ACTA ARITHMETICA
LXII.1 (1992)

Some variations and consequences of the Kummer–Mirimanoff congruences

by

Takashi Agoh (Chiba)

1. Introduction. Let p be an odd prime, $\mathbb{Z}$ the ring of integers, $\mathbb{Z}_p$ the ring of all rational numbers which are p-integral, $\varphi_m(X)$ the *Mirimanoff polynomial*, i.e.,

$$\varphi_m(X) = \sum_{i=1}^{p-1} i^{m-1} X^i \qquad (m \in \mathbb{Z})$$

and B_n the *n-th Bernoulli number* defined by

$$B(X) \equiv \frac{X}{e^X - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} X^k \,.$$

Also we denote by $[f(v)]_0^{(n)}$ the value of $d^n\{f(v)\}/dv^n$ at $v = 0$ for a differentiable function $f(v)$ of v.

We consider the equation

$$x^p + y^p + z^p = 0\,, \qquad p \nmid xyz\,, \tag{1.1}$$

where x, y and z are non-zero integers prime to each other.

Let $g = (p-3)/2$ and

$$W = \left\{ -\frac{y}{x}, -\frac{x}{y}, -\frac{z}{y}, -\frac{y}{z}, -\frac{x}{z}, -\frac{z}{x} \right\}.$$

It is well known that if the equation (1.1) holds, then $t \in W$ is a solution of the system of congruences ([7], see also [10])

$$\text{(K)} \qquad \begin{cases} \varphi_{p-1}(X) \equiv 0 \pmod{p}, \\ B_{2n}\varphi_{p-2n}(X) \equiv 0 \pmod{p}, \quad n = 1, 2, \ldots, g\,. \end{cases}$$

On the other hand, it has been shown by Mirimanoff [9] that this system is equivalent to

$$\text{(M)} \qquad \begin{cases} \varphi_{p-1}(X) \equiv 0 \pmod{p}, \\ \varphi_l(X)\varphi_{p-l}(X) \equiv 0 \pmod{p}, \quad l = 2, \ldots, g+1\,. \end{cases}$$

This fact follows easily from the relation

$$\frac{1+X}{2}\varphi_{p-1}(X)+\frac{1-X}{m+1}\sum_{j=2}^{p-2-m}\binom{p-1-m}{j}B_j\varphi_{p-j}(X)$$
$$\equiv-\sum_{i=2}^{m+1}\binom{m}{i-1}\varphi_i(X)\varphi_{p-i}(X)\ (\operatorname{mod} p)\qquad (\text{cf. [3]})\,,$$

where $X\not\equiv 1\ (\operatorname{mod} p)$ and m is any integer with $1\le m\le p-4$.

The congruences in (K) and (M) are the so-called *Kummer–Mirimanoff* ones, which have many kinds of interesting variations and consequences.

Let $B'_i=\{(1-2^i)/i\}B_i$ for $i\ge 1$. It is clear that the system (K) implies

$$(\mathrm{K}')\qquad \begin{cases}\varphi_{p-1}(X)\equiv 0\ (\operatorname{mod} p),\\ B'_{2n}\varphi_{p-2n}(X)\equiv 0\ (\operatorname{mod} p),\quad n=1,2,\dots,g\,.\end{cases}$$

We easily see that if 2 is a primitive root mod p, then this system is equivalent to (K).

For $m\ge 1$ and $n\ge 1$ let $S_m(0)=S'_m(0)=0$, $S_m(n)=\sum_{i=1}^n i^m$ and $S'_m(n)=\sum_{i=1}^n(-1)^{n-i}i^m$. Also, denote by $|n|$ an integer such that $n\equiv|n|$ $(\operatorname{mod} p)$ and $0\le|n|\le p-1$, and by $\overline{n}$ an integer such that $n\overline{n}\equiv p-1$ $(\operatorname{mod} p)$ and $1\le\overline{n}\le p-1$ for a given integer n with $p\nwarrow n$.

The main results of this paper are the following:

Theorem 1. *Let $X\not\equiv\pm1\ (\operatorname{mod} p)$. Then $t\in W$ is a solution of the system* (K) *if and only if t is a solution of any one of the systems of congruences*

$$(\mathrm{I})\qquad \sum_{i=1}^{p-1} iS_{p-3}(|ik|)X^i\equiv 0\ (\operatorname{mod} p)\qquad (1\le k\le p-1)\,;$$

$$(\mathrm{II})\qquad \sum_{i=1}^{p-1} i^m S_{p-2-m}(|ik|)X^i\equiv 0\ (\operatorname{mod} p)\qquad (m=2m'-1, 1\le m'\le g\,,$$
$$\textit{and } m=p-3; k \textit{ is any fixed integer with } 1\le k\le p-1)\,;$$

$$(\mathrm{III})\qquad \sum_{i=1}^{p-1} S_{p-2}(|ik|)X^i\equiv 0\ (\operatorname{mod} p)\qquad (1\le k\le p-1)\,;$$

$$(\mathrm{IV})\qquad \sum_{i=1}^{\overline{k}-1} S_{p-2}(|ik|)X^i\equiv 0\ (\operatorname{mod} p)\qquad (1\le k\le p-2)\,.$$

Theorem 2. *Let $X\not\equiv\pm1\ (\operatorname{mod} p)$. Then $t\in W$ is a solution of the system* (K′) *if and only if t is a solution of any one of the systems of con-*

gruences

$$\text{(I}'\text{)}\qquad \sum_{i=1}^{p-1} iS'_{p-3}(|ik|)X^i \equiv 0 \pmod p \qquad (1 \le k \le p-1)\,;$$

$$\text{(II}'\text{)}\qquad \begin{cases} \varphi_{p-1}(X) \equiv 0 \pmod p\,, \\ \sum_{i=1}^{p-1} i^m S'_{p-2-m}(|ik|)X^i \equiv 0 \pmod p \qquad (m = 2m'-1\,, \end{cases}$$

$1 \le m' \le g$; *k is any fixed integer with* $1 \le k \le p-1)$;

$$\text{(III}'\text{)}\qquad \sum_{i=1}^{p-1} S'_{p-2}(|ik|)X^i \equiv 0 \pmod p \qquad (1 \le k \le p-1)\,;$$

$$\text{(IV}'\text{)}\qquad \sum_{i=1}^{\overline{k}-1} S'_{p-2}(|ik|)X^i \equiv 0 \pmod p \qquad (1 \le k \le p-2)\,.$$

Further, we shall give some assertions relating to the equation (1.1), as consequences of the Kummer–Mirimanoff congruences and the theorems stated above.

We note that Theorem 1 has been essentially proved by Agoh [3] and Thaine [11]. For Theorem 2 we shall use the same method of proof. Therefore, in Section 3 we shall recall the proof of Theorem 1 and use its idea in Section 4 to prove Theorem 2.

2. Preliminaries. First we note that $t \not\equiv 0, 1 \pmod p$ for each $t \in W$ because $p \nmid xyz$, and also we may replace t by any element of the set

$$H = \left\{t, \frac{1}{t}, 1-t, \frac{1}{1-t}, \frac{t-1}{t}, \frac{t}{t-1} \pmod p\right\}$$

because $x + y + z \equiv 0 \pmod p$. Denote by ${}^{\#}H$ the number of elements of H. If $t^2 - t + 1 \equiv 0 \pmod p$, then ${}^{\#}H = 2$. However, by a result of Pollaczek this case does not occur (see e.g. [10]). If $t \equiv -1, 2, 1/2 \pmod p$, then ${}^{\#}H = 3$, hence $H \equiv \{-1, 2, 1/2\} \pmod p$. In other cases the elements of H are pairwise non-congruent modulo p, i.e., ${}^{\#}H = 6$. Therefore, we see that if $t \equiv -1 \pmod p$, then we may take another element $t' \in H$ such that $t' \not\equiv -1 \pmod p$.

Next, we shall give some elementary lemmas which will be needed in the following sections.

The theorem of von Staudt–Clausen completely describes the denominator of B_m. That is, if $m \ge 2$ is an even integer, then

$$\text{(2.1)}\qquad B_m = \gamma_m - \sum_{p-1\,|\,m} \frac{1}{p}\,,$$

where γ_m is an integer and the sum is taken over all primes p such that $p-1\,|\,m$.

Lemma 1. *Let $m\ge 2$ be an even integer. If $p-1\nmid m$, then $B_m\in\mathbb{Z}_p$. If $p-1\,|\,m$, then $pB_m\in\mathbb{Z}_p$, more precisely $pB_m\equiv -1 \pmod p$.*

Proof. This is an easy consequence of (2.1). ∎

Lemma 2. *Let $U(v)=1/(e^v+1)$. Then for $m\ge 0$*

$$[U(v)]_0^{(m)}=B'_{m+1}\in\mathbb{Z}_p\,.$$

Proof. By Lemma 1 and Fermat's little theorem, clearly $B'_{m+1}\in\mathbb{Z}_p$ for all $m\ge 0$. On the other hand, since $vU(v)=B(v)-B(2v)$, we have $(m+1)\times[U(v)]_0^{(m)}=[B(v)-B(2v)]_0^{(m+1)}=(1-2^{m+1})B_{m+1}=(m+1)B'_{m+1}$. ∎

Lemma 3. *Let $m\ge 1$ and $l\ge 1$. Then*

$$S_m(l)=\frac{1}{m+1}\sum_{i=0}^{m}\binom{m+1}{i}B_i(l+1)^{m+1-i}\,, \tag{1}$$

$$S'_m(l)=\sum_{i=0}^{m-1}\binom{m}{i}B'_{i+1}(l+1)^{m-i}+\{1-(-1)^{l+1}\}B'_{m+1}\,. \tag{2}$$

Proof. By using the identity

$$v\Big\{\sum_{i=0}^{l}e^{iv}\Big\}=B(v)e^{(l+1)v}-B(v)\,,$$

we have

$$\begin{aligned}(m+1)S_m(l)&=[B(v)e^{(l+1)v}]_0^{(m+1)}-[B(v)]_0^{(m+1)}\\&=\sum_{i=0}^{m}\binom{m+1}{i}B_i(l+1)^{m+1-i}\,.\end{aligned}$$

On the other hand, since

$$\sum_{i=0}^{l}(-1)^{l-i}e^{iv}=U(v)e^{(l+1)v}-(-1)^{l+1}U(v)\,,$$

by Lemma 2 we have

$$\begin{aligned}S'_m(l)&=[U(v)e^{(l+1)v}]_0^{(m)}-(-1)^{l+1}U(v)\\&=\sum_{i=0}^{m-1}\binom{m}{i}B'_{i+1}(l+1)^{m-i}+\{1-(-1)^{l+1}\}B'_{m+1}\,.\end{aligned}$$ ∎

Lemma 4. *For $m\ge 1$ and $n\ge 1$,*

$$S_m(np)\equiv S_m(np-1)\equiv\begin{cases}0 \pmod p & \text{if } p-1\nmid m\,,\\ n(p-1) \pmod p & \text{if } p-1\,|\,m\,.\end{cases}$$

Proof. Set $l = np-1$ in (1) of Lemma 3. Then the result clearly follows by Lemma 1. ∎

LEMMA 5. *For $m \ge 1$ and $n \ge 1$,*

$$S'_m(np) \equiv -S'_m(np-1) \equiv -\{1-(-1)^n\}B'_{m+1} \pmod{p}.$$

In particular,

$$S'_{p-2}(np) \equiv -S'_{p-2}(np-1) \equiv \{1-(-1)^n\}q_p(2) \pmod{p},$$

where $q_p(r)$ is the Fermat quotient with base r, i.e., $q_p(r) = (r^{p-1}-1)/p$.

Proof. The congruence $S'_m(np) \equiv -S'_m(np-1) \pmod{p}$ is trivial. Set $l = np-1$ in (2) of Lemma 3. Since $B'_{i+1} \in \mathbb{Z}_p$ for all $i \ge 0$, we have

$$\begin{aligned} S'_m(np-1) &\equiv \sum_{i=0}^{m-1} \binom{m}{i} B'_{i+1}(np)^{m-i} + \{1-(-1)^{np}\}B'_{m+1} \\ &\equiv \{1-(-1)^n\}B'_{m+1} \pmod{p}. \end{aligned}$$

In particular, letting $m = p-2$ we have from Lemma 1

$$\begin{aligned} S'_{p-2}(np-1) &\equiv \{1-(-1)^n\}B'_{p-1} = \{1-(-1)^n\}q_p(2)pB_{p-1} \\ &\equiv -\{1-(-1)^n\}q_p(2) \pmod{p}. \quad ∎ \end{aligned}$$

LEMMA 6. *Let $D(a,b) = (i^j)$ $(i = a, a+1, \ldots, b;\ j = 0, 1, \ldots, b-a;$ $1 \le a < b \le p-1)$ be a square matrix of order $b-a+1$. Then* $\det(D(a,b)) \not\equiv 0 \pmod{p}$.

Proof. Since $\det(D(a,b))$ is of Vandermonde type, the result clearly follows. ∎

LEMMA 7. *Let α and s be integers with $p \nmid \alpha$. Then*

$$q_p(\alpha) - q_p(sp-\alpha) \equiv -\frac{s}{\alpha} \pmod{p}.$$

Proof. Since

$$q_p(sp-\alpha) \equiv \binom{p-1}{p-2} s(-\alpha)^{p-2} + q_p(\alpha) \pmod{p},$$

the lemma is trivial. ∎

This lemma shows that if $q_p(\alpha) \equiv 0 \pmod{p}$, then $q_p(sp-\alpha) \equiv 0 \pmod{p}$ if and only if $p \mid s$. In other words, if $p \nmid s$, then we cannot write $sp = \alpha + \beta$, where $q_p(\alpha) \equiv q_p(\beta) \equiv 0 \pmod{p}$.

3. Proof of Theorem 1.

In this section the proof of Theorem 1 is given. To prove the assertion for the system (IV) we shall employ Thaine's ingenious method, in a different form.

Proof of Theorem 1. In [3] we showed the equality

$$\begin{aligned}(3.1)\quad & k^{p-1-m}\varphi_p(X)+\frac{p-1-m}{2}k^{p-2-m}\varphi_{p-1}(X)\\ &\qquad+\sum_{i=2}^{p-2-m}\binom{p-1-m}{i}k^{p-1-m-i}\{B_i\varphi_{p-i}(X)\}\\ &\qquad=(p-1-m)\sum_{i=1}^{p-1}i^mS_{p-2-m}(ik)X^i\,,\end{aligned}$$

where k and m are integers such that $1\le k\le p-1$ and $m\le p-3$. In particular, if $m=p-3$, then the sum on the left hand side vanishes.

If $p-1 \nwarrow p-2-m$, then by Lemma 4 we have

$$S_{p-2-m}(ik)\equiv S_{p-2-m}(|ik|)\ (\mathrm{mod}\,p)\,.$$

Hence from (3.1) we can deduce

$$(3.2)\qquad k\varphi_{p-1}(X)\equiv 2\sum_{i=1}^{p-1}i^{p-3}S_1(|ik|)X^i\ (\mathrm{mod}\,p)$$

and

$$\begin{aligned}(3.3)\quad & k^{p-2-m}\varphi_{p-1}(X)\\ &\qquad+\frac{2}{p-1-m}\sum_{i=2}^{p-2-m}\binom{p-1-m}{i}k^{p-1-m-i}\{B_i\varphi_{p-i}(X)\}\\ &\qquad\equiv 2\sum_{i=1}^{p-1}i^mS_{p-2-m}(|ik|)X^i\ (\mathrm{mod}\,p)\qquad(0\le m\le p-4)\,.\end{aligned}$$

Note that the above congruences are valid unless $X\equiv 1\ (\mathrm{mod}\,p)$. In fact, if $X\not\equiv 1\ (\mathrm{mod}\,p)$, then $\varphi_p(X)\equiv(X^p-X)/(X-1)\equiv 0\ (\mathrm{mod}\,p)$.

Suppose that $t\in W$ is a solution of the system (K). Noting that $B_i=0$ for an odd integer $i\ge 3$, from (3.2) and (3.3) we have

$$(3.4)\qquad \sum_{i=1}^{p-1}i^mS_{p-2-m}(|ik|)t^i\equiv 0\ (\mathrm{mod}\,p)\qquad(0\le m\le p-3)\,.$$

Conversely, if (3.4) holds, then from (3.2) and (3.3)

$$(3.5)\qquad \varphi_{p-1}(t)\equiv 0\ (\mathrm{mod}\,p)\,,$$

$$\begin{aligned}(3.6)\quad & k^{p-2-m}\varphi_{p-1}(t)\\ &\qquad+\frac{2}{p-1-m}\sum_{i=2}^{p-2-m}\binom{p-1-m}{i}k^{p-1-m-i}\{B_i\varphi_{p-i}(t)\}\\ &\qquad\equiv 0\ (\mathrm{mod}\,p)\qquad(0\le m\le p-4)\,.\end{aligned}$$

(1) (K)⇒(I). Take $m = 1$ in (3.4).

(2) (I)⇒(K). Observe (3.6) for $m = 1$ and $k = 1, 2, \ldots, p-1$. From Lemma 6 the result clearly follows.

(3) (K)⇒(II). The congruences in (II) for $X = t$ are included in (3.4). So the result is obvious.

(4) (II)⇒(K). Take successively $m = p-4,\ p-6, \ldots, 1$ in (3.6). In view of (3.2) (hence (3.5)) the result follows.

(5) (K)⇒(III). Take $m = 0$ in (3.4).

(6) (III)⇒(K). By means of Lemma 6 the assertion follows from (3.6) for $m = 0$ and $k = 1, 2, \ldots, p-1$.

We note that, as a matter of fact, in (2) and (6) it is enough to take fewer than $p-1$ k's.

By Lemma 4 we have $S_{p-2}(p-1) \equiv 0 \pmod{p}$, hence for each $a = 1, 2, \ldots, p-1$

$$\begin{aligned} S_{p-2}(a) &\equiv -\sum_{i=1}^{p-1-a} (a+i)^{p-2} \equiv S_{p-2}(p-1-a) \\ &\equiv S_{p-2}(p-a) + a^{p-2} \equiv S_{p-2}(a-1) + a^{p-2} \pmod{p}\,. \end{aligned} \tag{3.7}$$

We now define the polynomials $P_k(X)$ and $Q_k(X)$ by

$$P_k(X) = \sum_{l=1}^{p-1} S_{p-2}(|lk|)X^l \qquad (1 \le k \le p-1)\,,$$

$$Q_k(X) = \begin{cases} \sum_{l=1}^{\overline{k}-1} S_{p-2}(|lk|)X^l & (1 \le k \le p-2)\,, \\ 0 \quad (k = p-1)\,. \end{cases}$$

Since $S_{p-2}(|\overline{k}k|) = S_{p-2}(p-1) \equiv 0 \pmod{p}$ by Lemma 4,

$$P_k(X) \equiv Q_k(X) + X^{\overline{k}} \Big\{ \sum_{j=1}^{p-\overline{k}-1} S_{p-2}(|(\overline{k}+j)k|)X^j \Big\} \pmod{p}\,.$$

Noting that $p-1-|jk-1| \equiv p-jk \equiv j(p-k) \pmod{p}$, by (3.7) we have

$$\begin{aligned} S_{p-2}(|(\overline{k}+j)k|) &= S_{p-2}(|jk-1|) \equiv S_{p-2}(p-1-|jk-1|) \\ &= S_{p-2}(|j(p-k)|) \pmod{p}\,. \end{aligned}$$

Also $\overline{p-k} = p - \overline{k}$, hence

$$P_k(X) \equiv Q_k(X) + X^{\overline{k}} Q_{p-k}(X) \pmod{p}\,. \tag{3.8}$$

Similarly, using (3.7) we have

$$\begin{aligned} P_k(X) &\equiv \sum_{l=1}^{p-1} S_{p-2}(p-|lk|)X^l - \overline{k}\varphi_{p-1}(X) \\ &\equiv \sum_{l=1}^{p-1} S_{p-2}(|lk|-1)X^l - \overline{k}\varphi_{p-1}(X) \pmod{p}. \end{aligned}$$

Here, since

$$\begin{aligned} S_{p-2}(|jk|-1) &= S_{p-2}(|(\overline{k}+j)k|), \\ S_{p-2}(|(p-\overline{k})k|-1) &= S_{p-2}(0) = 0, \\ S_{p-2}(|(p-\overline{k}+i)k|-1) &= S_{p-2}(|ik|), \end{aligned}$$

it follows that

$$\begin{aligned} P_k(X) \equiv \sum_{j=1}^{p-\overline{k}-1} S_{p-2}(|(\overline{k}+j)k|)X^j + X^{p-\overline{k}}\Big\{\sum_{i=1}^{\overline{k}-1} S_{p-2}(|ik|)X^i\Big\} \\ -\overline{k}\varphi_{p-1}(X) \pmod{p}, \end{aligned}$$

that is,

$$P_k(X) \equiv Q_{p-k}(X) + X^{p-\overline{k}}Q_k(X) - \overline{k}\varphi_{p-1}(X) \pmod{p}. \tag{3.9}$$

(7) (III)⇒(IV). Assume that $P_k(t) \equiv 0 \pmod{p}$ $(1 \le k \le p-1)$. By (6) we have $\varphi_{p-1}(t) \equiv 0 \pmod{p}$. So, from (3.8) and (3.9), $(t^p-1)Q_k(t) \equiv 0 \pmod{p}$, which gives $Q_k(t) \equiv 0 \pmod{p}$ because $t \not\equiv 1 \pmod{p}$. That is, $t \in W$ satisfies the system (IV).

(8) (IV)⇒(III). Assuming $Q_k(t) \equiv 0 \pmod{p}$ $(1 \le k \le p-1)$ we obviously see $P_k(t) \equiv 0 \pmod{p}$ from (3.8), i.e., $t \in W$ is a solution of (III).

This completes the proof of the theorem. ■

Note that in the above discussion concerning the polynomials $P_k(X)$ and $Q_k(X)$ we used notations and expressions different from Thaine's. However, the reasoning is essentially the same as in his paper [11]. We emphasize that all arguments in the proof of the theorem start from the equality (3.1).

4. Proof of Theorem 2. In this section we shall give the proof of Theorem 2 by using a similar method to that of Theorem 1.

Proof of Theorem 2. Let k and m be integers such that $1 \le k \le p-1$ and $m \le p-3$. We now use the following identity:

$$\omega_{k,m,X}(v) = \mu_{k,m,X}(v) + \nu_{k,m,X}(v),$$

where

$$\begin{aligned}\omega_{k,m,X}(v) &= \{U(v)e^v\}\{\varphi_{m+1}(Xe^{kv})\}\,,\\ \mu_{k,m,X}(v) &= \sum_{i=1}^{p-1} i^m\Big\{\sum_{j=0}^{ik}(-1)^j e^{(ik-j)v}\Big\}X^i\,,\\ \nu_{k,m,X}(v) &= -\varphi_{m+1}((-1)^k X)U(v)\,.\end{aligned}$$

By Lemma 2,

$$[U(v)e^v]_0^{(0)} = 1/2\,,\qquad [U(v)e^v]_0^{(i)} = [1-U(v)]_0^{(i)} = -B'_{i+1}\qquad (i\ge 1)$$

and also

$$[\varphi_{m+1}(Xe^{kv})]_0^{(i)} = k^i\varphi_{m+1+i}(X)\qquad (i\ge 0)\,.$$

Therefore

$$[\omega_{k,m,X}(v)]_0^{(l)} = \tfrac{1}{2}k^l\varphi_{m+l+1}(X) - \sum_{i=1}^{l}\binom{l}{i}B'_{i+1}\{k^{l-i}\varphi_{m+1+l-i}(X)\}$$

for $l\ge 1$. Also we have

$$\begin{aligned}[\mu_{k,m,X}(v)]_0^{(l)} &= \sum_{i=1}^{p-1} i^m S'_l(ik)X^i\,,\\ [\nu_{k,m,X}(v)]_0^{(l)} &= -\varphi_{m+1}((-1)^k X)B'_{l+1}\,.\end{aligned}$$

Consequently, we deduce from the above identity that if $l\ge 1$, then

$$\begin{aligned}&\tfrac{1}{2}k^l\varphi_{m+l+1}(X) - \sum_{i=1}^{l}\binom{l}{i}k^{l-i}\{B'_{i+1}\varphi_{m+1+l-i}(X)\}\\ &\qquad\qquad = \sum_{i=1}^{p-1} i^m S'_l(ik)X^i - \varphi_{m+1}((-1)^k X)B'_{l+1}\,.\end{aligned}$$

In particular, taking $l = p-2-m$ we have

$$\begin{aligned}(4.1)\quad &\tfrac{1}{2}k^{p-2-m}\varphi_{p-1}(X) - \sum_{i=1}^{p-2-m}\binom{p-2-m}{i}k^{p-2-m-i}\{B'_{i+1}\varphi_{p-1-i}(X)\}\\ &\qquad = \sum_{i=1}^{p-1} i^m S'_{p-2-m}(ik)X^i - \varphi_{m+1}((-1)^k X)B'_{p-1-m}\,.\end{aligned}$$

Here, by Lemma 5,

$$\begin{aligned}S'_{p-2-m}(ik) &= S'_{p-2-m}(|ik|) + (-1)^{\alpha(ik)}S'_{p-2-m}\Big(\Big[\frac{ik}{p}\Big]p\Big)\\ &\equiv S'_{p-2-m}(|ik|) - (-1)^{\alpha(ik)}\{1-(-1)^{[ik/p]}\}B'_{p-1-m}\ (\mathrm{mod}\, p)\,,\end{aligned}$$

where $\alpha(n)=n-[n/p]p$, $[n/p]$ being the greatest integer in $[n/p]$. Hence, from the above equality we get the congruence

$$\begin{aligned}(4.2)\quad \tfrac{1}{2}k^{p-2-m}\varphi_{p-1}(X)-&\sum_{i=1}^{p-2-m}\binom{p-2-m}{i}k^{p-2-m-i}\{B'_{i+1}\varphi_{p-1-i}(X)\}\\ &\equiv\sum_{i=1}^{p-1}i^mS'_{p-2-m}(|ik|)X^i-\varphi_{m+1}((-1)^kX)B'_{p-1-m}\\ &\quad-\Big\{\sum_{i=1}^{p-1}(-1)^{\alpha(ik)}\{1-(-1)^{[ik/p]}\}i^mX^i\Big\}B'_{p-1-m}\ (\operatorname{mod} p)\,.\end{aligned}$$

If $t\in W$ is a solution of the system (K′), then from (4.2) we have

$$\begin{aligned}(4.3)\quad \sum_{i=1}^{p-1}i^mS'_{p-2-m}(|ik|)t^i&\equiv\varphi_{m+1}((-1)^kt)B'_{p-1-m}\\ &\quad+\Big\{\sum_{i=1}^{p-1}(-1)^{\alpha(ik)}\{1-(-1)^{[ik/p]}\}i^mt^i\Big\}B'_{p-1-m}\ (\operatorname{mod} p)\,.\end{aligned}$$

In particular, if we take $m=0$ and $k=1$ in (4.3), then

$$\sum_{i=1}^{p-1}S'_{p-2}(i)t^i\equiv\varphi_1(-t)B'_{p-1}\equiv\left\{\frac{t^p+1}{t+1}-1\right\}B'_{p-1}\equiv 0\ (\operatorname{mod} p)\,,$$

because $t\not\equiv -1\ (\operatorname{mod} p)$ and $B'_{p-1}\in\mathbb{Z}_p$. On the other hand, by Lemma 5,

$$\begin{aligned}(4.4)\quad (t+1)\sum_{i=1}^{p-1}S'_{p-2}(i)t^i&=\sum_{i=1}^{p-1}\{S'_{p-2}(i)+S'_{p-2}(i-1)\}t^i+S'_{p-2}(p-1)t^p\\ &\equiv\varphi_{p-1}(t)-2q_p(2)t\equiv -2q_p(2)t\ (\operatorname{mod} p)\,.\end{aligned}$$

Consequently, assuming that $t\in W$ is a solution of the system (K′) we get $q_p(2)\equiv 0\ (\operatorname{mod} p)$ (see also the proof in [1]).

(1) (K′) ⇒(I′). Take $m=1$ in (4.3). Since $B'_{p-2}=0$, we know that $t\in W$ is a solution of (I′).

(2) (I′) ⇒(K′). By Lemma 6 the assertion clearly follows from (4.2) with $m=1$.

(3) (K′) ⇒(II′). Since $B'_{p-1-m}=0$ for $m=1,3,\ldots,p-4$, we see from (4.3) that $t\in W$ is a solution of (II′) $(m=1,3,\ldots,p-4)$ for a fixed k with $1\le k\le p-1$.

(4) (II′) ⇒(K′). By taking successively $m=p-4,\ p-6,\ldots,1$ in (4.2) we obtain the result, since $B'_{2i+1}=0$ $(i\ge 1)$.

(5) (K′) ⇒(III′). We take $m = 0$ in (4.3):

$$\begin{aligned}(4.5)\quad &\sum_{i=1}^{p-1} S'_{p-2}(|ik|)t^i \\ &\equiv \varphi_1((-1)^k t)B'_{p-1} + \Big\{\sum_{i=1}^{p-1} (-1)^{\alpha(ik)}\{1-(-1)^{[ik/p]}\}t^i\Big\}B'_{p-1} \pmod p\,.\end{aligned}$$

Here $B'_{p-1} \equiv -q_p(2) \equiv 0 \pmod p$, as stated above. Therefore,

$$\sum_{i=1}^{p-1} S'_{p-2}(|ik|)t^i \equiv 0 \pmod p\,, \tag{4.6}$$

i.e., $t \in W$ is a solution of the system (III′).

(6) (III′) ⇒(K′). We see from (4.4) that if $t \in W$ is a solution of (III′), then $q_p(2) \equiv 0 \pmod p$. Hence, by (4.2) with $m = 0$ it follows that

$$\begin{aligned}&\tfrac{1}{2}k^{p-2}\varphi_{p-1}(t) - \sum_{i=1}^{p-2}\binom{p-2}{i}k^{p-2-i}\{B'_{i+1}\varphi_{p-1-i}(t)\} \\ &\equiv \sum_{i=1}^{p-1} S'_{p-2}(|ik|)t^i - \varphi_1((-1)^k t)B'_{p-1} \\ &\quad - \Big\{\sum_{i=1}^{p-1}(-1)^{\alpha(ik)}\{1-(-1)^{[ik/p]}\}t^i\Big\}B'_{p-1} \\ &\equiv \sum_{i=1}^{p-1} S'_{p-2}(|ik|)t^i + q_p(2)\Big\{\varphi_1((-1)^k t) + \sum_{i=1}^{p-1}(-1)^{\alpha(ik)}\{1-(-1)^{[ik/p]}\}t^i\Big\} \\ &\equiv 0 \pmod p\,.\end{aligned}$$

By Lemma 6 the assertion follows.

(7) (K′) ⇒(IV′). If $t \in W$ is a solution of (K′), then we may assume that (4.6) holds.

Since $S'_{p-2}(p-1) \equiv -2q_p(2) \pmod p$ by Lemma 5, we have, for each $a = 1, 2, \ldots, p-1$,

$$\begin{aligned}(4.7)\quad S'_{p-2}(a) &\equiv (-1)^{a-1}\sum_{i=1}^{p-1-a}(-1)^{a+i}(a+i)^{p-2} + (-1)^{a-1}2q_p(2) \\ &\equiv -S'_{p-2}(p-1-a) + (-1)^{a-1}2q_p(2) \\ &\equiv S'_{p-2}(p-a) + a^{p-2} + (-1)^{a-1}2q_p(2) \\ &\equiv -S'_{p-2}(a-1) + a^{p-2} \pmod p\,.\end{aligned}$$

Let $P'_k(X)$ and $Q'_k(X)$ be the polynomials defined by

$$P'_k(X) = \sum_{l=1}^{p-1} S'_{p-2}(|lk|)X^l \quad (1 \le k \le p-1)\,,$$
$$Q'_k(X) = \begin{cases} \sum_{l=1}^{\overline{k}-1} S'_{p-2}(|lk|)X^l & (1 \le k \le p-2)\,, \\ 0 \quad (k = p-1)\,. \end{cases}$$

Since $S_{p-2}(|\overline{k}k|) = S_{p-2}(p-1) \equiv -2q_p(2) \pmod{p}$, we can write

$$P'_k(X) \equiv Q'_k(X) - 2q_p(2)X^{\overline{k}} + X^{\overline{k}}\Big\{ \sum_{j=1}^{p-\overline{k}-1} S'_{p-2}(|(\overline{k}+j)k|)X^j \Big\} \pmod{p}\,.$$

By (4.7) we have

$$\begin{aligned} S'_{p-2}(|(\overline{k}+j)k|) &\equiv S'_{p-2}(|jk|-1) \equiv -S'_{p-2}(p-|jk|) + (-1)^{|jk|}2q_p(2) \\ &\equiv\ - S'_{p-2}(|j(p-k)|) + (-1)^{|jk|}2q_p(2) \pmod{p}\,. \end{aligned}$$

Also $\overline{p-k} = p - \overline{k}$, hence

$$\begin{aligned} (4.8) \qquad & \sum_{j=1}^{p-\overline{k}-1} S'_{p-2}(|(\overline{k}+j)k|)X^j \\ & \qquad \equiv -Q'_{p-k}(X) + 2q_p(2) \sum_{j=1}^{p-\overline{k}-1} (-1)^{|jk|}X^j \pmod{p}\,, \end{aligned}$$

which gives

$$\begin{aligned} (4.9) \qquad P'_k(X) &\equiv Q'_k(X) - X^{\overline{k}}Q'_{p-k}(X) \\ & \quad + 2q_p(2)\Big\{ \sum_{j=1}^{p-\overline{k}-1} (-1)^{|jk|}X^j - 1 \Big\} X^{\overline{k}} \pmod{p}\,. \end{aligned}$$

On the other hand, since

$$S'_{p-2}(|jk|-1) = S'_{p-2}(|(\overline{k}+j)k|)\,,$$
$$S'_{p-2}(|(p-\overline{k})k|-1) = S'_{p-2}(0) = 0$$

and

$$S'_{p-2}(|(p-\overline{k}+i)k|-1) = S'_{p-2}(|ik|)\,,$$

using again (4.7) we obtain

$$P'_k(X) \equiv\ - \sum_{l=1}^{p-1} S'_{p-2}(|lk|-1)X^l - \overline{k}\varphi_{p-1}(X)$$

$$\equiv -\sum_{j=1}^{p-\overline{k}-1} S'_{p-2}(|(\overline{k}+j)k|)X^j - X^{p-\overline{k}}\Big\{\sum_{i=1}^{\overline{k}-1} S'_{p-2}(|ik|)X^i\Big\}$$
$$-\,\overline{k}\varphi_{p-1}(X) \pmod p\,.$$

Therefore, from (4.8),

$$P'_k(X) \equiv Q'_{p-k}(X) - X^{p-\overline{k}}Q'_k(X) - \overline{k}\varphi_{p-1}(X) - 2q_p(2)\sum_{j=1}^{p-\overline{k}-1}(-1)^{|jk|}X^j \pmod p\,. \tag{4.10}$$

Assume that $t \in W$ is a solution of (K′). Then, as stated above, $q_p(2) \equiv 0 \pmod p$ and $P'_k(t) \equiv 0 \pmod p$. So, from (4.9) and (4.10) we obtain

$$(t^p - 1)Q'_k(t) \equiv (t-1)Q'_k(t) \equiv 0 \pmod p\,.$$

Since $t \not\equiv 1 \pmod p$, it follows that

$$Q'_k(t) \equiv 0 \pmod p \qquad (1 \le k \le p-2)\,.$$

(8) (IV′) ⇒(K′). Using (4.7) we have

$$S'_{p-2}((p-1)/2) \equiv (-1)^{(p-3)/2}q_p(2) \pmod p\,,$$

which gives

$$Q'_2(X) \equiv S'_{p-2}((p-1)/2)X \equiv (-1)^{(p-3)/2}q_p(2)X \pmod p\,.$$

This shows that if $t \in W$ is a solution of (IV′), then $q_p(2) \equiv 0 \pmod p$ because $t \not\equiv 0 \pmod p$. Hence from (4.9) we deduce $P'_k(t) \equiv 0 \pmod p$. By the same argument as in (6) we see that $t \in W$ is a solution of (K′).

This completes the proof of Theorem 2. ■

5. Some propositions. In this section we shall give some propositions relating to the equation (1.1), which are consequences of the Kummer–Mirimanoff congruences and the theorems proved above.

(i) It is clear from (3.8) and (3.9) that a relation between $Q_k(X)$ and $Q_{p-k}(X)$ may be given by

$$(1 - X^{p-\overline{k}})Q_k(X) - (1 - X^{\overline{k}})Q_{p-k}(X) \equiv -\overline{k}\varphi_{p-1}(X) \pmod p\,,$$

that is,

$$\frac{1 - X^{p-\overline{k}}}{1-X}Q_k(X) - \frac{1 - X^{\overline{k}}}{1-X}Q_{p-k}(X) \equiv -\overline{k}Q_1(X) \pmod p\,. \tag{5.1}$$

On the other hand, we can show

$$Q_k(1) \equiv -\overline{k}q_p(\overline{k}) \pmod p\,. \tag{5.2}$$

In fact, by (3.7) and Lemma 3 we have

$$\begin{aligned} S_{p-2}(|ik|) &\equiv S_{p-2}(p-1-|ik|) \equiv -\sum_{j=0}^{p-2}\binom{p-1}{j}B_j(-ik)^{p-1-j} \\ &\equiv -\sum_{j=0}^{p-2}\binom{p-1}{j}(\overline{k}^{\,j}B_j)i^{p-1-j} \pmod{p}, \end{aligned}$$

hence by Lemma 1,

$$\begin{aligned} Q_k(1) &\equiv -\Big[B(\overline{k}v)\Big\{\sum_{i=0}^{\overline{k}-1}e^{iv}\Big\}\Big]_0^{(p-1)} + \binom{p-1}{p-1}\overline{k}^{\,p}B_{p-1} \\ &= -[\overline{k}B(v)]_0^{(p-1)} + \overline{k}^{\,p}B_{p-1} = (\overline{k}^{\,p}-\overline{k})B_{p-1} \equiv -\overline{k}q_p(\overline{k}) \pmod{p}, \end{aligned}$$

i.e., (5.2) holds (see also Proposition 3 in [11]).

Set $X = 1$ in (5.1). Then from (5.2),

$$-(p-\overline{k})\overline{k}q_p(\overline{k}) + \overline{k}(p-\overline{k})q_p(p-\overline{k}) \equiv \overline{k}(p-1)q_p(p-1) \equiv -\overline{k} \pmod{p},$$

which gives, for $\overline{k} = \alpha$,

$$q_p(\alpha) - q_p(p-\alpha) \equiv \overline{\alpha} \pmod{p} \quad (1 \le \alpha \le p-1).$$

This is, however, nothing but a special case of Lemma 7.

Furthermore, we can deduce

$$Q_k(-1) \equiv \frac{1+(-1)^{\overline{k}}}{2}\overline{k}q_p(2) \pmod{p}.$$

To prove this, consider the identity

$$B(\overline{k}v)\sum_{i=0}^{\overline{k}-1}(-1)^{i+1}e^{iv} = (-1)^{\overline{k}}\overline{k}vU(v) - \{1-(-1)^{\overline{k}}\}B(\overline{k}v)U(v).$$

Here we have

$$\begin{aligned} &\Big[B(\overline{k}v)\sum_{i=0}^{\overline{k}-1}(-1)^{i+1}e^{iv}\Big]_0^{(p-1)} \\ &= \sum_{j=0}^{p-2}\binom{p-1}{j}(\overline{k}^{j}B_j)\Big\{\sum_{i=1}^{\overline{k}-1}(-1)^{i+1}i^{p-1-j}\Big\} - \binom{p-1}{p-1}\overline{k}^{\,p-1}B_{p-1}\frac{1-(-1)^{\overline{k}}}{2}, \end{aligned}$$

and also, since $B_jB'_{p-j} = 0$ unless $j = 1$ or $p-1$, and $B'_{p-1} \equiv -q_p(2) \pmod{p}$,

$$\big[(-1)^{\overline{k}}\overline{k}vU(v) - \{1-(-1)^{\overline{k}}\}B(\overline{k}v)U(v)\big]_0^{(p-1)}$$

$$= (-1)^{\overline{k}}\overline{k}(p-1)B'_{p-1} - \{1-(-1)^{\overline{k}}\}\sum_{j=0}^{p-1}\binom{p-1}{j}\overline{k}^{\,j}B_jB'_{p-j}$$

$$\equiv (-1)^{\overline{k}}\overline{k}q_p(2) - \frac{1-(-1)^{\overline{k}}}{2}\left\{\binom{p-1}{1}\overline{k}q_p(2) + \binom{p-1}{p-1}\overline{k}^{\,p-1}B_{p-1}\right\}$$

$$\equiv \frac{1+(-1)^{\overline{k}}}{2}\overline{k}q_p(2) - \frac{1-(-1)^{\overline{k}}}{2}\overline{k}^{\,p-1}B_{p-1} \pmod{p}.$$

Hence from the above identity

$$Q_k(-1) = \sum_{i=1}^{\overline{k}-1}(-1)^iS_{p-2}(|ik|) \equiv \sum_{i=1}^{\overline{k}-1}(-1)^{i+1}\left\{\sum_{j=0}^{p-2}\binom{p-1}{j}(\overline{k}^{\,j}B_j)i^{p-1-j}\right\}$$

$$\equiv \frac{1+(-1)^{\overline{k}}}{2}\overline{k}q_p(2) \pmod{p}.$$

As an immediate consequence of the assertion of Theorem 1 for the system (IV), the simple proofs of the Wieferich and Mirimanoff criteria for (1.1) are now given.

Proposition 1. *Let $p > 3$. If the equation* (1.1) *holds*, *then*

$$q_p(2) \equiv 0 \pmod{p} \quad \text{and} \quad q_p(3) \equiv 0 \pmod{p}.$$

Proof. By (5.2) we have

$$Q_{\overline{2}}(t) \equiv Q_{\overline{2}}(1)t \equiv -2q_p(2)t \equiv 0 \pmod{p}$$

and

$$\begin{aligned} Q_{\overline{3}}(t) &\equiv \tfrac{1}{2}\{Q_{\overline{3}}(1) - Q_{\overline{3}}(-1)\}t + \tfrac{1}{2}\{Q_{\overline{3}}(1) + Q_{\overline{3}}(-1)\}t^2 \\ &\equiv -\tfrac{3}{2}q_p(3)t(1+t) \equiv 0 \pmod{p}, \end{aligned}$$

which gives $q_p(2) \equiv q_p(3) \equiv 0 \pmod{p}$, because $t(1+t) \not\equiv 0 \pmod{p}$. ■

If ${}^{\#}H = 3$, then a more precise condition for $q_p(2)$ than in Proposition 1 may be given, namely if the equation (1.1) holds and ${}^{\#}H = 3$, then $q_p(2) \equiv 0 \pmod{p^3}$. The proof is as follows:

It is well known since Fleck that if (1.1) holds, then

$$x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \equiv 1 \pmod{p^3} \quad \text{(see e.g. [10])}. \tag{5.3}$$

Suppose that ${}^{\#}H = 3$, i.e., $H \equiv \{-1, 2, 1/2\} \pmod{p}$. If $t = -y/x \equiv -1 \pmod{p}$, then $y^p \equiv x^p \pmod{p^2}$. Using (5.3) repeatedly we have $y \equiv x \pmod{p^2}$, hence $y^p \equiv x^p \pmod{p^3}$, and so $y \equiv x \pmod{p^3}$. This gives $y^p \equiv x^p \pmod{p^4}$, therefore $0 = x^p + y^p + z^p \equiv 2x^p + z^p \pmod{p^4}$. Since $x^{p(p-1)} \equiv z^{p(p-1)} \equiv 1 \pmod{p^4}$, we have $2^{p-1} \equiv 2^{p-1}x^{p(p-1)} \equiv (-z^p)^{p-1} \equiv 1 \pmod{p^4}$. If $t = -y/x \equiv 2 \pmod{p}$, then $y^p \equiv -2^px^p \pmod{p^2}$. By Proposition 1 and (5.3) this implies $0 = x^p+y^p+z^p \equiv (1-2^p)x^p+z^p \equiv -x+z$

$(\bmod p^2)$, hence $x^p \equiv z^p \pmod{p^3}$, which gives $x \equiv z \pmod{p^3}$, and so $x^p \equiv z^p \pmod{p^4}$. Therefore $0 = x^p + y^p + z^p \equiv y^p + 2z^p \pmod{p^4}$, hence $2^{p-1} \equiv 2^{p-1}z^{p(p-1)} \equiv (-y^p)^{p-1} \equiv 1 \pmod{p^4}$. By symmetry we also have the same result for the case $t \equiv 1/2 \pmod{p}$.

Several other criteria for the equation (1.1) of type similar to Proposition 1 have been successively obtained by various authors (Frobenius, Vandiver, Pollaczek, Morishima and others). These Fermat quotient criteria are deduced as consequences of the Kummer–Mirimanoff congruences. However, to get them with larger bases we need a refined argument and an intricate computation.

We now suppose that if the equation (1.1) holds, then

$$q_p(r_i) \equiv 0 \pmod{p}, \qquad i = 1, 2, \ldots, m,$$

where r_i is the ith prime (i.e., $r_1 = 2$, $r_2 = 3$, $r_3 = 5, \ldots$) with $r_i < p$. Here, assume that r_m is the largest known prime today satisfying the above congruence as a criterion of (1.1).

Consider the sets

$$G = \Big\{ \prod_{i=1}^{m} r_i^{e_i} \mid e_i \geq 0 \ (i = 1, 2, \ldots, m) \Big\}$$

and

$$N = \{-1, 1\} \cup \{u \in \mathbb{Z} \mid q_p(u) \not\equiv 0 \pmod{p} \text{ and } p \nmid u\}.$$

Proposition 2. *Let p be an odd prime and s be a positive integer prime to p. If there exist integers $a, b \in G$ and $k, l \in N$ such that*

$$sp = ak + bl \quad \text{and} \quad q_p(k) - q_p(l) \not\equiv -\frac{s}{ak} \pmod{p},$$

then the equation (1.1) *has no solution for the exponent p.*

Proof. Since $a, b \in G$ and $q_p(ij) \equiv q_p(i) + q_p(j) \pmod{p}$ if $p \nmid ij$, taking $\alpha = ak$ in Lemma 7 we have

$$q_p(ak) - q_p(sp - ak) \equiv q_p(k) - q_p(l) \equiv -\frac{s}{ak} \pmod{p},$$

contrary to the assumption. ∎

As an example, take $s = k = 1$ and $l = \pm 1$ in Proposition 2. If p can be written in the form $p = a \pm b$ $(a, b \in G)$, then we know that (1.1) has no solution for the exponent p. This has already been proved by various authors. However, the question whether there are infinitely many primes in the set $\{a \pm b \mid a, b \in G\}$ is still open.

Proposition 3. *Let p be an odd prime and let s_1, s_2 be positive integers prime to p. If there exist integers $a_i, b_i \in G$ $(i = 1, 2)$ and $k, l \in N$ such that*

$$s_1 p = a_1 k + b_1 l\,, \qquad s_2 p = a_2 k + b_2 l \qquad \textit{and} \qquad s_1 a_2 \not\equiv s_2 a_1 \pmod{p}\,,$$

then the equation (1.1) *has no solution for the exponent p.*

Proof. Similarly to the proof of Proposition 2,

$$q_p(k) - q_p(l) \equiv -\frac{s_i}{a_i k} \pmod{p} \qquad (i = 1, 2)\,.$$

From these congruences for $i = 1$ and 2 we have $s_1 a_2 \equiv s_2 a_1 \pmod{p}$, contrary to the assumption. ∎

We note that the condition $s_1 a_2 \not\equiv s_2 a_1 \pmod{p}$ in the above proposition is equivalent to $s_1 b_2 \not\equiv s_2 b_1 \pmod{p}$.

On the other hand, we can state

Proposition 4. *If the equation* (1.1) *holds, then $t \in W$ is a solution of the systems of congruences*

$$\sum_{i=1}^{p-1} (-1)^{|ik|} \binom{p-1}{|ik|} X^i \equiv 0 \pmod{p^2} \qquad (1 \le k \le p-1)\,, \tag{V}$$

$$\sum_{i=1}^{\overline{k}-1} (-1)^{|ik|} \binom{p-1}{|ik|} X^i \equiv \sum_{i=1}^{\overline{k}-1} X^i \pmod{p^2} \qquad (1 \le k \le p-2)\,. \tag{VI}$$

Proof. By (5.3) it follows that $\varphi_1(t) = (t^p - t)/(t-1) \equiv 0 \pmod{p^3}$. Also we have

$$\begin{aligned}\binom{p-1}{|ik|} &\equiv (-1)^{|ik|} + (-1)^{|ik|-1} p\left(1 + \frac{1}{2} + \ldots + \frac{1}{|ik|}\right) \\ &\equiv (-1)^{|ik|}\{1 - pS_{p-2}(|ik|)\} \pmod{p^2}\,.\end{aligned}$$

Since $P_k(t) \equiv 0 \pmod{p}$ and $Q_k(t) \equiv 0 \pmod{p}$ by Theorem 1, this gives

$$\sum_{i=1}^{p-1} (-1)^{|ik|} \binom{p-1}{|ik|} t^i \equiv \varphi_1(t) - pP_k(t) \equiv 0 \pmod{p^2}$$

and

$$\sum_{i=1}^{\overline{k}-1} (-1)^{|ik|} \binom{p-1}{|ik|} t^i \equiv \sum_{i=1}^{\overline{k}-1} t^i - pQ_k(t) \equiv \sum_{i=1}^{\overline{k}-1} t^i \pmod{p^2}\,. \tag{5.4}$$

So the assertion follows. ∎

We may rewrite the above system (V) as follows:

$$\sum_{i=1}^{p-1} (-1)^i \binom{p-1}{i} X^{|ik|} \equiv 0 \pmod{p^2} \qquad (1 \le k \le p-1)\,.$$

Indeed, if k' is an integer such that $k'k \equiv 1 \pmod p$ and $1 \le k' \le p-1$, and if $j = |ik|$, then $|jk'| \equiv ikk' \equiv i \pmod p$, which shows that the statement is true.

We can derive the following expression for the Fermat quotient modulo p, for $r = 2, 3, \ldots, p-1$:

$$q_p(r) \equiv \frac{1}{rp}\left\{\sum_{i=1}^{r-1} (-1)^{|i\overline{r}|}\binom{p-1}{|i\overline{r}|} - (r-1)\right\} \pmod p\,. \tag{5.5}$$

In fact, from the first relation in (5.4),

$$\sum_{i=1}^{\overline{k}-1} (-1)^{|ik|}\binom{p-1}{|ik|} \equiv \overline{k} - 1 - pQ_k(1) \pmod{p^2}\,.$$

Letting $\overline{k} = r$ (so $k = \overline{r}$), by (5.2) we obtain the result.

In particular, take $r = 2$ (so $\overline{r} = (p-1)/2$) in (5.5):

$$q_p(2) \equiv \frac{1}{2p}\left\{(-1)^{(p-1)/2}\binom{p-1}{(p-1)/2} - 1\right\} \pmod p\,.$$

Here we have

$$\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2}\{1 - pS_{p-2}((p-1)/2)\} \pmod{p^2}\,,$$

which gives

$$q_p(2) \equiv -\tfrac{1}{2}S_{p-2}([p/2]) \pmod p\,. \tag{5.6}$$

Next, take $r = 3$ in (5.5). If $p \equiv 1 \pmod 3$, then $\overline{r} = (p-1)/3$. Since $\overline{r}$ is even, we have

$$\begin{aligned} q_p(3) &\equiv \frac{1}{3p}\left\{\binom{p-1}{(p-1)/3} + \binom{p-1}{2(p-1)/3} - 2\right\} \\ &= \frac{2}{3p}\left\{\binom{p-1}{(p-1)/3} - 1\right\} \equiv -\tfrac{2}{3}S_{p-2}((p-1)/3) \pmod p\,. \end{aligned}$$

If $p \equiv 2 \pmod 3$, then $\overline{r} = (2p-1)/3$, which is odd. Hence

$$\begin{aligned} q_p(3) &\equiv \frac{1}{3p}\left\{-\binom{p-1}{(2p-1)/3} - \binom{p-1}{(p-2)/3} - 2\right\} \\ &= -\frac{2}{3p}\left\{\binom{p-1}{(p-2)/3} + 1\right\} \equiv -\tfrac{2}{3}S_{p-2}((p-1)/3) \pmod p\,. \end{aligned}$$

Consequently, for any odd prime $p > 3$ we have

$$q_p(3) \equiv -\tfrac{2}{3}S_{p-2}([p/3]) \pmod p\,. \tag{5.7}$$

More generally, if r is an odd integer with $3 \le r \le p-2$, then

$$q_p(r) \equiv -\frac{2}{r} \sum_{i=1}^{(r-1)/2} S_{p-2}(\delta(i,r)) \ (\operatorname{mod} p)\,,$$

where $\delta(i,r) \in \{|i\overline{r}|, |(r-i)\overline{r}|\}$, and if r is an even integer with $4 \le r \le p-1$, then

$$q_p(r) \equiv -\frac{1}{r}\Big\{2 \sum_{i=1}^{r/2-1} S_{p-2}(\delta(i,r)) + S_{p-2}(|(r/2)\overline{r}|)\Big\} \ (\operatorname{mod} p)\,. \tag{5.8}$$

These congruences easily follow from (5.5), because $p-1-|i\overline{r}| = |(r-i)\overline{r}|$ and hence

$$\binom{p-1}{|i\overline{r}|} = \binom{p-1}{|(r-i)\overline{r}|} \equiv (-1)^{\delta(i,r)}\{1 - pS_{p-2}(\delta(i,r))\} \ (\operatorname{mod} p^2)\,.$$

Of course, we may deduce the above expressions for $q_p(r)$ directly from (5.2).

Using (5.6), (5.7) and (5.8) we now arrive at Lehmer's criteria from [8]:

PROPOSITION 5. *Let* $p > 3$. *If the equation* (1.1) *holds*, *then for* $n = 2,3,4$ *and* 6

$$S_{p-2}([p/n]) \equiv 0 \ (\operatorname{mod} p)\,.$$

Proof. By Proposition 1, $q_p(2) \equiv q_p(3) \equiv 0 \ (\operatorname{mod} p)$, hence we see from (5.6) and (5.7) that the result follows for $n = 2$ and 3. Let $r = 4$. If $p \equiv 1 \ (\operatorname{mod} 4)$, then $\overline{r} = (p-1)/4$, so $|\overline{r}| = [p/4]$ and $|(r/2)\overline{r}| = [p/2]$. If $p \equiv 3 \ (\operatorname{mod} 4)$, then $\overline{r} = (3p-1)/4$, so $|(r-1)\overline{r}| = [p/4]$ and $|(r/2)\overline{r}| = [p/2]$. Hence from (5.8),

$$q_p(4) \equiv -\tfrac{1}{4}\{2S_{p-2}([p/4]) + S_{p-2}([p/2])\} \ (\operatorname{mod} p)\,.$$

Next let $r = 6$. If $p \equiv 1 \ (\operatorname{mod} 6)$, then $\overline{r} = (p-1)/6$, so $|\overline{r}| = [p/6]$, $|2\overline{r}| = [p/3]$ and $|(r/2)\overline{r}| = [p/2]$. Similarly, if $p \equiv 5 \ (\operatorname{mod} 6)$, then $\overline{r} = (5p-1)/6$, so $|(r-1)\overline{r}| = [p/6]$, $|(r-2)\overline{r}| = [p/3]$ and $|(r/2)\overline{r}| = [p/2]$. Therefore we have, from (5.8),

$$q_p(6) \equiv -\tfrac{1}{6}\{2\{S_{p-2}([p/6]) + S_{p-2}([p/3])\} + S_{p-2}([p/2])\} \ (\operatorname{mod} p)\,.$$

Since $q_p(ij) \equiv q_p(i) + q_p(j) \ (\operatorname{mod} p)$, we deduce $q_p(4) \equiv q_p(6) \equiv 0 \ (\operatorname{mod} p)$, which shows, by the above congruences, that the result follows also for $n = 4$ and 6. ■

Lehmer [8] has proved this proposition in another way.

Incidentally, from the congruences in the proof above we obtain

$$S_{p-2}([p/4]) \equiv -3q_p(2) \ (\operatorname{mod} p)\,,$$
$$S_{p-2}([p/6]) \equiv -2q_p(2) - \tfrac{3}{2}q_p(3) \ (\operatorname{mod} p)\,.$$

Further, assuming the Frobenius–Vandiver criterion $q_p(5) \equiv 0 \pmod{p}$ (cf. [10]) for (1.1) with $p > 5$ we can derive the same statement as in Proposition 5 also for $n = 5$, i.e., $S_{p-2}([p/5]) \equiv 0 \pmod{p}$. For brevity, set $c_i = S_{p-2}(|\overline{5}i|)$ $(i = 1, 2, 3, 4)$. Since $\deg(Q_{\overline{5}}(X)) = 4$, if $Q_{\overline{5}}(t) \equiv 0 \pmod{p}$ for all $t \in H$ and $c_i \not\equiv 0 \pmod{p}$ for at least one of $i = 1, 2, 3, 4$, it follows that ${}^{\#}H \neq 6$, i.e., ${}^{\#}H = 3$. If $q_p(5) \equiv 0 \pmod{p}$ and ${}^{\#}H = 3$, i.e., $H \equiv \{-1, 2, 1/2\} \pmod{p}$, then

$$\begin{aligned} Q_{\overline{5}}(1) &= c_1 + c_2 + c_3 + c_4 \equiv -5q_p(5) \equiv 0 \pmod{p}\,, \\ Q_{\overline{5}}(-1) &= -c_1 + c_2 - c_3 + c_4 \equiv \{(1 + (-1)^5)/2\} q_p(2) \equiv 0 \pmod{p}\,, \\ (1/2)Q_{\overline{5}}(2) &= c_1 + 2c_2 + 4c_3 + 8c_4 \equiv 0 \pmod{p}\,, \\ 2^4 Q_{\overline{5}}(1/2) &= 8c_1 + 4c_2 + 2c_3 + c_4 \equiv 0 \pmod{p}\,. \end{aligned}$$

Since

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 2 & 4 & 8 \\ 8 & 4 & 2 & 1 \end{pmatrix} = 2 \cdot 3^3 \not\equiv 0 \pmod{p}\,,$$

it follows that $c_1 \equiv c_2 \equiv c_3 \equiv c_4 \equiv 0 \pmod{p}$. For each case $p \equiv 1, 2, 3$ and $4 \pmod 5$ we have $\overline{5} = (p-1)/5$, $(3p-1)/5, (2p-1)/5$ and $(4p-1)/5$, respectively. Therefore, $[p/5] \in \{|\overline{5}i| \mid i = 1, 2, 3, 4\}$, i.e.,

$$S_{p-2}([p/5]) \in \{c_i \mid i = 1, 2, 3, 4\}$$

for all $p > 5$, which shows $S_{p-2}([p/5]) \equiv 0 \pmod{p}$.

Conversely, it is easy to show that $S_{p-2}([p/5]) \equiv 0 \pmod{p}$ implies $q_p(5) \equiv 0 \pmod{p}$.

If $p > 5$ and ${}^{\#}H = 6$, then $c_i \equiv 0 \pmod{p}$ for all $i = 1, 2, 3, 4$. So we have $Q_{\overline{5}}(1) \equiv 0 \pmod{p}$, which gives $q_p(5) \equiv 0 \pmod{p}$ by (5.2). In this case it is also obvious that $S_{p-2}([p/5]) \equiv 0 \pmod{p}$.

By observing in particular the case $m = -1$ in (3.1) we know that (K) is equivalent to the following Fueter system (see (VI) and (VII) in [5], and also Theorem 3 in [3]):

$$\text{(F)} \qquad \begin{cases} \displaystyle\sum_{i=1}^{p-1} q_p(i) X^i \equiv 0 \pmod{p}\,, \\ \displaystyle\sum_{i=1}^{p-1} \frac{1}{i} \left[\frac{ik}{p}\right] X^i \equiv 0 \pmod{p} \quad (2 \leq k \leq p-1)\,. \end{cases}$$

(ii) From (4.9) and (4.10) we may give a relation between $Q'_k(X)$ and

$Q'_{p-k}(X)$:

$$(5.9)\qquad (1+X^{p-\overline{k}})Q'_k(X)-(1+X^{\overline{k}})Q'_{p-k}(X)$$
$$\equiv\ -\overline{k}\varphi_{p-1}(X)+2q_p(2)X^{\overline{k}}$$
$$-\ 2q_p(2)(1+X^{\overline{k}})\sum_{j=1}^{p-\overline{k}-1}(-1)^{|jk|}X^j \pmod p\,.$$

For $k=1,2,\ldots,p-2$ we can show

$$(5.10)\qquad Q'_k(1)\equiv -q_p(2)\Big\{\sum_{i=1}^{\overline{k}-1}(-1)^{|ik|}\Big\} \pmod p\,.$$

In fact, from Lemma 3 and (4.7) it follows that

$$\begin{aligned}S'_{p-2}(|ik|) =&\ -S'_{p-2}(p-1-|ik|)-(-1)^{|ik|}2q_p(2)\\ =&\ -\sum_{l=0}^{p-3}\binom{p-2}{l}B'_{l+1}(p-|ik|)^{p-2-l}\\ &-\{1+(-1)^{|ik|}\}B'_{p-1}-(-1)^{|ik|}2q_p(2)\\ \equiv&\ -\sum_{l=0}^{p-3}\binom{p-2}{l}B'_{l+1}\overline{k}^{\,l+1}i^{p-2-l}\\ &+\{1-(-1)^{|ik|}\}q_p(2) \pmod p\,.\end{aligned}$$

We now use the identity

$$(5.11)\qquad vU(\overline{k}v)\Big\{\sum_{i=0}^{\overline{k}-1}e^{iv}\Big\}=B(v)-2U(\overline{k}v)B(v)\,.$$

Since $[U(\overline{k}v)]_0^{(m)}=\overline{k}^{\,m}B'_{m+1}$ for $m\ge 0$, it follows that

$$\begin{aligned}&\Big[vU(\overline{k}v)\Big\{\sum_{i=0}^{\overline{k}-1}e^{iv}\Big\}\Big]_0^{(p-1)}=(p-1)\Big[U(\overline{k}v)\Big\{\sum_{i=0}^{\overline{k}-1}e^{iv}\Big\}\Big]_0^{(p-2)}\\ &\quad=(p-1)\Big\{\sum_{l=0}^{p-3}\binom{p-2}{l}\overline{k}^{l}B'_{l+1}\Big(\sum_{i=1}^{\overline{k}-1}i^{p-2-l}\Big)+\overline{k}^{\,p-1}B'_{p-1}\Big\}\\ &\quad\equiv-\sum_{l=0}^{p-3}\binom{p-2}{l}\overline{k}^{l}B'_{l+1}\Big(\sum_{i=1}^{\overline{k}-1}i^{p-2-l}\Big)+q_p(2) \pmod p\,.\end{aligned}$$

On the other hand, since $B'_{j+1}B_{p-1-j}=0$ unless $j=0$ or $p-2$,

$$\begin{aligned}[B(v)-2U(\overline{k}v)B(v)]_0^{(p-1)} &= B_{p-1}-2\sum_{j=0}^{p-1}\binom{p-1}{j}\overline{k}^{\,j}B'_{j+1}B_{p-1-j}\\ &= B_{p-1}-2\Big\{\binom{p-1}{0}B'_1B_{p-1}+\binom{p-1}{p-2}\overline{k}^{\,p-2}B'_{p-1}B_1\Big\}\\ &\equiv \overline{k}^{\,p-2}q_p(2)\ (\operatorname{mod} p)\,.\end{aligned}$$

Therefore, from (5.11),

$$\begin{aligned}\sum_{l=0}^{p-3}\binom{p-2}{l}\overline{k}^{\,l+1}B'_{l+1}\Big(\sum_{i=1}^{\overline{k}-1}i^{p-2-l}\Big) &\equiv \overline{k}(1-\overline{k}^{p-2})q_p(2)\\ &\equiv (\overline{k}-1)q_p(2)\ (\operatorname{mod} p)\,,\end{aligned}$$

which implies

$$\begin{aligned}Q'_k(1)=\sum_{i=1}^{\overline{k}-1}S'_{p-2}(|ik|) &\equiv (1-\overline{k})q_p(2)+\sum_{i=1}^{\overline{k}-1}\{1-(-1)^{|ik|}\}q_p(2)\\ &= -q_p(2)\Big\{\sum_{i=1}^{\overline{k}-1}(-1)^{|ik|}\Big\}\ (\operatorname{mod} p)\,,\end{aligned}$$

as required.

Furthermore, for $k=1,2,\ldots,p-1$ we obtain

$$Q'_k(-1)\equiv q_p(2)\Big\{\frac{1-(-1)^{\overline{k}}}{2}(\overline{k}-1)-\sum_{i=1}^{\overline{k}-1}(-1)^{|ik|+i}\Big\}\ (\operatorname{mod} p)\,. \tag{5.12}$$

To prove this we use the following identity:

$$\overline{k}U(\overline{k}v)\Big\{\sum_{i=0}^{\overline{k}-1}(-1)^i e^{iv}\Big\}=(-1)^{\overline{k}-1}\overline{k}U(v)+\{1+(-1)^{\overline{k}}\}\overline{k}U(\overline{k}v)U(v)\,.$$

Since $[\overline{k}U(\overline{k}v)]_0^{(m)}=\overline{k}^{\,m+1}B'_{m+1}$ $(m\geq 0)$, we have

$$\begin{aligned}\Big[\overline{k}U(\overline{k}v)\Big\{\sum_{i=0}^{\overline{k}-1}(-1)^i e^{iv}\Big\}\Big]_0^{(p-2)} &= \sum_{l=0}^{p-3}\binom{p-2}{l}\overline{k}^{\,l+1}B'_{l+1}\Big\{\sum_{i=1}^{\overline{k}-1}(-1)^i i^{p-2-l}\Big\}\\ &\quad+\binom{p-2}{p-2}\overline{k}^{\,p-1}B'_{p-1}\Big\{\frac{1-(-1)^{\overline{k}}}{2}\Big\}\,,\end{aligned}$$

and also

$$\begin{aligned}&[(-1)^{\overline{k}-1}\overline{k}U(v)+\{1+(-1)^{\overline{k}}\}\overline{k}U(\overline{k}v)U(v)]_0^{(p-2)}\\ &\qquad=(-1)^{\overline{k}-1}\overline{k}B'_{p-1}+\{1+(-1)^{\overline{k}}\}\sum_{l=0}^{p-2}\binom{p-2}{l}\overline{k}^{\,l+1}B'_{l+1}B'_{p-1-l}\,.\end{aligned}$$

Hence it follows that

$$\begin{aligned}Q'_k(-1)&=\sum_{i=1}^{\overline{k}-1}S'_{p-2}(|ik|)(-1)^i\\ &\equiv-\sum_{i=1}^{\overline{k}-1}\sum_{l=0}^{p-3}\binom{p-2}{l}\overline{k}^{\,l+1}B'_{l+1}(-1)^i i^{p-2-l}+q_p(2)\sum_{i=1}^{\overline{k}-1}\{1-(-1)^{|ik|}\}(-1)^i\\ &\equiv q_p(2)\bigg\{\frac{1-(-1)^{\overline{k}}}{2}\overline{k}+(-1)^{\overline{k}}\bigg\}+q_p(2)\sum_{i=1}^{\overline{k}-1}\{1-(-1)^{|ik|}\}(-1)^i\\ &\equiv q_p(2)\bigg\{\frac{1-(-1)^{\overline{k}}}{2}(\overline{k}-1)-\sum_{i=1}^{\overline{k}-1}(-1)^{|ik|+i}\bigg\}\ (\operatorname{mod}p)\,,\end{aligned}$$

i.e., (5.12) is proved.

We immediately conclude from (5.12) that if $\overline{k}$ is even, then

$$Q'_k(-1)\equiv-q_p(2)\bigg\{\sum_{i=1}^{\overline{k}-1}(-1)^{|ik|+i}\bigg\}\ (\operatorname{mod}p)\,. \tag{5.13}$$

Independently of the above argument, we may infer from (5.9) that if $\overline{k}$ is odd, then

$$Q'_k(-1)\equiv q_p(2)(\overline{k}-1)\ (\operatorname{mod}p)\,. \tag{5.14}$$

PROPOSITION 6. *If the equation* (1.1) *holds*, *then* $Q'_k(1)\equiv 0\ (\operatorname{mod}p)$ *and* $Q'_k(-1)\equiv 0\ (\operatorname{mod}p)$ *for* $k=1,2,\ldots,p-2$.

Proof. Since $q_p(2)\equiv 0\ (\operatorname{mod}p)$ by Proposition 1, the result is immediate from (5.10), (5.13) and (5.14). ■

From (4.1) we may deduce that (K′) is equivalent to the system of congruences

$$\sum_{i=1}^{p-1}i^m S'_{p-2-m}(ik)X^i\equiv 0\ (\operatorname{mod}p)\qquad(1\le m\le p-3)\,,$$

where k is any fixed even integer with $2\le k\le p-1$.

This fact can be easily seen by taking successively $m=p-3,p-4,\ldots,1$ in (4.1).

In [2] we treated a special case for $m = -1$ in (4.1) and proved that $t \in W$ is a solution of (K$'$) if and only if t is a solution of the system of congruences

$$\text{(A)} \qquad \sum_{i=1}^{p-1} \frac{\varepsilon_{ik}}{i} X^i \equiv 0 \pmod{p} \qquad (1 \le k \le p-1),$$

where $\varepsilon_n = 1$ if $|n|$ is odd and $\varepsilon_n = 0$ otherwise, i.e., $\varepsilon_n = \{1 - (-1)^{|n|}\}/2$.

The system (A) essentially coincides with the following variation, due to Granville (see Theorem L3-(h) in [6]), of Benneton's system from [4]:

$$\text{(BG)} \qquad \sum_{\substack{i=1 \\ |ik|>[p/2]}}^{p-1} \frac{1}{i} X^i \equiv 0 \pmod{p} \qquad (1 \le k \le p-1).$$

References

[1] T. Agoh, *On the criteria of Wieferich and Mirimanoff*, C. R. Math. Rep. Acad. Sci. Canada 8 (1986), 49–52.

[2] —, *On Fermat's last theorem*, ibid. 11 (1990), 11–15.

[3] —, *On the Kummer–Mirimanoff congruences*, Acta Arith. 55 (1990), 141–156.

[4] G. Benneton, *Sur le dernier théorème de Fermat*, Ann. Sci. Univ. Besançon Math. 3 (1974), 15 pp.

[5] R. Fueter, *Kummers Kriterium zum letzten Theorem von Fermat*, Math. Ann. 85 (1922), 11–20.

[6] A. J. Granville, *Diophantine equations with varying exponents* (*with special reference to Fermat's last theorem*), Ph.D. thesis, Queen's Univ., 1989, 206 pp.

[7] E. E. Kummer, *Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen, für den Fall, daß die Klassenanzahl durch λ theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Abhandl. Königl. Akad. Wiss. Berlin 1857, 41–74.

[8] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. 39 (1938), 350–360.

[9] D. Mirimanoff, *L'équation indéterminée $x^l + y^l + z^l = 0$ et le critérium de Kummer*, J. Reine Angew. Math. 128 (1905), 45–68.

[10] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, New York 1979.

[11] F. Thaine, *On the first case of Fermat's last theorem*, J. Number Theory 20 (1985), 128–142.

DEPARTMENT OF MATHEMATICS
SCIENCE UNIVERSITY OF TOKYO
NODA CHIBA, 278 JAPAN

Received on 9.9.1991
and in revised form on 8.10.1991 (2169)