Honam Mathematical J. **33** (2011), No. 2, pp. 153–161

A REMARK OF $P_{i,k}$ ON ELLIPTIC CURVES AND APPLICATION FOR MANCHESTER CODING

Daeyeoul Kim and Min-Soo Kim

Abstract. Greg([Greg]) considered that

$$N_k = \sum_{i=1}^{k} (-1)^{i+1} P_{i,k}(p) N_1^i,$$

where the $P_{i,k}$'s were polynomials with positive integer coefficients. In this paper, we will give the equations for $\sum P_{i,k}$ modulo 3. Using this, if we send a information for elliptic curve to sender, we can make a new checksum method for Manchester coding in IEEE 802.3 or IEEE 802.4.

1. Introduction

The zeta function of a curve C is defined to be the exponential generating function

$$Z(C,T) = \exp\left(\sum_{k\geq 1} N_k \frac{T^k}{k}\right),$$

where N_k equals the number of points on C over F_{p^k}. A result due to Weil [W] is that the zeta function of an elliptic curve, in fact any curve, $Z(C,T)$ is rational, and moreover can be expressed as

$$Z(C,T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1-(\alpha+\beta)T+\alpha\beta T^2}{(1-T)(1-qT)}.$$

The inverse roots α and β satisfy a functional equation which reduces to $\alpha\beta = p$ in the elliptic curve case. The value $v = \alpha + \beta$ is related to $N_1 = p+1-v$. In addition, the discriminant of the quadratic polynomial

Received March 2, 2011. Accepted April 5, 2011.
2000 Mathematics Subject Classification. 11A07.
Key words and phrases. Congruences, Elliptic curve.
This work was supported by NAP of Korea Research Council of Foundamental Science & Technology.

in the numerator is negative, and so the quadratic has two conjugate roots $\frac{1}{\alpha}$ and $\frac{1}{\beta}$ with absolute value $\frac{1}{\sqrt{p}}$. Writing the numerator in the form $1 - vT + pT^2 = (1 - \alpha T)(1 - \beta T)$ and taking the derivatives of logarithms of both sides, one can obtain the number of F_{p^k}-points on E, denoted by N_k, as follows:

$$N_k = p^k + 1 - \alpha^k - \beta^k, \quad k = 1, 2, \ldots. \tag{1.1}$$

Proposition 1.1 ([Greg], Theorem 2.1)**.**

$$N_k = \sum_{i=1}^{k} (-1)^{i+1} P_{i,k}(p) N_1^i,$$

where the $P_{i,k}$'s are polynomials with positive integer coefficients.

Let $p > 3$ be a prime, and let $\mathbb{F}_p$ be the finite field of p elements. From now on we let E_A^B denote the elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$ where $A, B \in \mathbb{F}_p$. The set of points $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ together with a point O at infinity is called the set of points of E_A^B in $\mathbb{F}_p$ and is denoted by $E_A^B(\mathbb{F}_p)$. And let $\#E_A^B(\mathbb{F}_p)$ be the cardinality of the set $E_A^B(\mathbb{F}_p)$. For a more detailed information about elliptic curves in general, see [Si].

In 2003(2009), we calculated the number of points on elliptic curves $E_A^0 : y^2 = x^3 + Ax$ over $\mathbb{F}_p$ mod 8 (or 24) ([PDE], [ISDBC], [DHS]). Recently, we deduced following.

Proposition 1.2 ([DJ])**.** *Let $E_A^0 : y^2 = x^3 + Ax$ be an elliptic curve modulo p with $p > 3$, and let $3t^2 \equiv 1 \pmod{p}$ and let q_1' be a quadratic non-residue modulo p with $q_1' q_1 = q_4$.*

1. *Let $p = a^2 + b^2 \equiv 1 \pmod{24}$ be a prime with $6|b$. If $-1 + 2t = q_4$, then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 0 \pmod{24} & \text{if } A = q_4 \\ 4 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1 \pmod{2} \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod{2} \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1 \pmod{2} \\ 4 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2 \pmod{4} \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod{4} \end{cases}$$

and if $-1+2t=q_2$, *then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 16 \pmod{24} & \text{if } A=q_4 \text{ and } r\equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } A=q_4 \text{ and } r\equiv 0 \pmod 2 \\ 12 \pmod{24} & \text{if } A=q_2 \text{ and } r\equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } A=q_2 \text{ and } r\equiv 0 \pmod 2 \\ 2 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 1 \pmod 2 \\ 4 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 0 \pmod 4. \end{cases}$$

2. *If* $p=a^2+b^2\equiv 1 \pmod{24}$ *is a prime with* $2|b$ *and* $3 \not| b$, *then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 8 \pmod{24} & \text{if } A=q_4 \text{ and } r\equiv 1 \pmod 2 \\ 16 \pmod{24} & \text{if } A=q_4 \text{ and } r\equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A=q_4 \text{ and } r\equiv 0 \pmod 4 \\ 20 \pmod{24} & \text{if } A=q_2 \text{ and } r\equiv 1 \pmod 2 \\ 16 \pmod{24} & \text{if } A=q_2 \text{ and } r\equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A=q_2 \text{ and } r\equiv 0 \pmod 4 \\ 18 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 1 \pmod 2 \\ 12 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 0 \pmod 4 \\ 10 \pmod{24} & \text{if } A=q_1' \text{ and } r\equiv 1 \pmod 2 \\ 12 \pmod{24} & \text{if } A=q_1' \text{ and } r\equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A=q_1' \text{ and } r\equiv 0 \pmod 4. \end{cases}$$

3. *Let* $p=a^2+b^2\equiv 13 \pmod{24}$ *be a prime with* $6|b$. *If* $-1+2t=q_4$, *then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 12 \pmod{24} & \text{if } A=q_4 \text{ and } r\equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } A=q_4 \text{ and } r\equiv 0 \pmod 2 \\ 16 \pmod{24} & \text{if } A=q_2 \text{ and } r\equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } A=q_2 \text{ and } r\equiv 0 \pmod 2 \\ 2 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 1 \pmod 2 \\ 4 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 0 \pmod 4 \end{cases}$$

and if $-1+2t=q_2$, *then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 4 \pmod{24} & \text{if } A=q_4 \text{ and } r\equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } A=q_4 \text{ and } r\equiv 0 \pmod 2 \\ 0 \pmod{24} & \text{if } A=q_2 \\ 2 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 1 \pmod 2 \\ 4 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A=q_1 \text{ and } r\equiv 0 \pmod 4. \end{cases}$$

4. *If* $p = a^2 + b^2 \equiv 13 \pmod{24}$ *is a prime with* $2|b$ *and* $3 \not| b$, *then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 20 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1 \pmod 2 \\ 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 4 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1 \pmod 2 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 4 \\ 10 \pmod{24} & \text{if } A(-1+2t) = q_2 \text{ and } r \equiv 1 \pmod 2 \\ 12 \pmod{24} & \text{if } A(-1+2t) = q_2 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A(-1+2t) = q_2 \text{ and } r \equiv 0 \pmod 4 \\ 18 \pmod{24} & \text{if } A(-1+2t) = q_4 \text{ and } r \equiv 1 \pmod 2 \\ 12 \pmod{24} & \text{if } A(-1+2t) = q_4 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A(-1+2t) = q_4 \text{ and } r \equiv 0 \pmod 4. \end{cases}$$

5. *If* $p \equiv 5 \pmod{24}$ *is a prime, then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 4 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1,3 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 4 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1,2,3,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 4,5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 4 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 4 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 0 \pmod 8 \end{cases}$$

or

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 20 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1,3 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 4 \pmod 8 \\ 4 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1,3,4 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 2,5,6,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 4 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 4 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 0 \pmod 8. \end{cases}$$

6. *If* $p \equiv 17 \pmod{24}$ *is a prime, then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 8 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1,2,3,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 4,5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 8 \\ 4 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1,3 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 4 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 4 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 4 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 0 \pmod 8 \end{cases}$$

or

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1,3,4 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 2,5,6,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1,3 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 4 \pmod 8 \\ 4 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 4 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 4 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 0 \pmod 8. \end{cases}$$

Using these propositions, we shall make new relations for $P_{i,k}$ mod 3. Furthermore, if we send a information for elliptic curve to sender, we can make a new checksum method for Manchester coding in IEEE 802.3 or IEEE 802.4.

2. $P_{i,k}$ derived from (q,t)-Wheel Numbers modulo 24

Let $\sum_{j=a}^{b} f(j) := f(a) + f(a+1) + f(a+2) + \cdots + f(b-1) + f(b)$, for example, $\sum_{j=\frac{1}{2}}^{\frac{5}{2}} f(j) = f(\frac{1}{2}) + f(\frac{3}{2}) + f(\frac{5}{2})$, and let $[k]_p := \frac{1-p^k}{1-p}$ and $(a;j)_n := (a)(a+j)(a+2j)\cdots(a+(n-1)j)$.

Theorem 2.1. *Let $k \geq 2$ be a integer. Then we get the following:*

1. $P_{1,k}(p) = (k)_1[k]_p = k\sum_{i=0}^{k} p^i$.
2. $P_{2,k}(p) = \sum_{j=-(\frac{k}{2}-1)}^{\frac{k}{2}-1} \left(\frac{k}{2} - j; j\right)_3 p^{\frac{k}{2}+j-1}$.

Proof. (1) Let $\#E(F_{p^k}) := N_k := p^k + 1 - \alpha^k - \beta^k$. The proof goes by induction on k. For $k = 2$ the assertion is trivial. Assume that $N_l = l[l]_p (2 \leq l \leq k-1)$. We easily check that $\alpha^k + \beta^k = 1 + p^k - N_k = 1 + p^k - \sum_{i=1}^{k}(-1)^{i+1}P_{i,k}(p)N_1^i$ and $(\alpha+\beta)(\alpha^{k-1} + \beta^{k-1}) -$

$\alpha\beta(\alpha^{k-2}+\beta^{k-2}) = (1+p-N_1)(1+p^{k-1}-\sum_{i=1}^{k-1}(-1)^{i+1}P_{i,k}(p)N_1^i)$ and $P_{1,k}(p)N_1 = (1+p)P_{1,k-1}(p)N_1 + (1+p^{k-1})N_1 - pP_{1,l-2}(p)N_1$. By induction, $P_{1,k-1}(p) = (k-1)[k-1]_p$ and $P_{1,k-2}(p) = (k-2)[k-2]_p$, we get $P_{1,k} = (k)_1[k]_p$.

(2) Similarly, putting $P_{2,k}(p) = \sum_{j=-(\frac{k}{2}-1)}^{\frac{k}{2}-1} \left(\frac{k}{2}-j;j\right)_3 p^{\frac{k}{2}+j-1}$ and using the induction, we get the result. □

By Proposition 1.1 and Proposition 1.2, we get the following identities:

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 4 \equiv 4P_{1,k}(1) + 8\sum_{i=2}^{k}(-1)^i P_{i,k}(1) \pmod{24} & \text{if } k \equiv 1 \pmod 2 \\ 0 \equiv 4P_{1,k}(1) + 8\sum_{i=2}^{k}(-1)^i P_{i,k}(1) \pmod{24} & \text{if } k \equiv 0 \pmod 2 \\ 2 \equiv 2P_{1,k}(1) - 4P_{2,k}(1) + 8\sum_{i=3}^{k} P_{i,k}(1) \pmod{24} & \text{if } k \equiv 1 \pmod 2 \\ 4 \equiv 2P_{1,k}(1) - 4P_{2,k}(1) + 8\sum_{i=3}^{k} P_{i,k}(1) \pmod{24} & \text{if } k \equiv 2 \pmod 4 \\ 0 \equiv 2P_{1,k}(1) - 4P_{2,k}(1) + 8\sum_{i=3}^{k} P_{i,k}(1) \pmod{24} & \text{if } k \equiv 0 \pmod 4, \end{cases}$$

which can be simplified as

$$1 \equiv P_{1,k}(1) + 2\sum_{i=2}^{k}(-1)^i P_{i,k}(1) \pmod 6 \text{ if } k \equiv 1 \pmod 2, \tag{2.1}$$

$$0 \equiv P_{1,k}(1) + 2\sum_{i=2}^{k}(-1)^i P_{i,k}(1) \pmod 6 \text{ if } k \equiv 0 \pmod 2, \tag{2.2}$$

$$1 \equiv P_{1,k}(1) - 2P_{2,k}(1) + 4\sum_{i=3}^{k} P_{i,k}(1) \pmod{12} \text{ if } k \equiv 1 \pmod 2, \tag{2.3}$$

$$2 \equiv P_{1,k}(1) - 2P_{2,k}(1) + 4\sum_{i=3}^{k} P_{i,k}(1) \pmod{12} \text{ if } k \equiv 2 \pmod 4, \tag{2.4}$$

$$0 \equiv P_{1,k}(1) - 2P_{2,k}(1) + 4\sum_{i=3}^{k} P_{i,k}(1) \pmod{12} \text{ if } k \equiv 0 \pmod 4. \tag{2.5}$$

From now on, we will give only simplified forms.

$$2 \equiv \sum_{i=1}^{k}(-1)^k P_{i,k}(1) \pmod 3 \text{ if } k \equiv 1 \pmod 2, \tag{2.6}$$

$$0 \equiv \sum_{i=1}^{k}(-1)^k P_{i,k}(1) \pmod 3 \text{ if } k \equiv 0 \pmod 2, \tag{2.7}$$

$$1 \equiv P_{1,k}(1) \pmod 2 \text{ if } k \equiv 1 \pmod 2, \tag{2.8}$$

$$0 \equiv P_{1,k}(1) \pmod 2 \text{ if } k \equiv 0 \pmod 2, \tag{2.9}$$

$$1 \equiv \sum_{i=1}^{k} P_{i,k}(1) \pmod 3 \text{ if } k \equiv 1 \pmod 2, \tag{2.10}$$

$$2 \equiv \sum_{i=1}^{k} P_{i,k}(1) \pmod 3 \text{ if } k \equiv 2 \pmod 4, \tag{2.11}$$

$$0 \equiv \sum_{i=1}^{k} P_{i,k}(1) \pmod 3 \text{ if } k \equiv 0 \pmod 4, \tag{2.12}$$

$$1 \equiv P_{1,k}(1) - 2\sum_{i=2}^{k} P_{i,k}(1) \pmod 6 \text{ if } k \equiv 1 \pmod 2, \tag{2.13}$$

$$2 \equiv P_{1,k}(1) - 2\sum_{i=2}^{k} P_{i,k}(1) \pmod 6 \text{ if } k \equiv 2 \pmod 4, \tag{2.14}$$

$$0 \equiv -P_{1,k}(1) + 2\sum_{i=2}^{k} P_{i,k}(1) \pmod 6 \text{ if } k \equiv 0 \pmod 4, \tag{2.15}$$

$$1 \equiv P_{1,k}(1) + 2P_{2,k}(1) \pmod 3 \text{ if } k \equiv 1 \pmod 2, \tag{2.16}$$

$$2 \equiv P_{1,k}(1) + 2P_{2,k}(1) \pmod 3 \text{ if } k \equiv 2 \pmod 4, \tag{2.17}$$

$$0 \equiv P_{1,k}(1) + 2P_{2,k}(1) \pmod 3 \text{ if } k \equiv 0 \pmod 4, \tag{2.18}$$

$$5 \equiv 5P_{1,k}(1) - 2P_{2,k}(1) + 4\sum_{i=3}^{k}(-1)^i P_{i,k}(1) \pmod{12} \text{ if } k \equiv 1 \pmod 2, \tag{2.19}$$

$$6 \equiv 5P_{1,k}(1) - 2P_{2,k}(1) + 4\sum_{i=3}^{k}(-1)^i P_{i,k}(1) \pmod{12} \text{ if } k \equiv 2 \pmod 4, \tag{2.20}$$

$$0 \equiv 5P_{1,k}(1) - 2P_{2,k}(1) + 4\sum_{i=3}^{k}(-1)^i P_{i,k}(1) \pmod{12} \text{ if } k \equiv 0 \pmod 4. \tag{2.21}$$

By (6.6), (6.7) and (6.10)-(6.12) we are led to

$$0 \equiv \sum_{i:\ \text{even}}^{k} P_{i,k}(1) \pmod 3 \text{ if } k \equiv 1 \pmod 2, \tag{2.22}$$

$$1 \equiv \sum_{i:\ \text{odd}}^{k} P_{i,k}(1) \pmod 3 \text{ if } k \equiv 1 \pmod 2, \tag{2.23}$$

$$1 \equiv \sum_{i:\ \text{even}}^{k} P_{i,k}(1) \equiv \sum_{i:\ \text{odd}}^{k} P_{i,k}(1) \pmod 3 \text{ if } k \equiv 2 \pmod 4, \tag{2.24}$$

$$0 \equiv \sum_{i:\ \text{even}}^{k} P_{i,k}(1) \equiv \sum_{i:\ \text{odd}}^{k} P_{i,k}(1) \pmod 3 \text{ if } k \equiv 0 \pmod 4. \tag{2.25}$$

We summarize (2.1) up to (2.25) as follows.

Theorem 2.2. *Let $k \geq 2$ be a integer. Then we get the following:*

1.
$$\sum_{i=1}^{k} P_{i,k}(1) \equiv \begin{cases} 1 \pmod 3 & \text{if } k \equiv 1 \pmod 2 \\ 2 \pmod 3 & \text{if } k \equiv 2 \pmod 4 \\ 0 \pmod 3 & \text{if } k \equiv 0 \pmod 4. \end{cases}$$

2.
$$\sum_{i=1}^{k} (-1)^k P_{i,k}(1) \equiv \begin{cases} 2 \pmod 3 & \text{if } k \equiv 1 \pmod 2 \\ 0 \pmod 3 & \text{if } k \equiv 0 \pmod 2. \end{cases}$$

3.
$$\sum_{i:\ even}^{k} P_{i,k}(1) \equiv \begin{cases} 0 \pmod 3 & \text{if } k \equiv 0, 1, 3 \pmod 4 \\ 1 \pmod 3 & \text{if } k \equiv 2 \pmod 4. \end{cases}$$

4.
$$\sum_{i:\ odd}^{k} P_{i,k}(1) \equiv \begin{cases} 0 \pmod 3 & \text{if } k \equiv 0 \pmod 4 \\ 1 \pmod 3 & \text{if } k \equiv 1, 2, 3 \pmod 4. \end{cases}$$

Remark 2.3. Manchester encoding([Wi]) is a special type of unipolar signaling in which the signal is changed from a high to low (0) or low to high (1) in the middle of the signal. Manchester encoding is commonly used in local area networks (ethernet, token ring). If we send a information for elliptic curves to receiver, then we can use Theorem 2.2 as a checksum. For example, we write $00, 01, 10$ with 11 wrong information for IEEE 802.3 or IEEE 802.4.

References

[ISDBC] Inam, I., Soydan, G., Demirci, M. Bizim, O., Cangul, I. N.,Corrigendum On *The Number of Points on Elliptic Curves $E : y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod 8*, Commun. Korean Math. Soc. 22 (2007), no. 2, 207–208.

[DJ] D. Kim, W. Jeon, Remarks of the number of points on elliptic curves mod 24, submitted.

[Greg] M. Gregg, *Combinatorial aspects of elliptic curves,* Sem. Lothar. Combin. 56 (2006/07), Art. B56f, 31 pp.

[PDE] H. Park, D. Kim, E. Lee *The number of points on elliptic curves* $E : y^2 = x^3 + cx$ *over* $\mathbb{F}_p$ *mod* 8, Commun. Korean Math. Soc. 18(2003), 31–37.

[DHS] S. You, H. Park and H. Kim *The number of points on elliptic curves* $E_A^0 : y^2 = x^3 + a^3$ *over* $\mathbb{F}_p$ *mod* 24, Honam Mathematical J. 31 (2009), No. 3, pp. 437–449.

[Si] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[W] A. Weil, *Sur Courbes Algébriques Variétés qui s'en Déduisent*, Hermann, Paris, 1948.

[Wi] Stalling, William, Data and Computer Communications, Printice Hall. 2004

Daeyeoul Kim
National Institute for Mathematical Sciences,
Daejeon 305-340, Korea.
E-mail: daeyeoul@nims.re.kr

Min-Soo Kim
Department of Mathematics, KAIST,
Daejeon 305-701, Korea.
E-mail: minsoo@kaist.ac.kr