Reported originally at Genova Univ. (Italy) on June 5, 1996.

SOME SIMPLE IDEAS FOR FAMOUS PROBLEMS

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093
People's Republic of China
E-mail: zwsun@nju.edu.cn
Homepage: http://pweb.nju.edu.cn/zwsun

1. The Least Positive kth Power Nonresidue mod p

Let p be an odd prime and k a positive integer with $(k, p-1) > 1$. A famous problem is to evaluate the smallest positive kth power nonresidue $n_k(p)$ modulo p. By Pólya's estimate for character sums $n_k(p) < \sqrt{p}\log p$ (see L. K. Hua's book 'Introduction to Number Theory', Springer-Verlag, 1982). The estimate of Pólya was later improved by D. A. Burgess in 1957, thus one can show that $n_k(p) = O(p^{1/A+\varepsilon})$ where $A = 4e^{1-1/(k,p-1)}$ (see Y. Wang, On the estimation of character sums and its applications, Sci. Record (N.S.), 7(1964),78–83).

Here we introduce a simple elementary method due to myself.

Let n be $n_k(p)$ or $n_k(p)-1$ according to whether -1 is a kth power residue mod p. Note that $-n$ is a kth power nonresidue mod p. For $i = 1, \cdots, n_k(p)-1$, clearly $p - in$ is a kth power nonresidue mod p; if $p - in > 0$ then we must have $p - in \geqslant n_k(p) \geqslant n$ and hence $p-(i+1)n > 0$ since p is a prime. As $p - n > 0$, by the above $p - n_k(p)n > 0$ and so

$$p > n_k(p)(n_k(p)-1) + \frac{1}{4} = \left(n_k(p) - \frac{1}{2}\right)^2, \quad \text{i.e. } n_k(p) < \sqrt{p} + \frac{1}{2}.$$

2. On Odd Integers not of the Form $2^n + p$

In 1849 A. de Polignac conjectured that sufficiently large odd integers are of the form $2^n + p$ where n is a positive integer and p is a prime. In 1950 P. Erdös proved that there are infinitely many odd positive integers for which the conjecture fails. In his ingenious proof he introduced the concept of cover of $\mathbb{Z}$.

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ we let

$$a(n) = a + n\mathbb{Z} = \{x \in \mathbb{Z} :\ x \equiv a \pmod{n}\}.$$

It will be called a residue class (with modulus n) or an arithmetic sequence (with difference n). A finite system

$$A = \{a_s(n_s)\}_{s=1}^k \tag{1}$$

of such sets is said to be a cover or covering system (CS) (of $\mathbb{Z}$) if each integer lies in at least one of the classes in (1).

Erdös [1950, Summa Brasil. Math.; MR 13,437]: *There is an infinite arithmetic progression of odd integers no term of which is of the form $2^n + p$, where $n \in \mathbb{N} = \{0, 1, 2, \cdots\}$ and p is an odd prime.*

In the proof of Erdös, the common difference is $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 31 \cdot 241$.

Let

$$a_1 = 0,\ a_2 = 0,\ a_3 = 1,\ a_4 = 3,\ a_5 = 7,\ \ a_6 = 23;$$

$$n_1 = 2,\ n_2 = 3,\ n_3 = 4,\ n_4 = 8,\ n_5 = 12,\ n_6 = 24.$$

It is easy to check that $A = \{a_s(n_s)\}_{s=1}^6$ forms a cover of $\mathbb{Z}$ with distinct moduli. For each $s = 1, \cdots, 6$ we can choose a primitive prime factor p_s of $2^{n_s} - 1$, in fact we may let $p_1 = 3,\ p_2 = 7,\ p_3 = 5,\ p_4 = 17,\ p_5 = 13,\ p_6 = 241$.

Let x be any integer satisfying the following congruences:

$$x \equiv 1 \pmod{2},\ x \equiv 3 \pmod{31},\ x \equiv 2^{a_s} \pmod{p_s}\ (s = 1, \cdots, 6).$$

As $|\{2^n + p_s \bmod 31 :\ n \in \mathbb{N},\ 1 \leqslant s \leqslant 6\}| \leqslant 5 \times 6$, there is an $r \in \mathbb{Z}$ such that $2^n + p_s \not\equiv r \pmod{31}$ for all $n \in \mathbb{N}$ and $s = 1, \cdots, 6$, in fact we can take $r = 3$.

Suppose that $x = 2^n + p$ where $n \in \mathbb{N}$ and p is an odd prime. Since A is a cover of $\mathbb{Z}$, for some $s = 1, \cdots, 6$ we have $n \equiv a_s \pmod{n_s}$ and hence $p = p_s$ because

$$p = x - 2^n = x - 2^{a_s}(2^{n_s})^{\frac{n-a_s}{n_s}} \equiv x - 2^{a_s} \cdot 1 \equiv 0 \pmod{p_s}.$$

But no $x - p_s$ with $(1 \leqslant s \leqslant 6)$ can equal 2^n because $x \equiv 3 \not\equiv 2^n + p_s \pmod{31}$. This contradiction ends the proof.

In this direction some other important things are as follows.

R. Crocker [1971, Pacific J. Math.]: *There are infinitely many positive odd integers not of the form* $2^u + 2^v + p$ *where* u, v *are positive integers and* p *is an odd prime.*

J. L. Selfrige [Richard K. Guy, Unsolved Problems in Number Theory, 1994, 2ed.]: One of 3,5,7,13,17,19,73 always divides $78557 \cdot 2^n + 1$.

Z. W. Sun [Proc. Amer. Math. Soc. 128(2000)]: *If*

$$x \equiv 47867742232066880047611079 \pmod{M}$$

where M *is a 29-digit number given by*

$$\prod_{p \leqslant 19} p \times 31 \times 37 \times 41 \times 61 \times 73 \times 97 \times 109 \times 151 \times 241 \times 257 \times 331$$
$$= 66483084961588510124010691590,$$

then x *is not of the form* $\pm p^a \pm q^b$ *where* p, q *are primes and* a, b *are nonnegative integers.*

Z. W. Sun and M. H. Le [Acta Arith. 99(2001)]: *If* $n > 3$, *then* $2^{2^n} - 1 \neq 2^a + 2^b + p^\alpha$ *where* $a, b, \alpha \in \mathbb{N}$, $a \neq b$ *and* p *is a prime.*

Open Questions [Erdös,1981, Recent Progress in Analytic Number Theory; R.K. Guy, 1981,A19]: *Whether for some* r *every integer can be written in the form*

$p+2^{u_1}+\cdots+2^{u_s}$ with $s\leqslant r$? Whether every $n\not\equiv 0$ (mod 4) is of the form $2^k+\theta$ where θ is squarefree?

3. Covers with Distinct Moduli Cannot Be Exact

Let $N=[n_1,\cdots,n_k]$. Observe that

$$\left|\left\{0\leqslant x<N:\ x\in\bigcup_{s=1}^k a_s(n_s)\right\}\right|\leqslant\sum_{s=1}^k|\{0\leqslant x<N:\ x\in a_s(n_s)\}|=\sum_{s=1}^k\frac{N}{n_s}.$$

So, when (1) forms a cover we have $\sum_{s=1}^k\frac{1}{n_s}\geqslant 1$ and the equality holds if and only if (1) covers each integer exactly once.

Soon after his invention of CS, Erdös made the following conjecture.

Erdös' Conjecture. *If system*

$$A=\{a_s(n_s)\}_{s=1}^k\quad(1<n_1<\cdots<n_k)\tag{2}$$

forms a cover of $\mathbb{Z}$, then $\sum_{s=1}^k\frac{1}{n_s}>1$, i.e. (2) covers some integer more than once.

Davenport-Mirsky-Newman-Rado [1950's, see Guy,1981, F14]. *If*

$$A=\{a_s(n_s)\}_{s=1}^k\quad(1<n_1\leqslant\cdots\leqslant n_{k-1}\leqslant n_k)\tag{3}$$

covers each integer exactly once then $n_{k-1}=n_k$.

Proof. Without loss of generality we let $0\leqslant a_s<n_s$ $(1\leqslant s\leqslant k)$. For $|z|<1$ we have

$$\sum_{s=1}^k\frac{z^{a_s}}{1-z^{n_s}}=\sum_{s=1}^k\sum_{q=0}^\infty z^{a_s+qn_s}=\sum_{n=0}^\infty z^n=\frac{1}{1-z}.$$

If $n_{k-1}<n_k$ then

$$\infty=\lim_{\substack{z\to e^{2\pi i/n_k}\\|z|<1}}\frac{z^{a_k}}{1-z^{n_k}}=\lim_{\substack{z\to e^{2\pi i/n_k}\\|z|<1}}\left(\frac{1}{1-z}-\sum_{s=1}^{k-1}\frac{z^{a_s}}{1-z^{n_s}}\right)<\infty,$$

a contradiction!

Observe that (3) is an exact cover if and only if $\sum_{s=1}^{k} \chi_s(x) \equiv 1$ where

$$\chi_s(x) = \begin{cases} 1, & \text{if } x \equiv a_s \pmod{n_s}; \\ 0, & \text{otherwise.} \end{cases}$$

Sun [1991, J. Nanjing Univ. (Nat. Sci. Edi.)]. *For $s = 1, \cdots, k$ let ψ_s be an arithmetical function periodic mod n_s such that $\sum_{r=0}^{n_s-1} \psi_s(r)\xi^r \neq 0$ for some primitive n_sth root ξ of unity. If $[n_1, \cdots, n_k]$ is not the smallest positive period of the function $\psi = \psi_1 + \cdots + \psi_k$ then there must exist some s, t such that $n_s = n_t$ and $\psi_s \neq \psi_t$.*

A nice generalization of Erdös' conjecture is

Herzög-Schönheim's Conjecture [1974, Canad. Math. Bull.]. *Let G be a group and $G_1, \cdots, G_k$ its subgroups of distinct indices. Then, for any $a_1, \cdots, a_k \in G$ system*

$$\{a_s G_s\}_{s=1}^{k} \tag{4}$$

cannot be an exact cover (i.e. a partition) of G.

M.A.Berger-A.Felzenbaum-A.S.Fraenkel [1986, Canad. Math. Bull.; 1987, Fund. Math.]. *The H-S conjecture holds for finite nilpotent groups and supersolvable groups.*

Z. W. Sun [*On the Herzog-Schönheim conjecture for uniform covers of groups*, J. Algebra, 2004]: *Let G be a group and $G_1, \cdots, G_k$ its subnormal subgroups with $[G : G_1] \leqslant \cdots \leqslant [G : G_k]$ such that (4) covers each element of G with the same multiplicity for some $a_1, \cdots, a_k \in G$. Then the indices $[G : G_1], \cdots, [G : G_k]$ cannot be distinct unless $k = 1$, and if each of them occurs at most $M \geq 2$ times then the (natural) logarithm of the smallest index $[G : G_1]$ is not more than $\frac{e^\gamma}{\log 2} M \log^2 M + O(M \log M \log\log M)$ where the O-constant is absolute.*

4. Some Local-Global Results

S. K. Stein's Conjecture [1958, Math. Ann., MR 20#17]: *If (2) is disjoint* *(i.e. the residue classes in (2) are pairwise disjoint) then there is an integer* $x \notin \bigcup_{s=1}^{k} a_s(n_s)$ *with* $1 \leqslant x \leqslant 2^k$.

Erdös [1962, Mat. Lapok 13, MR 33#4020]: Stein's conjecture is true if 2^k is replaced by $k \cdot 2^k$.

Erdös' Conjecture: *If* $A = \{a_s(n_s)\}_{s=1}^{k}$ *covers integers from 1 to* 2^k *then it is a cover.*

R. B. Crittenden–C.L.Vanden Eynden [1969, Bull. Amer. Math. Soc., MR 40#2596; 1970, Proc. Amer. Math. Soc., MR 41#3365]: The Erdös conjecture holds.

It should be mentioned that the proof given by Critten-Vanden Eynden is long, indirect and awkward. Since $\{2^{s-1}(2^s)\}_{s=1}^{k}$ covers $\{1, 2, \cdots, 2^k - 1\}$ but does not cover $0(2^k)$, 2^k above is best possible.

Crittenden-Eynden's Conjecture: *Let* $A = \{a_s(n_s)\}_{s=1}^{k}$ *where* $k, n_1, \cdots, n_k$ *are integers greater than a given nonnegative integer* l*. Then* A *forms a cover whenever it covers integers from 1 to* $2^{k-l}(l+1)$.

Observe that the system consisting of residue classes

$$r(m)\ (r = 1, \cdots, m-1), \quad 2^{s-1}m(2^s m)\ (s = 1, \cdots, k-m+1)$$

covers integers from 1 to $2^{k-m+1}m - 1$, but does not cover $2^{k-m+1}m$. So if the Crittenden-Eynden conjecture holds it's best possible in some sense.

Since 1989 some progress has happened dramatically.

M. Z. Zhang [1989, J. Sichuan Univ.]: *If* $A = \{a_s(n_s)\}_{s=1}^{k}$ *forms a cover then* $\sum_{i \in I} \frac{1}{n_i} \in \mathbb{Z}^+$ *for some* $I \subseteq \{1, \cdots, k\}$.

Proof.(Zhang) For $s > 1$ we have

$$\begin{aligned}
0 &= \sum_{n=1}^{\infty} \frac{1}{n_s} \prod_{t=1}^{k} \left(1 - e^{2\pi i \frac{n+a_t}{n_t}}\right) \\
&= \sum_{n=1}^{\infty} \frac{1}{n^s} \left(1 + \sum_{\emptyset \neq I \subseteq \{1,\cdots,k\}} (-1)^{|I|} e^{2\pi i \sum_{t\in I} \frac{n+a_t}{n_t}}\right) \\
&= \zeta(s) + \sum_{\emptyset \neq I \subseteq \{1,\cdots,k\}} (-1)^{|I|} e^{2\pi i \sum_{t\in I} \frac{a_t}{n_t}} \sum_{n=1}^{\infty} \frac{e^{2\pi i n \sum_{t\in I} 1/n_t}}{n^s}.
\end{aligned}$$

If $\sum_{t\in I} \frac{1}{n_t} \notin \mathbb{Z}^+$ for all $I \subseteq \{1,\cdots,k\}$ then

$$\infty = \lim_{s\to 1+0} \zeta(s) = - \sum_{\emptyset \neq I \subseteq \{1,\cdots,k\}} (-1)^{|I|} e^{2\pi i \sum_{t\in I} \frac{a_t}{n_t}} \sum_{n=1}^{\infty} \frac{1}{n} e^{2\pi i n \sum_{t\in I} \frac{1}{n_t}} < \infty,$$

a contradiction!

Sun [1992, Israel J. Math.]: *Let $A = \{a_s(n_s)\}_{s=1}^{k}$ be an exact m-cover. Then for each $n = 0, 1, \cdots, m$ there exist at least $\binom{m}{n}$ subsets I of $\{1, \cdots, k\}$ such that $\sum_{i\in I} \frac{1}{n_s}$ equals n. The bounds $\binom{m}{n}$ $(0 \leqslant n \leqslant m)$ are best possible.*

Inspired by these work, soon Sun obtained the following surprising result:

Sun [Acta Arith. 72(1995)]: *For system*

$$\mathcal{A} = \{\alpha_s + \beta_s \mathbb{Z}\}_{s=1}^{k} \quad \text{where } \alpha_1, \cdots, \alpha_k \in \mathbb{R} \text{ and } \beta_1, \cdots, \beta_k \in \mathbb{R}^+, \tag{5}$$

it forms an m-cover of $\mathbb{Z}$ (i.e. each integer is covered at least m times) if it covers $|S|$ consecutive integers at least m times where

$$S = \left\{ \left\{ \sum_{s\in I} \frac{1}{\beta_s} \right\} : \ I \subseteq \{1, \cdots, k\} \right\}.$$

Let's prove this in the case $m = 1$.

Note that $x \in \mathbb{Z}$ is covered by $\mathcal{A}$ if and only if

$$\begin{aligned}
0 &= \prod_{s=1}^{k} \left(1 - e^{2\pi i (\alpha_s - x)/\beta_s}\right) \\
&= \sum_{I \subseteq \{1,\cdots,k\}} (-1)^{|I|} e^{2\pi i \sum_{s\in I} \alpha_s/\beta_s} \left(e^{-2\pi i \sum_{s\in I} 1/\beta_s}\right)^x .
\end{aligned}$$

So

$$\begin{aligned}
&\mathcal{A} \text{ covers } |S| \text{ consecutive integers } x, x+1, \cdots, x+|S| \\
\iff & \sum_{I\subseteq\{1,\cdots,k\}} (-1)^{|I|} e^{2\pi i \sum_{s\in I}\frac{\alpha_s}{\beta_s}} \left(e^{-2\pi i\sum_{s\in I}\frac{1}{\beta_s}}\right)^{x+j} = 0 \text{ for } j = 0, \cdots, |S|-1 \\
\iff & \sum_{\theta\in S} \sum_{\substack{I\subseteq\{1,\cdots,k\} \\ \{\sum_{s\in I}\frac{1}{\beta_s}\}=\theta}} (-1)^{|I|} e^{2\pi i\sum_{s\in I}\frac{\alpha_s}{\beta_s}} \left(e^{-2\pi i\theta}\right)^j = 0 \text{ for } j = 0, 1, \cdots, |S|-1 \\
\iff & \sum_{\substack{I\subseteq\{1,\cdots,k\} \\ \{\sum_{s\in I}\frac{1}{\beta_s}\}=\theta}} (-1)^{|I|} e^{2\pi i\sum_{s\in I}\frac{\alpha_s}{\beta_s}} = 0 \text{ for all } \theta \in S \\
\iff & \sum_{I\subseteq\{1,\cdots,k\}} (-1)^{|I|} e^{2\pi i\sum_{s\in I}\frac{\alpha_s}{\beta_s}} \left(e^{-2\pi i\sum_{s\in I}\frac{1}{\beta_s}}\right)^{q} = 0 \ \text{ for all } q\in\mathbb{Z} \\
\iff & \mathcal{A} \text{ covers every integer } q.
\end{aligned}$$

It follows from the above result that

Sun [Acta Arith. 72(1995)]: *Let $k \geqslant l \geqslant 0$ be integers. Then $2^{k-l}(l+1)$ is the smallest $n \in \mathbb{Z}^+$ such that any system of k residue classes with at least l equal moduli forms an m-cover whenever it covers n consecutive integers at least m times.*

5. Equivalence of Two Systems

For a finite system $A = \{a_s(n_s)\}_{s=1}^k$ of residue classes we define its covering map $w_A : \mathbb{Z} \to \mathbb{Z}$ as follows:

$$w_A(x) = |\{1 \leqslant s \leqslant k :\ x \equiv a_s \pmod{n_s}\}|$$

If two such systems A and B have the same covering map then we say that they are equivalent which is written as $A \sim B$. Notice that A forms an exact cover if and only if $A \sim \{0(1)\}$, in particular $\{r(n)\}_{r=0}^{n-1} \sim \{0(1)\}$.

Znám [1975, Acta Arith.] *Let $A = \{a_s(n_s)\}_{s=1}^k$ $(0 \leqslant a_s < n_s)$ and $B = \{b_t(m_t)\}_{t=1}^l$ $(0 \leqslant b_t < m_t)$. If $n_1 < \cdots < n_k$, $m_1 < \cdots < m_l$ and $\{a_s(n_s)\}_{s=1}^k \sim \{b_t(m_t)\}_{t=1}^l$ then $A = B$.*

Sun [Nanjing Univ. J. Math. Biquarterly., 1989; J. Algebra, 2001] *Let F be a complex-valued function F such that $\left(\frac{x+r}{n}, ny\right) \in Dom(F)$ for all $r = 0, 1, \cdots, n-1$ whenever $(x, y) \in Dom(F)$ and $n \in \mathbb{Z}^+$. Then the following statements are equivalent:*

(a) Whenever $\{a_s(n_s)\}_{s=1}^k \sim \{b_t(m_t)\}_{t=1}^l$,

$$\sum_{s=1}^k F\left(\frac{x+a_s}{n_s}, n_s y\right) = \sum_{t=1}^l F\left(\frac{x+b_t}{m_t}, m_t y\right) \quad \text{for all } (x,y) \in Dom(F).$$

(b) For all $(x, y) \in Dom(F)$ and $n \in \mathbb{Z}^+$ we have

$$\sum_{r=0}^{n-1} F\left(\frac{x+r}{n}, ny\right) = F(x, y).$$

If function F has the above required property then we call it a uniform function.

There are many uniform functions.

An identity of Hermite is as follows:

$$\sum_{r=0}^{n-1} \left[x + \frac{r}{n}\right] = [nx] \qquad \text{for } x \in \mathbb{R} \text{ and } n \in \mathbb{Z}^+.$$

This shows that $F(x, y) = [x]$ is a uniform function.

Let m be a nonnegative integer and $B_m(x)$ the mth Bernoulli polynomial. A theorem of Rabbe states that

$$\sum_{r=0}^{n} B_m\left(z + \frac{r}{n}\right) = n^{1-m} B_m(nz) \quad \text{for } n \in \mathbb{Z}^+ \text{ and } z \in \mathbb{C},$$

i.e. $G(x, y)$ is a uniform function where $G(x, y) = B_m(x) y^{m-1}$.

Let

$$f(x, y) = \Gamma(x) y^{x-\frac{1}{2}} / \sqrt{2\pi} \qquad \text{for } x \neq 0, -1, -2, \cdots \text{ and } y > 0.$$

The multiplication formula of Gauss says that

$$\prod_{r=0}^{n-1} \Gamma\left(z + \frac{r}{n}\right) = (2\pi)^{\frac{n-1}{2}} n^{\frac{1}{2}-nz} \Gamma(nz) \quad \text{for } n \in \mathbb{Z}^+ \text{ and } z \neq 0, -1, -2, \cdots.$$

Equivalently, $\log f$ is a uniform function where

$$f(x, y) = \Gamma(x) y^{x-\frac{1}{2}} / \sqrt{2\pi} \qquad \text{for } x, y > 0.$$

6. On $B_{p-1}(a/q) - B_{p-1} \pmod p$

In this section we introduce recent work of A. Granville and Sun [Pacific J. Math. 117(1996)].

It has long been known that the nth Bernoulli polynomial $B_n(t)$, where

$$B_n(t) = \sum_{k=0}^{n} \binom{n}{k} B_k t^{n-k}$$

and B_k, the kth Bernoulli number, defined by the power series

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!} \ ,$$

take 'special' values at certain rational numbers with small denominators:

$$\begin{aligned} B_n(1) = B_n(0) &= B_n \quad \text{for } n \neq 1 \\ B_n\left(\frac{1}{2}\right) &= (2^{1-n} - 1)B_n; \end{aligned} \tag{1}$$

and for all even $n \geq 2$,

$$\begin{aligned} B_n\left(\frac{1}{3}\right) &= B_n\left(\frac{2}{3}\right) = (3^{1-n} - 1)\frac{B_n}{2}, \\ B_n\left(\frac{1}{4}\right) &= B_n\left(\frac{3}{4}\right) = (4^{1-n} - 2^{1-n})\frac{B_n}{2}, \\ B_n\left(\frac{1}{6}\right) &= B_n\left(\frac{5}{6}\right) = (6^{1-n} - 3^{1-n} - 2^{1-n} + 1)\frac{B_n}{2}. \end{aligned} \tag{2}$$

It is not known if $B_n(a/q)$ has as simple a 'closed form' for any other rational a/q with $1 \leq a \leq q-1$ and $(a, q) = 1$, though this has long been considered an interesting question.

In 1938 E. Lehmer [Ann. Math.] showed amongst other things that (1) and (2) imply

$$\begin{aligned} &B_{p-1}\left(\frac{1}{2}\right) - B_{p-1} \equiv \frac{2^p - 2}{p} \pmod p \\ &B_{p-1}\left(\frac{1}{3}\right) - B_{p-1} \equiv B_{p-1}\left(\frac{2}{3}\right) - B_{p-1} \equiv \frac{1}{2} \cdot \frac{3^p - 3}{p} \pmod p \\ &B_{p-1}\left(\frac{1}{4}\right) - B_{p-1} \equiv B_{p-1}\left(\frac{3}{4}\right) - B_{p-1} \equiv \frac{3}{2} \cdot \frac{2^p - 2}{p} \pmod p \\ &B_{p-1}\left(\frac{1}{6}\right) - B_{p-1} \equiv B_{p-1}\left(\frac{5}{6}\right) - B_{p-1} \equiv \frac{1}{2} \cdot \frac{3^p - 3}{p} + \frac{2^p - 2}{p} \pmod p \end{aligned} \tag{3}$$

The two important things to note about (3) are that,

(i): We've evaluated $B_{p-1}(\frac{a}{q}) - B_{p-1} \pmod p$ where $\varphi(q) = 1$ or 2 (φ is Euler's totient function);

(ii): Each of the terms of the right hand side, like 2^p, 3^p, are numbers taken from a first-order linear recurrence sequence ($u_{n+1} = 2u_n$ and $u_{n+1} = 3u_n$ respectively).

The next class of examples are those q for which $\varphi(q) = 4$, namely $q = 5, 8, 10, 12$.

Theorem (A. Granville and Z. W. Sun, 1996)**.** *Let p be an odd prime relatively prime to a fixed $q \in \{5, 8, 10, 12\}$. Then we can determine $B_{p-1}(a/q) - B_{p-1}$ mod p (with $1 \le a \le q$ and $(a, q) = 1$) as follows:*

$$B_{p-1}\left(\frac{a}{5}\right) - B_{p-1} \equiv \frac{5}{4}\left(\left(\frac{ap}{5}\right)\frac{1}{p}F_{p-(\frac{5}{p})} + \frac{5^{p-1}-1}{p}\right) \pmod p;$$
$$B_{p-1}\left(\frac{a}{8}\right) - B_{p-1} \equiv \left(\frac{2}{ap}\right)\frac{2}{p}P_{p-(\frac{2}{p})} + 4 \cdot \frac{2^{p-1}-1}{p} \pmod p;$$
$$B_{p-1}\left(\frac{a}{10}\right) - B_{p-1} \equiv \frac{15}{4}\left(\frac{ap}{5}\right)\frac{1}{p}F_{p-(\frac{5}{p})} + \frac{5}{4} \cdot \frac{5^{p-1}-1}{p} + \frac{2(2^{p-1}-1)}{p} \pmod p;$$
$$B_{p-1}\left(\frac{a}{12}\right) - B_{p-1} \equiv \left(\frac{3}{a}\right)\frac{3}{p}S_{p-(\frac{3}{p})} + \frac{3(2^{p-1}-1)}{p} + \frac{3}{2} \cdot \frac{3^{p-1}-1}{p} \pmod p;$$

where $(-)$ is the Jacobi symbol, and we define the following second-order linear recurrence sequences:

$$F_0 = 0,\ F_1 = 1,\ \textit{and } F_{n+2} = F_{n+1} + F_n \quad \textit{for all } n \ge 0$$

$$P_0 = 0,\ P_1 = 1,\ \textit{and } P_{n+2} = 2P_{n+1} + P_n \quad \textit{for all } n \ge 0$$

$$S_0 = 0,\ S_1 = 1,\ \textit{and } S_{n+2} = 4S_{n+1} - S_n \quad \textit{for all } n \ge 0.$$

In general Granville and Sun showed that $B_{p-1}(a/q) - B_{p-1} \equiv q(U_p - 1)/(2p) \pmod p$, where U_n is a certain linear recurrence of order $[q/2]$ which depends only on a, q and the least positive residue of $p \pmod q$. This can be re-written as a sum of linear recurrence sequences of order $\le \varphi(q)/2$.