Proc. Edinburgh Math. Soc. 45(2002), no. 1, 155–160

A NOTE ON INTEGERS OF THE FORM $2^n + cp$

Zhi-Wei Sun and Si-Man Yang

In 1950 P. Erdös proved that if $x \equiv 2036812 \pmod{5592405}$ and $x \equiv 3 \pmod{62}$ then x is not of the form $2^n + p$ where n is a nonnegative integer and p is a prime. In this note we present a theorem on integers of the form $2^n + cp$, in particular we completely determine all those integers c relatively prime to 5592405 such that the residue class 2036812(mod 5592405) contains integers of the form $2^n + cp$.

In 1849 A. de Polignac [P] claimed that any sufficiently large odd integer is of the form $2^n + p$ where n is a nonnegative integer and p is a prime. P. Erdös [E1] proved that any integer congruent to 2036812 modulo 5592405 and 3 modulo 62 cannot be the sum of a power of two and a prime, a clear proof of this result was presented by W. Sierpiński [S]. (See [C], [G], [GS] and [S2] for further developments.) In his ingenious proof, Erdös introduced the concept of cover of $\mathbb{Z}$. For $a, n \in \mathbb{Z}$ with $n > 0$ we put

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

and call it a *residue class* (with *modulus* n). A finite system

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

of such classes is said to be a *cover* (of $\mathbb{Z}$) if $\bigcup_{s=1}^k a_s(\text{mod } n_s) = \mathbb{Z}$. If (1) forms a cover but none of its proper subsystems does, then we say that (1) is a *minimal cover*. For problems and results concerning covers of $\mathbb{Z}$, one may see Erdös [E2], R.K. Guy [Gu] and the introduction of [S1].

A well-known result of A.S. Bang [B] (also rediscovered by K. Zsigmondy [Z], G.D. Birkhoff and H.S. Vandiver [BV]) states that for each integer $n > 1$ with $n \neq 6$, there exists a prime factor of $2^n - 1$ not dividing $2^m - 1$ for any $0 < m < n$, such a prime is called a *primitive* (*prime*) *divisor* of $2^n - 1$. In [R] the reader can find all prime divisors of $2^n - 1$ with $n \leqslant 22$.

Our main result in this note is as follows:

2000 *Mathematics Subject Classification.* Primary 11P32; Secondary 11A07, 11B25, 11B75.

The first author is responsible for all the communications, and supported by the Teaching and Research Award Program for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of P. R. China.

Theorem. *Let (1) be a minimal cover with* $0 \leqslant a_s < n_s$ *for* $s = 1, \cdots, k$. *Suppose that distinct primes* $p_1, \cdots, p_k$ *are primitive divisors of* $2^{n_1} - 1, \cdots, 2^{n_k} - 1$ *respectively. Put* $\bigcap_{s=1}^k 2^{a_s} (\mathrm{mod}\ p_s) = a (\mathrm{mod}\ d)$ *where* $a \in \mathbb{Z}$ *and* $d = p_1 \cdots p_k$, *and write*

$$(2) \qquad \Big(a_t (\mathrm{mod}\ n_t) \setminus \bigcup_{\substack{s=1 \\ s \neq t}}^{k} a_s (\mathrm{mod}\ n_s)\Big) \cap \{0, 1, \cdots, N-1\} = \{b_1^{(t)}, \cdots, b_{l_t}^{(t)}\}$$

for $t = 1, \cdots, k$ *where* N *is the least common multiple* $[n_1, \cdots, n_k]$ *of the moduli* $n_1, \cdots, n_k$. *Set*

$$(3) \qquad S(A) = \bigcup_{t=1}^{k} \bigcup_{j=1}^{l_t} \frac{a - 2^{b_j^{(t)}}}{p_t} \left(\mathrm{mod}\ \frac{d}{p_t}\right)$$

where all the $(a - 2^{b_j^{(t)}})/p_t$ *are integers. Then an integer* c *divisible by none of* $p_1, \cdots, p_k$ *belongs to* $S(A)$ *if and only if* $a(\mathrm{mod}\ d)$ *contains integers of the form* $2^n + cp$ *where* $n \geqslant 0$ *is an integer and* p *is a prime.*

Proof. Let $1 \leqslant t \leqslant k$ and $1 \leqslant j \leqslant l_t$. Since $b_j^{(t)} \equiv a_t \ (\mathrm{mod}\ n_t)$, $a \equiv 2^{a_t} \equiv 2^{b_j^{(t)}} \ (\mathrm{mod}\ p_t)$. Let $c \equiv (a - 2^{b_j^{(t)}})/p_t \ (\mathrm{mod}\ d/p_t)$.

Since $d = p_1 \cdots p_k$ divides $2^N - 1$, for any nonnegative integer $n \equiv b_j^{(t)} \ (\mathrm{mod}\ N)$ we have

$$2^n + cp_t \equiv 2^{b_j^{(t)}} + cp_t \equiv a \ (\mathrm{mod}\ d).$$

Next we prove the sufficiency. Let c be an integer relatively prime to d. Suppose that $2^n + cp \equiv a \ (\mathrm{mod}\ d)$ for some integer $n \geqslant 0$ and prime p. Since (1) forms a cover, $n \equiv a_t \ (\mathrm{mod}\ n_t)$ for some $1 \leqslant t \leqslant k$. Observe that $2^n \equiv 2^{a_t} \equiv a \ (\mathrm{mod}\ p_t)$. So $p_t \mid cp$ and hence $p = p_t$. For any $s = 1, \cdots, k$ with $s \neq t$, we have $p \neq p_s$ and thus $n \not\equiv a_s \ (\mathrm{mod}\ n_s)$. Therefore $n \equiv b_j^{(t)} \ (\mathrm{mod}\ N)$ for some $j = 1, \cdots, l_t$. It follows that

$$cp_t = cp \equiv a - 2^n \equiv a - 2^{b_j^{(t)}} \ (\mathrm{mod}\ d),$$

i.e.

$$c \equiv \frac{a - 2^{b_j^{(t)}}}{p_t} \left(\mathrm{mod}\ \frac{d}{p_t}\right).$$

So $c \in S(A)$.

The proof is now complete. □

Remark 1. Note that $(a - 2^{b_j^{(t)}})/p_t$ is relatively prime to d/p_t, for, if $1 \leqslant s \leqslant k$ and $s \neq t$ then $b_j^{(t)} \not\equiv a_s \ (\mathrm{mod}\ n_s)$ and hence $a - 2^{b_j^{(t)}} \not\equiv a - 2^{a_s} \equiv 0 \ (\mathrm{mod}\ p_s)$. In practice we can split $(a - 2^{b_j^{(t)}})/p_t (\mathrm{mod}\ d/p_t)$ into p_t residue classes modulo d, exactly one of which contains only multiples of p_t and should be deleted for our purpose.

Remark 2. Under the conditions of the Theorem, the authors [YS] showed in 1998 that if c is divisible by a unique prime among $p_1, \cdots, p_k$, then there exists a positive integer n such that $2^n + cp \in a(\text{mod } d)$ for infinitely many primes p.

P. Erdös used the following cover

$$B = \{0(\text{mod } 2), 0(\text{mod } 3), 1(\text{mod } 4), 3(\text{mod } 8), 7(\text{mod } 12), 23(\text{mod } 24)\} \tag{4}$$

to get counterexamples to the claim of A. de Polignac. It is easy to check that the moduli $2, 3, 4, 8, 12, 24$ have primitive prime divisors

$$3, \ 7, \ 5, \ 17, \ 13, \ 241$$

respectively. Notice that the intersection

$$2^0(\text{mod } 3) \cap 2^0(\text{mod } 7) \cap 2(\text{mod } 5) \cap 2^3(\text{mod } 17) \cap 2^7(\text{mod } 13) \cap 2^{23}(\text{mod } 241) \tag{5}$$

is $2036812(\text{mod } 5592405)$. Erdös showed that

$$2036812(\text{mod } 5592405) \cap 1(\text{mod } 2) \cap 3(\text{mod } 31)$$

contains no integers of the form $2^n + p$. Our Theorem yields the following complete result.

Corollary. *Let c be an integer relatively prime to*

$$3 \times 5 \times 7 \times 13 \times 17 \times 241 = 5592405.$$

Then the residue class $2036812(\text{mod } 5592405)$ *contains integers of the form* $2^n + cp$ *with n being a nonnegative integer and p being a prime, if and only if c is congruent to one of the following numbers modulo* 5592405*:*

$$20054, 43259, 66464, 89669, 112874, 119692, 136079, 156668,$$
$$159284, 182489, 205694, 228899, 252104, 275309, 286292, 298514,$$
$$321719, 344924, 368129, 381148, 391334, 405724, 407356, 407362,$$
$$414539, 437744, 448657, 460949, 484154, 507359, 530564, 553769,$$
$$576974, 586853, 600179, 623384, 646589, 657092, 669794, 678596,$$
$$678932, 692999, 716204, 739409, 762614, 777622, 785819, 809024,$$
$$832229, 855434, 878639, 901844, 925049, 948254, 971459, 994664,$$
$$1017038, 1017869, 1041074, 1064279, 1085207, 1087484, 1106587, 1110689,$$

1133894, 1157099, 1180304, 1203509, 1226714, 1249919, 1273124, 1296329, 1319534, 1342739, 1365944, 1389149, 1412354, 1435552, 1435559, 1447223, 1458764, 1481969, 1499629, 1505174, 1525837, 1525843, 1528379, 1551584, 1574789, 1597994, 1621199, 1644404, 1667609, 1690814, 1714019, 1737224, 1760429, 1764517, 1783634, 1806839, 1830044, 1853249, 1876454, 1884122, 1899659, 1922864, 1946069, 1969274, 1992479, 2015684, 2038889, 2062094, 2085299, 2108504, 2131709, 2154914, 2178119, 2193547, 2201324, 2224529, 2247734, 2270939, 2294144, 2307593, 2317349, 2340554, 2363759, 2386964, 2410169, 2422447, 2433374, 2456579, 2479784, 2502989, 2526194, 2537611, 2542987, 2543071, 2549399, 2572604, 2595809, 2619014, 2642219, 2642686, 2644318, 2644324, 2665424, 2688629, 2711834, 2735039, 2737778, 2751412, 2758244, 2781449, 2804654, 2827859, 2851064, 2874269, 2897474, 2943884, 2967089, 2990294, 3009106, 3013499, 3036704, 3059909, 3080377, 3083114, 3106319, 3129524, 3152729, 3167963, 3175934, 3199139, 3222344, 3245549, 3268754, 3291959, 3315164, 3338369, 3361574, 3384779, 3407984, 3409342, 3431189, 3454394, 3477599, 3481952, 3500804, 3524009, 3547214, 3570419, 3593624, 3598148, 3616829, 3640034, 3663239, 3686444, 3709649, 3732854, 3736591, 3738307, 3756059, 3761167, 3762799, 3779264, 3802469, 3825674, 3848879, 3872084, 3895289, 3918494, 3941699, 3964904, 3988109, 4011314, 4028333, 4034519, 4057682, 4057724, 4067272, 4080929, 4104134, 4127339, 4150544, 4173749, 4196954, 4220159, 4243364, 4266569, 4280867, 4289774, 4312979, 4336184, 4359389, 4382594, 4385362, 4396237, 4401746, 4405799, 4406866, 4407122, 4407202, 4407206, 4429004, 4452209, 4458518, 4475414, 4498619, 4521824, 4545029, 4568234, 4591439, 4614644, 4637849, 4661054, 4684259, 4707464, 4725202, 4730669, 4753874, 4777079, 4800284, 4823489, 4846694, 4855702, 4869899, 4873241, 4879648, 4881286, 4888703, 4893104, 4916309, 4939514, 4962719, 4985924, 5009129, 5032334, 5054167, 5055539, 5078744, 5079782, 5101949, 5125154, 5148359, 5171564, 5194769, 5217974, 5241179, 5264384, 5287589, 5310794, 5318888, 5333999, 5357204, 5380409,

$$5383132, 5403614, 5426819, 5450024, 5473229, 5496434, 5519639, 5542844,$$
$$5566049, 5589254.$$

Proof. Note that system B in (4) forms a minimal cover with

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

and

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

Recall that $3, 7, 5, 17, 13, 241$ are primitive prime divisors of $2^{n_1} - 1, \cdots, 2^{n_6} - 1$ respectively. Obviously $[n_1, \cdots, n_6] = 24$. Let $R = \{0, 1, \cdots, 23\}$ and

$$S_t = a_t (\text{mod } n_t) \setminus \bigcup_{\substack{s=1 \\ s \neq t}}^{6} a_s (\text{mod } n_s) \quad \text{for } t = 1, \cdots, 6. \tag{6}$$

Then

$$S_1 = 0(\text{mod } 2) \setminus 0(\text{mod } 3) \quad \text{and} \quad S_1 \cap R = \{2, 4, 8, 10, 14, 16, 20, 22\},$$

$$S_2 = 0(\text{mod } 3) \setminus (0(\text{mod } 2) \cup 1(\text{mod } 4) \cup 3(\text{mod } 8)) \text{ and } S_2 \cap R = \{15\},$$

$$S_3 = 1(\text{mod } 4) \setminus 0(\text{mod } 3) \quad \text{and} \quad S_3 \cap R = \{1, 5, 13, 17\},$$

$$S_4 = 3(\text{mod } 8) \setminus (0(\text{mod } 3) \cup 7(\text{mod } 12)) \quad \text{and} \quad S_4 \cap R = \{11\},$$

$$S_5 = 7(\text{mod } 12) \setminus 3(\text{mod } 8) \qquad \text{and} \qquad S_5 \cap R = \{7\},$$

$$S_6 = 23(\text{mod } 24) \qquad \text{and} \qquad S_6 \cap R = \{23\}.$$

By computation we find that $S(B)$ consists of the following residue classes:

$$678936, 678932, 678852, 678596, 673476, 657092, 329412, 1144971 \text{ mod } 5592405/3;$$

$$286292(\text{mod } 5592405/7);\ 407362, 407356, 405724, 381148 \text{ mod } 5592405/5;$$

$$119692(\text{mod } 5592405/17);\ 156668(\text{mod } 5592405/13);\ 20054(\text{mod } 5592405/241).$$

In view of the Theorem and Remark 1, we can now obtain the desired result by trivial calculations. □

Remark 3. Observe that $5589254 \equiv -3151 \ (\text{mod } 5592405)$. By the above corollary, for any integer $c \in [-3150, 20054)$ divisible by none of 3,5,7,13,17,241, the residue class $20036812(\text{mod } 5592405)$ contains no integers of the form $2^n + cp$ where $n \geqslant 0$ is an integer and p is a prime.

Acknowledgement. The authors are indebted to the referee for his helpful suggestions.

References

[B] A.S. Bang, *Taltheoretiske Undersgelser*, Tidsskrift for Mat. **4** (1886), no. 5, 70–80, 130–137.

[BV] G.D. Birkhoff and H.S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. Math. **5** (1904), 173–180.

[C] R. Crocker, *On a sum of a prime and two powers of two*, Pacific J. Math. **36** (1971), 103–107.

[E1] P.Erdös, *On integers of the form* $2^k + p$ *and some related problems*, Summa Brasil. Math. **2** (1950), 113–123.

[E2] P.Erdös, *Problems and results in number theory*, in: H. Halberstam and C. Holley, eds., Recent Progress in Analytic Number Theory, vol. 1, Academic Press, New York, 1981, pp. 1–13.

[G] P.X. Gallagher, *Primes and powers of* 2, Invent. Math. **29** (1975), 125–142.

[GS] A. Granville and K. Soundararajan, *A binary additive problem of Erdös and the order of* 2 mod p^2, Ramanujan J. **2** (1998), 283–298.

[Gu] R. K. Guy, *Unsolved Problems in Number Theorey* (2nd, ed.), Springer-Verlag, New York, 1994, pp. 251–256.

[P] A. de Polignac, *Recherches nouvelles sur les nombres premiers*, C. R. Acad. Sci. Paris Math. **29** (1849), 397–401, 738–739.

[R] D. Richard, *All arithmetical sets of powers of primes are first-order definable in terms of the successor function and the coprimeness predicate*, Discrete Math. **53** (1985), 221–247.

[S] W. Sierpiński, *Elementary Theory of Numbers*, PWN-Polish Scientific Publishers, North-Holland, Amsterdam, 1987, pp. 445–448.

[S1] Zhi-Wei Sun, *Covering the integers by arithmetic sequences* II, Trans. Amer. Math. Soc. **348** (1996), 4279–4320.

[S2] Zhi-Wei Sun, *On integers not of the form* $p^a \pm q^b$, Proc. Amer. Math. Soc. **128** (2000), 997–1002.

[YS] Si-Man Yang and Zhi-Wei Sun, *Covers with less than* 10 *moduli and their applications*, J. Southeast Univ. (English Edition) **14** (1998), no. 2, 106–114.

[Z] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 265–284.

Department of Mathematics, Nanjing University, Nanjing 210093, the People's Republic of China. *E-mail*: `zwsun@nju.edu.cn`

Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543.