Euler's Convenient Numbers

§0. Introduction

In the classical consideration of numbers of the form $x^2 + ny^2$, we find a set of convenient formulas for certain values of n. Recall in Cox (see [1, 2.28]) a list is given of congruences for primes p:

Proposition 0.1. *If p is a prime, then*

$$p = x^2 + 6y^2 \Leftrightarrow p = 1, 7 \pmod{24}$$
$$p = x^2 + 10y^2 \Leftrightarrow p = 1, 9, 11, 19 \pmod{40}$$
$$p = x^2 + 13y^2 \Leftrightarrow p = 1, 9, 17, 25, 29, 49 \pmod{52}$$
$$p = x^2 + 15y^2 \Leftrightarrow p = 1, 19, 31, 49 \pmod{60}$$
$$p = x^2 + 21y^2 \Leftrightarrow p = 1, 25, 37 \pmod{84}$$
$$p = x^2 + 22y^2 \Leftrightarrow p = 1, 9, 15, 23, 25, 31, 47, 49, 71, 81 \pmod{88}$$
$$p = x^2 + 30y^2 \Leftrightarrow p = 1, 31, 49, 79 \pmod{120}.$$

Certain numbers n, as we shall see, yield a nice set of congruences. Specifically, numbers n such that if m is odd, $(m, n) = 1$, and $m = x^2 + ny^2$ has only one solution for non-negative x, y, then m is prime. It turns out 11 is not such a number. For example, using the previous condition, $2^2 + 11 \cdot 1^2$ is the only representation of 15 as $x^2 + 11y^2$, yet 15 is not prime. If we wish to find primes such that $p = x^2 + 11y^2$, then we would have to use the methods of class field theory (as developed in Cox, [1, §5-9]).

The numbers n that do provide convenient congruences are aptly named *convenient numbers.* Although class field theory makes the existence of these numbers less crucial for computing primes of the form $x^2 + ny^2$, they are still interesting for historical and computational reasons. For example, Euler was able to find the prime

$$18{,}518{,}809 = 197^2 + 1848 \cdot 100^2$$

by noticing 1848 is convenient. In this paper, we will see that there are only finitely many of these numbers. In fact, the highest such number is 1848--*if* the Riemann hypothesis holds! If it does not, there is at most one more (pretty large) such number. This last fact is a deep result due to Weinberger that we will sketch at the end. First, we recall some basic theorems and facts from genus theory.

§1. Genus Theory

Proposition 1.1. *Let $D \equiv 0, 1 \pmod 4$ be an integer and m be an odd integer relatively prime to D. Then m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue modulo m. As a corollary, if n is an integer and p is an odd prime not dividing n, then $(\frac{-n}{p}) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.*

Proof. See [1, Lemma 2.5] and [1, Corollary 2.6] in Cox. □

Theorem 1.2. (Classification of Primitive Positive Definite Forms) *Let $D \equiv 0, 1 \pmod 4$ with $D < 0$, and let $C(D)$ be the set of primitive positive definite forms of discriminant D. Then Dirichlet composition induces a well-defined binary operation on $C(D)$, which makes $C(D)$ into a finite Abelian group whose order is the class number $h(D)$. Furthermore, the identity element of $C(D)$ is the class containing the principal form*

$$\begin{aligned} &x^2 - \tfrac{D}{4}y^2 && \text{if } D \equiv 0 \pmod 4, \\ &x^2 + xy + \tfrac{1-D}{4}y^2 && \text{if } D \equiv 1 \pmod 4) \end{aligned}$$

and the inverse of the class containing the form $ax^2 + bxy + cy^2$ is the class containing $ax^2 - bxy + cy^2$.

Proof. See [1, Theorem 3.9] in Cox. □

Definition 1.3. *The group $C(D)$ in the previous theorem is called the* class group. *The principal form of discriminant D is called the* principal class. *The form $ax^2 - bxy + cy^2$ is called the* opposite *of $ax^2 + bxy + cy^2$, so that the opposite form gives the inverse under Dirichlet composition.*

Proposition 1.4. *A reduced form $f(x, y) = ax^2 + bxy + cy^2$ of discriminant D has order ≤ 2 in the class group $C(D)$ if and only if $b = 0, a = b$ or $a = c$.*

Proof. See [1, Lemma 3.10] in Cox. □

Proposition 1.5. *Let $D \equiv 0, 1 \pmod 4$ with $D < 0$. Take r to be the number of odd primes dividing D. Define the number μ as follows: if $D \equiv 1 \pmod 4$,* then *$\mu = r$, and if $D \equiv 0 \pmod 4$, then $D = -4n$, where $n > 0$, and μ is given by:*

$$\mu = \begin{cases} r & \text{if } n \equiv 3 \pmod 4 \\ r+1 & \text{if } n \equiv 1, 2 \pmod 4 \\ r+1 & \text{if } n \equiv 4 \pmod 8 \\ r+2 & \text{if } n \equiv 0 \pmod 8). \end{cases}$$

Then the class group $C(D)$ has exactly $2^{\mu-1}$ elements of order ≤ 2.

Proof. See [1, Proposition 3.11] in Cox. □

Theorem 1.6. (Main Theorem of Genus Theory) *Let $D \equiv 0, 1 \pmod 4$ with $D < 0$. Then*

(i) *All genera of forms of discriminant D consist of the same number of classes.*

(ii) *There are $2^{\mu-1}$ genera of forms of discriminant D, where μ is given in the previous proposition.*

(iii) *The principal genus consists of the classes in $C(D)^2$, the subgroup of squares in the class group $C(D)$*

Proof. See [1, Theorem 3.15] in Cox. □

Proposition 1.7. *Let $f(x,y)$ and $g(x,y)$ be primitive forms of discriminant $D \neq 0$, positive definite if $D < 0$. Then the following statements are equivalent:*

(i) *$f(x,y)$ and $g(x,y)$ are in the same genus, i.e., they represent the same values in $(\mathbb{Z}/d\mathbb{Z})^*$.*

(ii) *$f(x,y)$ and $g(x,y)$ represent the same values in $(\mathbb{Z}/m\mathbb{Z})^*$ for all non-zero integers m.*

(iii) *$f(x,y)$ and $g(x,y)$ are equivalent modulo m for all non-zero integers m.*

Proof. See [1, Theorem 3.21] in Cox. □

§2. Convenient numbers

In §0, we introduced convenient numbers: those n for which genus theory gives a congruence condition for $x^2 + ny^2$. In this section, we will pass to the language of classes using our knowledge from §1. Notice that investigating convenient numbers is the same as considering each genus of discriminant $-4n$ that consists of a single class. The following theorems make this precise.

Theorem 2.1. *Let n be a positive integer. Then the following statements are equivalent:*

(i) *Every genus of forms of discriminant $-4n$ consists of a single class.*

(ii) *If $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$, or $a = c$.*

(iii) *Two forms of discriminant $-4n$ are equivalent if and only if they are properly equivalent.*

(iv) *The class group $C(-4n)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some integer m.*

(v) *The class number $h(-4n)$ equals $2^{\mu-1}$, where μ is as in Proposition 1.5.*

Proof. Let $C = C(-4n)$ be the class group for discriminant $-4n$. Assume each genus of forms of discriminant $-4n$ consists of a single class. We will show that if $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$, or $a = c$. From Proposition 1.4, it suffices to show that a reduced form of discriminant D has order 1 or 2 in C. From Theorem 1.6(iii) (the main theorem of genus theory), we know that the principal genus is C^2. Since we assumed each genus of forms of discriminant $-4n$ consists of a single class, by definition this gives $C^2 = \{1\}$. Hence, each element in C has order ≤ 2. This shows (i) $\Longrightarrow$ (ii).

Assume that if $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$, or $a = c$. We will show two forms of discriminant $-4n$ are equivalent if and only if they are properly equivalent. The right-to-left implication is obvious. Without loss of generality, consider two equivalent reduced forms of discriminant $-4n$, say

$$f(x,y) = ax^2 + bxy + cy^2 \text{ and } g(x,y) = dx^2 + exy + fy^2.$$

Then by definition there are $p, q, r, s \in \mathbb{Z}$ so that

$$f(x,y) = g(px+qy, rx+sy)$$

with $ps - qr = \pm 1$. First, notice we can use our assumption to give $b = 0, a = b$, or $a = c$. We claim that f is properly equivalent to g or its opposite. If f is not properly equivalent to g, it must be improperly equivalent to g, that is, $ps - qr = -1$. But then if we let g' denote the opposite of g,

$$\begin{aligned} g'(-px-qy, rx+sy) &= d(-px-qy)^2 - e(-px-qy)(rx+sy) + f(rx+sy)^2 \\ &= d(px+qy)^2 + e(px+qy)(rx+sy) + f(rx+sy)^2 \\ &= g(px+qy, rx+sy) = f(x,y), \end{aligned}$$

with $(-p)s - (-q)r = -(ps-qr) = -(-1) = 1$. Hence, f is properly equivalent to the opposite of g. This proves the claim. We continue by showing that reduced forms are properly equivalent to their opposite (so in particular, f and g are properly equivalent to their opposite). Let $h(x,y) = \alpha x^2 + \beta xy + \gamma y^2$ be a reduced form and h' its opposite. If $\beta = 0$, then this is trivial. If $\alpha = -\beta$, then

$$\begin{aligned} h(x,y) &= \alpha x^2 + \beta xy + \gamma y^2 = \alpha x^2 - \alpha xy + \gamma y^2 = \alpha x^2 - 2\alpha xy + \alpha y^2 + \alpha xy - \alpha y^2 + \gamma y^2 \\ &= \alpha(x-y)^2 + \alpha(x-y)y + \gamma y^2 = \alpha(x-y)^2 - \beta(x-y)y + \gamma y^2 = h'(x-y, y) \end{aligned}$$

so that since $1 \cdot 1 - (-1) \cdot 0 = 1$, by definition h is properly equivalent to h'. Similarly, if $\alpha = \gamma$, then

$$h(x,y) = \alpha x^2 + \beta xy + \gamma y^2 = \alpha x^2 + \beta xy + \alpha y^2 = \alpha(-y)^2 - \beta(-y)x + \alpha x^2 = h'(-y, x),$$

so that again h is properly equivalent to h'. Hence, we have shown that the original f and g are properly equivalent to each other or their opposite, but since they are reduced, that means their opposites are properly equivalent to each other, and hence f and g are properly equivalent. This shows (ii) ⇒ (iii).

Assume two forms of discriminant $-4n$ are equivalent if and only if they are properly equivalent. We want to show the class group $C \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{Z}$. It is easy to see any form is equivalent to its opposite through $(x,y) \mapsto (x,-y)$. Hence, by our assumption, for any form in C its opposite must lie in C as well since they are properly equivalent. Then the last statement from Theorem 1.2 tells us the opposite of a form and its inverse are in the same class in C, so that each class is its own inverse. In other words, C is a finite abelian group with all elements of order 2. Then by the classification of finite abelian groups, $C \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{Z}$ (since a component of any other $\mathbb{Z}/d\mathbb{Z}$ for $d > 2$ would give an element of order d). This shows that (iii) ⇒ (iv).

Furthermore, assume $C \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{Z}$. By Theorem 1.6(ii), the number of genera is the index of C^2 in C, that is, $2^{\mu-1}$. Hence, the class number

$$h(-4n) = |C| = [C : C^2] \cdot |C^2| = 2^{\mu-1}|C^2|.$$

Since we assumed $C \cong (\mathbb{Z}/2\mathbb{Z})^m$, obviously $C^2 \cong 1$. Hence, $h(-4n) = 2^{\mu-1}$. This prove (iv) ⇒ (v).

Finally, assume $h(-4n) = 2^{\mu-1}$. Then as above, $h(-4n) = 2^{\mu-1}|C^2|$ means that $C^2 \cong 1$, so that by Theorem 1.6(iii), the principal genus consists of a single class. However, the genera of forms all consist of the same number of classes, so each genus consists of a single class. This means (v) ⇒ (i), which concludes the proof. □

We will now make the connection between convenient numbers and forms of discriminant $-4n$ whose genus consists of a single class. For sake of preciness, we will use Euler's traditional definition of a convenient number.

Definition 2.2 *Let m be an odd number relatively prime to n, which is properly represented by $x^2 + ny^2$. If the equation $m = x^2 + ny^2$ has only one solution with $x, y \geq 0$, then m is a prime number, and n is called a* convenient number.

Proposition 2.3. *A positive integer n is a convenient number if and only if for forms of discriminant $-4n$, every genus consists of a single class.*

The above proposition asserts the n in Theorem 2.1 can be given by all five equivalent definitions (i)-(v).

Lemma 2.4. *Let m be a positive odd number relatively prime to $n > 1$. Then the number of ways that m is properly represented by a reduced form of discriminant $-4n$ is*

$$2 \prod_{p\,|\,m} \left(1 + \left(\tfrac{-n}{p}\right)\right).$$

Proof. Let $n > 1$ and $m > 0$ be odd with $(m, n) = 1$. Let p be a prime dividing m. We will show that $x^2 \equiv -n \pmod{m}$ has

$$\prod_{p\,|\,m} \left(1 + \left(\tfrac{-n}{p}\right)\right)$$

solutions. Recall that a polynomial

$$f(x) \equiv 0 \pmod{r}$$

has $\prod n_i$ solutions, where n_i is the number of solutions of $f(x) \equiv 0 \pmod{p_i^{d_i}}$ with $r = \prod p_i^{d_i}$ the prime decomposition of r. (This is a direct application of the Chinese Remainder Theorem; for a detailed proof, see [12, Theorem 5.25] in Apostol). In other words, to find the number of solutions for

$$x^2 + n \equiv 0 \pmod{m},$$

it is sufficient to know the number of solutions of

$$x^2 + n \equiv 0 \left(\operatorname{mod} p_i^{d_i}\right),$$

where $p_i^{d_i}$ is a component of the prime decomposition of $m = \prod p_i^{d_i}$. However, notice that if $(\frac{-n}{p_i}) = -1$, then this last equation has no solutions, so indeed it has $0 = 1 + (\frac{-n}{p_i})$ $= n_i$ solutions. Now consider $(\frac{-n}{p}) = 1$. This means there is at least one solution. Assume there were multiple solutions, that is, there is a y such that

$$x^2 \equiv y^2 \equiv -n \left(\operatorname{mod} p_i^{d_i}\right) \text{ (with } p \nmid y).$$

Then $p_i^{d_i}$ divides $x^2 - y^2 = (x-y)(x+y)$. However, it can only divide one of the two factors since $(x+y)+(x+y) = 2x$ and $p \nmid 2x$ (i.e., it doesn't divide their sum). But then

$$x \equiv \pm y \left(\text{mod } p_i^{d_i}\right)$$

so indeed there are only two solutions. Again, there are $2 = 1 + \left(\frac{-n}{p_i}\right) = n_i$ solutions.

Hence, in total, there are

$$\prod n_i = \prod_{p \mid m} \left(1 + \left(\frac{-n}{p}\right)\right)$$

solutions to the congruence $x^2 \equiv -n \,(\text{mod } m)$.

Now, consider forms $g(x,y)$ of discriminant $-4n$ of the form

$$g(x,y) = mx^2 + 2bxy + cy^2 \;\; (0 \leq b < m). \tag{$*$}$$

Then the discriminant of $g(x,y)$ is $(2b)^2 - 4mc = -4n$. Hence, we need $b^2 - mc = -n$. However, since m and n are fixed, notice b determines c uniquely. Hence, this is precisely equivalent to solutions for

$$b^2 - mc \equiv -n \,(\text{mod } m), \text{ that is,}$$

$$b^2 \equiv -n \,(\text{mod } m).$$

In other words, there is a bijection between $g(x,y)$ and solutions of $x^2 \equiv -n \,(\text{mod } m)$.

Take $f(x,y) = ax^2 + bxy + cy^2$ to be a form of discriminant $-4n$ and let $f(u,v) = m$ be a proper representation. Let r_0, s_0 be such that $us_0 - vr_0 = 1$, and let $r = r_0 + uk$ and $s = s_0 + vk$. Then as $k \in \mathbb{Z}$ varies, we get all solutions of $us - vr = 1$. Finally, let

$$g(x,y) = f(ux + ry, vx + sy).$$

Now

$$g(x,y) = a(ux+ry)^2 + b(ux+ry)(vx+sy) + c(vx+sy)^2 =$$

$$= au^2x^2 + 2aurxy + ar^2y^2 + buvx^2 + busxy + brvxy + brsy^2 + cv^2x^2 + 2cvsxy + cs^2y^2$$

$$= (au^2 + buv + cv^2)x^2 + (2aur + bus + brv + 2cvs)xy + (ar^2 + brs + cs^2)y^2$$

$$= mx^2 + (2(aur + cvs) + b(us + vr))xy + Cy^2.$$

Now, pick the unique $k \in \mathbb{Z}$ so that $us + vr = 0$. Then $0 \leq aur + cvs < m$ and so $g(x,y)$ is uniquely represented as $(*)$. Call this $g_{u,v}(x,y)$. Notice that the map sending a proper representation $f(u,v) = m$ to $g_{u,v}(x,y)$ is onto, since each of the above steps is reversible (so that we can start with $g_{u,v}(x,y)$ and show there is an $f(x,y)$ such that $g_{u,v}(x,y) = f(ux + ry, vx + sy)$).

Assume $g_{u',v'}(x,y) = g_{u,v}(x,y)$ with

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} u' & v' \\ r' & s' \end{pmatrix}^{-1} \begin{pmatrix} u & v \\ r & s \end{pmatrix}.$$

Using the fact $\alpha\delta - \beta\gamma = (us - rv)/(u's' - r'v')$ (by determinants) and expanding $f(\alpha x + \beta y, \gamma x + \delta y)$, we see that $f(\alpha x + \beta y, \gamma x + \delta y) = f(x, y)$. Then by the same argument as in [1, Theorem 2.8] in Cox (assuming $f(x, y)$ is reduced), $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Finally, this implies $g_{u',v'}(x, y) = g_{u,v}(x, y)$ if and only if $(u', v') = \pm (u, v)$ (just multiply by $\left(\begin{smallmatrix} u' & v' \\ r' & s' \end{smallmatrix}\right)$ on the left in the above matrix equation), so that the map sending a proper representation $f(u, v)$ to the form $g_{u,v}(x, y)$ is two-to-one in addition to being onto. Hence, by the earlier correspondence between forms as in $(*)$ and solutions of $x^2 \equiv -n \pmod{m}$, there are twice as many ways to properly represent m by a reduced form of discriminant $-4n$ as there are solutions to $x^2 \equiv -n \pmod{m}$. We have already computed the latter, so indeed there are

$$2 \prod_{p\,|\,m} \left(1 + \left(\tfrac{-n}{p}\right)\right)$$

representations in total. □

Corollary 2.5. *Let m be properly represented by a primitive positive definite form $f(x, y)$ of discriminant $-4768\ n$, $n > 1$, and assume that m is odd and relatively prime to n. If r denotes the number of prime divisors of m, then m is properly represented in exactly 2^{r+1} ways by a reduced form in the genus of $f(x, y)$.*

Proof. Since two forms representing m do not have disjoint values in $(\mathbb{Z}/4n\mathbb{Z})^*$, they must lie in the same genus. Then by Proposition 1.1, for each prime $p\,|\,m$, $\left(\frac{-n}{p}\right) = 1$ (since $(m, n) = 1$ implies $p \nmid n$), so that by the previous lemma m is properly represented in $2 \cdot 2^r = 2^{r+1}$ ways. □

Proof. (of Proposition 2.3) We will first show the right-to-left implication. Assume that for forms of discriminant $-4n$, every genus consists of a single class. By Definition 2.2, we need to show that if m is properly represented by $x^2 + ny^2$ and $m = x^2 + ny^2$ ($x, y \geq 0$), then m is prime. Since $x^2 + ny^2$ is the only reduced form in its genus, by the previous Corollary (2.5), m is properly represented by $x^2 + ny^2$ in 2^{r+1} ways. Now, since x can be positive or negative and y can be positive or negative, at least $1/4$ of these are the ones with x and y both positive. That is, there are 2^{r-1} ways of writing $m = x^2 + ny^2$ with $x, y \geq 0$. We assumed that m has a unique such solution, so that $2^{r-1} = 1$, that is, $r = 1$. In other words, m has a single prime divisor, so that $m = p^k$ for some $k \in \mathbb{Z}^+$. If $k = 1$, then m is already prime. If $k \geq 2$ (i.e., m is not a prime), then by Lemma 2.4, p^{k-2} has at least 2 representations. But then $m = p^k$ has at least 8 representations so m is properly represented in at least 2 ways with $x, y \geq 0$, which contradicts our assumption that it is represented in such a way uniquely. Hence, $k \geq 2$ gives a contradiction, so that indeed m is prime. By Definition 2.2., n is hence a convenient number.

Conversely, assume n is convenient. Take $f(x, y)$ to be a form of discriminant $-4n$, and let $g(x, y)$ be the Dirichlet composition of $f(x, y)$ with itself. Without loss of generality, assume that $g(x, y)$ is reduced. Then by Theorem 2.1, if $g(x, y) = x^2 + ny^2$ then since each element in the class group has order ≤ 2, each genus consists of a single class. Hence, it suffices to show $g(x, y) = x^2 + ny^2$. By way of contradiction, assume that $g(x, y) \neq x^2 + ny^2$. Assume $p \neq q$ are odd primes not dividing n which are represented by $f(x, y)$. Then since $g(x, y)$ is the Dirichlet composition of $f(x, y)$ with itself, pq is represented by $f(x, y)$. Then by Corollary 2.5, since $r = 2$, pq has $2^{2+1} = 8$ proper representations by a reduced forms of discriminant $-4n$. Since 1 of these is due to $g(x, y)$, there are at most 7 ways to write $pq = x^2 + ny^2$. If $x, y \geq 0$ satisfy this equation, then so do $(-x, y)$, $(x, -y)$, and $(-x, -y)$. Hence, if there were two unique solutions for $pq = x^2 + ny^2$ with $x, y \geq 0$, then there would be 8 in total, a contradiction. Hence, $pq = x^2 + ny^2$ has a unique solution for $x, y \geq 0$. Then since $(pq, n) = 1$, pq is properly represented by $x^2 + ny^2$, and $pq = x^2 + ny^2$ has a unique solution for $x, y \geq 0$, by Definition 2.2, pq should be a prime since n is convenient. Of course, it isn't, which gives the desired contradiction. Therefore, $g(x, y) = x^2 + ny^2$. □

In this section, we looked at convenient numbers more carefully, and showed their characterization by the statements in Theorem 2.1. We will now look concretely at which numbers are convenient.

§3. Existence of only finitely many convenient numbers

In the previous section, we used genus theory to talk about the connection between convenient numbers and forms of discriminant $-4n$ whose genus consists of a single class. Convenient numbers allow us to provide an elementary condition (congruence) for when a number $x^2 + ny^2$ is prime. Hence, we conclude by investigating which numbers are convenient. It can be checked manually that the following 65 integers $n \leq 1848$ are convenient numbers.

Table 3.1. *List of convenient numbers* ≤ 1848.

$h(-4n)$	all such n with one class per genus
1	$1, 2, 3, 4, 7$
2	$5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58$
4	$21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85,$ $88, 98, 102, 112, 130, 133, 177, 190, 232, 253$
8	$105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345,$ $357, 385, 408, 462, 520, 760$
16	$840, 1320, 1365, 1848$

Euler and Gauss noticed early on that there do not seem to be any more convenient numbers immediately after 1848. In 1914, D. N. Lehmer verified this up to 1,000,000 using sieve methods and an electro-mechanical computer (for more on this, read about the Lehmer sieve). Euler was very troubled by the sudden disappearance of convenient numbers past 1848 (the existence of infinitely many such numbers would make classical methods for finding large primes much more effective). In order to convince himself that there were indeed no such relatively small numbers past 1848, Euler proved the following proposition. This helped him narrow down which numbers could be convenient.

Proposition 3.2. *Let m be a convenient number. Then*

(i) *If* m *is a perfect square, then* $m = 1, 2, 3, 4$ *or* 5.

(ii) *If* $m \equiv 3 \pmod{4}$*, then* $4m$ *is convenient.*

(iii) *If* m *is convenient and* $m \equiv 4 \pmod{8}$*, then* $4m$ *is convenient.*

(iv) *If* $k \in \mathbb{Z}^+$ *so that* k^2m *is convenient, then* m *is convenient.*

(v) *If* $m \equiv 2 \pmod{3}$*, then* $9m$ *is convenient.*

(vi) *If* $m > 1$ *with* $m \equiv 1 \pmod{4}$*, then* $4m$ *is not convenient.*

(vii) *If* $m \equiv 2 \pmod{4}$*, then* $4m$ *is convenient.*

(viii) *If* $m \equiv 8 \pmod{16}$*, then* $4m$ *is not convenient.*

(ix) *If* $m \equiv 16 \pmod{32}$*, then* $4m$ *is not convenient.*

(x) *If there is a prime* p *with* $a \in \mathbb{Z}^+$ *such that* $m + a^2 = p^2 < 4m$*, then* $4m$ *is not convenient.*

Proof. Euler attempted to prove all of these in [3], but (iv), (vi), (viii), and (ix) had errors. Grube corrected these in [2], completing the proof of the theorem. If one spends time looking at these conditions, then it becomes increasingly clear that the convenient numbers significantly thin out at some point (e.g., 1848). □

This proposition certainly provides some insight into the nature of convenient numbers, but it does not give any information about how many there are. This did not become more apparent until 1934, when S. Chowla proved ([4]) that there are finitely many convenient numbers. This paper used the fact that

$$\lim_{d\to\infty} \frac{h(-d)}{g(-d)} = \infty,$$

where $g(d)$ denotes the number of genera of binary quadratic forms with discriminant d. In 1954, Briggs and Chowla used Siegel's asymptotic formula to give some concrete bounds (see [5]). Later, in 1963, E. Grosswald improved on this further by using the analytic class number formula (see [6]), and all this culminated in the most current result by Weinberger (see [7]), which states there are no convenient numbers past 1848 unless a weaker assumption than the Riemann hypothesis is false, in which case there is at most one.

Theorem 3.3. *There is at most one convenient number larger than* 1848.

The proof of this theorem uses some deep results discovered by Tatuzawa, and the proof of these is beyond the scope of this paper. We begin with a reminder of the notation and nature of L-series. First, the special case

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is the Riemann zeta function. This function has no zeros when $\text{Re}(s) > 1$, and it has trivial zeros for even negative numbers. Finally, any non-trivial zero lies in the strip $\{s \in \mathbb{C} \mid 0 < \text{Re}(s) < 1\}$, the "critical strip." The Riemann hypothesis states that any non-trivial zero has $\text{Re}(s) = \frac{1}{2}$; in other words, the only zeros of $\zeta(s)$ are the negative even numbers and those with real part $\frac{1}{2}$. It is obvious that lemmas 3.4 and 3.5 give a weaker criterion, and hence are not as strong as the Riemann hypothesis.

The generalization of $\zeta(s)$ is the Dirichlet L-series. If χ is a Dirichlet character, then

$$L(\chi, s) = \sum_{r=1}^{\infty} \frac{\chi(r)}{r^s},$$

for each complex number $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. The zeros of the L-series shares the same characteristics as the Riemann zeta function. Indeed, the generalized Riemann hypothesis states that in the critical strip, any $L(\chi, s) = 0$ satisfies $\mathrm{Re}(s) = \frac{1}{2}$. In our case, we will use

$$\chi(r) = \chi_{-d}(r) = \left(\tfrac{-d}{r}\right),$$

the Kronecker symbol (see [1, pg. 104] and [1, §7.D] in Cox). In this case,

$$L(\chi, x) = \sum_{r=1}^{\infty} \frac{\left(\frac{-d}{r}\right)}{r^s}.$$

Furthermore, assume $d = 4n > 4$ (so that we are excluding $n = 1$). For a quadratic field $k = \mathbb{Q}\left[\sqrt{-d}\right]$, we denote the class number by $h(-d)$. Furthermore, define $e(-d)$ be the least positive integer such that $P^{e(-d)} = 1$ for each P in the ideal class group $C = C(\mathcal{O}_k)$ (where 1 is understood as the ideal class of the principal ideals, which forms an identity on $C(\mathcal{O}_k)$). This number $e(-d)$ is called the exponent of the ideal class group. Then if $e(-d) = 2$, by definition each element $P \in C$ has order ≤ 2, so by Theorem 2.1 these n ($d = 4n$) are exactly the convenient numbers (where we have preserved some results using ideals instead of forms--see the last paragraph on [1, pg. 112 and Theorem 5.30 and Theorem 7.22], which states for $-d < 0$, $C(d_k) \cong C(\mathcal{O}_k)$). Finally, we assume the aforementioned lemmas.

Lemma 3.4. *For fixed $0 < \varepsilon < \frac{1}{2}$, if $d \geq e^{1/\varepsilon}$ and $L(\chi, 1) \leq \frac{0.655\varepsilon}{d^\varepsilon}$, then $L(\chi, s)$ has a real root s, with $1 - \varepsilon/4 \leq s < 1$.*

Lemma 3.5. *For fixed $\varepsilon > 0$, there is at most one d with $d \geq \max\left\{e^{1/\varepsilon}, e^{11.2}\right\}$ and $L(\chi, 1) \leq \frac{0.655\varepsilon}{d^\varepsilon}$.*

Proof. These lemmas are proved in Tatuzawa [17]. □

We can now start proving the theorem.

Notation. Let d_r be the product of the first r primes (starting at 2).

Lemma 3.6. *If $L(\chi, s) \neq 0$ in the interval $1 - \frac{1}{4 \log d} \leq s < 1$ with $d \geq d_{11}$, then $e(-d) > 2$ for all $d \geq d_{11}$. Without this hypothesis, there is at most one $d \geq d_{11}$ such that $e(-d) = 2$.*

Proof. As noted earlier, if $e(-d) > 2$, then n is not going to be a convenient number. In other words, this is saying there are no convenient numbers larger than d_{11}. It has already been checked computationally by D. H. Lehmer and J. D. Swift that there are no convenient numbers up to

$$d_{11} = 200{,}560{,}490{,}130 \approx 2 \cdot 10^{11}.$$

First, from Theorem 2.1, $h(-d) = 2^{\mu-1}$ when $e(-d) = 2$. If $\mu \geq 11$, then since 37 is the 11th prime, d_μ is the product of d_{11} (the first 11 primes) and subsequent primes larger than 37 (and the product of these latter $\mu - 11$ primes is obviously $\geq 37^{\mu-11}$). Then combined with the above approximation of d_{11}, we have

$$d_\mu \geq d_{11} 37^{\mu-11} \geq 2 \cdot 10^{11} \cdot 37^{\mu-11}. \tag{3.7}$$

Furthermore, $d \geq d_\mu$ when $e(-d) = 2$ (see [1, §7.D] in Cox). It is a result from algebraic number theory (see [14, Cohen], [15, Cohen], [16, Cohn], and a few hints in [1, §7.D] in Cox) that

$$h(-d) = \tfrac{L(\chi,1)}{k(-d)},$$

where

$$k(d) = \begin{cases} \frac{2\ln\eta(d)}{\sqrt{d}} & \text{for } d > 0, \\ \frac{2\pi}{w(d)\sqrt{-d}} & \text{for } d < 0 \end{cases}$$

is the Dirichlet structure constant with $\eta(d)$ the fundamental unit and $w(d)$ is the number of substitutions that leave the binary quadratic form unchanged, given by

$$w(d) = \begin{cases} 6 & \text{for } d = -3 \\ 4 & \text{for } d = -4 \\ 2 & \text{otherwise.} \end{cases}$$

Since we assumed $-d < 0$ and $d > 4$ (so that $w(d) = 2$ and $k(d) = 2\pi/2\sqrt{d} = \pi/\sqrt{d}$),

$$h(-d) = \frac{\sqrt{d}L(\chi,1)}{\pi}. \tag{3.8}$$

This is important as it gives a relationship between the class number $h(-d)$ and $L(\chi,1)$. As we will see, it is precisely this estimation of $h(-d)$ that will yield a contradiction for $e(-d) = 2$.

We will use the contrapositive of Lemma 3.4 with $\varepsilon = \frac{1}{\log d}$. We assumed $L(\chi,s) \neq 0$ in $1 - \varepsilon/4 \leq s \leq 1$, so if $L(\chi,1) \leq \frac{0.655\varepsilon}{d^\varepsilon}$ that would give a contradiction. Hence,

$$L(\chi,1) > \tfrac{0.655\varepsilon}{d^\varepsilon}.$$

Then from (3.8) and this fact,

$$\begin{aligned} 2^{\mu-1} = h(-d) = \frac{\sqrt{d}}{\pi}L(\chi,1) > \frac{\sqrt{d}}{\pi}\frac{0.655\varepsilon}{d^\varepsilon} &= \frac{0.655}{\pi}\frac{\sqrt{d}}{\ln d} \cdot \frac{1}{d^{1/\ln d}} \\ = \frac{0.655}{\pi e}\frac{\sqrt{d}}{\ln d} \geq \frac{0.655}{\pi e}\frac{\sqrt{d_{11}}}{\ln d_{11}} &\approx 1319.89 > 1319. \end{aligned}$$

Hence, we need $\mu > 11$. Now, we can keep going using (3.7),

$$\begin{aligned}2^{\mu-1} &> \frac{0.655}{\pi e}\frac{\sqrt{d}}{\ln d} > \frac{0.655}{\pi e}\cdot\frac{\sqrt{d_{11}37^{(\mu-11)}}}{\ln(d_{11}37^{(\mu-11)})} = \frac{0.655}{\pi e}\cdot\frac{\sqrt{d_{11}}\,37^{(\mu-11)/2}}{\ln d_{11}+(\mu{-}11)\ln 37}\\ &> \frac{0.655}{\pi e}\cdot\frac{\sqrt{d_{11}}\,6^{\mu-11}}{\ln d_{11}+(\mu{-}11)\ln 37} = \frac{0.655}{\pi e}\cdot\frac{\sqrt{d_{11}}\,3^{\mu-11}}{\ln d_{11}+(\mu{-}11)\ln 37}\cdot 2^{\mu-11}.\end{aligned}$$

Dividing both sides by $2^{\mu-11}$, we get

$$\tfrac{2^{\mu-1}}{2^{\mu-11}} = 2^{10} > \tfrac{0.655}{\pi e}\cdot\tfrac{\sqrt{d_{11}}\,3^{\mu-11}}{\ln d_{11}+(\mu-11)\ln 37} > 1319.$$

since obviously

$$\tfrac{0.655}{\pi e}\cdot\tfrac{\sqrt{d_{11}}\,3^{\mu-11}}{\ln d_{11}+(\mu-11)\ln 37} > \tfrac{0.655}{\pi e}\tfrac{\sqrt{d_{11}}}{\ln d_{11}}$$

so that we can use the lower bound 1319 found earlier. However, $2^{10} = 1024 \not> 1319$, so that our assumption $e(-d) = 2$ cannot be true. Hence, $e(-d) > 2$ for $d \geq d_{11}$.

Now assume we do not have the Riemann hypothesis. This time, we let $\varepsilon = \frac{1}{\ln d_{11}}$ but for Lemma 3.5. If $L \leq \frac{0.655\varepsilon}{d^{\varepsilon}}$, we don't have a contradiction. Otherwise, exclude the

$$d \geq \max\{e^{1/\varepsilon}, e^{11.2}\} = d_{11}$$

in the lemma from consideration. Then, again assume $e(-d) = 2$ so we can say

$2^{\mu-1} = h(-d) = \frac{\sqrt{d}}{\pi}L(\chi,1) > \frac{\sqrt{d}}{\pi}\frac{0.655\varepsilon}{d^{\varepsilon}} \geq \frac{\sqrt{d_{11}}}{\pi}\frac{0.655\varepsilon}{d_{11}^{\varepsilon}} = \frac{0.655}{\pi e}\cdot\frac{\sqrt{d_{11}}}{\ln d_{11}} > 1319$

so that $\mu > 11$. Now, using (3.7),

$$\begin{aligned}2^{\mu-1} = h(-d) &= \frac{\sqrt{d}}{\pi}\frac{0.655\varepsilon}{d^{\varepsilon}} \geq \frac{\sqrt{d_{11}37^{\mu-11}}}{\pi}\frac{0.655\varepsilon}{(d_{11}37^{\mu-11})^{\varepsilon}}\\ &= \frac{0.655}{\pi e}\frac{\sqrt{d_{11}}}{\ln d_{11}}\left(37^{\mu-11}\right)^{\frac{1}{2}-\frac{1}{\ln d_{11}}} > \frac{0.655}{\pi e}\frac{\sqrt{d_{11}}}{\ln d_{11}}37^{(\mu-11)/2}\\ &> \frac{0.655}{\pi e}\frac{\sqrt{d_{11}}}{\ln d_{11}}6^{\mu-11} > \frac{0.655}{\pi e}\frac{\sqrt{d_{11}}}{\ln d_{11}}2^{\mu-11} > 1319\cdot 2^{\mu-11}.\end{aligned}$$

Then, again,

$$\tfrac{2^{\mu-1}}{2^{\mu-11}} = 2^{10} = 1024 > 1319$$

which is a contradiction, so that $e(-d) > 2$ for all $d \geq d_{11}$ except at one most one. In other words, there are no convenient numbers beyond d_{11} when the Riemann hypothesis holds, and if it does not then there is at most one. Once again, it has been verified computationally that 1848 is the biggest convenient number $\leq d_{11}$. Therefore, this concludes the proof of Theorem 3.3. □

References

[1] Cox, D. *"Primes of the form $x^2 + ny^2$"*. Wiley, 1989.

[2] Grube, F. *Ueber einige Eulersche Sätze aus der Theorie der quadratischen Formen.* Zeitschrift für Mathematik und Physik 19 (1874), pp. 492-519.

[3] Euleri, L. *De formulis specei* $mxx + nyy$ *ad numeros primos explorandos idoneis earumque mirabilibus proprietatibus.* Opera Omnia, Series I, Vol. 4 ($=$ Commentationes Arithmeticae III), pp. 269-289.

[4] Chowla, S. *An extension of Heilbronn's Class Number Theorem.* Quarterly Journal of Mathematics (Oxford) 5 (1934), pp 304-307.

[5] Chowla, S. and Briggs, W. E. *On discriminants of binary quadratic forms with a single class in each genus*. Canadian Journal of Mathematics 6 (1954), pp 463-470.

[6] Grosswald, E. *Negative discriminants of binary quadratic forms with one class in each genus.* Acta Arithmetica 8 (1963), pp. 295-306.

[7] Weinberger, P. J. *Exponents of the class groups of complex quadratic fields*. Acta Arithmetica 22 (1973), pp. 117-124.

[8] Cohen, H. *A Course in Computational Algebraic Number Theory*. New York: Springer-Verlag, 1993.

[9] Cohen, H. *Advanced Topics in Computational Number Theory*. New York: Springer-Verlag, 2000.

[10] Cohn, H. Advanced Number Theory. New York: Dover, 1980.

[11] Tatuzawa, T. *On a theorem of Siegel*. Japanese Journal of Mathematics. 21 (1951), pp. 163-178.

[12] Apostol, T. *Introduction to Analytic Number Theory.* New York: Springer-Verlag, 1976.