NNTDM 17 (2011), 4, 1–8

Permutation polynomials and elliptic curves

Yotsanan Meemark and Attawut Wongpradit

Department of Mathematics, Faculty of Science, Chulalongkorn University
Bangkok, 10330, Thailand
e-mails: `yotsanan.m@chula.ac.th`, `zatthoth@gmail.com`

Abstract: In this work, we study the elliptic curve $E : y^2 = f(x)$, where $f(x)$ is a cubic permutation polynomial over some finite commutative ring R. In case R is the finite field $\mathbb{F}_q$, it turns out that the group of rational points on E is cyclic of order $q + 1$. This group is a product of cyclic groups if $R = \mathbb{Z}_n$, the ring of integers modulo a square-free n. In addition, we introduce a shift-invariant elliptic curve which is an elliptic curve $E : y^2 = f(x)$, where $y^2 - f(x)$ is a weak permutation polynomial. We end our paper with a necessary and sufficient condition for the existence of a shift-invariant elliptic curve over $\mathbb{F}_q$ and $\mathbb{Z}_n$.
Keywords: Elliptic curves, Permutation polynomials.
AMS Classification: 05A05, 11G20.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. An *elliptic curve* over $\mathbb{F}_q$, whose characteristic is greater than 3, is defined by an equation $E : y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$. The point (x, y) in $\mathbb{F}_q \times \mathbb{F}_q$ on the curve E is called a *rational point*. Let $E(\mathbb{F}_q)$ denote the set of all rational points together with a distinguished point at infinity, denoted ∞. There is an addition $+$, which makes $(E(\mathbb{F}_q), +)$ become an abelian group [1].

Elliptic curves over finite fields play an important role in many areas of modern cryptology. Following the work of Lenstra, Jr. [2] on integer factorizations, many researchers have used this idea to work out primality proving algorithms [3, 4]. Recent work on these topics can be found in [5]. Another application is to construct the public keys. When using elliptic curves for constructing a public key, it is sometimes necessary to find elliptic curves with a known number of points and its group structure over a given finite field. We recall the number of rational points and the group structure of $E(\mathbb{F}_q)$ in the following theorem.

Theorem 1.1. *[6] Let E be an elliptic curve over $\mathbb{F}_q$. Then:*

1. $|E(\mathbb{F}_q) - (q + 1)| < 2\sqrt{q}$, *and*

2. $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ *for some positive integers* n_1 *and* n_2*, and* n_1 *divides* $\gcd(n_2, q-1)$.

A *permutation polynomial* over $\mathbb{F}_q$ is a polynomial f whose function on $\mathbb{F}_q$ induced by f is a bijection. It is easy to see that every linear polynomial is a permutation polynomial. We observe that:

Theorem 1.2. *Let* $\mathbb{F}_q$ *be a finite field,* $a \in \mathbb{F}_q$ *and* $n \in \mathbb{N}$.

1. *If* $f(x)$ *is a permutation polynomial over* $\mathbb{F}_q$*, then* $f(x)+a$ *and* $f(x+a)$ *are also permutation polynomials.*

2. *A monomial* x^n *is a permutation polynomial over* $\mathbb{F}_q$ *if and only if* $\gcd(n, q-1) = 1$.

Proof. (1) They are just vertical and horizontal translations for a permutation $f(x)$.
(2) Clearly, $f(x) = x^n$ is an endomorphism on $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$. Recall that $\mathbb{F}_q^\times$ is cyclic, say generated by a. We have thus f is a permutation polynomial $\Leftrightarrow \langle a^n \rangle = \mathrm{im} f = \mathbb{F}_q^\times \Leftrightarrow \gcd(n, q-1) = 1$. □

Permutation polynomials over finite fields and over the ring of integers modulo n have been widely studied. There are a lot of applications in combinatorics and cryptography [7, 8] as well as many open problems. For the extensive studies, we refer the reader to Lidl and Niederreiter's book [9] Chapter 7.

In the next section, we study the group structure of elliptic curves $E : y^2 = f(x)$, where $f(x)$ is a cubic permutation polynomial. This work extends to an elliptic curve over a ring of integers modulo n in Section 3. In the final section, we define a shift-invariant elliptic curve, inspired by the property of a weak permutation polynomial, and characterize this type of elliptic curve on the finite fields as well as the ring of integers modulo n.

2 Elliptic curves with permutation polynomials over finite fields

Since $a^q = a$ for all $a \in \mathbb{F}_q$, as a function, we can work only on permutation polynomials modulo $x^q - x$, namely polynomials of degree $< q$. We record a further result on degree of permutation polynomials in:

Theorem 2.1. *[9] If* $f(x)$ *is a permutation polynomial over* $\mathbb{F}_q$*, then*

$$\deg(f(x)^t \bmod (x^q - x)) \leq q - 2$$

for all $t \leq q-2$ *and* $\gcd(t, q) = 1$.

The following result characterizes permutation polynomials over finite fields of characteristic greater than 3.

Theorem 2.2. *Let* q *be a power of prime* $p > 3$ *and* $f(x) = x^3 - ax + b$ *a cubic polynomial over* $\mathbb{F}_q$*. Then* f *is a permutation polynomial if and only if* $\gcd(3, q-1) = 1$ *and* $a = 0$.

Proof. By Theorem 1.2 (1), it suffices to consider only when $b = 0$, i.e. $f(x) = x^3 - ax$. Assume that $a \neq 0$.

Case 1. $q \equiv 1 \mod 3$. Then $q - 1 = 3n$ for some $n \in \mathbb{N}$. We have $\gcd(n, q) = 1$ and $n < q - 2$. Also, $\deg(f(x)^n) = \deg(x^3 - ax)^n = 3n = q - 1 > q - 2$.

Case 2. $q \equiv 2 \mod 3$. Then $q - 2 = 3n$ for some $n \in \mathbb{N}$, so $q + 1 = 3(n + 1)$. Thus, $\gcd(n + 1, q) = 1$ and $n + 1 < q - 2$. Observe that

$$\begin{aligned} f(x)^{n+1} &= (x^3 - ax)^{n+1} \\ &= x^{3(n+1)} - (n+1)ax^{3n+1} + \text{ lower terms} \\ &\equiv -(n+1)ax^{3n+1} + \text{ lower terms} \mod x^q - x. \end{aligned}$$

Since $x^{3(n+1)} = x^{q+1} \equiv x^2 \mod x^q - x$. From $a \neq 0$ and $\gcd(n + 1, q) = 1$, we conclude that $\deg(f(x)^{n+1} \mod x^q - x) = 3n + 1 = q - 1 > q - 2$.

Hence, both cases contradict Theorem 2.1, so $f(x) = x^3 - ax$ is not a permutation polynomial if $a \neq 0$. That is, $f(x) = x^3$ is the only permutation polynomial of this form. By Theorem 1.2, we also have $\gcd(3, q - 1) = 1$.

The converse of this theorem follows directly from Theorem 1.2 (1) and (2). This completes our proof. □

Finally, we count the number of points of $E(\mathbb{F}_q)$ for the elliptic curve $E : y^2 = f(x) = x^3 + b$, $b \in \mathbb{F}_q$, where q is odd greater than 3, and determine its group structure. Observe that for each $x \in \mathbb{F}_q$, if

$$f(x) = \begin{cases} 0, & \text{then } (x, 0) \text{ occurs in } E(\mathbb{F}_q); \\ r^2, & \text{then } (x, r) \text{ and } (x, -r) \text{ occur in } E(\mathbb{F}_q); \\ c, & \text{then there is no rational point in } E(\mathbb{F}_q), \end{cases}$$

where c is a non-square. Thus, in terms of χ, the quadratic character of $\mathbb{F}_q$, we obtain

$$|E(\mathbb{F}_q)| = 1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(f(x))) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x)).$$

Since $f(x)$ is a permutation polynomial, $\sum_{x \in \mathbb{F}_q} \chi(f(x)) = \sum_{x \in \mathbb{F}_q} \chi(x) = 0$. This implies $|E(\mathbb{F}_q)| = q + 1$.

From Theorem 1.1 (2), we know that $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ for some positive integers n_1 and n_2, and n_1 divides $\gcd(n_2, q - 1)$. Since n_1 divides $|E(\mathbb{F}_q)| = q + 1$, $n_1 = 1$ or 2. Assume that $n_1 = 2$. Then $E(\mathbb{F}_q) \cong \mathbb{Z}_2 \times \mathbb{Z}_{n_2}$ which contains 3 points of order two. Since $f(x) = x^3 + b$ has only one root in $\mathbb{F}_q$, say a, $(a, 0)$ is the unique double point in $E(\mathbb{F}_q)$. This contradiction gives $n_1 = 1$. Hence, $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_2}$. Therefore, we have shown:

Theorem 2.3. *Let $E : y^2 = x^3 + b$ be an elliptic curve with permutation polynomial over $\mathbb{F}_q$. Then $E(\mathbb{F}_q)$ is a cyclic group of order $q + 1$, i.e., $E(\mathbb{F}_q) \cong \mathbb{Z}_{q+1}$.*

3 Elliptic curves with permutation polynomials over the ring of integers modulo n

To extend the study, we consider elliptic curves with permutation polynomials over the rings of integers modulo n, where n is not prime. We start with the necessary and sufficient conditions to determine a cubic permutation polynomial over the ring $\mathbb{Z}_n$.

Theorem 3.1. *[10] For any $n = \prod_{i=1}^{k} {p_i}^{r_i}$, $f(x)$ is a permutation polynomials over the rings of integers modulo n if and only if $f(x)$ is also a permutation polynomials over the rings of integers modulo $p_i^{r_i}$ for all i.*

Therefore, it suffices to consider only a permutation polynomials over the rings $\mathbb{Z}_{p^r}$.

Theorem 3.2. *[10] If $f(x) = ax^3 - bx + c$ is a permutation polynomial over $\mathbb{Z}_{p^r}$, where $p > 3$ is a prime, then $r = 1$, $p \equiv 2 \mod 3$, $b = 0$ and $a \in \mathbb{Z}_{p^r}^{\times}$.*

Corollary 3.3. *If there is an elliptic curve with a permutation polynomial over a ring of integers modulo n, then n is an odd composite square-free integer whose prime divisor is congruent to 2 modulo 3.*

We then work only the case of an elliptic curve with permutation polynomial over a ring $\mathbb{Z}_n$. Let $n = \prod_{i=1}^{k} p_i$, where $p_i < p_{i+1}$ are odd primes which are congruent to 2 modulo 3 and let $E : y^2 = x^3 + b$ be an elliptic curve with permutation polynomial over $\mathbb{Z}_n$. To define a group operation on $E(\mathbb{Z}_n)$, we apply the projections $\pi_i : P = (x, y) \mod n \to P_{p_i} = (x, y) \mod p_i$. Using the Chinese remainder theorem, we know that $\pi = (\pi_1, \ldots, \pi_k) : E(\mathbb{Z}_n) \to E(\mathbb{Z}_{p_1}) \times \cdots \times E(\mathbb{Z}_{p_k})$ is a bijection. Thus, an addition $+$ for $E(\mathbb{Z}_n)$ can be defined by using the addition on $E(\mathbb{Z}_{p_i})$ and the map π. The following theorem interprets the group structure of $(E(\mathbb{Z}_n), +)$.

The next corollary gives the group structure of an elliptic curve with permutation polynomial over $\mathbb{Z}_n$. Its proof is evident from the above observation.

Corollary 3.4. *Let $n = \prod_{i=1}^{k} p_i$, where $p_i < p_{i+1}$ are odd primes which are congruent to 2 modulo 3 and $E : y^2 = x^3 + b$ be an elliptic curve with permutation polynomial over $\mathbb{Z}_n$. Then*

$$E(\mathbb{Z}_n) \cong \mathbb{Z}_{p_1+1} \times \cdots \times \mathbb{Z}_{p_k+1}.$$

4 Permutation polynomials in two variables and shift-invariant elliptic curves

In this section, we study permutation polynomials in two variables over a finite ring. Let $f(x, y)$ be a polynomial in two variables with coefficients in a finite ring R. We say that f is a *weak permutation polynomial* if for every r in R, the inverse image of r under f is of cardinality $|R|$. We begin with a simple form of weak permutation polynomials over a finite field.

Theorem 4.1. *Let R be a finite ring. Let $g(y)$ and $f(x)$ be polynomials in $R[x,y]$. Then a polynomial in two variables $g(y) - f(x)$ is a weak permutation polynomial if $f(x)$ or $g(y)$ is a permutation polynomial over R.*

Proof. First, notice that for any permutation polynomial $p(x)$, the map $\phi : \{(x,y) \in R \times R \mid g(y) = p(x)\} \to R$ defined by $\phi(x,y) = y$ is a bijection. This makes $|\{(x,y) \in R \times R \mid g(y) = p(x)\}| = |R|$.

Without loss of generality, suppose $f(x)$ is a permutation polynomial. To show that $g(y) - f(x)$ is weak, we determine the cardinality of $\{(x,y) \in R \times R \mid g(y) - f(x) = r\}$ for an arbitrary r in R. Since $f(x) + r$ is also a permutation polynomial, we have $|\{(x,y) \in R \times R \mid g(y) - f(x) = r\}| = |\{(x,y) \in R \times R \mid g(y) = f(x) + r\}| = |R|$, for all $r \in R$. $\square$

Corollary 4.2.
1. *If $E : y^2 = f(x)$ is an elliptic curve with permutation polynomial over $\mathbb{F}_q$, then $y^2 - f(x)$ is a weak permutation polynomial in $\mathbb{F}_q[x,y]$.*
2. *If $E : y^2 = f(x)$ is an elliptic curve with permutation polynomial over $\mathbb{Z}_n$, then $y^2 - f(x)$ is a weak permutation polynomial in $\mathbb{F}_q[x,y]$.*

For any elliptic curve $E : y^2 = f(x)$ and $\alpha \in \mathbb{F}_q$, we let E_α denote the *α-shifted elliptic curve*, $y^2 = f(x) + \alpha$. The previous corollary shows an interesting property of elliptic curves with permutation polynomials. Together with Theorem 2.3, we can see that $E(\mathbb{F}_q) \cong E_\alpha(\mathbb{F}_q)$ for every α in $\mathbb{F}_q$, this leads us to define a *shift-invariant elliptic curve* as an elliptic curve E whose numbers of its rational points do not change when it is shifted by any constant in $\mathbb{F}_q$. Also, we may define a shift-invariant elliptic curve on $\mathbb{Z}_n$ in the same way.

Theorem 4.3. *An elliptic curve E over a finite field $\mathbb{F}_q$ whose characteristic is greater than 3 is a shift-invariant elliptic curve if and only if it is an elliptic curve with permutation polynomial.*

Proof. Let $E : y^2 = f(x)$ be a shift-invariant elliptic curve. Then for any α in $\mathbb{F}_q$, the cardinality of the set of rational points of E_α must be the same constant K. For each $\gamma \in f(\mathbb{F}_q)$, the image of $\mathbb{F}_q$ under f, let $n_\gamma = |f^{-1}(\gamma)|$. Note that $\sum_{\gamma \in f(\mathbb{F}_q)} n_\gamma = |\mathbb{F}_q| = q$.

Assume that $0 \notin f(\mathbb{F}_q)$. Then for any $\gamma \in f(\mathbb{F}_q)$, $\chi(\gamma) = 1$ or -1. Thus,

$$K = \sum_{\gamma \in f(\mathbb{F}_q)} (1 + \chi(\gamma)) = 2 \sum_{\substack{\gamma \in f(\mathbb{F}_q) \\ \chi(\gamma)=1}} n_\gamma$$

must be even. In each $\alpha \in f(\mathbb{F}_q)$, $0 \in f_{-\alpha}(\mathbb{F}_q)$, the image set of $f(x) - \alpha$. We then consider rational points of $E_{-\alpha}$ to obtain

$$\begin{aligned} K = \sum_{\gamma \in f_{-\alpha}(\mathbb{F}_q)} (1 + \chi(\gamma)) &= \sum_{\substack{\gamma \in f_{-\alpha}(\mathbb{F}_q) \\ \chi(\gamma)=0}} (1 + \chi(\gamma)) + \sum_{\substack{\gamma \in f_{-\alpha}(\mathbb{F}_q) \\ \chi(\gamma)=1}} (1 + \chi(\gamma)) \\ &= n_\alpha + 2 \sum_{\substack{\gamma \in f_{-\alpha}(\mathbb{F}_q) \\ \chi(\gamma)=1}} n_\gamma \end{aligned}$$

which forces n_α be even for any arbitrary α in $f(\mathbb{F}_q)$. This is contrary to the fact that $\sum_{\gamma\in f(\mathbb{F}_q)} n_\gamma = q$ is odd. Hence, $0 \in f(\mathbb{F}_q)$.

Finally, suppose f is not onto and let $\beta \notin f(\mathbb{F}_q)$. Counting rational points of $E_{-\beta}$ gives $0 \notin f_{-\beta}(\mathbb{F}_q)$. Thus, $K = 2\sum_{\substack{\gamma\in f_{-\beta}(\mathbb{F}_q)\\ \chi(\gamma)=1}} n_\gamma$ and when we count rational points of $E_{-\alpha}$, we still get $K = n_\alpha + 2\sum_{\substack{\gamma\in f_{-\alpha}(\mathbb{F}_q)\\ \chi(\gamma)=1}} n_\gamma$ for every α in $f(\mathbb{F}_q)$. A contradiction occurs in the same way because $\sum_{\gamma\in f(\mathbb{F}_q)} n_\gamma = q$ is odd. The opposite direction is clear. $\square$

Next, we study a shift-invariant elliptic curve $E : y^2 = f(x)$ on the ring of integers modulo n. For any $r \in \mathbb{Z}_n$, the cardinality of the set of rational points of E_r must equal the same constant K. Let $N_f(r) = |f^{-1}(r)|$ and let $s(r)$ be the number of roots of the equation $y^2 = r$ in $\mathbb{Z}_n$. We have

$$K = \sum_{r\in f(\mathbb{Z}_n)} s(r)\cdot N_f(r) = \sum_{(r+a)\in f_a(\mathbb{Z}_n)} s(r+a)\cdot N_{f+a}(r+a)$$

when E is shifted by a constant $a \in \mathbb{Z}_n$. Moreover,

$$\sum_{r\in\mathbb{Z}_n} s(r) = \sum_{r\in\mathbb{Z}_n} |\{y\in\mathbb{Z}_n : y^2 = r\}| = \left|\bigcup_{r\in\mathbb{Z}_n}\{y\in\mathbb{Z}_n : y^2 = r\}\right| = |\mathbb{Z}_n| = n.$$

Note that for all $r \in \mathbb{Z}_n$, $N_{f+a}(r+a) = N_f(r)$ and $\sum_{r\in f(\mathbb{Z}_n)} N_f(r) = \left|\bigcup_{r\in\mathbb{Z}_n} f^{-1}(r)\right| = |\mathbb{Z}_n| = n$.

To answer the next question *"Is there any shift-invariant elliptic curve in the ring of integer modulo n?"*. By the Chinese remainder theorem, it suffices to work only with the case n is a prime power. The following theorem gives us the number of square roots of an element in this type of ring.

Theorem 4.4 (Guass, D.A., art.104 [11]). *Let p be an odd prime, n a positive integer, a a residue modulo p^n and $s(a)$ denote the number of square roots of a. Then one of the following statements holds:*

(i) if p does not divide a, then $s(a) = 2$,

(ii) if p divides a but p^n does not divide a, then write $a = p^k m$ where $p \nmid m$,

- *if k is odd, then $s(a) = 0$,*
- *if $k = 2u$ is even, then $s(a) = 2p^u$, or*

(iii) if p^n divides a, then $s(a) = p^{n-\lfloor\frac{n+1}{2}\rfloor}$.

The technique used in the proof Theorem 4.3 can be extended to prove the next theorem which describes a shift-invariant elliptic curve over the ring of integers modulo n.

Theorem 4.5. *Let $n = \prod_{i=1}^k p_i^{n_i}$ where $p_i > 3$ for all i. Then an elliptic curve E over a ring of integers modulo n is a shift-invariant elliptic curve if and only if it is an elliptic curve with permutation polynomial.*

Proof. In $\mathbb{Z}_{{p_i}^{n_i}}$, we know from the previous theorem that 0 is the only residue whose number of square roots is odd. Thus the equation

$$\vec{y}^2 = (y_1^2, y_2^2, \ldots, y_k^2) = (a_1, a_2, \ldots, a_k)$$

in $\prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}} \cong \mathbb{Z}_n$ has odd roots only when $a_i = 0$ for all i. Suppose on the contrary that $(0, 0, \ldots, 0) \notin f(\prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}})$. Then

$$K = \sum_{\vec{r} \in f(\prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}})} s(\vec{r}) \cdot N_f(\vec{r})$$

is even. Shifting with $-\vec{s}$ gives

$$N_f(\vec{s}) = N_{f_{-\vec{s}}}(\vec{0}) = K - \sum_{\substack{\vec{r} \in f_{-\vec{s}}(\prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}}) \\ \vec{r} \neq (0,0,\ldots,0)}} s(\vec{r}) \cdot N_{f_{-\vec{s}}}(\vec{r})$$

which turns out to be even for all $\vec{s} \in \prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}}$. On the other hand, $\sum_{\vec{s} \in f(\mathbb{Z}_{{p_i}^{n_i}})} N_f(\vec{s}) = \prod_{i=1}^{k} {p_i}^{n_i} = n$ is odd. Hence, $(0, 0, \ldots, 0)$ is in the image of f. Again, f must be onto unless $(0, 0, \ldots, 0) \notin f_{-\vec{t}}(\prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}})$ for some $\vec{t} \in \prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}}$ which leads to a contradiction in the same way. This completes the proof. $\square$

Together with Corollary 3.3, we may conclude from Theorem 4.5 that:

Corollary 4.6. *If there is a shift-invariant elliptic curve over a ring of integers modulo n, then n is an odd composite square-free integer whose prime divisor is congruent to 2 modulo 3.*

References

[1] Washington, L.C. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall, 2008.

[2] Lenstra Jr, H.W. Factoring integers with elliptic curves. *Annals of Mathematics*, vol. 126, 1987, 649–673.

[3] Diffie W., M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, Vol. 22, 1976, 644–654.

[4] Coppersmith, D., A.M. Odlzyko, and R. Schroeppel. Discrete logarithms in GF (p). *Algorithmica*, Vol. 1, 1986, 1–15.

[5] Liu, D., D. Huang, P. Luo, Y. Dai. New schemes for sharing points on an elliptic curve. *Computers & Mathematics with Applications*, Vol. 56, 2008, 1556–1561.

[6] Silverman, J.H. *The Arithmetic of Elliptic Curves*, Springer Verlag, 2009.

[7] Lidl, R. On cryptosystems based on polynomials and finite fields. *Advances in Cryptology: Proceedings of EUROCRYPT 84-A Workshop on the Theory and Application of Cryptographic Techniques*, Paris, France, April 1984, 1985, p. 10.

[8] Shankar, B.R. Combinatorial properties of permutation polynomials over some finite rings Zn. *IJSDI age*, Vol. 1, 1985, 1–6.

[9] Lidl R., H. Niederreiter. Finite fields and their applications. *Handbook of Algebra*, Vol. 1, 1996, 321–363.

[10] Chen, Y.L., J. Ryu, O.Y. Takeshita. A simple coefficient test for cubic permutation polynomials over integer rings. *Communications Letters*, IEEE, Vol. 10, 2006, 549–551.

[11] Gauss, C. F. *Disquisitiones Arithmeticae*, 1801. English translation by Arthur A. Clarke. Springer-Verlag, New York, 1986.