Integers not represented by $2x^2 + xy + 3y^2 + z^3 - z$

William C. Jagy, following Irving Kaplansky

March 25, 2009

1 Discriminant -23

We have just enough information to show that, with any integers x, y, z,

$$2x^2 + xy + 3y^2 + z^3 - z \neq C,$$

where $C \in \{\pm 1, \pm 599, \pm 14951, \pm 9314449\}$. What these C have in common is being odd and the existence of an integer F such that $27C^2 - 23F^2 = 4$.

Note that, as $27 \cdot 12^2 - 23 \cdot 13^2 = 1$, we get $27 \cdot 24^2 - 23 \cdot 26^2 = 4$. But we discard the possible C value 24, as it is even and $3^3 - 3 = 24$ and $(-3)^3 - (-3) = -24$, so ± 24 are represented by $2x^2 + xy + 3y^2 + z^3 - z$ with $x, y = 0$. The same thing happens with the next even C values, as taking $z = 72$ gives $z^3 - z = 373176$ and $z = 1797$ gives $z^3 - z = 5,802,886,776$. The even (positive) values of C seem to be represented by $z^3 - z$ with z values given by the modified Fibonacci sequence $z_1 = 3,\ z_2 = 72,\ z_{n+1} = 25z_n - z_{n-1}$. It should be straightforward to prove this using automorphs of the indefinite binary quadratic form $g(x, y) = 27x^2 - 23y^2$.

The polynomial $T(x, y, z) = 2x^2 + xy + 3y^2 + z^3 - z$ represented every other number n with $-10,000,000 \leq n \leq 10,000,000$. The largest value of $2x^2 + xy + 3y^2$ required was 52,914,341, which occurred in $T(1702, -4257, -382) = -2,828,245$.

We Conjecture that $2x^2 + xy + 3y^2 + z^3 - z \neq \pm C$ whenever $C > 0$ is an integer prime to 2 and 3 and there is an integer F with

$$27C^2 - 23F^2 = 4.$$

Lemma: if an integer n has an integer representation as $n = 2x^2+xy+3y^2$, then n is divisible by some prime $q = 2u^2 + uv + 3v^2$.

We use $\langle \alpha, \beta, \gamma \rangle$ to denote the (positive) binary quadratic form $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$. For discriminant -23, the entire class group $H(-23) = \{\langle 1, 1, 6\rangle, \langle 2, 1, 3\rangle, \langle 2, -1, 3\rangle\}$ has only three elements, written $h(-23) = 3$.

Theorem: If $D = -23F^2 = 4 - 27C^2$, and if the 3-rank of $H(-23F^2)$ is 1, then the congruence

$$w^3 - w + C \equiv 0 \bmod p$$

has three solutions for a prime $p > 3$ if and only if $p = u^2 + uv + 6v^2$.

This follows Corollary 4 on page 408 of Spearman and Williams [3].

Note $h(-23) = 3$, so when $F = 1$ the 3-rank is 1. Here $C = \pm 1$. This is also the original case, from Table 1 on page 134 of Hudson and Williams [2].

When $F = 649 = 11 \cdot 59$, we get $h(-23 \cdot 649^2) = 3 \cdot 12 \cdot 58 = 2088$ and $h/3 = 696$. Here $\langle 2, 1, 1210953\rangle^{696} = \langle 121, 33, 20018\rangle$ which is not the identity, so the 3-Sylow subgroup of $H(-23 \cdot 649^2)$ is cyclic order 9. This is the initial screening for 3-rank 1 on page 142 of Buell [1]. Here $C = \pm 599$.

When $F = 16199 = 97 \cdot 167$, we get $h(-23 \cdot 16199^2) = 3 \cdot 98 \cdot 166 = 48804$ and $h/3 = 16268$, which is not divisible by 3. So the 3-Sylow subgroup of $H(-23 \cdot 16199^2)$ is cyclic order 3. Here $C = \pm 14951$.

Note that $w^3 - w$ is always divisible by 2 and 3. Furthermore all our $C \in \{\pm 1, \pm 599, \pm 14951\}$ are prime to 2 and 3. So, for $C \in \{\pm 1, \pm 599, \pm 14951\}$, we see by the Theorem above that $w^3 - w + C \equiv 0 \bmod q$ does not have three solutions for $q = 2u^2 + uv + 3v^2$. By the Stickelberger parity theorem on page 397 of [3], $w^3 - w + C \equiv 0 \bmod q$ does not have ANY solutions for $q = 2u^2 + uv + 3v^2$. That is, $w^3 - w + C$ is not divisible by 2 or 3 or by any other $q = 2u^2 + uv + 3v^2$.

Finally, by the Lemma above, $w^3 - w + C$ is not represented by $2u^2 + uv + 3v^2$. We can write

$$2x^2 + xy + 3y^2 \neq w^3 - w + C,$$

$$2x^2 + xy + 3y^2 - w^3 + w \neq C.$$

Take $z = -w$,

$$2x^2 + xy + 3y^2 + z^3 - z \neq C,$$

for $C \in \{\pm 1, \pm 599, \pm 14951\}$.

When $F = 10091951 = 3037 \cdot 3323$ and $C = \pm 9314449$ we need to investigate further. Here $h(-23 \cdot 10091951^2) = 3 \cdot 3036 \cdot 3324 = 30,274,992$. This time we can not apply Corollary 4 of [3], as the 3-Sylow subgroup is not cyclic, it is $C(9) \cdot C(3)$. Indeed, it is generated by the two positive binary quadratic forms

$$K = \langle 1664081, 1248161, 352153806 \rangle, \quad L = \langle 13840047, 2497291, 42426308 \rangle.$$

K is of order 9 and L is of order 3. Every element of the 27 in the 3-Sylow subgroup is expressible in one way as $K^i\, L^j$ with $1 \leq i \leq 9,\ 1 \leq j \leq 3$.

All is not lost. We switch to Corollary 3 of [3].

The Theorem on page 398 of [3] reads: there is a unique subgroup $J = J(A,B,C)$ of index 3 in $H(D)$ with the following property: If p is any prime (greater than 3) such that $(D|p) = +1$ then $x^3 + Ax^2 + Bx + C \equiv 0 \bmod p$ has three solutions if and only if p is represented by one of the forms in $J = J(A,B,C)$.

Here $C = 9314449$, the two polynomials of concern are $w^3 - w + 9314449$ and $w^3 - w - 9314449$. The subgroups J of the previous paragraph are thus $J(0,-1,-9314449)$ and in $J(0,-1,9314449)$.

Now $L = \langle 13840047, 2497291, 42426308 \rangle$ represents 882829609, which is prime. Let $p = 882829609$. Then

$$w^3 - w + 9314449 \equiv (499096069 + w)(575999180 + w)(690563969 + w) \bmod p,$$

$$w^3 - w - 9314449 \equiv (192265640 + w)(306830429 + w)(383733540 + w) \bmod p.$$

So $p = 882829609$ is represented by a form in $J(0,-1,-9314449)$ and in $J(0,-1,9314449)$. As p is represented only by L and its opposite, it follows that L is in $J(0,-1,-9314449)$ and in $J(0,-1,9314449)$.

Next, we quote page 407 of [3] where it is pointed out that the subgroup of cubes is contained in every subgroup of index 3 in $H(D)$, including $J(0,-1,-9314449)$ and in $J(0,-1,9314449)$. The 3-Sylow subgroup has exactly nine cube roots of the identity. It follows that the cubing map is exactly 9 to 1. That is, the subgroup of cubes has index 9 in the full group $H(D)$.

Any possible cube root of L would also be in the 3-Sylow subgroup, so we know by inspection of the decomposition that L is not a cube in $H(D)$. So, if we denote by N the subgroup of cubes, we find that L is not in N. Then by counting, $J(0,-1,9314449) = N \cup LN \cup L^2N$ and $J(0,-1,-9314449) = N \cup LN \cup L^2N$. So these are the same group, and we write

$$J = J(0,-1,9314449) = J(0,-1,-9314449).$$

On page 408 of [3], a surjective homomorphism κ is defined:

$$\kappa : H(-23F^2) \to H(-23)$$

by

$$\kappa([a, bF, cF^2]) = [a, b, c]$$

where$[a, b, c]$ denotes the equivalence class of the form $\langle a, b, c\rangle$, and where equivalence is defined by changes of variable of determinant $+1$.

We quote Corollary 3 of [3]. If $[H(-23) : \kappa(J(0, -1, \pm 9314449))] = 3$, then $w^3 - w \pm 9314449 \equiv 0 \bmod p$ has three solutions if and only if p is represented by a form in $\kappa(J(0, -1, \pm 9314449))$.

We already know that $L \in J$. Now we want to know $\kappa(L)$. The change of variable defined by

$$\begin{pmatrix} 1 & 12086845986053 \\ 0 & 1 \end{pmatrix}$$

takes

$$L = \langle 13840047, 2497291, 42426308\rangle$$

to the equivalent

$$L' = \langle 13840047, 33151670381423\, F, 19852411792360947154\, F^2\rangle$$

so

$$\kappa(L') = \langle 13840047, 33151670381423, 19852411792360947154\rangle.$$

This is not Gauss reduced, and $\kappa(L')$ reduces to the identity form $\langle 1, 1, 6\rangle$. In short,

$$\kappa(L) = \langle 1, 1, 6\rangle.$$

As κ is a homomorphism, all cubes in $H(-23F^2)$ map to the only cube in $H(-23)$, that being the identity $\langle 1, 1, 6\rangle$. Every form in J is a cube or the product of a cube with L or L^2. We now know that L also maps to the identity, from which it follows that all of J maps to the identity. That is, $[H(-23) : \kappa(J)] = 3$. By Corollary 3 of [3], $w^3 - w \pm 9314449 \equiv 0 \bmod p$ has three solutions if and only if p is represented by $\langle 1, 1, 6\rangle$.

That is, $w^3 - w \pm 9314449 \equiv 0 \bmod q$ does not have three solutions for $q = 2u^2 + uv + 3v^2$. Note that $w^3 - w$ is divisible by 6, but 9314449 is prime to 6. By the Stickelberger parity theorem on page 397 of [3], $w^3 - w \pm 9314449 \equiv 0 \bmod q$ does not have ANY solutions for $q = 2u^2 + uv + 3v^2$. So $w^3 - w \pm 9314449$ is not divisible by 2 or 3 or by any other $q = 2u^2 + uv + 3v^2$.

Finally, by the Lemma above, $w^3 - w \pm 9314449$ is not represented by $2u^2 + uv + 3v^2$, and

$$2x^2 + xy + 3y^2 + z^3 - z \neq \pm 9314449.$$

We Conjecture that $2x^2 + xy + 3y^2 + z^3 - z \neq \pm C$ whenever $C > 0$ is prime to 2 and 3 and

$$27C^2 - 23F^2 = 4.$$

There are an infinite set of such (C, F) pairs with $C > 0, F > 0$, as

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix} \begin{pmatrix} C \\ F \end{pmatrix} = \begin{pmatrix} 7775C + 7176F \\ 8424C + 7775F \end{pmatrix}$$

gives a new (C, F) pair from an old, and

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix} \equiv \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \mod 6 .$$

The (C, F) pairs I know about are all generated from $(1, -1)$ or $(1, 1)$:

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 599 \\ 649 \end{pmatrix}$$

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 14951 \\ 16199 \end{pmatrix}$$

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix} \begin{pmatrix} 599 \\ 649 \end{pmatrix} = \begin{pmatrix} 9314449 \\ 10091951 \end{pmatrix}$$

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix} \begin{pmatrix} 14951 \\ 16199 \end{pmatrix} = \begin{pmatrix} 232488049 \\ 251894449 \end{pmatrix}$$

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix} \begin{pmatrix} 9314449 \\ 10091951 \end{pmatrix} = \begin{pmatrix} 144839681351 \\ 156929837401 \end{pmatrix}$$

Recall that we were ignoring the even values of C, as they all seem to be values of $z^3 - z$.

The even (C,F) pairs I know about are all generated from $(24,26)$:

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix}\begin{pmatrix} 24 \\ 26 \end{pmatrix} = \begin{pmatrix} 373176 \\ 404326 \end{pmatrix}$$

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix}\begin{pmatrix} 373176 \\ 404326 \end{pmatrix} = \begin{pmatrix} 5802886776 \\ 6287269274 \end{pmatrix}$$

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix}\begin{pmatrix} 5802886776 \\ 6287269274 \end{pmatrix} = \begin{pmatrix} 90234888993624 \\ 97767036806374 \end{pmatrix}$$

$$\begin{pmatrix} 7775 & 7176 \\ 8424 & 7775 \end{pmatrix}\begin{pmatrix} 90234888993624 \\ 97767036806374 \end{pmatrix} = \begin{pmatrix} 1403152518047966424 \\ 1520277416051846426 \end{pmatrix}$$

References

[1] D. A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. Springer-Verlag, 1989.

[2] Richard H. Hudson and Kenneth S. Williams. Representation of primes by the principal form of discriminant $-D$ when the classnumber $h(-D)$ is 3. *Acta Arithmetica*, 57:131–153, 1991.

[3] Blair K. Spearman and Kenneth S. Williams. The cubic conguence $x^3 + Ax^2 + Bx + C \equiv 0 \bmod p$ and binary quadratic forms. *Journal of the London Mathematical Society*, 46:397–410, 1992.