PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 128, Number 4, Pages 997–1002
S 0002-9939(99)05502-1
Article electronically published on October 27, 1999

ON INTEGERS NOT OF THE FORM $\pm p^a \pm q^b$

ZHI-WEI SUN

(Communicated by David E. Rohrlich)

ABSTRACT. In 1975 F. Cohen and J.L. Selfridge found a 94-digit positive integer which cannot be written as the sum or difference of two prime powers. Following their basic construction and introducing a new method to avoid a bunch of extra congruences, we are able to prove that if

$$x \equiv 47867742232066880047611079 \pmod{6648303402501871163986252749 0},$$

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

1. INTRODUCTION

In 1849 A. de Polignac [P] asked whether any positive odd integer can be expressed in the form $2^n + p$ where n is a nonnegative integer and p is 1 or a (positive) prime; actually Euler had already noted the counterexample 959. Using the Brun sieve N.P. Romanoff [Ro] proved that a positive proportion of the odd integers may be written in this way. On the other hand, van der Corput [Co] showed that the set of positive odd integers not representable in the form has a positive density, and by means of cover of the ring $\mathbb{Z}$ of the integers P. Erdös [E] constructed a residue class of odd numbers which contains no integers of the desired form.

Let $\mathbb{N} = \{0, 1, 2, \cdots\}$ and $\mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$. For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ we call

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

a *residue class* with *modulus* n. A finite system

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

of such sets is said to be a *cover* (of $\mathbb{Z}$) if every integer belongs to some residue classes in A. Notice that the characteristic function of the set $\bigcup_{s=1}^k a_s(n_s)$ is periodic mod N where N denotes the least common multiple of $n_1, \cdots, n_k$.

Inspired by the work of Erdös, in 1975 F. Cohen and J.L. Selfridge [CS] observed that the 26-digit number

$$M = 47867742232066880047611079 \tag{2}$$

plus or minus a power of 2 can never be a prime, but they gave no reasons why additional congruences (similar to $x \equiv 3 \pmod{31}$ in the proof of Erdös presented in [Si]) can be avoided there. (See their Theorem 1 and its proof.) They then deduced

Received by the editors June 16, 1998.
2000 *Mathematics Subject Classification.* Primary 11B75; Secondary 11B25, 11P32.
This research was supported by the National Natural Science Foundation of the People's Republic of China and the Return-from-abroad Foundation of the Chinese Educational Committee.

(in their Theorem 2) that there exist odd numbers not of the form $\pm 2^a \pm p^b$ where p is a prime, $a, b \in \mathbb{N}$ and any choice of signs may be made. To find the least positive odd integer having the property is an interesting open problem. (Cf. section A19 of R.K. Guy [Gu].) Through a computer search Cohen and Selfridge noted that the number is greater than $2^{18} = 262144$, and in [CS] they showed that the 94-digit number

$$612066990606727677809211560175662548195761616 31$$
$$-92298173436854933451240674174209468558999326569$$

is indeed not of the form $\pm 2^a \pm p^b$.

In view of Goldbach's conjecture, we should seek integers not representable by the sum or difference of two prime powers only among odd numbers not of the above form. In this paper we adopt the construction in Theorem 1 of Cohen and Selfridge [CS] and show that we can deduce their Theorem 2 without using a lot of extra congruences. Thus we have

Theorem. *Let x be any integer congruent to M modulo*

$$6648303402501871163986252749 0$$

where M is as in (2). Then x cannot be written in the form $\pm p^a \pm q^b$ where p, q are primes, $a, b \in \mathbb{N}$ and any choice of signs may be made.

Since M is prime to the 29-digit modulus in the above theorem, with the help of Dirichlet's theorem there are infinitely many primes p such that $p + 2^n$ and $|p - 2^n|$ are both composite for all $n = 0, 1, 2, \cdots$. This gives an affirmative answer to the question raised by M.V. Vassilev-Missana [VM].

For other related topics, the reader is referred to [Cr], [Ga], [Gu], [GS] and [Su].

2. Proof of the Theorem

For $n \in \mathbb{Z}^+$ by a *primitive divisor* of $2^n - 1$ we mean a factor of $2^n - 1$ not dividing $2^m - 1$ for any $0 < m < n$. It is known that $2^n - 1$ has a primitive prime divisor if $n \neq 1, 6$. (Such results were first given by K. Zsigmondy [Z] and then rediscovered by G.D. Birkhoff and H.S. Vandiver [BV]; they were clearly stated and applied by D. Richard [Ri].)

Lemma 1. *Let (1) be a cover of $\mathbb{Z}$ with $0 \leqslant a_s < n_s$ for $s = 1, \cdots, k$, and let distinct primes $p_1, \cdots, p_k$ be divisors of $2^{n_1} - 1, \cdots, 2^{n_k} - 1$ respectively. Let $P(x)$ be any polynomial with integer coefficients. Let $n \in \mathbb{N}$ and $x \in \bigcap_{s=1}^k P(2^{a_s})(p_s)$. If $|x - P(2^n)|$ is a prime power, then there exists a unique $s \in \{1, \cdots, k\}$ for which $n = a_s + an_s$ and $|x - P(2^n)| = p_s^b$ for some $a, b \in \mathbb{N}$.*

Proof. By the Chinese Remainder Theorem, $S = \bigcap_{s=1}^k P(2^{a_s})(p_s)$ is a residue class. Suppose that $|x - P(2^n)| = p^b$ where p is a prime and b is a nonnegative integer. Let $I = \{1 \leqslant s \leqslant k : \ n \in a_s(n_s)\}$. For $s \in I$ clearly

$$x - P(2^n) \equiv x - P(2^{a_s}) \equiv 0 \ (\mathrm{mod}\, p_s)$$

and hence $p_s = p$. So I has a single element. The lemma is proved.

Lemma 2. *The systems*

$$A = \{1(2),\ 0(4),\ 6(8),\ 10(12),\ 10(16),\ 18(24),\ 2(48)\}$$

and

$$B = \{0(2),\ 0(3),\ 2(5),\ 5(9),\ 3(10),\ 4(15),\\ 11(18),\ 1(20),\ 25(30),\ 17(36),\ 35(36),\ 31(60)\}$$

form covers of $\mathbb{Z}$.

Proof. Apparently $2(16) \subseteq 2(48) \cup 18(24) \cup 10(12)$; from this it is easy to see that A forms a cover of $\mathbb{Z}$. As for system B, evidently $5(6) \subseteq 5(9) \cup 11(18) \cup 17(36) \cup 35(36)$ and

$$1(6) \subseteq 2(5) \cup 3(10) \cup 4(15) \cup 1(20) \cup 25(30) \cup 31(60),$$

so B is also a cover.

Remark. The two covers in Lemma 2 were first used by Cohen and Selfridge [CS].

For convenience we adopt the following notation for $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$:

$$R_m(a) = \{r \in \mathbb{Z} :\ -m/2 < r \leqslant m/2 \text{ and } a^n \in r(m) \text{ for some } n \in \mathbb{N}\}. \tag{3}$$

Proof of the Theorem. Let systems A and B be as in Lemma 2. For those moduli n in cover A, we can assign to $2^n - 1$ primitive prime divisors 3, 5, 17, 13, 257, 241, 97 respectively. For those moduli m in cover B, we may assign to $2^m - 1$ primitive prime divisors

$$3,\ 7,\ 31,\ 73,\ 11,\ 151,\ 19,\ 41,\ 331,\ 109,\ 37,\ 61$$

respectively. In order to apply Lemma 1, we let S denote the residue class

$$\begin{aligned} &-2(3) \cap -2^0(5) \cap -2^6(17) \cap -2^{10}(13) \cap -2^{10}(257) \cap -2^{18}(241) \cap -2^2(97) \\ &\quad = 1(3) \cap -1(5) \cap 4(17) \cap 3(13) \cap 4(257) \cap 64(241) \cap -4(97) \\ &\quad = -2887734236(19916152035) \end{aligned}$$

and we let T stand for

$$\begin{aligned} &2^0(3) \cap 2^0(7) \cap 2^2(31) \cap 2^5(73) \cap 2^3(11) \cap 2^4(151) \\ &\quad \cap 2^{11}(19) \cap 2^1(41) \cap 2^{25}(331) \cap 2^{17}(109) \cap 2^{35}(37) \cap 2^{31}(61) \\ =&1(3) \cap 1(7) \cap 4(31) \cap 32(73) \cap -3(11) \cap 16(151) \\ &\quad \cap -4(19) \cap 2(41) \cap -31(331) \cap 54(109) \cap 19(37) \cap -2(61) \\ =&1059133928568910972(5007223647777439011). \end{aligned}$$

Let x be any integer in the residue class

$$1(2) \cap S \cap T = M(66483034025018711639862527490).$$

As an odd integer x is not of the form $\varepsilon_1 p_1^{\alpha_1} + \varepsilon_2 p_2^{\alpha_2}$ where p_1, p_2 are odd primes, $\alpha_1, \alpha_2 \in \mathbb{N}^+$ and $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$. We need only show that neither $|x + 2^n|$ nor $|x - 2^n|$ can be a prime power. By Lemma 1 it suffices to deduce a contradiction in each of the following cases where $a, b \in \mathbb{N}$ and $\varepsilon \in \{1, -1\}$.

Case A1. $x = -2^{1+2a} + \varepsilon 3^b$.

Since $R_{13}(3) = \{1, 3, -4\}$ and $R_{13}(4) = \{\pm 1, \pm 3, \pm 4\}$, by the congruence $x \equiv 3 \pmod{13}$ we must have

$$3^b \in 1(13) \text{ (i.e. } 3 \mid b),\ \varepsilon = 1 \ \&\ 4^a \in -1(13) \text{ (i.e. } 6 \mid a - 3),$$

or

$$3^b\in 3(13)\ (\text{i.e. } 3\mid b-1),\ \varepsilon=-1\ \&\ 4^a\in -3(13)\ (\text{i.e. } 6\mid a+1),$$

or

$$3^b\in -4(13)\ (\text{i.e. } 3\mid b-2),\ \varepsilon=1\ \&\ 4^a\in 3(13)\ (\text{i.e. } 6\mid a-2).$$

So, for some $c,d\in\mathbb{Z}$ the integer x has one of the following three forms:

$$-2^{1+2(6c+3)}+3^{3d},\quad -2^{1+2(6c-1)}-3^{3d+1},\quad -2^{1+2(6c+2)}+3^{3d+2}.$$

As $x\in 1(7)$, x must be of the last form and d must be odd. Thus

$$x=-2^{12c+5}+3^{3d+2}\equiv -2-2^d\not\equiv -1\ (\mathrm{mod}\,5).$$

Case A2. $x=-2^{0+4a}+\varepsilon 5^b$.

Since $x\equiv -1+\varepsilon(-1)^b\equiv 1\ (\mathrm{mod}\,3)$, we have $\varepsilon=(-1)^{b-1}$. Clearly $2^3\equiv 1\ (\mathrm{mod}\,7)$ and $x=-2^{4a}-(-5)^b\equiv -2^a-2^b\equiv 1\ (\mathrm{mod}\,7)$. Therefore

$$2^a\in 2(7)\ \&\ 2^b\in 2^2(7),\quad \text{or}\quad 2^a\in 2^2(7)\ \&\ 2^b\in 2(7),$$

i.e. $x=-2^{4(1+3c)}-(-5)^{2+3d}$ or $-2^{4(2+3c)}-(-5)^{1+3d}$ for some $c,d\in\mathbb{Z}$. If x is of the former form, then $x\equiv -3+5^d\not\equiv 3\ (\mathrm{mod}\,13)$. Thus $x=-2^{8+12c}-(-5)^{1+3d}\equiv 4+5^{d+1}\ (\mathrm{mod}\,13)$. As $x\in 3(13)$ we find that $d=1+4e$ for some $e\in\mathbb{Z}$. Now

$$\begin{aligned}x&=-2^{8+12c}-(-5)^{1+3(1+4e)}=-(2^4)^{2+3c}-(5^4)^{1+3e}\\&\equiv -(-1)^{2+3c}-(-4)^{1+3e}\equiv(-1)^{c-1}+4^{e+1}\not\equiv 4\ (\mathrm{mod}\,17).\end{aligned}$$

Case A3. $x=-2^{6+8a}+\varepsilon 17^b$.

As $R_{13}(-4)=\{1,-4,3\}$ and $R_{13}(4)=\{\pm1,\pm3,\pm4\}$, we find that $x\equiv(-4)^a+\varepsilon 4^b\not\equiv 3\ (\mathrm{mod}\,13)$.

Case A4. $x=-2^{10+12a}+\varepsilon 13^b$.

In this case, $x\equiv -2+\varepsilon(-1)^b\not\equiv 1\ (\mathrm{mod}\,7)$.

Case A5. $x=-2^{10+16a}+\varepsilon 257^b$.

Since $x\equiv -1+\varepsilon(-1)^b\equiv 1\ (\mathrm{mod}\,3)$, we have $\varepsilon=(-1)^{b-1}$. Note that $x=-2^{10+16a}-(-257)^b\equiv -4-(-2)^b\equiv 4\ (\mathrm{mod}\,17)$. So $b=3+8d$ for some $d\in\mathbb{Z}$. As $R_{13}(3)=\{1,3,-4\}$,

$$\begin{aligned}x&=-2^{10+16a}-(-257)^{3+8d}\\&\equiv 2^{4+4a}-3^{3+8d}\equiv 3^{a+1}-3^{2d}\not\equiv 3\ (\mathrm{mod}\,13).\end{aligned}$$

Case A6. $x=-2^{18+24a}+\varepsilon 241^b$.

Apparently $x\equiv -2^2+\varepsilon\not\equiv -1\ (\mathrm{mod}\,5)$.

Case A7. $x=-2^{2+48a}+\varepsilon 97^b$.

In this case $x\equiv -4+\varepsilon(-1)^b\not\equiv 1\ (\mathrm{mod}\,7)$.

Case B1. $x=2^{0+2a}+\varepsilon 3^b$.

Observe that $x\equiv 4^a+\varepsilon(-1)^b4^b\equiv 1\ (\mathrm{mod}\,7)$. As $R_7(4)=\{1,4,2\}$, either $4^a\equiv\varepsilon(-1)^b4^b\equiv 4\ (\mathrm{mod}\,7)$, or $4^a\equiv 2\ (\mathrm{mod}\,7)$ and $\varepsilon(-1)^b4^b\equiv -1\ (\mathrm{mod}\,7)$. In the former case, $\varepsilon=(-1)^b$ and $a,b\equiv 1\ (\mathrm{mod}\,3)$; in the latter case, $\varepsilon=(-1)^{b-1}$, $3\mid a-2$ and $3\mid b$. So, for some integers c and d, either

$$x=2^{2(1+3c)}+(-1)^b3^b=2^{2+6c}+(-3)^{1+3d}\equiv 4(-1)^c-3(-1)^d\not\equiv 3\ (\mathrm{mod}\,13)$$

or

$$x=2^{2(2+3c)}-(-1)^b3^b=2^{4+6c}-(-3)^{3d}\equiv 3(-1)^c-(-1)^d\not\equiv 3\ (\mathrm{mod}\,13).$$

Case B2. $x = 2^{0+3a} + \varepsilon 7^b$.

As $x \equiv (-1)^a + \varepsilon \equiv 1 \pmod 3$, $\varepsilon = -1$ and $a = 1 + 2c$ for some $c \in \mathbb{Z}$. Notice that

$$x = 2^{3(1+2c)} - 7^b \equiv 8(-1)^c - 7^b \pmod{5 \times 13}.$$

When $2 \mid c$, $7^b \equiv 5 \pmod{13}$ since $x \in 3(13)$; thus $12 \mid b-3$ and hence $x \equiv 8 - 7^b \equiv -2 - 2^3 \not\equiv -1 \pmod 5$. So $2 \nmid c$ and hence $7^b \in 2(13)$ (i.e. $12 \mid b+1$). Therefore for some $d, e \in \mathbb{Z}$ we have

$$x = 2^{3+6(1+2e)} - 7^{12d-1} \equiv -(-2^3)^e + 8(7^3)^{4d} \equiv -(-8)^e + 8 \not\equiv -4 \pmod{19},$$

since $R_{19}(-8) = \{1, -8, 7\}$.

Case B3. $x = 2^{2+5a} + \varepsilon 31^b$.

In view of the congruence $x \equiv 1 \pmod 3$, $\varepsilon = -1$ and $a = 1 + 2c$ for some $c \in \mathbb{Z}$. Thus $x = 2^{7+10c} - 31^b \equiv -2(-1)^c - 1 \not\equiv -1 \pmod 5$.

Case B4. $x = 2^{5+9a} + \varepsilon 73^b$.

As $x \equiv -(-1)^a + \varepsilon \equiv 1 \pmod 3$, $\varepsilon = -1$ and $a = 2c$ for some $c \in \mathbb{Z}$. So $x = 2^{5+18c} - 73^b \equiv -5(-1)^c - (-1)^b \not\equiv 19 \pmod{37}$.

Case B5. $x = 2^{3+10a} + \varepsilon 11^b$.

Since $x \equiv -1 + \varepsilon(-1)^b \equiv 1 \pmod 3$, we have $\varepsilon = (-1)^{b-1}$. Observe that

$$x = 2^{3+10a} - (-11)^b \equiv -2(-1)^a - (-1)^b \equiv -1 \pmod 5.$$

So $a = 2c$ and $b = 1 + 2d$ for some $c, d \in \mathbb{Z}$. Now

$$x = 2^{3+20c} - (-11)^{1+2d} \equiv 8(-1)^c + 28 \times 2^d \equiv 4 \pmod{17}.$$

Therefore $7 \times 2^d \equiv 1 - 2(-1)^c \pmod{17}$. As $R_{17}(2) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$, we must have $2 \nmid c$ and $8 \mid d - 5$. Write $c = 1 + 2e$ and $d = 5 + 8f$ where $e, f \in \mathbb{Z}$. Then

$$\begin{aligned} x &= 2^{3+20(1+2e)} + 11^{1+2(5+8f)} = 2^{23+40e} + 11 \times 121^{5+8f} \\ &\equiv -2^3 + 11(-2)^{5+8f} \equiv -8 + 99 \times 256^f \equiv -8 + 17 \times 10^f \equiv 2 \pmod{41}. \end{aligned}$$

It follows that $10^{f-1} \equiv -12 \pmod{41}$. But $R_{41}(10) = \{1, 10, 18, 16, -4\}$, so we have a contradiction.

Case B6. $x = 2^{4+15a} + \varepsilon 151^b$.

Note that $x \equiv 8^a + \varepsilon \pmod{15}$. So $x \notin \varepsilon(3) \cup \varepsilon(5)$. But $\varepsilon \in \{1, -1\}$ and $x \in 1(3) \cap -1(5)$, so we have a contradiction.

Case B7. $x = 2^{11+18a} + \varepsilon 19^b$.

Using the fact $x \in 1(3)$ we obtain that $\varepsilon = -1$. As

$$x = 2^{11+18a} - 19^b \equiv 2^{3+2a} - (-1)^b \equiv -2(-1)^a - (-1)^b \equiv -1 \pmod 5,$$

$a = 2c$ and $b = 1 + 2d$ for some $c, d \in \mathbb{Z}$. Now

$$x = 2^{11+36c} - 19^{1+2d} \equiv 8(-1)^{9c} - 2^{1+2d} \equiv 4 \pmod{17}.$$

Thus $4^d \equiv 2$ or $-6 \pmod{17}$, which is impossible.

Case B8. $x = 2^{1+20a} + \varepsilon 41^b$.

Observe that $x \equiv 2 + \varepsilon \not\equiv -1 \pmod 5$.

Case B9. $x = 2^{25+30a} + \varepsilon 331^b$.

Since $x \in 1(3)$, we have $\varepsilon = -1$. Note that $x \equiv 2^{1+2a} - 1^b \not\equiv -1 \pmod 5$.

Case B10. $x = 2^{17+36a} + \varepsilon 109^b$.

Clearly $\varepsilon = -1$ since $x \in 1(3)$. Now $x \equiv 2 - (-1)^b \not\equiv -1 \pmod 5$.

Case B11. $x = 2^{35+36a} + \varepsilon 37^b$.

Evidently $x \equiv 10 + \varepsilon(-1)^b \not\equiv -4 \pmod{19}$.

Case B12. $x = 2^{31+60a} + \varepsilon 61^b$.

Notice that $x \equiv 8 + \varepsilon \pmod{15}$. This contradicts the fact $x \in 1(3) \cap -1(5) = 4(15)$.

The proof of the Theorem is now complete.

Added in proof. By means of the software MAPLE, the author and Mr. Yun-Zhi Zou (at Sichuan University) have shown that any positive integer not more than 2^{25} can be written as the sum or difference of two prime powers.

References

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

[CS] F. Cohen and J.L. Selfridge, *Not every number is the sum or difference of two prime powers*, Math. Comput. **29** (1975), 79–81. MR **51:**12758

[Co] J.G. van der Corput, *On de Polignac's conjecture*, Simon Stevin **27** (1950), 99–105. MR **11:**714e

[Cr] R. Crocker, *On a sum of a prime and two powers of two*, Pacific J. Math. **36** (1971), 103–107. MR **43:**3200

[E] P. Erdös, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113–123. MR **13:**437i

[Ga] P.X. Gallagher, *Primes and powers of* 2, Invent. Math. **29** (1975), 125–142. MR **52:**315

[Gu] R.K. Guy, *Unsolved Problems in Number Theory* (2nd ed.), Springer-Verlag, New York, 1994, sections A19,B21,F13. MR **96e:**11002

[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. CMP 99:01

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

[Ri] 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. MR **86h:**03103

[Ro] N.P. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. **57** (1934), 668–678.

[Si] W. Sierpiński, *Elementary Theory of Numbers*, PWN-Polish Scientific Publishers, North-Holland, Amsterdam, 1987, pp. 445–448. MR **89f:**11003

[Su] Zhi-Wei Sun, *On prime divisors of integers $x \pm 2^n$ and $x2^n \pm 1$*, to appear.

[VM] M.V. Vassilev-Missana, *Note on 'extraordinary primes'*, Notes Number Theory Discrete Math. **1** (1995), 111–113. **MR** 97g:11004.

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

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: zwsun@netra.nju.edu.cn