ACTA ARITHMETICA
150.4 (2011)

The formulas for the coefficients of the sum and product of p-adic integers with applications to Witt vectors

by

KEJIAN XU (Siping and Qingdao), ZHAOPENG DAI (Beijing) and ZONGDUO DAI (Beijing)

1. Introduction. For any two p-adic integers $a, b \in \mathbb{Z}_p$, assume that we have the p-adic expansions:

$$\begin{aligned} a &= a_0 + a_1 p + a_2 p^2 + \cdots, \\ b &= b_0 + b_1 p + b_2 p^2 + \cdots, \\ a + b &= c_0 + c_1 p + c_2 p^2 + \cdots, \\ -a &= d_0 + d_1 p + d_2 p^2 + \cdots, \\ ab &= e_0 + e_1 p + e_2 p^2 + \cdots. \end{aligned}$$

In this paper, the following problem is investigated:

PROBLEM. *For any t, express c_t, d_t, e_t by some polynomials over $\mathbb{F}_p$ of $a_0, a_1, \ldots, a_t$, $b_0, b_1, \ldots, b_t$.*

In Sections 2 and 3, we write out the polynomials for c_t and d_t explicitly. In Section 4, we deal with the case of ab, which is rather complicated, and we give an expression for e_t, which reduces the problem to the one about some kind of partitions of the integer p^t.

We apply the results to operations on Witt vectors ([14]). Let R be an associative ring. The *Witt vectors* are vectors $(a_0, a_1, \ldots)$, $a_i \in R$, with addition and multiplication defined as follows:

$$\begin{aligned} (a_0, a_1, \ldots) \dot{+} (b_0, b_1, \ldots) &= (S_0(a_0, b_0), S_1(a_0, a_1; b_0, b_1), \ldots), \\ (a_0, a_1, \ldots) \dot{\times} (b_0, b_1, \ldots) &= (M_0(a_0, b_0), M_1(a_0, a_1; b_0, b_1), \ldots), \end{aligned}$$

where S_n, M_n are rather complicated polynomials in $\mathbb{Z}[x_0, x_1, \ldots, x_n; y_0, y_1, \ldots, y_n]$ and can be uniquely but only recurrently determined by Witt polynomials (see [14]). Up to now it has seemed to be too involved to find

2010 *Mathematics Subject Classification*: 11D88, 13F35, 11C08.
Key words and phrases: p-adic integer, addition, multiplication, Witt vector.

DOI: 10.4064/aa150-4-3

simplified forms of S_n and M_n for all n, and therefore no explicit expressions for S_n and M_n are given yet. It is well known that all Witt vectors with addition $\dot{+}$ and multiplication $\dot{\times}$ defined above form a ring, called the ring of Witt vectors with coefficients in R and denoted by $\mathbf{W}(R)$. A similar problem is whether addition and multiplication of Witt vectors can be expressed explicitly. From [14] it is well known that we have the canonical isomorphism

$$\mathbf{W}(\mathbb{F}_p) \cong \mathbb{Z}_p,$$

given by

$$(a_0, a_1, \ldots) \mapsto \sum_{i=0}^{\infty} \tau(a_i)p^i,$$

where τ is the Teichmüller lifting. By this isomorphism, the operations on $\mathbb{Z}_p$ can be transmitted to those on $\mathbf{W}(\mathbb{F}_p)$. But, here the elements of $\mathbb{Z}_p$ are expressed with respect to the multiplicative residue system $\tau(\mathbb{F}_p)$, not the ordinary least residue system $\{0, 1, \ldots, p-1\}$. So, for $p > 5$ the operations on $\mathbb{Z}_p$ and hence on $\mathbf{W}(\mathbb{F}_p)$ do not coincide with the ordinary operations on p-adic integers, while in the case of $p = 2$, we have $\tau(\mathbb{F}_2) = \{0, 1\}$, that is, the two residue systems coincide. Hence, our results in the case of $p = 2$ imply that the operations on Witt vectors in $\mathbf{W}(\mathbb{F}_2)$ can be written explicitly. As for the case of $p = 3$, we have $\tau(\mathbb{F}_3) = \{-1, 0, 1\}$, but it is difficult to apply our results directly to $\mathbf{W}(\mathbb{F}_3)$. In a recent private communication, Browkin considered the transformation between the coefficients of a p-adic integer expressed in the ordinary least residue system and the numerically least residue system, and proposed the following problem, which provides us with a way to apply our results to $\mathbf{W}(\mathbb{F}_3)$.

Browkin's problem. *Let p be an odd prime. Every p-adic integer c can be written in two forms:*

$$c = \sum_{i=0}^{\infty} a_i p^i = \sum_{j=0}^{\infty} b_j p^j,$$

where a_i and b_j belong respectively to the sets

$$\{0, 1, \ldots, p-1\} \quad \textit{and} \quad \{0, \pm 1, \pm 2, \ldots, \pm (p-1)/2\}.$$

Obviously every b_j is a polynomial in $a_0, a_1, \ldots, a_j$ (and conversely). Can one write these polynomials explicitly?

In Section 5, we solve Browkin's problem, that is, we present the required polynomials. As an application, in Section 6 we can write the operations in $\mathbf{W}(\mathbb{F}_3)$ explicitly.

It should be pointed that the explicit formulas obtained in this paper are useful; in particular, the second author has found many applications in

T-functions. In fact, in 2002 A. Klimov and A. Shamir proposed the theory of T-functions which are important classes of cryptographic primitives ([5]–[9]). They have analyzed their properties, such as invertibility, cycle structure, etc. and have shown that one can effectively construct mappings with required properties. Thus, T-functions can be used in stream ciphers, block ciphers, pseudo-random number generators, hash functions, and so on. Recently, TSC-series stream ciphers ([3], [4], [13]) which are based on T-functions were proposed by Hong et al. as one of the candidates for the ECRYPT Stream Cipher project. As is well known, almost all of the applications require T-functions to have the single cycle property. To characterize this property, Klimov and Shamir introduced the notion of even and odd parameters and their main tool was the bit-slice analysis ([12]). More recently, Dai et al. give an equivalent but more explicit characterization of even and odd parameters from the point of view of the Algebraic Normal Form of T-functions ([11], [2]). Furthermore, they deeply develop the bit-slice analysis of T-functions and present a new method to determine whether a T-function is a single cycle. But the key tool used in Dai's work is our explicit formulas for the sum and product of 2-adic integers obtained in this paper.

2. Addition. By convention, for the empty set $\emptyset$, we let $\prod_{i\in\emptyset} = 1$.

THEOREM 2.1. *Assume that*

$$A=\sum_{i=0}^{r} a_i p^i, \qquad B=\sum_{i=0}^{r} b_i p^i, \qquad A+B=\sum_{i=0}^{r+1} c_i p^i,$$

where $a_i, b_i, c_i \in \{0,1,\dots,p-1\}$ *and* $r \ge 1$. *Then* $c_0 = a_0 + b_0 \pmod p$ *and for* $1 \le t \le r+1$,

$$c_t = a_t + b_t + \sum_{i=0}^{t-1}\left(\sum_{k=1}^{p-1}\binom{a_i}{k}\binom{b_i}{p-k}\right)\prod_{j=i+1}^{t-1}\binom{a_j+b_j}{p-1} \pmod p.$$

Proof. We need the following two lemmas.

LEMMA 2.2 (Lucas). *If* $A=\sum_{i=0}^{r} a_i p^i$, $B=\sum_{i=0}^{r} b_i p^i$, $0 \le a_i < p$, $0 \le b_i < p$, *then*

$$\binom{A}{B} = \prod_{i=0}^{r}\binom{a_i}{b_i} \pmod p.$$

In particular

$$a_t = \binom{A}{p^t} \pmod p, \qquad \forall t.$$

For the convenience of the readers, we include a short proof. In $\mathbb{F}_p[z]$ we have

$$\sum_{t=0}^{A}\binom{A}{t}z^t=(1+z)^A=\prod_{i=0}^{r}(1+z)^{a_ip^i}$$
$$=\prod_{i=0}^{r}(1+z^{p^i})^{a_i}=\prod_{i=0}^{r}\sum_{j=0}^{p-1}\binom{a_i}{j}z^{jp^i}$$
$$=\sum_{\substack{(j_0,\dots,j_r)\\0\le j_i\le p-1}}\binom{a_0}{j_0}\binom{a_1}{j_1}\cdots\binom{a_r}{j_r}z^{\sum_{i=0}^{r}j_ip^i}.$$

Comparing the coefficients of z^B on both sides we get the lemma.

LEMMA 2.3. $\displaystyle\binom{A+B}{t}=\sum_{\lambda+\mu=t}\binom{A}{\lambda}\binom{B}{\mu}.$

In fact, we have

$$\sum_t\binom{A+B}{t}z^t=(1+z)^{A+B}=(1+z)^A(1+z)^B$$
$$=\sum_\lambda\binom{A}{\lambda}z^\lambda\sum_\mu\binom{B}{\mu}z^\mu=\sum_t\Big(\sum_{\lambda+\mu=t}\binom{A}{\lambda}\binom{B}{\mu}\Big)z^t,$$

and the lemma follows from comparing the coefficients of z^t on both sides.

Now, we turn to the proof of the theorem. By the two lemmas, we have

$$c_t=a_t+b_t+\sum_{\lambda+\mu=p^t,\,p^{t-1}\|\lambda}\binom{A}{\lambda}\binom{B}{\mu}+\sum_{i=0}^{t-2}\sum_{\lambda+\mu=p^t,\,p^i\|\lambda}\binom{A}{\lambda}\binom{B}{\mu}\pmod p.$$

Let

$$\lambda=\lambda_ip^i+\lambda_{i+1}p^{i+1}+\cdots+\lambda_{t-1}p^{t-1},$$

where $1\le\lambda_i\le p-1, 0\le\lambda_j\le p-1$ for $i+1\le j\le t-1$. Then

$$\mu=p^t-\lambda=(p-\lambda_i)p^i+(p-1-\lambda_{i+1})p^{i+1}+\cdots+(p-1-\lambda_{t-1})p^{t-1}.$$

Consequently, by the Lucas lemma, we have in $\mathbb{F}_p$

$$\binom{A}{\lambda}=\binom{a_i}{\lambda_i}\prod_{j=i+1}^{t-1}\binom{a_j}{\lambda_j},\qquad\binom{B}{\mu}=\binom{b_i}{p-\lambda_i}\prod_{j=i+1}^{t-1}\binom{b_j}{p-1-\lambda_j},$$

$$\sum_{\lambda+\mu=p^t,\,p^{t-1}\|\lambda}\binom{A}{\lambda}\binom{B}{\mu}=\sum_{i=1}^{p-1}\binom{a_{t-1}}{i}\binom{b_{t-1}}{p-i}.$$

Therefore

$$\sum_{\lambda+\mu=p^t,\, p^i\|\lambda} \binom{A}{\lambda}\binom{B}{\mu}$$
$$= \sum_{\lambda_i=1}^{p-1} \sum_{\lambda_{i+1}=0}^{p-1} \cdots \sum_{\lambda_{t-1}=0}^{p-1} \binom{a_i}{\lambda_i}\binom{b_i}{p-\lambda_i} \prod_{j=i+1}^{t-1} \binom{a_j}{\lambda_j}\binom{b_j}{p-1-\lambda_j}$$
$$= \sum_{\lambda_i=1}^{p-1} \binom{a_i}{\lambda_i}\binom{b_i}{p-\lambda_i} \sum_{\lambda_{i+1}=0}^{p-1} \binom{a_{i+1}}{\lambda_{i+1}}\binom{b_{i+1}}{p-1-\lambda_{i+1}}$$
$$\cdots \sum_{\lambda_{t-1}=0}^{p-1} \binom{a_{t-1}}{\lambda_{t-1}}\binom{b_{t-1}}{p-1-\lambda_{t-1}}.$$

To all these sums but the first we apply Lemma 2.3 to get

$$\sum_{\lambda_i=1}^{p-1} \binom{a_i}{\lambda_i}\binom{b_i}{p-\lambda_i} \cdot \prod_{j=i+1}^{t-1} \binom{a_j+b_j}{p-1}.$$

Therefore

$$c_t = a_t+b_t+\sum_{k=1}^{p-1}\binom{a_{t-1}}{k}\binom{b_{t-1}}{p-k} + \sum_{i=0}^{t-2}\Bigg(\sum_{k=1}^{p-1}\binom{a_i}{k}\binom{b_i}{p-k}\Bigg)\prod_{j=i+1}^{t-1}\binom{a_j+b_j}{p-1}$$
$$= a_t+b_t+\sum_{i=0}^{t-1}\Bigg(\sum_{k=1}^{p-1}\binom{a_i}{k}\binom{b_i}{p-k}\Bigg)\prod_{j=i+1}^{t-1}\binom{a_j+b_j}{p-1} \pmod p. \ \blacksquare$$

COROLLARY 2.4. *Assume that*

$$a = \sum_{i=0}^{\infty} a_i p^i,\ \ b = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p, \qquad a+b = \sum_{i=0}^{\infty} c_i p^i,$$

with $a_i, b_i, c_i \in \{0,1,\ldots,p-1\}$. *Then* $c_0 = a_0+b_0 \pmod p$ *and for* $t \ge 1$,

$$c_t = a_t+b_t+\sum_{i=0}^{t-1}\Bigg(\sum_{j=1}^{p-1}\binom{a_i}{j}\binom{b_i}{p-j}\Bigg)\prod_{j=i+1}^{t-1}\binom{a_j+b_j}{p-1} \pmod p.$$

In particular, if $p=2$, *then* $c_0 = a_0+b_0 \pmod 2$ *and for* $t \ge 1$,

$$c_t = a_t+b_t+\sum_{i=0}^{t-1} a_i b_i \prod_{j=i+1}^{t-1}(a_j+b_j) \pmod 2. \ \blacksquare$$

COROLLARY 2.5. *Assume that* $a = \sum_{i=0}^{\infty} a_i 2^i \in \mathbb{Z}_2$ *and* $n \ge 1$.

(i) *If* $2^n a = \sum_{i=0}^{\infty} c_i 2^i \in \mathbb{Z}_2$, *then* $c_t = 0$ *for* $0 \le t < n$, *and* $c_t = a_{t-n} \pmod 2$ *for* $t \ge n$.

(ii) *If* $(2^n+1)a = \sum_{i=0}^{\infty} c_i 2^i \in \mathbb{Z}_2$, *then* $c_t = a_t$ *for* $0 \le t \le n-1$, $c_n = a_n + a_0 \pmod 2$ *and for* $t \ge n+1$,

$$c_t = a_t + a_{t-n} + \sum_{i=n}^{t-1} a_i a_{i-n} \prod_{j=i+1}^{t-1} (a_j + a_{j-n}) \pmod 2. \quad \blacksquare$$

COROLLARY 2.6. *Assume that* $a = \sum_{i=0}^{\infty} a_i 3^i \in \mathbb{Z}_3$ *and* $n \ge 1$. *If* $2a = \sum_{i=0}^{\infty} c_i 3^i \in \mathbb{Z}_3$, *then* $c_0 = -a_0 \pmod 3$ *and for* $t \ge 1$,

$$c_t = -a_t + \sum_{i=0}^{t-1} a_i(1-a_i) \prod_{j=i+1}^{t-1} a_j(2a_j - 1) \pmod 3. \quad \blacksquare$$

3. Additive inverse

THEOREM 3.1. *Let* $A = \sum_{i=0}^{r} a_i p^i$. *Assume that*

$$-A = \sum_{i=0}^{r} d_i p^i \pmod{p^{r+1}},$$

where $d_i \in \{0, 1, \ldots, p-1\}$. *Then* $d_0 = -a_0 \pmod p$ *and for* $1 \le t \le r$,

$$d_t = -a_t - 1 + \prod_{i=0}^{t-1} (1 - a_i^{p-1}) \pmod p.$$

Proof. Clearly, we can assume that $A \neq 0$. Then there exists an s such that $a_s \neq 0$ but $a_i = 0$ for $i < s$. This implies that

$$d_t = \begin{cases} -a_t \pmod p & \text{if } t \le s, \\ -a_t - 1 \pmod p & \text{if } t > s, \end{cases}$$

which is equivalent to

$$d_t = \begin{cases} -a_t \pmod p & \text{if } (a_0, a_1, \ldots, a_{t-1}) = (0, \ldots, 0), \\ -a_t - 1 \pmod p & \text{if } (a_0, a_1, \ldots, a_{t-1}) \neq (0, \ldots, 0). \end{cases}$$

Take $f(a_0, a_1, \ldots, a_{t-1}) = -1 + \prod_{i=0}^{t-1} (1 - a_i^{p-1}) \pmod p$. Clearly

$$f(a_0, a_1, \ldots, a_{t-1}) = \begin{cases} 0 \pmod p & \text{if } (a_0, a_1, \ldots, a_{t-1}) = (0, \ldots, 0), \\ -1 \pmod p & \text{if } (a_0, a_1, \ldots, a_{t-1}) \neq (0, \ldots, 0). \end{cases}$$

Therefore,

$$d_t = -a_t + f(a_0, a_1, \ldots, a_{t-1}) = -a_t - 1 + \prod_{i=0}^{t-1} (1 - a_i^{p-1}) \pmod p. \quad \blacksquare$$

COROLLARY 3.2. *Assume that*

$$a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p, \qquad -a = \sum_{i=0}^{\infty} d_i p^i,$$

with $a_i, d_i \in \{0, 1, \dots, p-1\}$. *Then* $d_0 = -a_0 \pmod p$ *and for* $t \geq 1$,

$$d_t = -a_t - 1 + \prod_{i=0}^{t-1}(1 - a_i^{p-1}) \pmod p.$$

If $p = 2$, *then* $d_0 = a_0$ *and for* $t \geq 1$,

$$d_t = a_t + 1 + \prod_{i=0}^{t-1}(1 + a_i) \pmod 2. \blacksquare$$

Remark 3.4. The problems considered in this section and in Corollaries 2.5 and 2.6 were suggested to us by J. Browkin.

4. Multiplication

4.1. Fundamental lemma

4.1.1. *Fundamental polynomials.* Let

$$\mathbb{K} = \Big\{\underline{k} = (k_1, \dots, k_{p-1}) : k_l \geq 0,\ 0 \leq \sum_{l=1}^{p-1} k_l \leq p-1\Big\}.$$

Clearly $\underline{0} = (0, \dots, 0) \in \mathbb{K}$. Let

$$\mathbb{K}^{(r+1)^2} = \underbrace{\mathbb{K} \times \dots \times \mathbb{K}}_{(r+1)^2},$$

and write $\underline{\underline{0}} = (\underline{0}, \dots, \underline{0}) \in \mathbb{K}^{(r+1)^2}$.

For any $\underline{k} = (k_1, \dots, k_{p-1}) \in \mathbb{K}$, $\underline{k} \neq \underline{0}$, define

$$\pi_{\underline{k}}(x, y) = \frac{y(y-1)\cdots(y - \sum_{l=1}^{p-1} k_l + 1)}{k_1! \cdots k_{p-1}!} \prod_{l=1}^{p-1}\Big(\frac{x(x-1)\cdots(x-l+1)}{l!}\Big)^{k_l} \pmod p,$$

and for $\underline{k} = \underline{0}$, define $\pi_{\underline{k}}(x, y) = 1$.

Let $\mathbf{I} = \{(i, j) : 0 \leq i, j \leq r\}$, and let $\underline{x} = (x_0, \dots, x_r)$, $\underline{y} = (y_0, \dots, y_r)$. Then for $\underline{\underline{k}} = (\dots, \underline{k}_{i,j}, \dots) \in \mathbb{K}^{(r+1)^2}$ with $\underline{k}_{i,j} = (k_{i,j,1}, \dots, k_{i,j,p-1})$, we define the function

$$\pi_{\underline{\underline{k}}}(\underline{x}, \underline{y}) = \prod_{(i,j)\in\mathbf{I}} \pi_{\underline{k}_{i,j}}(x_i, y_j),$$

and the norm

$$\|\underline{\underline{k}}\| = \sum_{(i,j)\in\mathbf{I}} \Big(\sum_{l=1}^{p-1} l k_{i,j,l}\Big) p^{i+j}.$$

Clearly, $\pi_{\underline{\underline{k}}}(\underline{x}, \underline{y})$ is a polynomial in $x_0, \dots, x_r$, $y_0, \dots, y_r$.

LEMMA 4.1. *Assume that* $\underline{0} \neq \underline{k} \in \mathbb{K}$. *Let* $0 \le a, b \le p-1$. *Then* $\pi_{\underline{k}}(a,b) = 0$ *if one of the following cases occurs:*

(i) $ab = 0$;
(ii) *there exists an* l *such that* $l > a$ *and* $k_l > 0$;
(iii) $\sum_{l=1}^{p-1} k_l > b$.

Proof. This can be checked directly. ∎

LEMMA 4.2. *Assume that* $\underline{\underline{0}} \neq \underline{\underline{k}} = (\dots, \underline{k}_{i,j}, \dots) \in \mathbb{K}^{(r+1)^2}$. *Let* $\underline{a} = (a_0, a_1, \dots, a_r)$ *and* $\underline{b} = (b_0, b_1, \dots, b_r)$. *Then* $\pi_{\underline{\underline{k}}}(\underline{a}, \underline{b}) = 0$ *if one of the following cases occurs:*

(i) *there exists* $(i,j) \in \mathbf{I}$ *such that* $a_i b_j = 0$ *and* $\underline{k}_{i,j} \neq \underline{0}$;
(ii) *there exist* $(i,j) \in \mathbf{I}$ *and* $l > a_i$ *such that* $k_{i,j,l} > 0$;
(iii) *there exists* $(i,j) \in \mathbf{I}$ *such that* $\sum_{l=1}^{p-1} k_{i,j,l} > b_j$.

Proof. This follows from Lemma 4.1. ∎

4.1.2. *Fundamental lemma*

LEMMA 4.3. *Assume that*

$$A = \sum_{i=0}^{r} a_i p^i, \qquad B = \sum_{i=0}^{r} b_i p^i, \qquad AB = \sum_{i=0}^{2r+1} e_i p^i.$$

Then $e_0 = a_0 b_0 \pmod p$ *and for* $1 \le t \le 2r+1$,

$$e_t = \sum_{\substack{\underline{\underline{k}} \in \mathbb{K}^{(t+1)^2} \\ \|\underline{\underline{k}}\| = p^t}} \pi_{\underline{\underline{k}}}(\underline{a}, \underline{b}) \pmod p,$$

where $\underline{a} = (a_0, a_1, \dots, a_t)$ *and* $\underline{b} = (b_0, b_1, \dots, b_t)$.

Proof. Define

$$\mathbf{I}(\underline{a}, \underline{b}) = \{(i,j) \in \mathbf{I} : 0 \le i, j \le t,\ a_i b_j \neq 0\}.$$

For any integers $0 < a, b < p$, set

$$\mathbb{K}(a,b) = \Big\{\underline{k} = (k_1, \dots, k_a, 0, \dots, 0) \in \mathbb{K} : k_l \ge 0, 1 \le \sum_{l=1}^{a} k_l \le b\Big\}.$$

Note that $\underline{0} \notin \mathbb{K}(a,b)$. We will denote $\underline{k} = (k_1, \dots, k_a, 0, \dots, 0)$ simply by $(k_1, \dots, k_a)$. Then, for $\underline{k} = (k_1, \dots, k_a) \in \mathbb{K}(a,b)$, we clearly have

$$\pi_{\underline{k}}(a,b) = \binom{b}{\underline{k}} \prod_{l=1}^{a} \binom{a}{l}^{k_l} \pmod p,$$

where

$$\binom{b}{\underline{k}} = \frac{b!}{k_1! \cdots k_a! (b - \sum_{l=1}^{a} k_l)!}.$$

For $\emptyset \neq S \subseteq \mathbf{I}(\underline{a}, \underline{b})$, define

$$\mathbb{K}_S(\underline{a}, \underline{b}) = \{(\ldots, \underline{k}_{i,j}, \ldots) \in \mathbb{K}^{(t+1)^2} : \underline{k}_{i,j} \in \mathbb{K}(a_i, b_j) \text{ for } (i,j) \in S; \\ \underline{k_{i,j}} = \underline{0} \text{ for } (i,j) \notin S\}.$$

If $\underline{\underline{k}} = (\ldots, \underline{k}_{i,j}, \ldots) \in \mathbb{K}_S(\underline{a}, \underline{b})$ with $\underline{k_{i,j}} = (k_{i,j,1}, \ldots, k_{i,j,a_i}) \in \mathbb{K}(a_i, b_j)$, then it is easy to show that

$$\pi_{\underline{\underline{k}}}(\underline{a}, \underline{b}) = \prod_{(i,j)\in S} \pi_{\underline{k}_{i,j}}(a_i, b_j) \pmod p,$$

$$\|\underline{\underline{k}}\| = \sum_{(i,j)\in S} \Big(\sum_{l=1}^{a_i} l k_{i,j,l}\Big) p^{i+j}.$$

Now, we have

$$\sum_{0\le\lambda\le AB} \binom{AB}{\lambda} z^\lambda = (1+z)^{AB} = \prod_{\substack{0\le i\le t\\ a_i\neq 0}} (1+z^{p^i})^{a_i B}$$

$$= \prod_{(i,j)\in\mathbf{I}(\underline{a},\underline{b})} \Big(1 + \sum_{l=1}^{a_i} \binom{a_i}{l} z^{lp^{i+j}}\Big)^{b_j}$$

$$= \prod_{(i,j)\in\mathbf{I}(\underline{a},\underline{b})} \Big(1 + \sum_{\underline{k}\in\mathbb{K}(a_i,b_j)} \binom{b_j}{\underline{k}} \prod_{l=1}^{a_i} \binom{a_i}{l}^{k_l} z^{\sum_{l=1}^{a_i} l k_l p^{i+j}}\Big)$$

$$= \prod_{(i,j)\in\mathbf{I}(\underline{a},\underline{b})} \Big(1 + \sum_{\underline{k}\in\mathbb{K}(a_i,b_j)} \pi_{\underline{k}}(a_i, b_j) z^{\sum_{l=1}^{a_i} l k_l p^{i+j}}\Big)$$

$$= 1 + \sum_{\emptyset\neq S\subseteq\mathbf{I}(\underline{a},\underline{b})} \sum_{\underline{\underline{k}}=(\ldots,\underline{k}_{i,j},\ldots)\in\mathbb{K}_S(\underline{a},\underline{b})} \prod_{(i,j)\in S} \pi_{\underline{k}_{i,j}}(a_i, b_j) \cdot z^{\sum_{(i,j)\in S}(\sum_{l=1}^{a_i} l k_{i,j,l}) p^{i+j}}$$

$$= 1 + \sum_{\emptyset\neq S\subseteq\mathbf{I}(\underline{a},\underline{b})} \sum_{\underline{\underline{k}}\in\mathbb{K}_S(\underline{a},\underline{b})} \pi_{\underline{\underline{k}}}(\underline{a}, \underline{b}) z^{\|\underline{\underline{k}}\|} \pmod p.$$

Comparing the coefficients of both sides and letting $\lambda = p^t$, from the Lucas lemma we have

$$e_t = \binom{AB}{p^t} = \sum_{\emptyset\neq S\in\mathbf{I}(\underline{a},\underline{b})} \sum_{\substack{\underline{\underline{k}}\in\mathbb{K}_S(\underline{a},\underline{b})\\ \|\underline{\underline{k}}\|=p^t}} \pi_{\underline{\underline{k}}}(\underline{a}, \underline{b}) = \sum_{\substack{\underline{\underline{k}}\in\mathbb{K}^{(t+1)^2}\\ \|\underline{\underline{k}}\|=p^t}} \pi_{\underline{\underline{k}}}(\underline{a}, \underline{b}) \pmod p.$$

The last step follows from Lemma 4.2. ∎

4.2. Multiplication formula

4.2.1. *T_p-partitions.* Now we shall give a simpler formula for e_t. Let $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ and $K := |\mathbb{K}^*|$. Then $|\mathbb{K}| = K + 1$ and we can write the elements of $\mathbb{K}$ as $\underline{k}(j)$, $0 \le j \le K$; in particular, let $\underline{k}(0) = \underline{0}$ for convenience. So

$$\mathbb{K}^* = \{\underline{k}(j) : 1 \le j \le K\}.$$

For $\underline{k} = (k_1, \dots, k_{p-1}) \in \mathbb{K}$, define

$$w(\underline{k}) = \sum_{j=1}^{p-1} j k_j.$$

In the following, we fix the vector:

$$\underline{w} := (w(\underline{k}(1)), \dots, w(\underline{k}(K))).$$

For $\underline{l} = (l_1, \dots, l_K) \in \mathbb{N}^K$ (the cartesian product of the set of non-negative integers), the size of $\underline{l}$ is defined as

$$|\underline{l}| = \sum_{j=1}^{K} l_j,$$

and the inner product of $\underline{w}$ and $\underline{l}$ is defined as

$$\underline{w} \cdot \underline{l} = \sum_{j=1}^{K} w(\underline{k}(j)) l_j.$$

For an integer $n \ge 0$, a T_p-*partition* of n is defined as

$$n = \sum_{j=0}^{t} (\underline{w} \cdot \underline{l}_j) p^j, \qquad \underline{l}_j \in \mathbb{N}^K,\ 0 \le |\underline{l}_j| \le 1 + j.$$

This partition is also written as

$$\underline{\underline{l}} = (\underline{l}_0, \dots, \underline{l}_t), \qquad 0 \le |\underline{l}_j| \le 1 + j.$$

We will write $\mathbf{L}_p(t)$ for the set of all possible T_p-partitions of p^t, that is,

$$\mathbf{L}_p(t) = \Big\{ \underline{\underline{l}} = (\underline{l}_0, \dots, \underline{l}_t) : \sum_{j=0}^{t} (\underline{w} \cdot \underline{l}_j) p^j = p^t,\ 0 \le |\underline{l}_j| \le 1 + j \Big\}.$$

If $p = 2$, then $K = 1$ and $\underline{l}_j$ is only a non-negative integer, so we can write $\underline{l}_j = l_j$. Clearly $l_0 = 0$. Hence, for $p = 2$, we have

$$\mathbf{L}_2(t) = \Big\{ \underline{\underline{l}} = (l_1, \dots, l_t) : \sum_{k=1}^{t} l_k 2^k = 2^t,\ 0 \le l_k \le k + 1 \Big\}.$$

If $p = 3$, then $K = 5$ and we have

$$\mathbb{K}^* = \{\underline{k}(1) = (1,0),\ \underline{k}(2) = (0,1),\ \underline{k}(3) = (2,0),\ \underline{k}(4) = (1,1),\ \underline{k}(5) = (0,2)\},$$

and therefore $\underline{w} = (1, 2, 2, 3, 4)$. Hence, for $p = 3$, we have

$$\mathbf{L}_3(t) = \Big\{ \underline{\underline{l}} = (\underline{l}_0, \ldots, \underline{l}_t) : \sum_{k=0}^{t} (l_{k1} + 2l_{k2} + 2l_{k3} + 3l_{k4} + 4l_{k5}) 3^k = 3^t, \\ 0 \le |\underline{l}_k| \le 1 + k \Big\},$$

where $\underline{l}_k = (l_{k1}, l_{k2}, l_{k3}, l_{k4}, l_{k5}), 0 \le k \le t$.

4.2.2. *Partitions of* $\mathbf{I}(m)$ *and symmetric polynomials.* Let $\mathbf{I}(m) = \{i : 0 \le i \le m\}$, $0 \le m \le t$. For $\underline{l} = (l_1, \ldots, l_K) \in \mathbb{N}^K$ with $|\underline{l}| \le 1 + m$, we call $\underline{S} = (S_1, \ldots, S_K)$ an $\underline{l}$*-partition* of $\mathbf{I}(m)$ if it satisfies

$$S_j \subseteq \mathbf{I}(m), \quad |S_j| = l_j, \\ S_j \cap S_{j'} = \emptyset, \quad \forall j \ne j', 1 \le j, j' \le K.$$

The set of all possible $\underline{l}$-partitions of $\mathbf{I}(m)$ is denoted by $\mathbf{I}(m, \underline{l})$, that is,

$$\mathbf{I}(m, \underline{l}) = \{(S_1, \ldots, S_K) : S_j \subseteq \mathbf{I}(m),\ |S_j| = l_j,\ S_j \cap S_{j'} = \emptyset, \\ \forall j \ne j',\ 1 \le j, j' \le K\}.$$

Defining $l_0 := 1 + m - \sum_{j=1}^{K} l_j$, we get

$$|\mathbf{I}(m, \underline{l})| = \frac{(1+m)!}{l_0! l_1! \cdots l_K!}.$$

For a given integer $m, 0 \le m \le t$, and $\underline{l} = (l_1, \ldots, l_K) \in \mathbb{N}^K$ with $|\underline{l}| \le 1 + m$, define the function

$$\tau_{\underline{l}}(x_0, \ldots, x_m; y_0, \ldots, y_m) = \sum_{\underline{S} = (S_1, \ldots, S_K) \in \mathbf{I}(m, \underline{l})} \prod_{j=1}^{K} \prod_{i \in S_j} \pi_{\underline{k}(j)}(x_i, y_{m-i}).$$

Clearly, $\tau_{\underline{l}}(x_0, \ldots, x_m; y_0, \ldots, y_m)$ is a polynomial which is symmetric with respect to the pairs $\{(x_i, y_{m-i}) : 0 \le i \le m\}$, that is, it is invariant under the permutations of the pairs.

When $p = 2$, we have $K = 1$, $\mathbb{K} = \{0, 1\}$ and hence $\underline{k}(1) = 1$ as well as $l := l_1 = \underline{l}$. So we have

$$\tau_{\underline{l}}(x_0, \ldots, x_m; y_0, \ldots, y_m) = \sum_{0 \le i_1 < \cdots < i_l \le m} \prod_{k=1}^{l} x_{i_k} y_{m-i_k} \\ = \tau_l(x_0 y_m, x_1 y_{m-1}, \ldots, x_m y_0),$$

where $\tau_l(X_0, X_1, \ldots, X_m)$ denotes the lth elementary symmetric polynomial of $X_0, X_1, \ldots, X_m$.

When $p = 3$, we have the ordered set $\mathbb{K}^* = \{(1,0), (0,1), (2,0), (1,1), (0,2)\}$. It is easy to check that when $x_i, y_j \in \mathbb{F}_3$, we have the following equality between polynomial functions:

$$\tau_{\underline{l}}(x_0,\dots,x_m;y_0,\dots,y_m) \\ = \sum_{\underline{S}=(S_1,S_2,S_3,S_4,S_5)\in\mathbf{I}(m,\underline{l})} f_{\underline{S}}(x_0,x_1,\dots,x_m;y_0,y_1,\dots,y_m),$$

where

$$f_{\underline{S}}(x_0,x_1,\dots,x_m;y_0,y_1,\dots,y_m) = \prod_{i_1\in S_1} x_{i_1}y_{m-i_1}\prod_{i_2\in S_2} x_{i_2}(1-x_{i_2})y_{m-i_2} \\ \times \prod_{i_3\in S_3} x_{i_3}^2 y_{m-i_3}(1-y_{m-i_3})\prod_{i\in S_4\cup S_5} x_i(1-x_i)y_{m-i}(y_{m-i}-1).$$

4.2.3. *Multiplication formula*

THEOREM 4.4. *Assume that*

$$A=\sum_{i=0}^{r} a_i p^i, \qquad B=\sum_{i=0}^{r} b_i p^i, \qquad AB=\sum_{i=0}^{2r+1} e_i p^i.$$

Then $e_0 = a_0b_0 \pmod p$ *and for* $1\le t\le 2r+1$,

$$e_t = \sum_{\underline{\underline{l}}=(\underline{l}_0,\dots,\underline{l}_t)\in\mathbf{L}_p(t)} \prod_{k=0}^{t} \tau_{\underline{l}_k}(a_0,\dots,a_k;b_0,\dots,b_k) \pmod p.$$

Proof. For $\underline{\underline{k}}=(\dots,\underline{k}_{i,j},\dots)\in\mathbb{K}^{(t+1)^2}$, let

$$\underline{\underline{S}}(\underline{\underline{k}})=(\underline{S}_0,\dots,\underline{S}_t), \qquad \underline{S}_m=(S_{m,1},\dots,S_{m,K}),$$
$$\underline{\underline{l}}(\underline{\underline{k}})=(\underline{l}_0,\dots,\underline{l}_t), \qquad \underline{l}_m=(l_{m,1},\dots,l_{m,K}),$$

where

$$S_{m,j}=\{i: 0\le i\le m,\ \underline{k}_{i,m-i}=\underline{k}(j)\}, \qquad |S_{m,j}|=l_{m,j}.$$

Clearly, we have

$$S_{m,j}\subseteq \mathbf{I}(m), \qquad S_{m,j}\cap S_{m,j'}=\emptyset, \qquad \forall j\ne j',$$

and

$$|\underline{l}_m| = \sum_{j=1}^{K} l_{m,j} \le 1+m.$$

So $\underline{S}_m\in\mathbf{I}(m,\underline{l}_m)$, and therefore

$$\underline{\underline{S}}(\underline{\underline{k}})\in\mathbf{I}(0,\underline{l}_0)\times\mathbf{I}(1,\underline{l}_1)\times\cdots\times\mathbf{I}(t,\underline{l}_t).$$

We need the following two lemmas.

LEMMA 4.5. $\|\underline{\underline{k}}\|=p^t$ *if and only if* $\underline{\underline{l}}(\underline{\underline{k}})\in\mathbf{L}_p(t)$.

In fact, noting that $w(\underline{0}) = 0$, we have

$$\begin{aligned}\|\underline{\underline{k}}\| &= \sum_{0\le i,j\le t} w(\underline{k}_{i,j})p^{i+j} = \sum_{0\le m\le t}\Big(\sum_{0\le i\le m} w(\underline{k}_{i,m-i})\Big)p^m \\ &= \sum_{0\le m\le t}\Big(\sum_{0\le i\le m,\,\underline{k}_{i,m-i}\neq\underline{0}} w(\underline{k}_{i,m-i})\Big)p^m \\ &= \sum_{0\le m\le t}\Big(\sum_{1\le j\le K}\sum_{i\in S_{m,j}} w(\underline{k}(j))\Big)p^m \\ &= \sum_{0\le m\le t}\Big(\sum_{1\le j\le K} l_{m,j}w(\underline{k}(j))\Big)p^m = \sum_{0\le m\le t}(\underline{w}\cdot\underline{l}_m)p^m,\end{aligned}$$

as required.

Lemma 4.6. *For a fixed $(\underline{l}_0,\dots,\underline{l}_t)\in\mathbf{L}_p(t)$, we have the bijection*

$$\{\underline{\underline{k}}\in\mathbb{K}^{(1+t)^2} : \underline{\underline{l}}(\underline{\underline{k}}) = (\underline{l}_0,\dots,\underline{l}_t)\}\to\mathbf{I}(0,\underline{l}_0)\times\cdots\times\mathbf{I}(t,\underline{l}_t),\qquad \underline{\underline{k}}\mapsto\underline{\underline{S}}(\underline{\underline{k}}).$$

Now, we turn to the proof of the theorem. From Lemmas 4.3, 4.5 and 4.6, we have

$$\begin{aligned}e_t &= \sum_{\substack{\underline{\underline{k}}\in\mathbb{K}^{(t+1)^2}\\ \|\underline{\underline{k}}\|=p^t}}\pi_{\underline{\underline{k}}}(\underline{a},\underline{b}) = \sum_{\substack{\underline{\underline{k}}\in\mathbb{K}^{(t+1)^2}\\ \underline{\underline{l}}(\underline{\underline{k}})\in\mathbf{L}_p(t)}}\pi_{\underline{\underline{k}}}(\underline{a},\underline{b}) = \sum_{\underline{\underline{l}}\in\mathbf{L}_p(t)}\ \sum_{\substack{\underline{\underline{k}}\in\mathbb{K}^{(t+1)^2}\\ \underline{\underline{l}}(\underline{\underline{k}})=(\underline{l}_0,\dots,\underline{l}_t)}}\pi_{\underline{\underline{k}}}(\underline{a},\underline{b}) \\ &= \sum_{\underline{\underline{l}}\in\mathbf{L}_p(t)}\ \sum_{(\underline{S}_0,\dots,\underline{S}_t)\in\prod_{m=0}^t\mathbf{I}(m,\underline{l}_m)}\ \prod_{m=0}^t\prod_{j=1}^K\prod_{i\in S_{m,j}}\pi_{\underline{k}(j)}(a_i,b_{m-i}) \\ &= \sum_{\underline{\underline{l}}\in\mathbf{L}_p(t)}\prod_{m=0}^t\ \sum_{\underline{S}_m\in\mathbf{I}(m,\underline{l}_m)}\ \prod_{j=1}^K\prod_{i\in S_{m,j}}\pi_{\underline{k}(j)}(a_i,b_{m-i}) \\ &= \sum_{\underline{\underline{l}}\in\mathbf{L}_p(t)}\prod_{m=0}^t\tau_{\underline{l}_m}(a_0,\dots,a_m;b_0,\dots,b_m)\ (\mathrm{mod}\ p).\ \blacksquare\end{aligned}$$

Corollary 4.7. *Assume that*

$$a = \sum_{i=0}^\infty a_ip^i,\qquad b = \sum_{i=0}^\infty b_ip^i,\qquad ab = \sum_{i=0}^\infty e_ip^i,$$

with $a_i,b_i,e_i\in\{0,1,\dots,p-1\}$. Then $e_0 = a_0b_0\ (\mathrm{mod}\ p)$ and for $t\ge 1$,

$$e_t = \sum_{\underline{\underline{l}}=(\underline{l}_0,\dots,\underline{l}_t)\in\mathbf{L}_p(t)}\ \prod_{k=0}^t\tau_{\underline{l}_k}(a_0,\dots,a_k;b_0,\dots,b_k)\ (\mathrm{mod}\ p).$$

In particular, if $p=2$, *we have* $e_0 = a_0b_0 \pmod 2$ *and for* $t \geq 1$,

$$e_t = \sum_{(l_1,\dots,l_t)\in \mathbf{L}_2(t)} \prod_{1\leq k\leq t} \tau_{l_k}(a_0b_k, a_1b_{k-1}, \dots, a_kb_0) \pmod 2;$$

if $p=3$, *we have* $e_0 = a_0b_0 \pmod 3$ *and for* $t \geq 1$,

$$e_t = \sum_{(\underline{l}_0,\dots,\underline{l}_t)\in \mathbf{L}_3(t)} \prod_{k=0}^{t} \sum_{\underline{S}} f_{\underline{S}}(a_0, a_1, \dots, a_k; b_0, b_1, \dots, b_k) \pmod 3,$$

where $\underline{S} = (S_1, S_2, S_3, S_4, S_5) \in \mathbf{I}(k, \underline{l}_k)$, *and*

$$f_{\underline{S}}(a_0, a_1, \dots, a_k; b_0, b_1, \dots, b_k) = \prod_{i_1\in S_1} a_{i_1}b_{k-i_1} \prod_{i_2\in S_2} a_{i_2}(1-a_{i_2})b_{k-i_2}$$
$$\times \prod_{i_3\in S_3} a_{i_3}^2 b_{k-i_3}(1-b_{k-i_3}) \prod_{i\in S_4\cup S_5} a_i(1-a_i)b_{k-i}(b_{k-i}-1). \blacksquare$$

REMARK 4.8. (i) We can give an algorithm to determine the set $\mathbf{L}_2(t)$.

(ii) For $p=2$, we once gave a rather complicated proof for the addition formula by simplifying the well-known recursion formulas for the addition of Witt vectors (see [14]), but we did not know whether the similar thing is possible for the multiplication formula. After reading that complicated proof, Browkin found a simple but quite different proof for our addition formula in the case of $p=2$ (see [1]). The present proofs, in particular those for the results in this section, were largely inspired by the following fact in the Lucas lemma:

$$a_t = \binom{A}{p^t} \pmod p,$$

which was first pointed out in [12]. This fact was also used in [10].

QUESTION 4.9. *How to simplify the expression of* e_t *further?*

5. Transformation of coefficients. In this section, we will solve Browkin's problem. First, we define the required polynomials as follows:

$$f_t(x_0, x_1, \dots, x_{t-1}) := \sum_{\lambda=0}^{t-1}\Big\{\sum_{c=1}^{(p-1)/2} [(x_\lambda + c)^{p-1} - 1]\Big\} \prod_{\lambda<i<t} (1 - x_i^{p-1}),$$

$$g_t(y_0, y_1, \dots, y_{t-1}) := \sum_{\lambda=0}^{t-1}\Big\{\sum_{c=(p+1)/2}^{p-1} [1 - (y_\lambda - c)^{p-1}]\Big\}$$
$$\times \prod_{\lambda<i<t} \left[1 - \left(y_i - \frac{p-1}{2}\right)^{p-1}\right],$$

where we also have the convention that $\prod_{i\in\emptyset} = 1$ for the empty set $\emptyset$.

THEOREM 5.1. *Assume that $p \geq 3$ is a prime. Let*

$$A = \sum_{i=0}^{\infty} a_i p^i = \sum_{j=0}^{\infty} b_j p^j \in \mathbb{Z}_p,$$

with $a_i \in \{0, \pm 1, \pm 2, \dots, \pm(p-1)/2\}$ and $b_j \in \{0, 1, \dots, p-1\}$. Then

$$b_t = a_t + f_t(a_0, a_1, \dots, a_{t-1}) \pmod{p}, \tag{5.1}$$

$$a_t = b_t + g_t(b_0, b_1, \dots, b_{t-1}) \pmod{p}. \tag{5.2}$$

Proof. To prove (5.1), we first define an index sequence. Let $j_0 = -1$. If after $k-1$ rounds ($k \geq 1$) we have j_{k-1}, then we go on with the following two steps:

(i) Let

$$i_k = \begin{cases} \infty & \text{if } \{i : j_{k-1} < i,\ -(p-1)/2 \leq a_i \leq -1\} = \emptyset, \\ \min\{i : j_{k-1} < i, -(p-1)/2 \leq a_i \leq -1\} & \text{otherwise.} \end{cases}$$

If $i_k = \infty$, then the index sequence is completed; otherwise, go on with the next step:

(ii) Let

$$j_k = \begin{cases} \infty & \text{if } \{i : i_k < i,\ 1 \leq a_i \leq (p-1)/2\} = \emptyset, \\ \min\{i : i_k < i,\ 1 \leq a_i \leq (p-1)/2\} & \text{otherwise.} \end{cases}$$

If $j_k = \infty$, the index sequence is completed; otherwise, go on with the $(k+1)$th round.

For $k \geq 1$ we define

$$b'_i = a_i, \qquad j_{k-1} < i < i_k, \quad \text{and} \quad b'_{i_k} = p + a_{i_k}, \tag{5.3}$$

$$b'_i = a_i - 1 + p, \quad i_k < i < j_k, \qquad \text{and} \quad b'_{j_k} = a_{j_k} - 1. \tag{5.4}$$

It is easy to check that $0 \leq b'_t < p$ for any t.

We will denote

$$I_k = \sum_{j_{k-1} < i \leq i_k} a_i p^i, \qquad J_k = \sum_{i_k < i \leq j_k} a_i p^i, \qquad \forall k \geq 1.$$

When $i_k = \infty$, from (5.3) we have

$$I_k = \sum_{j_{k-1} < i \leq i_k = \infty} a_i p^i = \sum_{j_{k-1} < i < i_k = \infty} a_i p^i = \sum_{j_{k-1} < i} b'_i p^i. \tag{5.5}$$

When $i_k < \infty$, from (5.3) we have

$$\begin{aligned} I_k = \sum_{j_{k-1} < i \leq i_k} a_i p^i &= \sum_{j_{k-1} < i < i_k} b'_i p^i + b'_{i_k} p^{i_k} - p^{1+i_k} \\ &= \sum_{j_{k-1} < i \leq i_k} b'_i p^i - p^{1+i_k}. \end{aligned} \tag{5.6}$$

When $j_k = \infty$, from (5.4) we have

$$-p^{1+i_k} + J_k = \sum_{i_k<i}(p-1)p^i + \sum_{i_k<i\le j_k=\infty} a_ip^i = \sum_{i_k<i}(a_i+p-1)p^i = \sum_{i_k<i} b'_ip^i. \tag{5.7}$$

When $j_k < \infty$, from (5.4) we have

$$\begin{aligned}-p^{1+i_k} + J_k &= \sum_{i_k<i}(p-1)p^i + \sum_{i_k<i\le j_k} a_ip^i \\ &= \sum_{i_k<i<j_k}(a_i+p-1)p^i + \Big[a_{j_k} + \sum_{0\le i}(p-1)p^i\Big]p^{j_k} \\ &= \sum_{i_k<i<j_k}(a_i+p-1)p^i + (a_{j_k}-1)p^{j_k} = \sum_{i_k<i\le j_k} b'_ip^i.\end{aligned} \tag{5.8}$$

When $j_k = \infty$, from (5.6) and (5.7) we have

$$I_k + J_k = \sum_{j_{k-1}<i} b'_ip^i. \tag{5.9}$$

When $j_k < \infty$, from (5.6) and (5.8) we have

$$I_k + J_k = \sum_{j_{k-1}<i\le i_k} b'_ip^i. \tag{5.10}$$

It is easy to see that

$$A = \begin{cases} I_1 + J_1 + \cdots + I_{k-1} + J_{k-1} + I_k & \text{if } i_k = \infty, \\ I_1 + J_1 + \cdots + I_k + J_k & \text{if } j_k = \infty, \\ \sum_{k\ge 1}(I_k + J_k) & \text{otherwise.} \end{cases}$$

Discussing the three cases separately, from (5.5)–(5.10) we have

$$A = \sum_{i\ge 0} b'_ip^i.$$

By the definition of the index sequence, for $k \ge 1$ we clearly have

- if $j_{k-1} < t \le i_k$, then $0 \le a_{t-1} \le (p-1)/2$, and $(a_0, a_1, \ldots, a_{t-1})$ is not of the form $(*, \ldots, *, -c, \underbrace{0, \ldots, 0}_{m})$ with $m \ge 0$ and $1 \le c \le (p-1)/2$;
- if $i_k < t \le j_k$, then $-(p-1)/2 \le a_{t-1} \le 0$, and $(a_0, a_1, \ldots, a_{t-1})$ is of the form $(*, \ldots, *, -c, \underbrace{0, \ldots, 0}_{m})$ with $m \ge 0$ and $1 \le c \le (p-1)/2$.

Hence, for $k \geq 1$ we have $i_k < t \leq j_k$ if and only if $(a_0, a_1, \ldots, a_{t-1})$ is of the form $(*, \ldots, *, -c, \underbrace{0, \ldots, 0}_{m})$ with $m \geq 0$ and $1 \leq c \leq (p-1)/2$. Note that modulo p we have

$$f_t(a_0, a_1, \ldots, a_{t-1}) \\ = \begin{cases} -1 & \text{if } (a_0, a_1, \ldots, a_{t-1}) = (*, \ldots, *, -c, 0, \ldots, 0),\ 1 \leq c \leq (p-1)/2, \\ 0 & \text{otherwise.} \end{cases}$$

So

$$a_t + f_t(a_0, a_1, \ldots, a_{t-1}) = \begin{cases} a_t \pmod p & \text{if } j_{k-1} < t \leq i_k,\ k \geq 1, \\ a_t - 1 \pmod p & \text{if } i_k < t \leq j_k,\ k \geq 1. \end{cases}$$

Therefore, from (5.3) and (5.4), we have

$$a_t + f_t(a_0, a_1, \ldots, a_{t-1}) = b'_t \pmod p. \tag{5.11}$$

By the uniqueness, we have $b_i = b'_i$ for any i, so (5.1) follows from (5.11).

In a similar way, we can prove (5.2). Similarly, we first define an index sequence. Let $j_0 = -1$ for the initial value. If after k rounds ($k \geq 1$) we have j_{k-1}, then we go on with the following two steps:

(i) Let

$$i_k = \begin{cases} \infty & \text{if } \{i : j_{k-1} < i, (p-1)/2 \leq b_i \leq p-1\} = \emptyset, \\ \min\{i : j_{k-1} < i,\ (p-1)/2 \leq b_i \leq p-1\} & \text{otherwise.} \end{cases}$$

If $i_k = \infty$, then the index sequence is completed; otherwise, go on with the next step:

(ii) Let

$$j_k = \begin{cases} \infty & \text{if } \{i : i_k < i, 0 \leq b_i < (p-1)/2\} = \emptyset, \\ \min\{i : i_k < i,\ 0 \leq b_i < (p-1)/2\} & \text{otherwise.} \end{cases}$$

If $j_k = \infty$, the index sequence is completed; otherwise, go on with the $k+1$ round.

For $k \geq 1$ we define

$$a'_i = b_i, \quad j_{k-1} < i < i_k, \quad \text{and} \quad a'_{i_k} = b_{i_k} - p, \tag{5.12}$$

$$a'_i = b_i + 1 - p, \quad i_k < i < j_k, \quad \text{and} \quad a'_{j_k} = b_{j_k} + 1. \tag{5.13}$$

It is easy to check that $-(p-1)/2 \leq a'_t \leq (p-1)/2$ for any t.

For $k \geq 1$, let

$$I_k = \sum_{j_{k-1} < i \leq i_k} b_i p^i, \qquad J_k = \sum_{i_k < i \leq j_k} b_i p^i.$$

When $i_k = \infty$, from (5.12) we have

$$I_k = \sum_{j_{k-1} < i \leq i_k = \infty} b_i p^i = \sum_{j_{k-1} < i} a'_i p^i. \tag{5.14}$$

When $i_k < \infty$, from (5.12) we have

$$I_k = \sum_{j_{k-1}<i\le i_k} b_i p^i = \sum_{j_{k-1}<i<i_k} b_i p^i + b_{i_k} p^{i_k} = \sum_{j_{k-1}<i\le i_k} b_i p^i + p^{1+i_k}. \tag{5.15}$$

When $j_k = \infty$, from (5.13) we have

$$p^{1+i_k} + J_k = -\sum_{i_k<i}(p-1)p^i + \sum_{i_k<i\le j_k=\infty} b_i p^i = \sum_{i_k<i} a'_i p^i. \tag{5.16}$$

When $j_k < \infty$, from (5.13) we have

$$\begin{aligned} p^{1+i_k} + J_k &= -\sum_{i_k<i}(p-1)p^i + \sum_{i_k<i\le j_k} b_i p^i \\ &= \sum_{i_k<i<j_k}(b_i - p + 1)p^i + (b_{j_k}+1)p^{j_k} - p^{1+j_k} - \sum_{j_k<i}(p-1)p^i \\ &= \sum_{i_k<i\le j_k} a'_i p^i. \end{aligned} \tag{5.17}$$

Then, similarly from (5.14)–(5.17), we have

$$A = \sum_{i\ge 0} a'_i p^i.$$

By the definition of the index sequence, for $k \ge 1$ we have:

- if $j_{k-1} < t \le i_k$, then $0 \le b_{t-1} \le (p-1)/2$, and $(b_0, b_1, \dots, b_{t-1})$ is not of the form $(*, \dots, *, c, \underbrace{(p-1)/2, \dots, (p-1)/2}_{m})$ with $m \ge 0$ and $(p-1)/2 < c < p$;
- if $i_k < t \le j_k$, then $(p-1)/2 \le b_{t-1} < p$, and $(b_0, b_1, \dots, b_{t-1})$ is of the form $(*, \dots, *, c, \underbrace{(p-1)/2, \dots, (p-1)/2}_{m})$ with $m \ge 0$ and $(p-1)/2 < c < p$.

Therefore, for $k \ge 1$ we have $i_k < t \le j_k$ if and only if $(b_0, b_1, \dots, b_{t-1})$ is of the form $(*, \dots, *, c, \underbrace{(p-1)/2, \dots, (p-1)/2}_{m})$ with $m \ge 0$ and $(p-1)/2 < c < p$. Note that modulo p we have

$$\begin{aligned} &g_t(b_0, b_1, \dots, b_{t-1}) \\ &= \begin{cases} 1 & \text{if } (b_0, b_1, \dots, b_{t-1}) \\ & \qquad = (*, \dots, *, c, (p-1)/2, \dots, (p-1)/2), (p-1)/2 < c < p, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

So

$$b_t + g_t(b_0, b_1, \dots, b_{t-1}) = \begin{cases} b_t + 1 \pmod p & \text{if } j_{k-1} < t \le i_k,\ k \ge 1, \\ b_t \pmod p & \text{if } i_k < t \le j_k,\ k \ge 1. \end{cases}$$

Hence

$$b_t + g_t(b_0, b_1, \ldots, b_{t-1}) = a'_t \pmod{p}. \tag{5.18}$$

As above, by uniqueness we know that (5.2) follows from (5.18). ∎

An alternative proof. After reading the previous version of this paper, Browkin gave an alternative proof for Theorem 5.1. Now, we only give a sketch of his proof of the equality (5.1).

Let $\sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} b_i p^i$, where $a_i \in \{0, \pm 1, \pm 2, \ldots, \pm(p-1)/2\}$, $b_i \in \{0, 1, \ldots, p-1\}$. For $k \geq 0$ denote

$$A_k := \sum_{i=0}^{k} a_i p^i, \qquad B_k := \sum_{i=0}^{k} b_i p^i.$$

Clearly, for any $k \geq 0$, A_k and B_k satisfy $A_k \equiv B_k \pmod{p^{k+1}}$. We have

$$|A_k| < p^{k+1} \quad \text{and} \quad 0 \leq B_k < p^{k+1}. \tag{$*$}$$

In fact,

$$|A_k| \leq \sum_{i=0}^{k} |a_i| p^i \leq \frac{p-1}{2} \sum_{i=0}^{k} p^i = \frac{1}{2}(p^{k+1} - 1) < p^{k+1}$$

and

$$0 \leq B_k = \sum_{i=0}^{k} b_i p^i \leq (p-1) \sum_{i=0}^{k} p^i = p^{k+1} - 1 < p^{k+1}.$$

From $(*)$, it follows that

$$-p^{k+1} < -A_k \leq B_k - A_k \leq B_k + |A_k| < p^{k+1},$$

so $B_k - A_k = 0$ or p^{k+1}. More precisely

$$B_k = \begin{cases} A_k & \text{if } A_k \geq 0, \\ A_k + p^{k+1} & \text{if } A_k < 0. \end{cases} \tag{$**$}$$

From this, we know that $b_0 \equiv a_0 \pmod{p}$. Now, we determine $b_k \pmod{p}$ for $k \geq 1$.

(i) Assume that $A_{k-1} \geq 0$. Then from $(*)$ we have $A_{k-1} = B_{k-1}$. If $A_k \geq 0$, then $A_k = B_k$ similarly, so

$$A_{k-1} + a_k p^k = A_k = B_k = B_{k-1} + b_k p^k,$$

therefore $b_k = a_k$; if $A_k < 0$, then by $(**)$ we have $B_k = A_k + p^{k+1}$, and so

$$B_{k-1} + b_k p^k = B_k = A_k + p^{k+1} = A_{k-1} + a_k p^k + p^{k+1},$$

which implies $b_k = a_k + p$.

(ii) Assume that $A_{k-1} < 0$. If $A_k \geq 0$, then from $(**)$ we get

$$A_{k-1} + p^k + b_k p^k = B_{k-1} + b_k p^k = B_k = A_k = A_{k-1} + a_k p^k,$$

therefore $b_k = a_k - 1$; if $A_k < 0$, then from $(**)$ we get

$$A_{k-1} + p^k + b_k p^k = B_{k-1} + b_k p^k = B_k = A_k + p^{k+1} = A_{k-1} + a_k p^k + p^{k+1},$$

therefore $b_k = a_k + p - 1 \equiv a_k - 1 \pmod p$.

Thus we have proved

$$b_k - a_k \equiv \begin{cases} -1 \pmod p & \text{if } A_{k-1} < 0, \\ 0 \pmod p & \text{otherwise.} \end{cases}$$

Now we express these conditions by means of polynomials.

Let

$$A_{k-1} = \sum_{i=0}^{k-1} a_i p^i, \quad \text{where} \quad a_k = a_{k-1} = \cdots = a_{m+1} = 0,\ a_m \neq 0,$$

for some m, $0 \leq m \leq k$. From $A_{k-1} = A_m = A_{m-1} + a_m p^m$ and $|A_{m-1}| < p^m$ we conclude that $A_{k-1} < 0$ if and only if $a_m < 0$, which is equivalent to $a_m \in \{-1, -2, \ldots, -(p-1)/2\}$. So we get

$$b_k - a_k \equiv \begin{cases} -1 \pmod p & \text{if } (a_0, a_1, \ldots, a_{k-1}) = (*, \ldots, *, -c, 0, \ldots, 0), \\ 0 \pmod p & \text{otherwise,} \end{cases}$$

where $1 \leq c \leq (p-1)/2$. From the proof of Theorem 5.1, we know that $f_k(a_0, a_1, \ldots, a_{k-1})$ has the same property as $b_k - a_k$, so we have

$$b_k = a_k + f_k(a_0, a_1, \ldots, a_{k-1}) \pmod p. \ \blacksquare$$

Corollary 5.2. *Let*

$$A = \sum_{i=0}^{\infty} a_i 3^i = \sum_{j=0}^{\infty} b_j 3^j \in \mathbb{Z}_3$$

with $a_i \in \{0, \pm 1\}$ *and* $b_j \in \{0, 1, 2\}$. *Then*

$$b_t = a_t + \sum_{0 \leq \lambda < t} a_\lambda (a_\lambda - 1) \prod_{\lambda < i < t} (1 - a_i^2) \pmod 3,$$

$$a_t = b_t + \sum_{0 \leq \lambda < t} b_\lambda (1 - b_\lambda) \prod_{\lambda < i < t} b_i (2 - b_i) \pmod 3. \ \blacksquare$$

We can also give the formulas for the sum and the product of p-adic integers with respect to the numerically least residue system $\{0, \pm 1, \pm 2, \ldots, \pm (p-1)/2\}$. Define

$$a_t^{\vee} := a_t + \sum_{\lambda=0}^{t-1} \Big\{ \sum_{c=1}^{(p-1)/2} [(a_\lambda + c)^{p-1} - 1] \Big\} \prod_{\lambda < i < t} (1 - a_i^{p-1}),$$

$$b_t^{\wedge} := b_t + \sum_{\lambda=0}^{t-1} \Big\{ \sum_{c=(p+1)/2}^{p-1} [1 - (b_\lambda - c)^{p-1}] \Big\} \prod_{\lambda < i < t} [1 - (b_i - (p-1)/2)^{p-1}],$$

where $a_i \in \{0, \pm 1, \pm 2, \ldots, \pm (p-1)/2\}$ and $b_j \in \{0, 1, \ldots, p-1\}$.

THEOREM 5.3. *Let p be an odd prime. Assume that*

$$a=\sum_{i=0}^{\infty} a_i p^i, \quad b=\sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p, \quad -a=\sum_{i=0}^{\infty} d_i p^i,$$

$$a+b=\sum_{i=0}^{\infty} c_i p^i, \qquad ab=\sum_{i=0}^{\infty} e_i p^i,$$

with $a_i, b_i, c_i, d_i \in \{0, \pm 1, \pm 2, \dots, \pm(p-1)/2\}$. Then

(i) $c_0 = a_0 + b_0 \pmod p$ *and for $t \geq 1$,*

$$c_t = a_t + b_t^{\vee} + \sum_{i=0}^{t-1}\Bigg(\sum_{j=1}^{p-1}\binom{(p-1)/2+a_i}{j}\binom{b_i^{\vee}}{p-j}\Bigg) \times \prod_{j=i+1}^{t-1}\binom{(p-1)/2+a_j+b_j^{\vee}}{p-1} \pmod p.$$

In particular, if $p=3$, then $c_0 = a_0 + b_0^{\vee} \pmod 3$ and for $t \geq 1$,

$$c_t = a_t + b_t^{\vee} - \sum_{i=0}^{t-1}[(a_i+1)(a_i+b_i^{\vee}-1)b_i^{\vee}] \prod_{j=i+1}^{t-1}\binom{a_j+b_j^{\vee}+1}{2} \pmod 3.$$

(ii) $d_0 = -a_0^{\vee} \pmod p$ *and for $t \geq 1$,*

$$d_t = -a_t^{\vee} - 1 + \prod_{i=0}^{t-1}(1-a_i^{\vee p-1}) \pmod p.$$

In particular, if $p=3$, then $d_0 = -a_0^{\vee} \pmod 3$ and for $t \geq 1$,

$$d_t = -a_t^{\vee} - 1 + \prod_{i=0}^{t-1}(1-a_i^{\vee 2}) \pmod 3.$$

(iii) $e_0 = (a_0^{\vee} b_0^{\vee})^{\wedge} \pmod p$ *and for $t \geq 1$,*

$$e_t = \Bigg(\sum_{\underline{l}=(\underline{l}_0,\dots,\underline{l}_p)\in \mathbf{L}_p(t)} \prod_{k=0}^{t} \tau_{\underline{l}_k}(a_0^{\vee},\dots,a_k^{\vee}; b_0^{\vee},\dots,b_k^{\vee})\Bigg)^{\wedge} \pmod p.$$

Proof. (i) From Theorem 5.1, we have

$$a+b=\sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i^{\vee} p^i = \sum_{i=0}^{\infty}\Big(\frac{p-1}{2}+a_{t-1}\Big)p^i + \sum_{i=0}^{\infty} b_i^{\vee} p^i - \sum_{i=0}^{\infty}\Big(\frac{p-1}{2}\Big)p^i.$$

Note that $(p-1)/2 + a_{t-1}$, $b_i^{\vee} \in \{0, 1, \dots, p-1\}$. Let

$$\sum_{i=0}^{\infty}\Big(\frac{p-1}{2}+a_{t-1}\Big)p^i + \sum_{i=0}^{\infty} b_i^{\vee} p^i = \sum_{i=0}^{\infty} c_i' p^i, \qquad c_i' \in \{0, 1, \dots, p-1\}.$$

Then by Theorem 5.1 we have

$$c'_t = (p-1)/2 + a_t + b_t^{\vee} + \sum_{i=1}^{p-1} \binom{(p-1)/2 + a_{t-1}}{i} \binom{b_{t-1}^{\vee}}{p-i}$$
$$+ \sum_{i=0}^{t-2} \left(\sum_{j=1}^{p-1} \binom{(p-1)/2 + a_i}{j} \binom{b_i^{\vee}}{p-j} \right) \prod_{j=i+1}^{t-1} \binom{(p-1)/2 + a_j + b_j^{\vee}}{p-1} \pmod{p}.$$

Clearly $c_t = c'_t - (p-1)/2$.

(ii) This follows from Theorems 5.1 and 3.1.

(iii) This follows from Theorem 5.1, Corollary 2.4 and Corollary 4.7. ∎

6. Applications to Witt vectors. Now, we apply the above results to $(\mathbf{W}(\mathbb{F}_p), \dot{+}, \dot{\times})$, the ring of Witt vectors with coefficients in $\mathbb{F}_p$. Let $\dot{-}$ denote the additive inverse of Witt vectors.

THEOREM 6.1. *Let $a = (a_0, a_1, \ldots)$, $b = (b_0, b_1, \ldots) \in \mathbf{W}(\mathbb{F}_2)$. If in $\mathbf{W}(\mathbb{F}_2)$,*

$$a \dot{+} b = (c_0, c_1, \ldots),$$
$$\dot{-} a = (d_0, d_1, \ldots),$$
$$a \dot{\times} b = (e_0, e_1, \ldots),$$

then in $\mathbb{F}_2$ we have

(i) $c_0 = a_0 + b_0$ *and for* $t \geq 1$,

$$c_t = a_t + b_t + \sum_{i=0}^{t-1} a_i b_i \prod_{j=i+1}^{t-1} (a_j + b_j).$$

(ii) $d_0 = a_0$ *and for* $t \geq 1$,

$$d_t = a_t + 1 + \prod_{i=0}^{t-1} (1 + a_i).$$

(iii) $e_0 = a_0 b_0$ *and for* $t \geq 1$,

$$e_t = \sum_{(l_1, \ldots, l_t) \in \mathbf{L}_2(t)} \prod_{1 \leq k \leq t} \tau_{l_k}(a_0 b_k, a_1 b_{k-1}, \ldots, a_k b_0).$$

Proof. This follows from Corollaries 2.4 and 4.7. ∎

When $p = 3$, $a_t^{\vee}$ and $b_t^{\wedge}$ become

$$a_t^{\vee} = a_t + \sum_{0 \leq \lambda < t} a_\lambda (a_\lambda - 1) \prod_{\lambda < i < t} (1 - a_i^2),$$

$$b_t^{\wedge} = b_t + \sum_{0 \leq \lambda < t} b_\lambda (1 - b_\lambda) \prod_{\lambda < i < t} b_i (2 - b_i)$$

with $a_i \in \{0, \pm 1\}$ and $b_j \in \{0, 1, 2\}$, and then we have:

THEOREM 6.2. *Let* $a = (a_0, a_1, \ldots)$, $b = (b_0, b_1, \ldots) \in \mathbf{W}(\mathbb{F}_3)$. *If in* $\mathbf{W}(\mathbb{F}_3)$

$$\begin{aligned} a \dot{+} b &= (c_0, c_1, \ldots), \\ \dot{-}\, a &= (d_0, d_1, \ldots), \\ a \dot{\times} b &= (e_0, e_1, \ldots), \end{aligned}$$

then in $\mathbb{F}_3$ *we have*

(i) $c_0 = a_0 + b_0^{\vee}$ *and for* $t \geq 1$,

$$c_t = a_t + b_t^{\vee} - \sum_{i=0}^{t-1} [(a_i + 1)(a_i + b_i^{\vee} - 1) b_i^{\vee}] \prod_{j=i+1}^{t-1} \binom{a_j + b_j^{\vee} + 1}{2}.$$

(ii) $d_0 = -a_0^{\vee}$ *and for* $t \geq 1$,

$$d_t = -a_t^{\vee} - 1 + \prod_{i=0}^{t-1} (1 - a_i^{\vee 2}).$$

(iii) $e_0 = (a_0^{\vee} b_0^{\vee})^{\wedge}$ *and for* $t \geq 1$,

$$e_t = \Big(\sum_{(\underline{l}_0, \ldots, \underline{l}_t) \in \mathbf{L}_3(t)} \prod_{k=0}^{t} \sum_{\underline{S}} f_{\underline{S}}^{\vee}(a_0, a_1, \ldots, a_k; b_0, b_1, \ldots, b_k) \Big)^{\wedge},$$

where $\underline{S} = (S_1, S_2, S_3, S_4, S_5) \in \mathbf{I}(k, \underline{l}_k)$ *and*

$$\begin{aligned} f_{\underline{S}}^{\vee}(a_0, a_1, \ldots, a_k; b_0, b_1, \ldots, b_k) &= \prod_{i_1 \in S_1} a_{i_1}^{\vee} b_{k-i_1}^{\vee} \prod_{i_2 \in S_2} a_{i_2}^{\vee} (1 - a_{i_2}^{\vee}) b_{k-i_2}^{\vee} \\ &\times \prod_{i_3 \in S_3} a_{i_3}^{\vee 2} b_{k-i_3}^{\vee} (1 - b_{k-i_3}^{\vee}) \prod_{i \in S_4 \cup S_5} a_i^{\vee 2} (1 - a_i^{\vee}) b_{k-i}^{\vee} (b_{k-i}^{\vee} - 1). \end{aligned}$$

Proof. This follows from Corollaries 2.4 and 4.7 and Theorem 5.3 (see [14]). ∎

REMARK 6.3. (i) We can also write out for Witt vectors the results corresponding to Corollaries 2.5 and 2.6.

(ii) The formulas given in Theorem 6.2, in particular for e_t, are indeed complicated, but explicit.

QUESTION 6.4. *Can one give similar formulas for* $\mathbf{W}(\mathbb{F}_p)$ *for a prime* $p > 3$?

Acknowledgments. We are grateful to J. Browkin for many helpful suggestions, in particular, for suggesting the problems.

This research is supported by National Natural Science Foundation of China (10871106, 90604011, 60473025).

References

[1] J. Browkin, *The sum of dyadic numbers*, preprint.

[2] Z. P. Dai and Z. J. Liu, *The single cycle T-functions*, in preparation.

[3] J. Hong, D. Lee, Y. Yeom and D. Han, *A new class of single cycle T-functions*, in: Fast Software Encryption 2005, Lecture Notes in Comput. Sci. 3557, Springer, 2005, 68–82.

[4] J. Hong et al., *T-function based stream cipher TSC-3*, http://www.ecrypt.eu.org/stream/tsc3.html.

[5] A. Klimov, *Applications of T-functions in cryptography*, Ph.D. Thesis, Weizmann Institute of Science, 2005.

[6] A. Klimov and A. Shamir, *A new class of invertible mappings*, in: Workshop on Cryptographic Hardware and Embedded Systems 2002, Lecture Notes in Comput. Sci. 2523, Springer, 2003, 470–483.

[7] —, —, *Cryptographic applications of T-functions*, in: Selected Areas in Cryptography (SAC) 2003, Lecture Notes in Comput. Sci. 3006, Springer, 2004, 248–261.

[8] —, —, *New cryptographic primitives based on multiword T-functions*, in: Fast Software Encryption 2004, Lecture Notes in Comput. Sci. 3017, Springer, 2004, 1–15.

[9] —, —, *New applications of T-functions in block ciphers and hash functions*, in: Fast Software Encryption 2005, Lecture Notes in Comput. Sci. 3557, Springer, 2005, 18–31.

[10] B. Li and Z. D. Dai, *A general result and a new lower bound of linear complexity for binary sequences derived from sequences over* $\mathbb{Z}_{2^e}$, preprint.

[11] Z. J. Liu, Z. P. Dai and B. F. Wu, *Determination of one kind of single cycle T-function*, J. Systems Sci. Math. Sci. 30 (2010), no. 11, 1–8 (in Chinese).

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[13] D. Moon et al., *T-function based stream cipher TSC-4*, http://www.ecrypt.eu.org/stream/tsc3p2.html.

[14] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

Kejian Xu
College of Mathematics
Jilin Normal University
Siping 136000, China
and
College of Mathematics
Qingdao University
Qingdao 266071, China
E-mail: kejianxu@amss.ac.cn

Zhaopeng Dai
Institute of System Science
Academy of Mathematics and System Science
Chinese Academy of Sciences
Beijing 100080, China
E-mail: dzpeng@amss.ac.cn

Zongduo Dai
State Key Laboratory of Information Security
Graduate School of Chinese Academy of Sciences
Beijing 100049, China
E-mail: zongduodai@is.ac.cn

Received on 11.1.2010
and in revised form on 20.3.2011 (6257)