$ is a fixed block of $\mathcal{P}$, is constant (equal to $\sigma_{\mathcal{P},A}(\vec{v}, \vec{v'})$) when x ranges over a fixed block $\mathcal{B}(\mathcal{P}', \vec{v'})$ of $\mathcal{P}' = \mathfrak{P}'(\mathcal{P}, A)$
pairwise congruence-consistent	227	none
pairwise coset-intersection property	228	none

par_i	117	a bijective parametrization of $\mathcal{L}_i$; for $i < d$, this is obtained from par'_i by stretching all cycle lengths by the factor ℓ (the $\bar{f}$-cycle length of i)
par'_i	118	a bijective parametrization of $\mathcal{L}'_i$ (for $i < d$)
par''_i	122	a bijective parametrization of $\mathcal{L}''_i$
$\mathrm{par}'_{i,p}$	118	a bijective parametrization of $\mathcal{L}'_{i,p}$
partition-tree register	87	none
PCIP	228	short for "pairwise coset-intersection property"
PCIP-group	228	none
$\mathrm{per}(g)$	1	the set of g-periodic points in X
period (length) (of an argument under a function)	1	none
periodic	1	synonymous uses: periodic under f; f-periodic
period length (of a finite sequence)	172	none
$\mathrm{perl}_g(x)$	1	the period (length) of $x \in X$ under g
phase inversion	90	none
$\mathrm{pperl}_g(x)$	1	the pre-period (length) of $x \in X$ under g
pre-period (length)	1	none
pre-periodic	1	none
$\mathrm{proc}_{i,h}$	47	an auxiliary (procreation) number, used in the proof of Theorem 3.2.1
$\mathrm{proc}_k(x)$	17	the k-th procreation number in Γ of $x \in \mathrm{V}(\Gamma)$; also written $\mathrm{proc}_k^{(\Gamma)}(x)$ for greater clarity
procreation number	17	none
$\mathrm{proj}_{i,L}$	197	the projection mapping each tuple in $\mathcal{O}_{i,L}$ to its initial segment of length $n_{i_0} + n_{i_{-1}} + \cdots + n_{i_{-H_i}}$
proj_j	122	defined for $j \in \{1, 2\}$, it is the (class-sized) function mapping an ordered pair to its j-th entry
q	1	a prime power

$\mathcal{Q}_{i,h}$	56	the arithmetic partition $\mathcal{P}_{i,h} \wedge \mathcal{U}_i$ of C_i; plays an auxiliary role in the proof of Proposition 3.3.4; moreover, $\mathcal{P}_i := \mathcal{Q}_{i,H_i}$
quantum complexity	88	none
query algorithm	88	none
query model	88	none
r	7	a periodic point under f or g that represents a cycle of that function; exception: the use as an exponent in "r-th order cyclotomic mapping" (cf. the notation r_i)
r_i	3	defined for $i \in \{0, 1, \ldots, d-1\}$; a non-negative integer between 0 and $q-2$ associated with f; one has $f(x) = a_i x^{r_i}$ for all $x \in C_i$
$r_{i,p}(\vec{u}_p)$	122	same as $\mathrm{proj}_1(\mathrm{par}'_{i,p}(\vec{u}_p))$, the p-labeled entry of $\vec{r}_i(\vec{u})$
r'_i	60	used in Section 3.4 and Section 5.2.3; a certain coset representative of C_i
$r'_{i,\vec{u}}(\vec{k'})$	125	the unique element of $\mathbb{Z}/s'_i\mathbb{Z}$ that is congruent to $\bar{\mathcal{A}}_{i,p}^{k'_p \mathfrak{d}_{i,p,\vec{u}}}(r_{i,p}(\vec{u}_p))$ modulo p^{κ_p} for each $p \in \mathfrak{P}_i$; it is given by the formula $\sum_{p\in\mathfrak{P}_i} \bar{\mathcal{A}}_{i,p}^{k'_p \mathfrak{d}_{i,p,\vec{u}}}(r_{i,p}(\vec{u}_p)) \frac{s'_i}{p^{\kappa_p}} \mathrm{inv}_{p^{\kappa_p}}(\frac{s'_i}{p^{\kappa_p}})$
$\vec{r}$-admissible indexing function	40	none
$\vec{r}_i(\vec{u})$	122	the element $(\mathrm{proj}_1(\mathrm{par}'_{i,p}(\vec{u}_p)))_{p\in\mathfrak{P}_i}$ of $\prod_{p\in\mathfrak{P}_i} \mathbb{Z}/p^{\kappa_p}\mathbb{Z}$ associated with $\vec{u}$; these elements are representatives for the orbits of the natural (component-wise) action of $\langle \mathcal{A}_{i,p} : p \in \mathfrak{P}_i \rangle$ on $\prod_{p\in\mathfrak{P}_i} \mathbb{Z}/p^{\kappa_p}\mathbb{Z}$
$r^{\langle\psi\rangle}$	39	the set of points on the ψ-cycle of r, a special case of the notation x^G for the orbit of $x \in X$ under the natural action of $G \leq \mathrm{Sym}(X)$
$\mathfrak{r}$	33	variable denoting a primitive root
$\mathfrak{r}_p$	120	a primitive root modulo $p^{v_p(m)}$, where $m \in \mathbb{N}^+$ is clear from context (in Section 5.2.1, $m = s$)
$\mathcal{R}_i$	53	defined for $i \in \{0,1,\ldots,d-1\}$; it is the arithmetic partition $\bigwedge_{t=1}^{K} \mathcal{P}'_{j_t}$, where $j_1, j_2, \ldots, j_K$ are the $\bar{f}$-transient pre-images of i under $\bar{f}$; if i is $\bar{f}$-transient itself, then $\mathcal{R}_i = \mathcal{P}_i$
$\mathfrak{R}$	164	variable denoting a type-I or -II tree register
recursive tree description list	86	none
right-regular representation	23	none

rigid procreation	17	none
rooted tree	2	for us, synonymous with "directed rooted tree"
rt(Δ)	18	the root of Δ
s	8	the group order of C, i.e., $s = (q-1)/d$
s_i'	122	shorthand for $\prod_{p\in\mathfrak{P}_i} p^{\kappa_p}$
s_i''	146	shorthand for s/s_i'
$\mathfrak{s}$	40	variable denoting a shift (additive translation) of a finite abelian group; see in particular the notation $\mathfrak{s}_{\vec{r}}$ introduced after Problem 2.3.7
S_n	162	notation used in type-I and -II tree registers; it contains the information where the trees from the register occur in Γ_f
$S_{n,i}$	87	appears in the definition of a partition-tree register; it is either a specific logical sign tuple, or a set thereof, or a tuple of such sets; together, the $S_{n,i}$ encode the information which block of $\mathcal{P}_i$ corresponds to which rooted tree
$S_{n,i,h}$	87	for $i \neq d$ that is $\bar{f}$-periodic, this denotes one of the entries of the tuple $S_{n,i}$
$\overline{S}_{n,i}$	148	a special notation used in Section 5.2.3; the element-wise image of $S_{n,i}$ under $\vec{\nu}' \mapsto \vec{\nu}'^{-}$
$S_{n,\mathrm{per}}$	163	part of S_n in a type-II tree register; it stores the information for which $i \in \{0,1,\dots,d-1\}$ the rooted tree isomorphism type $\mathfrak{T}_n$ occurs above f-periodic vertices in C_i
$S_{n,\mathrm{trans}}$	163	part of S_n in a type-II tree register; it stores the information for which $i \in \{0,1,\dots,d-1\}$ the rooted tree isomorphism type $\mathfrak{T}_n$ occurs above f-transient vertices in C_i
$\mathcal{S}_{i,h}$	54	defined when $i \in \mathrm{per}(\bar{f}) \setminus \{d\}$ and $h \in \{0,1,\dots,H_i\}$; it is a certain arithmetic partition of C_i such that for $x \in C_i$ and $\mathfrak{h}(x) = h$, the isomorphism type $\mathrm{Tree}_{\Gamma_f}(x, C_{i'})$ only depends on the block of $\mathcal{S}_{i,h}$ in which x is contained
semidirect product	24	none
SF($\mathfrak{T}$)	64	simplified form of $\mathfrak{T}$
simplified	63	none
simplified form	64	none
spanned by	11	none
special type I	162	not to be confused with "type I"
special type II	162	not to be confused with "type II"

$\mathrm{Stab}_G(x)$	222	defined when G is a group acting on a set X and $x \in X$; it denotes the stabilizer of x in G
state space	1	none
$\mathrm{STRAG}(X, \mathcal{G})$	230	the underlying digraph of $\mathrm{TRAG}(X, \mathcal{G})$, which has no edge labels and no multiple edges $x \to x'$ for fixed $x, x' \in X$
successor	17	synonym: child
successor generations	17	none
sum of rooted tree isomorphism types	49	none
sum of simplified edge-weighted rooted tree isomorphism types	64	none
$\mathrm{Sym}(n)$	8	same as $\mathrm{Sym}(\{0, 1, \ldots, n-1\})$
$\mathrm{Sym}(X)$	8	symmetric group on X
synchronization	180	none
t	221	the translation $x \mapsto x + 1$ of the cyclic group $\mathbb{Z}/m\mathbb{Z}$ (m must be clear from context)
T	85	a formal variable, used for polynomial rings
$\mathcal{T}_m$	59	the trivial partition of $\mathbb{Z}/m\mathbb{Z}$ (all blocks are singletons)
$\mathcal{T}_{i,h}$	56	the arithmetic partition $\mathcal{S}_{i,h} \wedge \mathcal{U}_i$ of C_i; plays an auxiliary role in the proof of Proposition 3.3.4
$\mathfrak{T}$	221	the cyclic subgroup of $\mathrm{Sym}(\mathbb{Z}/m\mathbb{Z})$ generated by t
tensor product (of digraphs)	15	none
$\mathrm{TRAG}(X, \mathcal{G})$	230	the transformation graph associated with the set X and set $\mathcal{G}$ of functions $X \to X$
transient	1	synonymous uses: transient under f; f-transient
transition function	1	none
translation number	221	none
$\mathrm{Tree}_i(\mathcal{P}_i, B)$	61	defined when $B = \mathcal{B}(\mathcal{P}_i, \vec{v})$; the same as $\mathrm{Tree}_i(\mathcal{P}_i, \vec{v})$
$\mathrm{Tree}_i(\mathcal{P}_i, \vec{v})$	12	the rooted tree isomorphism type associated with the block $\mathcal{B}(\mathcal{P}_i, \vec{v})$ of $\mathcal{P}_i$

$\mathrm{Tree}_i(\mathcal{P}, M, \vec{\nu})$	49	defined when $\mathrm{Tree}_{\Gamma_f}(x, M)$ for $x \in C_i$ only depends on the $\mathcal{P}$-block in which x is contained (under the identification of C_i with $\mathbb{Z}/s\mathbb{Z}$ via ι_i); it denotes the common rooted tree isomorphism type $\mathrm{Tree}_{\Gamma_f}(x, M)$ for $x \in \mathcal{B}(\mathcal{P}, \vec{\nu})$
$\mathrm{Tree}_i(\mathcal{P}, \vec{\nu})$	49	shorthand for $\mathrm{Tree}_i(\mathcal{P}, \mathcal{B}(\mathcal{P}, \vec{\nu}))$; a natural extension of the notation $\mathrm{Tree}_i(\mathcal{P}_i, \vec{\nu})$ to arbitrary arithmetic partitions of C_i
$\mathrm{Tree}_i(\mathcal{P}'_j, C_j, \vec{\nu}^{(\mathcal{P}'_j)})$	53	defined when $i \in \{0, 1, \ldots, d-1\}$ and j is an $\bar{f}$-transient pre-image of i under $\bar{f}$; it denotes the common isomorphism type $\mathrm{Tree}_{\Gamma_f}(x, C_j)$ for $x \in \mathcal{B}(\mathcal{P}'_j, \vec{\nu}^{(\mathcal{P}'_j)}) \subseteq C_i$
$\mathrm{Tree}_i(\mathcal{R}_i, \bigcup_{t=1}^{K} C_{j_t}, \vec{\nu}^{(\mathcal{R}_i)})$	53	defined when $i \in \{0, 1, \ldots, d-1\}$ and the j_t are the $\bar{f}$-transient pre-images of i under $\bar{f}$; it denotes the common isomorphism type $\mathrm{Tree}_{\Gamma_f}(x, \bigcup_{t=1}^{K} C_{j_t})$ for $x \in \mathcal{B}(\mathcal{R}_i, \vec{\nu}^{(\mathcal{R}_i)}) \subseteq C_i$
$\mathrm{Tree}_i^{(h)}(\mathcal{P}_{i,h}, \vec{\nu}^{(\mathcal{P}_{i,h})})$	57	defined when $i < d$ is $\bar{f}$-periodic and $h \in \{0, 1, \ldots, H_i\}$; a rooted tree isomorphism type to which all $\mathrm{Tree}_{\Gamma_f}(x)$ for $x \in \mathcal{B}(\mathcal{P}_{i,h}, \vec{\nu}^{(\mathcal{P}_{i,h})}) \subseteq C_i$ with $\mathfrak{h}(x) = h$ are equal
$\mathrm{Tree}_i^{(h)}(\mathcal{S}_{i,h}, C_{i'}, \vec{\nu}^{(\mathcal{S}_{i,h})})$	57	defined when $i < d$ is $\bar{f}$-periodic and $h \in \{0, 1, \ldots, H_i\}$; a rooted tree isomorphism type to which all $\mathrm{Tree}_{\Gamma_f}(x, C_{i'})$ for $x \in \mathcal{B}(\mathcal{S}_{i,h}, \vec{\nu}^{(\mathcal{S}_{i,h})}) \subseteq C_i$ with $\mathfrak{h}(x) = h$ are equal
$\mathrm{Tree}_\Gamma(x)$	9	the tree above x in Γ
$\mathrm{Tree}_\Gamma(x, M)$	48	like $\mathrm{Tree}_\Gamma(x)$, but deleting all subgraphs $\mathrm{Tree}_\Gamma(y)$, where $y \to x$ and $y \notin M$
tree above x in Γ	9	none
tree necklace list (relative to a sequence of rooted tree isomorphism types)	173	none
tree necklace list (relative to a tree register)	174	none
type I	147	not to be confused with "special type I" or "type-I tree register"
type-I tree register	162	none
type II	147	not to be confused with "special type II" or "type-II tree register"
type-II tree register	163	none
type III	147	none

u	120	the first of up to two parameters making up $\vec{u}$
u_p	122	the first of up to two parameters making up $\vec{u}_p$
u'	120	the second of up to two parameters making up $\vec{u}$
u'_p	122	the second of up to two parameters making up $\vec{u}_p$
$\vec{u}$	120	general form of an element of the parameter set $Y_{i,p}$ (depends on p, which is suppressed in this notation; see also $\vec{u}_p$)
$\vec{u}_p$	122	the p-labeled component of $\vec{\vec{u}}$; it is an element of $Y_{i,p}$
$\vec{\vec{u}}$	122	general form of an element of the parameter set $\overline{Y}_i$
$\mathfrak{u}_{i,L}$	196	the function $\mathcal{O}_{i,L} \to \mathcal{O}_{i',L-1}$ mapping each tuple $\diamond_{t=0}^{H_i+L-1}\vec{o}'_t \in \mathcal{O}_{i,L}$ to the unique tuple $\diamond_{t=0}^{H_i+L-2}\vec{o}_t \in \mathcal{O}_{i',L-1}$ such that for each (f-periodic) point $x \in \mathcal{B}(\mathcal{Q}_{i,H_i+L-1}, \diamond_{t=0}^{H_i+L-1}\vec{o}'_t \diamond \vec{\xi}_{i,H_i})$, the unique f-periodic pre-image $x^{(-1)} \in C_{i'}$ of x under f lies in the block $\mathcal{B}(\mathcal{Q}_{i',H_i+L-2}, \mathfrak{u}_{i,L}(\diamond_{t=0}^{H_i+L-1}\vec{o}_t) \diamond \vec{\xi}_{i',H_i})$
U_i	83	defined for $\bar{f}$-periodic i, say of cycle length ℓ; it is the union $\bigcup_{t=0}^{\ell-1} C_{i_t}$ of the blocks C_j for all indices j on the $\bar{f}$-cycle of i
U_χ	90	phase inversion operator associated with χ
$\mathcal{U}_i$	55	defined when $i \in \{0, 1, \ldots, d-1\}$ is $\bar{f}$-periodic; it is the arithmetic partition $\mathfrak{P}(\theta_{i,h}(x) : h = 1, 2, \ldots, H_i)$ of C_i, the blocks of which are the subsets of C_i consisting of points with a common $\mathfrak{h}$-value
v	15	variable denoting an exponent in a prime factorization
$v_{p,k}$	120	shorthand for $v_{\mathfrak{p}_{p,k}}(p-1)$
$v'_{i,p}$	120	shorthand for $v_p(\mathrm{ord}_{p^{\kappa_p}}(\overline{\alpha}_i))$
$v'_{i,p,k}$	120	shorthand for $v_{\mathfrak{p}_{p,k}}(\mathrm{ord}_{p^{\kappa_p}}(\overline{\alpha}_i))$
$v''_{i,2}$	120	shorthand for $v_2(\mathrm{ord}_{2^{\kappa_2}}(-\overline{\alpha}_i))$
$\mathfrak{v}_i$	49	the number of vertices strictly above i in $\Gamma_{\bar{f}}$; in other words, $\mathfrak{v}_i = \lvert \mathrm{V}(\mathrm{Tree}_{\Gamma_{\bar{f}}}(i)) \rvert - 1$
V	17	variable denoting the vertex set of a digraph
$\mathrm{V}(\Gamma)$	9	the vertex set of Γ

$\mathcal{V}_{i,L}$	198	the arithmetic partition $\mathfrak{P}(\eta_{i,l}(x) : l \in \mathfrak{C}_{i,L})$ of C_i; if all f-periodic points in C_i have f-cycle length at most L, then $\mathcal{V}_{i,L}$ is the unique arithmetic partition of C_i such that one block of $\mathcal{V}_{i,L}$ consists of all f-transient points in C_i, while every other block of $\mathcal{V}_{i,L}$ consists of all f-periodic points of a common f-cycle length
w	21	variable denoting an element of the same ground set as x, y, z
$\mathfrak{w}$	63	variable denoting an edge weight
$\mathfrak{w}_k$	168	notation used in the proof of Lemma 5.3.2.2 (4); for fixed $i \in \{0, 1, \ldots, d-1\}$ and $t \in \mathbb{Z}$, it denotes the weight of the k-th edge from the left in the drawing of $\mathfrak{T}_{i_t,k}$ in Section 4.1
W	12	Lambert W function
$\mathcal{W}_{i,L}$	197	the arithmetic partition $\mathcal{V}_{i,L} \wedge \mathcal{Q}_{i,H_i+L-1}$ of C_i; if all f-periodic points in C_i have f-cycle length at most L, then for each f-periodic $x \in C_i$, the $\mathcal{W}_{i,L}$-block in which x is contained controls the isomorphism type of the connected component of Γ_f containing x
wreath product	8	none
x	1	an element of a ground set such as X or $\mathbb{F}_q$, or a variable in a congruence, depending on the context
x_n	3	a formal variable, used in cycle types
$x^{(t)}$	195	defined for $x \in \mathrm{per}(f)$ and $t \in \mathbb{Z}$; denotes $(f_{\lvert \mathrm{per}(f)})^t(x)$
$\mathfrak{x}$	9	variable denoting an element of $\mathfrak{X}$
$[\vec{\mathfrak{x}}]$	9	the cyclic sequence associated with the finite sequence $\vec{\mathfrak{x}}$ over $\mathfrak{X}$; also written $[\mathfrak{x}_0, \ldots, \mathfrak{x}_{L-1}]$ if $\vec{\mathfrak{x}} = (\mathfrak{x}_0, \ldots, \mathfrak{x}_{L-1})$
$\lvert\vec{\mathfrak{x}}\rangle$	90	defined when $\vec{\mathfrak{x}} \in \{0,1\}^n$; it is the n-qubit register encoding $\vec{\mathfrak{x}}$; physicists call this object a *ket*
X	1	a set (usually assumed to be finite)
$\mathcal{X}$	49	variable denoting an arithmetic partition; used, e.g., with enumerating indices $(\mathcal{X}_1, \mathcal{X}_2, \ldots)$ to avoid a clash with the notation $\mathcal{P}_i$
$\mathfrak{X}$	9	variable used to denote a set viewed as an alphabet, from whose elements finite sequences are formed
y	9	variable denoting an element of the same ground set as x
Y_i	117	the domain of definition of par_i, par'_i and par''_i
$Y_{i,p}$	118	the domain of definition of $\mathrm{par}'_{i,p}$
$\bar{Y}_i$	122	the parameter set $\prod_{p \in \mathfrak{P}_i} Y_{i,p}$

$\mathcal{Y}$	222	variable denoting an arithmetic partition (like $\mathcal{X}$)
$\mathfrak{Y}$	152	(used in Theorem 5.3.1.1) a special set of primes
z	15	variable denoting an element of the same ground set as x or y
$\mathcal{Z}_i$	87	appears in the definition of a partition-tree register; a specifically defined object that encodes enough information to reconstruct $\mathcal{P}_i$ (sometimes more)
$\mathbb{Z}/m\mathbb{Z}$	1	the ring of residues modulo m, with underlying set $\{0, 1, \ldots, m-1\}$
$(\mathbb{Z}/m\mathbb{Z})^*$	33	the multiplicative group of units of $\mathbb{Z}/m\mathbb{Z}$
α_i	47	the linear coefficient of A_i
$\bar{\alpha}_i$	53	the linear coefficient of $\mathcal{A}_i$
$\bar{\alpha}_{i,h}$	54	the linear coefficient of $\mathcal{A}_{i,h}$
$\bar{\alpha}'_i$	207	the linear coefficient of $\mathcal{A}'_i$
β_i	47	the constant coefficient of A_i
$\bar{\beta}_i$	118	the constant coefficient of $\mathcal{A}_i$
$\bar{\beta}_{i,h}$	54	the constant coefficient of $\mathcal{A}_{i,h}$
$\bar{\beta}'_i$	207	the constant coefficient of $\mathcal{A}'_i$
$\bar{\beta}''_i$	208	the constant coefficient of $(\mathcal{A}'_i)^{\mathrm{ord}_{s'_i}(\bar{\alpha}'_i)}$
γ	12	Euler–Mascheroni constant
Γ	1	variable denoting a (usually finite) digraph
$[\Gamma]_{\cong}$	18	the digraph isomorphism type of Γ
Γ^*	17	the dual digraph of Γ
Γ_g	1	the functional graph of g
$\Gamma_f^{(i)}$	83	the functional graph of $f_{\mid U_i}$
Γ_{per}	13	the induced subgraph of Γ_f on $\bigcup_{i \in \mathrm{per}(\bar{f})} C_i$
Δ	18	variable denoting a finite directed rooted tree
ζ	32	variable denoting a cycle of a function
$\eta_{i,l}(x)$	198	a certain s-congruence, which in case l is a multiple of ℓ (the $\bar{f}$-cycle length of i) characterizes the f-periodic points $x \in C_i$ with $f^l(x) = x$
$\theta_{i,h}(x)$	54	an s-congruence that characterizes when $x \in \mathbb{Z}/s\mathbb{Z}$ lies in the image of $\mathcal{A}_{i,h}$

$\Theta(x)$	55	a system of m-CCs in the single variable x
$\Theta_{i,h}(x)$	54	a system of (at most two) s-CCs that characterizes when $x \in C_i \cong \mathbb{Z}/s\mathbb{Z}$ has $\mathfrak{h}$-value h
ι	40	variable denoting an isomorphism or bijection; see in particular the notation $\iota_{\vec{r}}$ introduced after Problem 2.3.7
ι_i	8	the bijection $\mathbb{Z}/s\mathbb{Z} \to C_i$, $x \mapsto \omega^{i+dx}$
$\kappa_{i,p}$	120	shorthand for $\nu_p^{(\kappa_p)}(\bar{\beta}_i)$
κ_p	118	shorthand for $\nu_p(s)$
$\kappa_{\mathcal{P},A}(\vec{v},\vec{v}',J)$	28	technical parameter, used in the definition of $\sigma_{\mathcal{P},A}(\vec{v},\vec{v}')$
$\lambda(\mathcal{P},A)$	55	like $\mathfrak{P}'(\mathcal{P},A)$, with the last spanning congruence deleted
$\lambda_i^t(\mathcal{P})$	56	defined when $i < d$ is $\bar{f}$-periodic, $t \in \mathbb{N}_0$, and $\mathcal{P}$ is an arithmetic partition of C_i; it is the arithmetic partition of C_{i_t} defined recursively via $\lambda_i^0(\mathcal{P}) := \mathcal{P}$ and $\lambda_i^{t+1}(\mathcal{P}) := \lambda(\lambda_i^t(\mathcal{P}), A_{i_t})$
Λ	32	variable denoting a lift function $\mathbb{Z}/m_1\mathbb{Z} \to \mathbb{Z}/m_2\mathbb{Z}$, where $m_1, m_2 \in \mathbb{N}^+$ with $m_1 \mid m_2$ (i.e., $\Lambda(x) \equiv x \pmod{m_1}$ for all $x \in \mathbb{Z}/m_1\mathbb{Z}$); the details of its definition vary by context
μ_a	16	the endomorphism $x \mapsto ax$ of the group $\mathbb{Z}/m\mathbb{Z}$; m must be clear from context
ν	11	variable denoting a logical sign ($\emptyset$ or $\neg$)
$\nu_{l,l'}$	198	(used in Section 5.3.3) notation for a logical sign; it is defined as $\emptyset$ (the positive logical sign) if $l \mid l'$, and as $\neg$ otherwise
$\vec{\nu}_{i,L,l}$	198	the logical sign tuple $(\nu_{l,l'})_{l' \in \mathfrak{C}_{i,L}}$; if all f-periodic points in C_i have f-cycle length at most L and $l \in \mathfrak{C}_{i,L}$, then $\mathcal{B}(\mathcal{V}_{i,L}, \vec{\nu}_{i,L,l})$ consists precisely of those f-periodic $x \in C_i$ that have f-cycle length exactly l
$\vec{v}^+$	148	a special notation used in Section 5.2.3
$\vec{v}'^-$	148	a special notation used in Section 5.2.3; inverse to the notation $\vec{v}^+$
$\nu_p(n)$	16	the p-adic valuation of n
$\nu_p^{(v)}(n)$	16	defined as $\min\{v, \nu_p(n)\}$
$\vec{\xi}_{i,k}$	55	defined when $i \in \{0,1,\dots,d-1\}$ is $\bar{f}$-periodic and $k \in \{0,1,\dots,H_i\}$; it is the logical sign tuple of length H_i in which precisely the first k entries are equal to the positive logical sign; the block $\mathcal{B}(\mathcal{U}_i, \vec{\xi}_{i,k})$ consists just of those $x \in C_i$ that are of $\mathfrak{h}$-value k
$\pi(m)$	40	the set of prime divisors of m

$\rho_{\mathfrak{l}}$	23	the left-regular representation of a group G (clear from context) on itself, i.e., the function $G \to \mathrm{Sym}(G)$, $x \mapsto (y \mapsto xy)$
$\rho_{\mathfrak{r}}$	23	the right-regular representation of a group G (clear from context) on itself, i.e., the function $G \to \mathrm{Sym}(G)$, $x \mapsto (y \mapsto yx)$
σ	12	divisor sum function
$\sigma_{\mathcal{P},A}(\vec{\nu},\vec{\nu'})$	28	a technical parameter, for the significance of which see the comments on $\mathfrak{P}'(\mathcal{P},A)$
$\tau(m)$	156	the number of (positive) divisors of $m \in \mathbb{N}^+$
ϕ	33	Euler's totient function
φ	23	a variable denoting a group endomorphism
φ_i	47	defined for $i \in \{0,1,\ldots,d-1\}$ such that $a_i \neq 0$; it is μ_{α_i}, the group endomorphism of $\mathbb{Z}/s\mathbb{Z}$ associated with A_i
χ	90	a variable denoting a characteristic function
ψ	3	a permutation of X
ω	3	a primitive element of $\mathbb{F}_q$

Table A.2. Tabular overview of notation and terminology used in this memoir.