J. Fac. Educ. Tottori Univ.
(Nat. Sci.), **47** (1998) 5–12

A Property of Integers Related to Quadratic Fields

Kenichi SHIMIZU* and Kazuo GOTO†

(Received March 30, 1998)

1. Introduction

In this paper we show an interesting property of integers.

We discuss the integers having the following property: Let $n = ab$ be an integer and a any factor of n, then each integer $a + b$ is a prime.

For example, the integers having this property are 6, 30 and so on.

In fact, since $6 = 1 \cdot 6 = 2 \cdot 3$, thus we get prime numbers $1 + 6 = 7$ and $2 + 3 = 5$; since $30 = 1 \cdot 30 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6$, we get prime numbers $1 + 30 = 31$, $2 + 15 = 17$, $3 + 10 = 13$, and $5 + 6 = 11$.

We consider the relation between this phenomenon and certain imaginary quadratic fields.

2. Definition of SP-Numbers

Definition. *For a positive integer n, let a be any factor of n and $b = n/a$.*
The integer n is said to be Sum Prime number (abbreviated SP-number) if and only if

(1) *each integer $a + b$ is a prime, if $n \equiv 2$ (mod 4),*
(2) *each integer $(a + b)/2$ is a prime, if $n \equiv 1$ (mod 4),*
(3) *each integer $(a + b)/4$ is a prime, if $n \equiv 3$ (mod 4).*

Examples. We list up SP-numbers less than 1000.

(1) When $n \equiv 2$ (mod 4), SP-numbers are as follows:
2,6,10,22,30,42,58,70,78,82,102,130,190,210,310,330,358,
382,442,462,478,562,658,742,838,862,970.

(2) When $n \equiv 1$ (mod 4), SP-numbers are as follows:
5,9,13,21,25,33,37,57,61,73,85,93,105,121,133,145,157,165,
177,193,205,213,217,253,273,277,313,345,357,361,385,393,
397,421,445,457,541,553,565,613,633,661,673,697,733,757,
777,793,817,841,865,877,897,913,933,973,997.

(3) When $n \equiv 3$ (mod 4), SP-numbers are as follows:
7,11,19,27,43,51,67,75,91,115,123,147,163,187,211,235,267,
283,331,355,403,427,435,451,507,523,547,555,595,627,667,

---

* Department of Mathematics, Kenmei-Joshigakuin High School, Himeji, 670-0012, Japan
† Department of Mathematics, Faculty of Education, Tottori University, Tottori, 680-0945, Japan
Key words and phrases: SP-number, exponent, Minkovski bound

691,715,723,763,787,795,843,907.

We show the following propositions:

Proposition 1. *For a positive integer $n = k^2m$ such that $k > 1$ and $m > 1$ are integers, we have the following*:

(1) *The integer n is not a SP-number if $n \equiv 1$ or 2 (mod 4).*

(2) *If $n \equiv 3$ (mod 4) is a SP-number, then $m = 3$ and k is a prime.*

Proof.

(1) For $n \equiv 2$ (mod 4), $k + km = (1 + m)k$ is not a prime. So $n = k^2m$ is not a SP-number. For $n \equiv 1$ (mod 4), $\frac{1+m}{2}$ is an integer and $\frac{1+m}{2} > 1$ since $k^2 \equiv m \equiv 1$ (mod 4) and $m > 1$. Thus $\frac{k+km}{2} = \frac{1+m}{2}k$ is not a prime.

(2) Since $n \equiv 3$ (mod 4) is a SP-number, $\frac{k+km}{4} = \frac{1+m}{4}k$ is a prime. Hence $\frac{1+m}{4} = 1$ and k is a prime by $k > 1$. It follows that $m = 3$ and k is a prime.

Remark. The examples of the case (2) of Proposition 1 are $27 = 3^2 \cdot 3$, $75 = 5^2 \cdot 3$, $147 = 7^2 \cdot 3$ and so on.

Proposition 2. If $n \equiv 3$ (*mod* 4) *is a SP-number, then $n = 7$ or $n \equiv 3$ (mod 8).*

Proof. Let $n = ab \equiv 3$ (mod 4). One of a and b is congruent to 1 modulo 4 and the other is congruent to 3 modulo 4. So we may assume that $a \equiv 1$ (mod 4) and $b \equiv 3$ (mod 4). We put $a = 4k + 1$ and $b = 4l + 3$, where k and l are non-negative integers.

Since $n = ab$ is a SP-number, $(a + b)/4 = k + l + 1$ is a prime.

If $k + l + 1 = 2$, then $k = 1$ and $l = 0$, or $k = 0$ and $l = 1$. If $k = 1$ and $l = 0$, then we have $n = 15$. But $n = 15$ is not a SP-number. If $k = 0$ and $l = 1$, then we get $n = 7$, which is a SP-number.

If $k + l + 1$ is an odd prime, then $k + l$ is even. Hence we have $k \equiv l \equiv 0$ (mod 2) or $k \equiv l \equiv 1$ (mod 2). If $k \equiv l \equiv 0$ (mod 2), then we have $a \equiv 1$ (mod 8) and $b \equiv 3$ (mod 8). So $n = ab \equiv 3$ (mod 8). If $k \equiv l \equiv 1$ (mod 2), then we have $a \equiv 5$ (mod 8) and $b \equiv 7$ (mod 8). Thus $n = ab \equiv 3$ (mod 8).

This completes the proof of Proposition 2.

3. A Sufficient Condition for SP-Numbers

In this section we give a sufficient condition for SP-numbers.

We consider only imaginary quadratic fields $\mathbf{Q}(\sqrt{d})$, where d is a negative square-free rational integer.

Let Δ be the discriminant of $\mathbf{Q}(\sqrt{d})$ with

$$\Delta = \begin{cases} 4d & \text{if } d \equiv 2,3 \pmod 4, \\ d & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Let C_Δ be the class group of $\mathbf{Q}(\sqrt{d})$, and h_Δ the class number. We say that the exponent e_Δ of C_Δ is the least positive rational integer n such that I^n is principal for all ideals I of $\mathbf{Q}(\sqrt{d})$.

We have the following theorems.

Theorem 1. *If $e_\Delta = 1$ and $|d| \neq 1, 3$, then $|d|$ is a SP-number.*

Theorem 2. *If $e_\Delta = 2$ and $\Delta \equiv 0 \ (mod\ 4)$, then $|d|$ is a SP-number.*

Theorem 3. *If $e_\Delta = 2$, $\Delta \equiv 5 \ (mod\ 8)$, and $(1 + |\Delta|)/4$ is not a square, then $|\Delta| = |d|$ is a SP-number.*

Remark. If $\Delta \equiv 1$ (mod 8), i.e., $|\Delta| \equiv 7$ (mod 8), then $|\Delta| = 7$ is only SP-number by Proposition 2, in which case we have $e_\Delta = 1$. Hence if $e_\Delta = 2$ and $\Delta \equiv 1$ (mod 8), then we have no SP-numbers.

Proof of Theorem 1. The exponent $e_\Delta = 1$ if and only if the class number $h_\Delta = 1$. It is known that the number of the imaginary quadratic fields $\mathbf{Q}(\sqrt{d})$ with $h_\Delta = 1$ is finite. In fact, these imaginary quadratic fields are in the following nine cases,

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

By our assumption, we assume that $d \neq -1, -3$.
If $d = -2$, then $|d| = 1 \cdot 2$ and $1 + 2 = 3$ is a prime. Hence $|d| = 2$ is a SP-number.
Otherwise, $|d| \equiv 3$ (mod 4) and each $|d|$ is a prime. It is easy to check that each $(1 + |d|)/4$ is a prime. Thus we complete the proof of Theorem 1.

To prove Theorem 2 and 3, we describe some lemmas related to imaginary quadratic fields. First, we give the following lemma (see Sasaki [2]):

Lemma 1. *Let $I = [a, b + \omega]$ be a primitive ideal of $\mathbf{Q}(\sqrt{d})$ with $N(b + \omega) < N(\omega)^2$. Then I is principal if and only if $a = 1$ or $a = N(b + \omega)$.*

The number ω is equal to $\sqrt{d}$ or $(1 + \sqrt{d})/2$ as $\Delta \equiv 0$ or 1 (mod 4), respectively. The number $N(\alpha)$ is the norm of α, that is, $N(\alpha) = \alpha\alpha'$, where α' is the complex conjugate of α.

By using Lemma 1, we show the following lemma.

Lemma 2. *Let p be an odd prime. If $e_\Delta = 2$, $\left(\frac{\Delta}{p}\right) = 1$, and $p < M_\Delta$, then $p^2 = N(x + \omega)$ for a rational integer x, where $\left(\frac{\Delta}{p}\right)$ is the Legendre symbol and $M_\Delta = \sqrt{|\Delta|/3}$ is the Minkowski bound.*

Proof. By $\left(\frac{\Delta}{p}\right) = 1$, we have $p = PP'$ and $P \neq P'$, where P is the prime ideal and P' is the conjugate ideal of P.

The first step, we show that if p is odd, $\left(\frac{\Delta}{p}\right) = 1$, and $p < M_\Delta$, then $P^2 = [p^2, x + \omega]$ for a rational integer x. The second step, we prove that if $e_\Delta = 2$, then $p^2 = N(x + \omega)$.

We consider the case $\Delta \equiv 0 \pmod 4$.

Let $P = [p, x_1 + \omega]$, where x_1 is a non-negative rational integer less than p.

Then we have

$$P^2 = [p^2, p(x_1 + \omega), (x_1 + \omega)^2] = [p^2, px_1 + p\omega, x_1^2 + \omega^2 + 2x_1\omega]$$
$$= [p^2, px_1 + p\omega, x_1^2 + d + 2x_1\omega].$$

By $\left(\dfrac{\Delta}{p}\right) = 1$, we have $x_1 \neq 0$. Since p is odd and $0 < x_1 < p$, we get $\gcd(p, 2x_1) = 1$. Hence there exist rational integers s and t with $sp + 2tx_1 = 1$.

Thus

$$s(px_1 + p\omega) + t(x_1^2 + d + 2x_1\omega)$$
$$= (sp + 2tx_1)x_1 - t(x_1^2 - d) + (sp + 2tx_1)\omega = x_1 - t(x_1^2 + |d|) + \omega.$$

By $P = [p, x_1 + \omega]$, we have $N(x_1 + \omega) = x_1^2 + |d| \equiv 0 \pmod p$. Then $x_1^2 + |d| = pc$ for some positive rational integer c, so we have

$$s(px_1 + p\omega) + t(x_1^2 + d + 2x_1\omega) = x_1 - tpc + \omega.$$

Moreover, we obtain that $px_1 + p\omega = tcp^2 + p(x_1 - tpc + \omega)$, and

$$-csp^2 + 2x_1(x_1 - tpc + \omega) = -csp^2 + 2x_1^2 - 2tx_1pc + 2x_1\omega$$
$$= -csp^2 + x_1^2 - d - 2tx_1pc + x_1^2 + d + 2x_1\omega = -csp^2 + pc - 2tx_1pc + x_1^2 + d + 2x_1\omega$$
$$= -csp^2 + pc(1 - 2tx_1) + x_1^2 + d + 2x_1\omega = -csp^2 + pc \cdot sp + x_1^2 + d + 2x_1\omega$$
$$= x_1^2 + d + 2x_1\omega.$$

Therefore we obtain $P^2 = [p^2, x_1 - tpc + \omega]$.

Let $y_1 \equiv x_1 - tpc \pmod{p^2}$ and $0 < y_1 < p^2$. We get $P^2 = [p^2, y_1 + \omega]$.

Similarly, putting $P' = [p, x_2 + \omega]$, we can get $P'^2 = [p^2, y_2 + \omega]$ and $0 < y_2 < p^2$.

Since $x_1 \neq x_2$, we have $y_1 \neq y_2$. We may assume $0 < y_1 < y_2$. So we have $y_2 = p^2 - y_1 > y_1$. It follows $p^2 > 2y_1$.

By $p < M_\Delta$, we have $p^2 < 4|d|/3$. If $y_1 \geqq |d|$, then we get $p^2 > 2y_1 \geqq 2|d|$, which contradicts to $p^2 < 4|d|/3$. Therefore we get $y_1 < |d|$.

Set $x = y_1$, we obtain $P^2 = [p^2, x + \omega]$. Therefore we have proved that if p is odd, $\left(\dfrac{\Delta}{p}\right) = 1$, and $p < M_\Delta$, then $P^2 = [p^2, x + \omega]$ for a positive rational integer x.

Furthermore by $e_\Delta = 2$, we obtain that P^2 is a principal ideal.

Since $x < |d|$, we get

$$N(x + \omega) = x^2 + |d| \leqq (|d| - 1)^2 + |d| = |d|^2 - |d| + 1 < |d|^2 = N(\omega)^2.$$

Thus $N(x + \omega) < N(\omega)^2$.

Therefore by Lemma 1, we obtain $p^2 = N(x + \omega)$.

Next we consider the case $\Delta \equiv 1 \pmod 4$.

Let $P = [p, x_1 + \omega]$, where x_1 is a non-negative rational integer less than p. We have

$$P^2 = [p^2, p\,(x_1 + \omega), (x_1 + \omega)^2]$$
$$= [p^2, px_1 + p\omega, x_1^2 - (1 + |d|)/4 + (2x_1 + 1)\,\omega].$$

If gcd $(p, 2x_1 + 1) \neq 1$, then we get $2x_1 + 1 = p$ since $x_1 < p$. Hence we have

$$N(x_1 + \omega) = N\left(\frac{p-1}{2} + \omega\right) = \left(\frac{p-1}{2}\right)^2 + \frac{p-1}{2} + \frac{1+|d|}{4} = \frac{p^2+|d|}{4}.$$

Since $N(x_1 + \omega) \equiv 0 \pmod p$, we have $d \equiv 0 \pmod p$, which contradicts to $\left(\frac{\Delta}{p}\right) = 1$. Therefore we get gcd $(p, 2x_1 + 1) = 1$. By the same reason as in the case $\Delta \equiv 0 \pmod 4$, we obtain $P^2 = [p^2, y_1 + \omega]$, where $y_1 \equiv x_1 - tpc \pmod{p^2}$, and $pc = x_1^2 + x_1 + (1 + |d|)/4$. Similarly, we have $P'^2 = [p^2, y_2 + \omega]$.

We may assume $y_1 < y_2$.

Since $p \geqq 3$ and $p < M_\Delta = \sqrt{|d|/3}$, we have $|d| > 27$.

If $y_1 \geqq (|d| - 3)/4$, then we have $p^2 > 2y_1 \geqq (|d| - 3)/2$ by $y_2 = p^2 - y_1 > y_1$, which leads to a contradicton. Therefore $y_1 < (|d| - 3)/4$.

Set $x = y_1$, we obtain $P^2 = [p^2, x + \omega]$. Therefore we have proved that if p is odd, $\left(\frac{\Delta}{p}\right) = 1$, and $p < M_\Delta$, then $P^2 = [p^2, x + \omega]$ for a non-negative rational integer x.

Furthermore by $e_\Delta = 2$, we obtain that P^2 is a principal ideal.

Since $x < (|d| - 3)/4$, we get

$$N(x + \omega) = x^2 + x + \frac{1+|d|}{4}$$
$$< \left(\frac{|d|-3}{4}\right)^2 + \frac{|d|-3}{4} + \frac{1+|d|}{4} = \left(\frac{1+|d|}{4}\right)^2 = N(\omega)^2.$$

Hence $N(x + \omega) < N(\omega)^2$.

Therefore by Lemma 1, we obtain $p^2 = N(x + \omega)$.

Thus we complete the proof of Lemma 2.

Remark. By $p^2 = N(x + \omega)$, we have $x^2 < p^2$, i.e., $x < p$. Hence we get $x = x_1$.

Furthermore we show the following lemma.

Lemma 3. *Let $|d| = ab \equiv 2 \pmod 4$ be a square-free rational integer and p a prime. If $a + b \equiv 0 \pmod p$, then p is odd and* $\left(\frac{\Delta}{p}\right) = 1$.

Proof. We put $a + b = pc$, where $c \geqq 1$ is a rational integer. Since $a + b$ is odd, we get $p \neq 2$.

By $|d| = ab = a\,(pc - a) = acp - a^2$, it follows $a^2 \equiv d \pmod p$. So we have $(2a)^2 \equiv \Delta \pmod p$. If $a \equiv 0 \pmod p$, then we have $b \equiv 0 \pmod p$ since $a + b \equiv 0 \pmod p$. Hence $|d| \equiv 0 \pmod{p^2}$, which contradicts to d being square-free. Therefore we get $a \not\equiv 0 \pmod p$.

Thus we obtain $\left(\dfrac{\Delta}{p}\right)=1$, which completes the proof of Lemma 3.

By the same lines as in the proof of Lemma 3, we can prove the following two lemmas.

Lemma 4. *Let* $|d| = ab \equiv 1$ (*mod* 4) *be a square-free rational integer and p a prime. If* $\dfrac{a+b}{2} \equiv 0$ (*mod p*), *then p is odd and* $\left(\dfrac{\Delta}{p}\right)=1$.

Lemma 5. *Let* $|d| = ab \equiv 3$ (*mod* 8) *be a square-free rational integer and p a prime. If* $\dfrac{a+b}{4} \equiv 0$ (*mod p*), *then p is odd and* $\left(\dfrac{\Delta}{p}\right)=1$.

Using the above lemmas we prove Theorem 2 and 3.

Proof of Theorem 2. First, we consider the case of $|d| = ab \equiv 2$ (*mod* 4).

To prove that $|d|$ is a SP-number, we assume that $a + b$ is not a prime and p is the least prime which divides $a + b$. Let $c = (a + b)/p$.

By Lemma 3, we obtain that p is odd and $\left(\dfrac{\Delta}{p}\right)=1$.

We have $a + b \leqq 1 + |d|$, because

$$1 + |d| - (a + b) = 1 + ab - a - b = (a - 1)(b - 1) \geqq 0.$$

Hence we get $p^2 \leqq a + b \leqq 1 + |d|$.

Since $e_\Delta = 2$, we have $|d| \neq 2$. Hence $|d| \geqq 6$, it follows $1 + |d| < 4|d|/3$. Thus we get $p^2 < 4|d|/3$, i.e., $p < \sqrt{|\Delta|/3} = M_\Delta$.

Therefore by Lemma 2, we obtain $p^2 = N(x + \omega) = x^2 + |d|$ for a positive rational integer x.

If $x = 1$, then $p^2 = 1 + |d|$, that is, $|d| = p^2 - 1 = (p + 1)(p - 1) \equiv 0$ (mod 4) as $p \neq 2$, which leads to a contradiction.

Thus we get $x > 1$ and

$$a + b = pc \geqq p^2 = x^2 + |d| > 1 + |d|.$$

So we have $a + b > 1 + |d|$, which contradicts to $a + b \leqq 1 + |d|$.

Therefore $a + b$ is a prime.

Second, we consider the case of $|d| = ab \equiv 1$ (mod 4).

By the same way as mentioned above, assume that $(a + b)/2 = pc$, where p is the least prime divisor of $(a + b)/2$.

By Lemma 4, p is odd and $\left(\dfrac{\Delta}{p}\right)=1$.

Since $e_\Delta = 2$, we have $|d| \neq 1$. Hence $|d| \geqq 5$, it follows

$$p^2 \leqq \frac{a+b}{2} \leqq \frac{1+|d|}{2} < 1+|d| < \frac{4|d|}{3}.$$

Thus we get $p < M_\Delta$.

By Lemma 2, we obtain $p^2 = N(x + \omega) = x^2 + |d|$ for a positive rational integer x.

By the same reason as above, we have $x > 1$. So $p^2 = x^2 + |d| > 1 + |d|$.

Hence we get $a + b > (a + b)/2 \geqq p^2 > 1 + |d|$, which leads to a contradiction. This completes the proof of Theorem 2.

Furthermore we prove Theorem 3 by the same lines as in the proof of Theorem 2.

Proof of Theorem 3. Assume that $|d| = ab$ and $(a + b)/4 = pc$, where p is the least prime divisor of $(a + b)/4$.

By Lemma 5, p is odd and $\left(\dfrac{\Delta}{p}\right) = 1$.

Since $e_\Delta = 2$, we have $|d| \neq 3, 11, 19$. Hence $|d| > 19$.

We have

$$p \leqq \sqrt{\frac{a+b}{4}} \leqq \sqrt{\frac{1+|d|}{4}} < \sqrt{\frac{|d|}{3}} = M_\Delta.$$

By Lemma 2, we have $p^2 = N(x + \omega) = x^2 + x + (1 + |d|)/4$.

So we have

$$\frac{a+b}{4} = pc \geqq p^2 = x^2 + x + \frac{1+|d|}{4} > \frac{1+|d|}{4},$$

because $(1 + |d|)/4$ is not a square, we have $x \neq 0$.

Therefore we get $(a + b)/4 > (1 + |d|)/4$, i.e., $a + b > 1 + |d|$, which leads to a contradiction. This completes the proof of Theorem 3.

4. Numerical Observation of SP-Numbers

In section 3, we give a sufficient condition by Theorem 1, 2, and 3. It is known that there are only finitely many imaginary quadratic fields with $e_\Delta \leqq 2$ (see Chowla [3] or Weinberger [4]). But it seems that there are many SP-numbers.

In section 2, we list up SP-numbers less than 1000. In the list there are 123 SP-numbers; if $n \equiv 2 \pmod 4$, there are 27 SP-numbers, if $n \equiv 1 \pmod 4$, there are 57 SP-numbers, and if $n \equiv 3 \pmod 4$, there are 39 SP-numbers.

There are 2728 SP-numbers less than 100000.

The following table shows the number of SP-numbes and prime numbers less than n.

n	SP-numbers	prime numbers
100	31	25
1000	123	168
10000	532	1229
100000	2728	9592

By the above table, it seems that there are less SP-numbers than prime numbers. In fact we observe that there are less SP-numbers than prime numbers if $n \geqq 257$.

Are there infinitely many SP-numbers ?

References

[1] Mollin, R. A., Quadratics, CRC Press, Boca Raton, New York, London, Tokyo (1995).

[2] Sasaki, R., On a lower bound for the class number of an imaginary quadratic field, Proc. Japan Acad. Ser. A **62** (1986), 37–39.

[3] Chowla, S., An extention of Heilbronn's class-number theorem, Quart. J. Math. Oxford **5** (1934), 304–307.

[4] Weinberger, P. J., Exponents of the class groups of complex quadratic fields, Acta. Arith. **22** (1973), 117–124.