102. *Some Properties of Porges' Functions*

By Hiroshi IWATA

(Comm. by Kinjirô KUNUGI, M. J. A., June 10, 1969)

§ 1. **Introduction.** For fixed g and $s \in Z$,[1] let $f(n)$ be the sum of the sth powers of the digits in the scale of g of the natural number n. Porges [1], Isaacs [2], and Stewart [3] studied the properties of this function $f(n)$. The sequence $\{f^k(n)\}_{k=0}^{\infty}$, where $f^0(n)=n$, and $f^k(n)=f\{f^{k-1}(n)\}(k \in Z)$, is periodic for every $n \in Z$ (see [4]). K. Iséki [5], [6] reported all the periods for $s=3, 4, 5$, when $g=10$. Integers X and Y are said to be f-related if and only if there are non-negative integers l and m such that $f^l(X)=f^m(Y)$. Being f-related is an equivalence relation dividing Z into N disjoint sets of f-related integers (see [2]). Now let $P(g)$ be the set of all the periods of the sequences $\{f^k(n)\}_{k=0}^{\infty}(n \in Z)$ and let $M(g)$ be $\max\{\bar{A} \mid A \in P(g)\}$, where $\bar{A}$ is the number of elements of A when $s=2$. Then in the case of $s=2$, $N=N(g)$ is obviously the number of the elements of $P(g)$. In § 2 we will prove the following

Theorem 1. $\overline{\lim_{g\to\infty}} M(g)=\infty$ (1),

and

Theorem 2. $\overline{\lim_{g\to\infty}} N(g)=\infty$ (2).

When the circulation of $\{f^k(n)\}_{k=0}^{\infty}$ begins at $k=k(n)$th term, we get the sequence $\{h(n)\}_{n=1}^{\infty}$, where $h(n)=f^{k(n)}(n)$. In the case of $(g, s)=(3, 2)$, as easily proved, $H=\{h(n) \mid n \in Z\}=\{1, 2, 4, 5, 8\}$. In § 3, we will prove the following

Theorem 3. *For every pair (a, l), where $a \in H$, $l \in Z$, there exist infinitely many natural numbers k such that $h(k)=h(k+2)=\cdots=h(k+2l-2)=a$,*

Theorem 4. *Let $1 \leqq l \leqq 5$. For a given repeated permutation $E=(\xi_1, \xi_2, \cdots, \xi_l)$, where $\xi_\nu=1$ or 5, there exist infinitely many numbers b such that $(h(b), h(b+2), \cdots, h(b+2l-2))=(\xi_1, \xi_2, \cdots, \xi_l)$,*

Theorem 5. $(h(c), h(c+2), \cdots, h(c+10)) \neq (1, 5, 1, 1, 5, 1)$ *for all $c \in Z$ and*

Theorem 6. *Let $T(l)$ denote the number of the repeated permutations $(\xi_1, \xi_2, \cdots, \xi_l)$, where $\xi_\nu=1$ or 5, which can be realized by infinitely many number of finite partial sequences consist of l consecutive terms of $\{h(2n-1)\}_{n=1}^{\infty}$, then*

1) Z is the set of all natural numbers.

$$\lim_{l\to\infty} T(l)=\infty, \qquad \lim_{l\to\infty} T(l)/2^l=0.$$

§2. Proof of Theorem 1. If we put $g_n=2^{2^n}-1$, then $g_n \in Z$ and $g_n \geqq 3$. Adopting $(g_n, 2)$ as (g, s) referred in §1, we get $f^0(2)=2<f^1(2) =2^2<f^2(2)=2^{2^2}<\cdots<f^{n-1}(2)=2^{2^{n-1}}<g_n$, $f^n(2)=2^{2^n}=(11)g_n$ and $f^{(n+1)}(2)=2$. Therefore $P(g_n)$ includes a period $(2, 2^2, 2^{2^2}, \cdots, 2^{2^{n-1}})$ of length n. Hence $M(g_n)\geqq n$. This proves Theorem 1.

Proof of Theorem 2. Lemma 1. *Let P be the set of odd primes which divide at least one of elements of the set $F=\{(2n+1)^2+1 \mid n \in Z\}$. Then P is an infinite set.* (It is well known that if $p \in P$, then $p\equiv 1$ (mod. 4).)

Proof. 5 divides $10=(2.1+1)^2+1$, which is included in F. Hence $5 \in P$, i.e. $P \neq \phi$. If $P=\{p_1, p_2, \cdots, p_t\}$ is a finite set, then $a=(p_1p_2\cdots p_t)^2+1 \in F$, $a>2$. And $p_1\equiv p_2\equiv\cdots\equiv p_t\equiv 1$ (mod. 2) implies $a\equiv 2$ (mod. 8). Therefore a has at least one odd prime divisor p which is included in P. Then $p \mid a$, and $p_1 \nmid a$, $p_2 \nmid a$, $\cdots$, and $p_t \nmid a$ follow at once from the definition of the number a. Hence $p \neq p_\nu (\nu=1, 2, \cdots, t)$. This is a contradiction, for p is in $P=\{p_1, p_2, \cdots, p_t\}$, which proves Lemma 1.

Lemma 2. *For every $p \in P$, there exists a natural number x, which satisfies the congruence $2x^2+2x+1\equiv 0$ (mod. p)*

Proof. As $p \in P$, there exist a natural number n_p such that $p \mid 2n_p^2 +2n_p+1$ by the definition of P, for p is an odd number. Then $x=n_p$ satisfies the congruence $2x^2+2x+1\equiv 0$ (mod. p). By a theorem in the quadratic field $Q(\sqrt{-1})$, we can prove the next famous

Theorem. *Diophantine equation $x^2+y^2=n$, $x, y \in Z$, $x \geqq y$, $(x, y) =1$ has 2^{s-1} solutions (x, y), if $n=2p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$, where each of $p_1, p_2, \cdots, p_s$ is a prime number of the form $4m+1$, different from the others, and each of $a_1, a_2, \cdots, a_s$ is in Z.*

Lemma 3. *For every $l \in Z$, there exist at least $2l+1$ solutions (x, y), which satisfy the Diophantine equation*

$$x^2+y^2=B^2+1, \qquad x, y \in Z, x\geqq y \tag{1}$$

for a suitable choice of $B \in Z$.

Proof. As P is an infinite set and $\lim_{s\to\infty} 2^{s-1}=\infty$, we suppose that $p_1, p_2, \cdots, p_s \in P$, where $2^{s-1}>2l+1$. For each $p_\nu (1\leqq \nu \leqq s)$, there exists a natural number n_ν such that $2n_\nu^2+2n_\nu+1\equiv 0$ (mod. p_ν) by Lemma 2. As any two of $p_1, p_2, \cdots, p_s$ are relatively prime, we can find $n \in Z$ which satisfies the congruences $n\equiv n_\nu$ (mod. p_ν) $(\nu=1, 2, \cdots, s)$. Then $2n^2+2n+1=2n_\nu^2+2n_\nu+1\equiv 0$ (mod. p_ν) $(\nu=1, 2, \cdots, s)$. Hence putting $B=2n+1$, we get $B \in Z$, $B\equiv 1$ (mod. 2) and the divisibility of $B^2+1 =2(2n^2+2n+1)$ by $2p_1p_2\cdots p_s$. Since $2 \| B^2+1$, as referred above, we have $B^2+1=2p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}\cdots p_t^{a_t}$ as the canonical decomposition of

B^2+1. By the Theorem Diophantine equation

$$x^2+y^2=B^2+1, \quad x, y \in Z, \quad x \geqq y, \quad (x, y)=1 \tag{2}$$

has $2^{t-1}(\geqq 2^{s-1}>2l+1)$ solutions (x, y). Evidently every solution of (2) satisfies (1). Thus Lemma 3 is proved. Among all solutions of (1), only one solution $(x, y)=(B, 1)$ satisfies $x \geqq B$. Hence we get the following

Lemma 4. *If B is defined as in Lemma 3. Diophantine equation*

$$x^2+y^2=B^2+1, \quad x, y \in Z, \quad B-1 \geqq x \geqq y \tag{3}$$

has at least $2l$ solutions.

Let all the solutions of (3) be $(x_1, y_1), (x_2, y_2), \cdots, (x_u, y_u)$, where $u \geqq 2l$. $2 \| B^2+1$ implies $x_\nu \equiv y_\nu \equiv 1 \pmod{2}$ for $1 \leqq \nu \leqq u$, hence we get $X_\nu, Y_\nu \in Z, X_\nu, Y_\nu \leqq B-1$, where $X_\nu = \frac{1}{2}(B+x_\nu)$, $Y_\nu = \frac{1}{2}(1+y_\nu)$. And easy calculation leads us to $X_\nu^2+Y_\nu^2=BX_\nu+Y_\nu$, which means $f(BX_\nu+Y_\nu)=X_\nu^2+Y_\nu^2=BX_\nu+Y_\nu$, when $s=2$, $g=B$ (remember $X_\nu, Y_\nu \leqq B-1$). Hence, each $BX_\nu+Y_\nu$ itself forms an element of $P(B)$. If $X_\nu^2+Y_\nu^2=X_\mu^2+Y_\mu^2 \cdots$ $\cdots$ (4) for $(X_\nu, Y_\nu), (X_\mu, Y_\mu) \in \{(X_\lambda, Y_\lambda) \mid 1 \leqq \lambda \leqq u\}$, then $BX_\nu+Y_\nu=BX_\mu+Y_\mu \cdots$ (5). Regarding (4), (5) as a simultaneous equation of two unknowns X_μ and Y_μ, as easily proved, this equation has at most two solutions. From this, we can insist that if $1 \leqq n_1 < n_2 < n_3 \leqq u$, then equalities $X_{n_1}^2+Y_{n_1}^2=X_{n_2}^2+Y_{n_2}^2=X_{n_3}^2+Y_{n_3}^2$ don't hold. Hence the number set $\{X_\nu^2+Y_\nu^2 \mid 1 \leqq \nu \leqq u\}$ includes at least $\left[\frac{u}{2}\right](\geqq l)$ different elements, which implies $P(B) \geqq l$. Theorem 2 is proved.

§3. Proof of Theorem 3. 1°. $h((1)_3)=h((10)_3)=h((100)_3)=\cdots 1$, $h((110)_3)=h((1100)_3)=h((11000)_3)=\cdots=2$, $h((20)_3)=h((200)_3)=h((2000)_3)=\cdots=4$, $h((12)_3)=h((120)_3)=h((1200)_3)=\cdots=5$, $h((22)_3)=h((220)_3)=h((2200)_3)=\cdots=8$. Hence Theorem 3 is true when $l=1$.

2°. We can select b_1 such that $b_1 \geqq 6$, $h(b_1)=a$ by 1°. Define $b_2^{(c)}=(\overbrace{1\,1\cdots1}^{b_1-5}\ \overbrace{0\,0\cdots0}^{c}\,1\,2)_3$ $(c=0, 1, 2, \cdots)$. Then $f(b_2^{(c)})=f(b_2^{(c)}+2)=b_1$, and hence $h(b_2^{(c)})=h(b_2^{(c)}+2)=a$, Theorem 3 is true when $l=2$. At the same time, we can assert that for every $a \in H$, there exist infinitely many natural numbers b_2 such that $b_2 \equiv a \pmod{4}$, $h(b_2)=a$, and infinitely many natural numbers b_2' such that $b_2' \equiv a+2 \pmod{4}$, $h(b_2')=a$.

3°. We can find b, m such that $h(b)=h(b+4m)=a$, $b \geqq 2$, $b, m \in Z$ by 2°. Then for $b_3^{(c)}=(\overbrace{1\,1\cdots1}^{b-1}\ \overbrace{0\,0\cdots0}^{c}\ \overbrace{2\,2\cdots2}^{m-1}\ 1\,2)_3$ $(c=1, 2, 3, \cdots)$, $f(b_3)=f(b_3+2)=b+4m$, $f(b_3+4)=b$ which implies $h(b_3^{(c)})=h(b_3^{(c)}+2)=h(b_3^{(c)}+4)=a$. Theorem 3 is true for $l=3$.

4°. We can find b_3 such that $h(b_3)=h(b_3+2)=h(b_3+4)=a$ by 3°. Then for $b_4^{(c)}=(\overbrace{1\,1\cdots1}^{b_3}\ \overbrace{0\,0\cdots0}^{c})_3$ $(c=2, 3, \cdots)$, $f(b_4^{(c)})=b_3$, $f(b_4^{(c)}+2)$

$=f(b_4^{(c)}+6)=b_3+4$, $f(b_4^{(c)}+4)=b_3+2$, hence $h(b_4^{(c)})=h(b_4^{(c)}+2)=h(b_4^{(c)}+4)=h(b_4^{(c)}+6)=a$. Theorem 3 is true when $l=4$.

5°. We can find b_4 such that $h(b_4)=h(b_4+2)=h(b_4+4)=h(b_4+6)$, $b_4\geqq 4$ by 4°. Then for $b_5^{(c)}=(\overbrace{11\cdots 1}^{b_4-3}\ \overbrace{00\cdots 0}^{c}\ 102)_3$ $(c=0,1,2,\cdots)$, $f(b_5^{(c)})=f(b_5^{(c)}+4)=f(b_5^{(c)}+8)=f(b_5^{(c)}+10)=b_4+2$, $f(b_5^{(c)}+2)=b_4$, $f(b_5^{(c)}+6)=f(b_5^{(c)}+12)=f(b_5^{(c)}+14)=b_4+6$, hence $h(b_5^{(c)})=h(b_5^{(c)}+2)=\cdots=h(b_5^{(c)}+14)=a$. Theorem 3 is true for $1\leqq l\leqq 8$.

6°. Suppose that l is a natural number $\geqq 7$, and that there exist infinitely many natural numbers b such that $h(b)=h(b+2)=\cdots=h(b+2l-2)=a$. If we put $b_{l+1}^{(c)}=(\overbrace{11\cdots 1}^{b}\ \overbrace{00\cdots 0}^{c}\ \overbrace{00\cdots 0}^{[\frac{1}{2}(l-1)]})_3$ $(c=0,1,2,\cdots)$, then we get $b\leqq f(n)\leqq b+4\left[\frac{l-1}{2}\right]\leqq b+2l-2$, $f(n)\equiv b\equiv a \pmod{2}$ and $h(n)=a$ for all n such that $n\equiv b_{l+1}^{(c)} \pmod{2}$, $b_{l+1}^{(c)}\leqq n\leqq b_{l+1}^{(c)}+(\overbrace{22\cdots 2}^{[\frac{1}{2}(l-1)]})_3\cdots(1)$. The number of the integers which satisfy (1) is $\frac{1}{2}(3^{[\frac{l-1}{2}]}+1)$, which is greater than l for $l\geqq 7$. This shows that Theorem 3 for l implies Theorem 3 for $l+1$. A proof of Theorem 3 by mathematical induction completes.

Proof of Theorem 4. Let each of $\xi_1, \xi_2, \cdots, \xi_5$ be either 1 or 5, and let b be a natural number. Let us agree to denote $\varphi(b)=(\xi_1\xi_2\xi_3\xi_4\xi_5)$, if $h(b)=\xi_1$, $h(b+2)=\xi_2, \cdots, h(b+8)=\xi_5$. Then it is easy to verify that $\varphi((2120)_3)=(11111)$, $\varphi((10220)_3)=(11115)$, $\varphi((20210)_3)=(11151)$, $\varphi(1022)_3)=(11155)$, $\varphi((12200)_3)=(11511)$, $\varphi((2012)_3)=(11515)$, $\varphi((11001)_3)=(11551)$, $\varphi((1101)_3)=(11555)$, $\varphi((1011)_3)=(15111)$, $\varphi((12002)_3)=(15115)$, $\varphi((100)_3)=(15151)$, $\varphi((222222100)_3)=(15155)$, $\varphi((22222222111110)_3)=(15511)$, $\varphi((11010)_3)=(15515)$, $\varphi((1110)_3)=(15551)$, $\varphi((11100)_3)=(15555)$, $\varphi((2111)_3)=(51111)$, $\varphi((1020)_3)=(51115)$, $\varphi((12121)_3)=(51151)$, $\varphi((12011)_3)=(51155)$, $\varphi((1002)_3)=(51511)$, $\varphi((222222222021)_3)=(51515)$, $\varphi((22111002)_3)=(51551)$, $\varphi((11021)_3)=(51555)$, $\varphi((2222111101)_3)=(55111)$, $\varphi((2001)_3)=(55115)$, $\varphi((1121)_3)=(55151)$, $\varphi((11012)_3)=(55155)$, $\varphi((12110)_3)=(55511)$, $\varphi((1112)_3)=(55515)$, $\varphi((12101)_3)=(55551)_3$, $\varphi((11111)_3)=(55555)$. Adding a natural number $x\leqq 8$ to each b above mentioned, does not change the digit of the highest term of b in the scale of 3. Therefore the number given by inserting a finite number of zeros between the digit of the highest term and the digit of the second highest term of b is mapped by the function h to the same integer as $h(b)$. Theorem 4 is proved.

Proof of Theorem 5. It is easy to verify that if $n\equiv 1$ or $n\equiv 5 \pmod{18}$, then $f(n)=f(n+2)$ and therefore $h(n)=h(n+2)$. Similarly,

$n \equiv 11 \pmod{18}$ implies $h(n)=h(n+4)$. Hence, if $b \equiv 1 \pmod{18}$, then $h(b)=h(b+2)$ and therefore $(h(b), h(b+2), h(b+4), h(b+6), h(b+8), h(b+10)) \neq (151151)$. Similarly we can easily verify that when r is one of 3, 5, 7, 9, 11, 13, 15, 17, the number $18n+r$ satisfies one of the equalities $h(b+2)=h(b+4)$, $h(b)=h(b+2)$, $h(b+4)=h(b+8)$, $h(b+2)=h(b+6)$, $h(b+8)=h(b+10)$, $h(b+6)=h(b+8)$, $h(b+8)=h(b+10)$, $h(b+2)=h(b+4)$. Each of these equalities show $(h(b), h(b+2), h(b+4), h(b+6), h(b+8), h(b+10)) \neq (151151)$. Theorem 5 is proved.

Proof of Theorem 6. As $l \in Z$, there exist an increasing sequence $\{b_\nu\}_{\nu=1}^{\infty}$ such that $h(b_\nu)=h(b_\nu+2)=\cdots=h(b_\nu+2l-2)=1$ by Theorem 1. Besides, Theorem 1 teaches us that there exist infinitely many b's such that $h(b)=5$. Thus for each ν, there exists $k_\nu(\geqq l)$ such that $h(b_\nu)=h(b_\nu+2)=\cdots=h(b_\nu+2k_\nu-2)$ and $h(b_\nu+2k_\nu)=5$. Then $\{h(b_\nu+2k_\nu-2(l-i)+2k-2)\}_{k=1}^{l}=(\overbrace{11\cdots1}^{l-i}5\,\xi_{1,\nu}^{(i-1)}\xi_{2,\nu}^{(i-1)}\cdots\xi_{i-1,\nu}^{(i-1)})$, where $2 \leqq i \leqq l-1$, $\xi_{1,\nu}^{(i-1)}, \xi_{2,\nu}^{(i-1)}, \cdots, \xi_{i-1,\nu}^{(i-1)}=1$ or 5. As each of $l-2$ permutations above mentioned are different from the others, we get $T(l) \geqq l-2$, which proves $\lim_{l\to\infty} T(l)=\infty$. For every natural number $l \geqq 9$, there exists a natural number t such that $9(t+1)>l \geqq 9t$. If $a \equiv 1 \pmod{18}$, then $f(a)=f(a+2)$ and hence $h(a)=h(a+2)$. Therefore in every progression $h(b)$, $h(b+2)$, $\cdots$, $h(b+2l-2)$, t equalities $h(c)=h(c+2)$, $h(c+18)=h(c+20)$, $\cdots$, $h(c+18(t-1))=h(c+18(t-1)+2)$ hold for a suitable natural number $c \leqq 7$. This fact implies $T(l) \leqq 7.2^l/2^t$, hence $T(l)/2^l \leqq 7/2^t \leqq 7.2^{-\frac{l}{9}} \to 0$ (as $l \to \infty$). Theorem 6 is proved.

References

[1] A. Porges: A set of eight numbers. Amer. Math. Monthly., **52**, 379–382 (1945).

[2] R. Isaacs: Iterates of fractional order. Canadian J. Math., **2**, 409–416 (1950).

[3] B. M. Stewart: Sums of functions of digits. Canadian J. Math., **12**, 374–380 (1960).

[4] W. Sierpiński: Elementary theory of numbers (Translated from Polish by A. Hulanicki), 268.

[5] K. Chikawa, K. Iséki, and T. Kusakabe: On a problem by H. Steinhaus. Acta Arithmetica., **7**, 251–252 (1962).

[6] K. Chikawa, K. Iséki, T. Kusakabe, and K. Shibamura: Computations of cyclic parts of Steinhaus problem for power 5. Acta Arithmetica, **7**, 253–254 (1962).