Proceedings of the Edinburgh Mathematical Society (2002) **45**, 155–160 ©

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

ZHI-WEI SUN[1] AND SI-MAN YANG[2]

[1]*Department of Mathematics, Nanjing University, Nanjing 210093, The People's Republic of China* (zwsun@nju.edu.cn)

[2]*Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543*

(Received 15 February 2000)

Abstract In 1950 Erdös proved that if $x \equiv 2\,036\,812 \pmod{5\,592\,405}$ and $x \equiv 3 \pmod{62}$, then x is not of the form $2^n + p$, where n is a non-negative 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 5 592 405 such that the residue class $2\,036\,812(\text{mod}\,5\,592\,405)$ contains integers of the form $2^n + cp$.

Keywords: integers of the form $2^n + cp$; cover of $\mathbb{Z}$; residue class; primitive prime divisor

AMS 2000 *Mathematics subject classification:* Primary 11P32
Secondary 11A07; 11B25; 11B75

In 1849 de Polignac [**4**] claimed that any sufficiently large odd integer is of the form 2^n+p, where n is a non-negative integer and p is a prime. Erdös [**5**] proved that any integer congruent to $2\,036\,812 \bmod 5\,592\,405$ and $3 \bmod 62$ cannot be the sum of a power of two and a prime, a clear proof of this result was presented by Sierpiński [**11**] (see [**3**, **7**, **8**, **13**] 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 $\mathbb{Z}$ see [**6**], [**9**] and the introduction of [**12**].

A well-known result of Bang [**1**] (also rediscovered by Zsigmondy [**15**] and Birkhoff and Vandiver [**2**]) 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 [**10**] the reader can find all prime divisors of $2^n - 1$ with $n \leqslant 22$.

Our main result in this note is the following theorem.

https://doi.org/10.1017/S0013091500000924 Published online by Cambridge University Press

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

$$\left(a_t(\operatorname{mod} n_t) \setminus \bigcup_{\substack{s=1 \\ s \neq t}}^{k} a_s(\operatorname{mod} n_s)\right) \cap \{0, 1, \ldots, N-1\} = \{b_1^{(t)}, \ldots, b_{l_t}^{(t)}\} \tag{2}$$

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

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

where all the $(a - 2^{b_j^{(t)}})/p_t$ are integers. Then an integer c divisible by none of $p_1, \ldots, p_k$ belongs to $S(A)$ if and only if $a(\operatorname{mod} d)$ 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 $1 \leqslant j \leqslant l_t$. As $b_j^{(t)} \equiv a_t \ (\operatorname{mod} n_t)$, $a \equiv 2^{a_t} \equiv 2^{b_j^{(t)}} (\operatorname{mod} p_t)$. Let $c \equiv (a - 2^{b_j^{(t)}})/p_t \ (\operatorname{mod} d/p_t)$. Since $d = p_1 \cdots p_k$ divides $2^N - 1$, for any non-negative integer $n \equiv b_j^{(t)} \ (\operatorname{mod} N)$ we have

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

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

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

i.e.

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

So $c \in S(A)$.

The proof is now complete. □

Remark 2. 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 $b_j^{(t)} \not\equiv a_s \ (\operatorname{mod} n_s)$, and hence $a - 2^{b_j^{(t)}} \not\equiv a - 2^{a_s} \equiv 0 \ (\operatorname{mod} p_s)$. In practice we can split $(a - 2^{b_j^{(t)}})/p_t(\operatorname{mod} d/p_t)$ 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 3. Under the conditions of Theorem 1, the authors [**14**] showed that if c is divisible by a unique prime among $p_1, \ldots, p_k$, then there exists a positive integer n such that $2^n + cp \in a(\operatorname{mod} d)$ for infinitely many primes p.

Erdös used the following cover

$$B = \{0(\bmod 2), 0(\bmod 3), 1(\bmod 4), 3(\bmod 8), 7(\bmod 12), 23(\bmod 24)\} \quad (4)$$

to get counterexamples to the claim of de Polignac. It is easy to check that 2^2-1, 2^3-1, 2^4-1, 2^8-1, $2^{12}-1$, $2^{24}-1$ have primitive prime divisors

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

respectively. Notice that the intersection

$$2^0(\bmod 3) \cap 2^0(\bmod 7) \cap 2(\bmod 5) \cap 2^3(\bmod 17) \cap 2^7(\bmod 13) \cap 2^{23}(\bmod 241) \quad (5)$$

is $2\,036\,812(\bmod 5\,592\,405)$. Erdös showed that

$$2\,036\,812(\bmod 5\,592\,405) \cap 1(\bmod 2) \cap 3(\bmod 31)$$

contains no integers of the form $2^n + p$. Our Theorem 1 yields the following complete result.

Corollary 4. *Let c be an integer relatively prime to*

$$3 \times 5 \times 7 \times 13 \times 17 \times 241 = 5\,592\,405.$$

Then the residue class $2\,036\,812(\bmod 5\,592\,405)$ contains integers of the form $2^n + cp$, with n being a non-negative integer and p being a prime, if and only if c is congruent to one of the following numbers modulo $5\,592\,405$:

20 054	43 259	66 464	89 669	112 874	119 692	136 079
156 668	159 284	182 489	205 694	228 899	252 104	275 309
286 292	298 514	321 719	344 924	368 129	381 148	391 334
405 724	407 356	407 362	414 539	437 744	448 657	460 949
484 154	507 359	530 564	553 769	576 974	586 853	600 179
623 384	646 589	657 092	669 794	678 596	678 932	692 999
716 204	739 409	762 614	777 622	785 819	809 024	832 229
855 434	878 639	901 844	925 049	948 254	971 459	994 664
1 017 038	1 017 869	1 041 074	1 064 279	1 085 207	1 087 484	1 106 587
1 110 689	1 133 894	1 157 099	1 180 304	1 203 509	1 226 714	1 249 919
1 273 124	1 296 329	1 319 534	1 342 739	1 365 944	1 389 149	1 412 354
1 435 552	1 435 559	1 447 223	1 458 764	1 481 969	1 499 629	1 505 174
1 525 837	1 525 843	1 528 379	1 551 584	1 574 789	1 597 994	1 621 199
1 644 404	1 667 609	1 690 814	1 714 019	1 737 224	1 760 429	1 764 517
1 783 634	1 806 839	1 830 044	1 853 249	1 876 454	1 884 122	1 899 659

https://doi.org/10.1017/S0013091500000924 Published online by Cambridge University Press

1 922 864	1 946 069	1 969 274	1 992 479	2 015 684	2 038 889	2 062 094
2 085 299	2 108 504	2 131 709	2 154 914	2 178 119	2 193 547	2 201 324
2 224 529	2 247 734	2 270 939	2 294 144	2 307 593	2 317 349	2 340 554
2 363 759	2 386 964	2 410 169	2 422 447	2 433 374	2 456 579	2 479 784
2 502 989	2 526 194	2 537 611	2 542 987	2 543 071	2 549 399	2 572 604
2 595 809	2 619 014	2 642 219	2 642 686	2 644 318	2 644 324	2 665 424
2 688 629	2 711 834	2 735 039	2 737 778	2 751 412	2 758 244	2 781 449
2 804 654	2 827 859	2 851 064	2 874 269	2 897 474	2 943 884	2 967 089
2 990 294	3 009 106	3 013 499	3 036 704	3 059 909	3 080 377	3 083 114
3 106 319	3 129 524	3 152 729	3 167 963	3 175 934	3 199 139	3 222 344
3 245 549	3 268 754	3 291 959	3 315 164	3 338 369	3 361 574	3 384 779
3 407 984	3 409 342	3 431 189	3 454 394	3 477 599	3 481 952	3 500 804
3 524 009	3 547 214	3 570 419	3 593 624	3 598 148	3 616 829	3 640 034
3 663 239	3 686 444	3 709 649	3 732 854	3 736 591	3 738 307	3 756 059
3 761 167	3 762 799	3 779 264	3 802 469	3 825 674	3 848 879	3 872 084
3 895 289	3 918 494	3 941 699	3 964 904	3 988 109	4 011 314	4 028 333
4 034 519	4 057 682	4 057 724	4 067 272	4 080 929	4 104 134	4 127 339
4 150 544	4 173 749	4 196 954	4 220 159	4 243 364	4 266 569	4 280 867
4 289 774	4 312 979	4 336 184	4 359 389	4 382 594	4 385 362	4 396 237
4 401 746	4 405 799	4 406 866	4 407 122	4 407 202	4 407 206	4 429 004
4 452 209	4 458 518	4 475 414	4 498 619	4 521 824	4 545 029	4 568 234
4 591 439	4 614 644	4 637 849	4 661 054	4 684 259	4 707 464	4 725 202
4 730 669	4 753 874	4 777 079	4 800 284	4 823 489	4 846 694	4 855 702
4 869 899	4 873 241	4 879 648	4 881 286	4 888 703	4 893 104	4 916 309
4 939 514	4 962 719	4 985 924	5 009 129	5 032 334	5 054 167	5 055 539
5 078 744	5 079 782	5 101 949	5 125 154	5 148 359	5 171 564	5 194 769
5 217 974	5 241 179	5 264 384	5 287 589	5 310 794	5 318 888	5 333 999
5 357 204	5 380 409	5 383 132	5 403 614	5 426 819	5 450 024	5 473 229
5 496 434	5 519 639	5 542 844	5 566 049	5 589 254		

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

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

and

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

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

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

Then

$$\begin{aligned}
S_1 &= 0(\mathrm{mod}\,2) \setminus 0(\mathrm{mod}\,3), & S_1 \cap R &= \{2,4,8,10,14,16,20,22\};\\
S_2 &= 0(\mathrm{mod}\,3) \setminus (0(\mathrm{mod}\,2) \cup 1(\mathrm{mod}\,4) \cup 3(\mathrm{mod}\,8)), & S_2 \cap R &= \{15\};\\
S_3 &= 1(\mathrm{mod}\,4) \setminus 0(\mathrm{mod}\,3), & S_3 \cap R &= \{1,5,13,17\};\\
S_4 &= 3(\mathrm{mod}\,8) \setminus (0(\mathrm{mod}\,3) \cup 7(\mathrm{mod}\,12)), & S_4 \cap R &= \{11\};\\
S_5 &= 7(\mathrm{mod}\,12) \setminus 3(\mathrm{mod}\,8), & S_5 \cap R &= \{7\};\\
S_6 &= 23(\mathrm{mod}\,24), & S_6 \cap R &= \{23\}.
\end{aligned}$$

Let $d = 5\,592\,405$. By computation we find that $S(B)$ consists of the following residue classes:

$$678\,936,\ 678\,932,\ 678\,852,\ 678\,596,\ 673\,476,\ 657\,092,\ 329\,412,\ 1\,144\,971 \bmod d/3;$$
$$286\,292(\mathrm{mod}\,d/7);\quad 407\,362,\ 407\,356,\ 405\,724,\ 381\,148 \bmod d/5;$$
$$119\,692(\mathrm{mod}\,d/17);\quad 156\,668(\mathrm{mod}\,d/13);\quad 20\,054(\mathrm{mod}\,d/241).$$

In view of Theorem 1 and Remark 2, we can now obtain the desired result through trivial calculations. □

Remark 5. Observe that $5\,589\,254 \equiv -3151 \ (\mathrm{mod}\,5\,592\,405)$. By Corollary 4, for any integer $c \in [-3150, 20\,054)$ divisible by none of 3, 5, 7, 13, 17, 241, the residue class $2\,003\,6812(\mathrm{mod}\,5\,592\,405)$ contains no integers of the form $2^n + cp$, where $n \geqslant 0$ is an integer and p is a prime.

Acknowledgements. Z.-W.S. was 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 the People's Republic of China. The authors are indebted to the referee for his helpful suggestions.

References

1. A. S. Bang, Taltheoretiske Undersgelser, *Tidsskrift Mat.* **4** (1886), 70–80, 130–137.
2. G. D. Birkhoff and H. S. Vandiver, On the integral divisors of $a^n - b^n$, *Ann. Math.* **5** (1904), 173–180.
3. R. Crocker, On a sum of a prime and two powers of two, *Pac. J. Math.* **36** (1971), 103–107.
4. A. de Polignac, Recherches nouvelles sur les nombres premiers, *C. R. Acad. Sci. Paris Sér. I* **29** (1849), 397–401, 738–739.
5. P. Erdös, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.* **2** (1950), 113–123.
6. P. Erdös, Problems and results in number theory, in *Recent progress in analytic number theory* (ed. H. Halberstam and C. Holley), vol. 1, pp. 1–13 (Academic, 1981).
7. P. X. Gallagher, Primes and powers of 2, *Invent. Math.* **29** (1975), 125–142.
8. 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.
9. R. K. Guy, *Unsolved problems in number theory*, 2nd edn, pp. 251–256 (Springer, 1994).

10. 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.
11. W. Sierpiński, *Elementary theory of numbers*, pp. 445–448 (PWN-Polish Scientific Publishers, North-Holland, Amsterdam, 1987).
12. Z.-W. Sun, Covering the integers by arithmetic sequences, II, *Trans. Am. Math. Soc.* **348** (1996), 4279–4320.
13. Z.-W. Sun, On integers not of the form $p^a \pm q^b$, *Proc. Am. Math. Soc.* **128** (2000), 997–1002.
14. S.-M. Yang and Z.-W. Sun, Covers with less than 10 moduli and their applications, *J. Southeast Univ.* (English edition) **14**(2) (1998), 106–114.
15. K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* **3** (1892), 265–284.

https://doi.org/10.1017/S0013091500000924 Published online by Cambridge University Press