REPRESENTATION OF PRIMES BY CUBIC FORMS

STEVEN CHARLTON

Contents

1. Introduction

In the book *Primes of the form* $x^2 + ny^2$, Cox [Cox11] discusses the history and theory behind the answering to the question of which primes the binary quadratic form $x^2 + ny^2$ represents. Using techniques and results from class field theory, specifically the Hilbert class field and ring class fields, this question is completely answered when $n > 0$. A similar answer can be given using the narrow (Hilbert) class field and narrow ring class fields when $n < 0$, although this is not discussed in the book.

It appears less study has been made of the analogous question for cubic forms. In this writeup I will give some idea of how the results from [Cox11] can be generalised to the case of ternary cubic forms.

As an aside, I will first investigate how the narrow class number of a cubic field relates to the number of totally positive fundamental units. After this we will see the correspondence between ideal classes in a cubic number field, and ternary cubic forms.

Using this I will focus first on the cubic number field $\mathbb{Q}(\sqrt[3]{11})$, which has class number 2. This will give rise to 2 ternary cubic forms, one corresponding to the principal ideal class (the so-called norm form), and one corresponding to the non-principal ideal class. Using the Hilbert class field I will determine exactly which primes each of these forms represents, including which primes are represented simultaneously by both forms – a feature which does not occur in the quadratic case.

2. Narrow class numbers of cubic fields

In the quadratic case, one has the result that $h_K^+ = h_K$ if and only if the fundamental unit u has norm -1. Otherwise $h_K^+ = 2h_K$, and in particular this always holds for imaginary quadratic fields. What is the analogous result for cubic fields?

Date: December 13, 2015.

First, let us give an equivalent characterisation in the quadratic case. Recall that $N(\alpha) = \prod_i \sigma_i(\alpha)$. In a real quadratic field, u exists. If $-1 = N(u) = \sigma_1(u)\sigma_2(u)$, then $\sigma_1(u)$ and $\sigma_2(u)$ have opposite signs. Otherwise $1 = N(u) = \sigma_1(u)\sigma_2(u)$, and so $\sigma_1(u)$ and $\sigma_2(u)$ have the same sign. By using $-u$ in place of u we can force $\sigma_1(u) = \sigma_2(u) > 0$, so u is *totally positive*. Let us call a fundamental unit u totally positive if u or $-u$ is totally positive; equivalently if $\sigma_i(u)$ all have the same sign. We this obtain that for a real quadratic field, $h_K^+ = h_K$ if the fundamental unit u is totally positive. If u is not totally positive, then $h_K^+ = 2h_K$.

For a cubic field we obtain the following.

Case sig(K) = (1, 2): Let u be the fundamental unit. Since there is only one real embedding σ_1, necessarily u is totally positive. Thus $h_K^+ = h_k$.

Case sig(K) = (3, 0): Let u_1, u_2 be the fundamental units. Consider the set $S = \{ u_1, u_2, u_1u_2 \}$, and let S^+ be those elements which are totally positive. If $\#S^+ = 0$, then $h_K^+ = h_K$. If $\#S^+ = 1$, then $h_K^+ = 2h_K$. Otherwise $\#S^+ = 3$ and then $h_K^+ = 4h_K$.

These situations can all occur, as illustrated below.

Field	Signature	Fundamental units	Real σ_i signs	$\#S^+$	h_k	h_k^+	$[h_K^+ : h_K]$
$2+t^3$	(1,2)	$-1-\theta$	$+$		1	1	1
$1-3t+t^3$	(3,0)	$2-\theta-\theta^2$ $2-\theta^2$	$++-$ $-+-$	0	1	1	1
$1-4t+t^3$	(3,0)	$-\theta$ $2-\theta$	$+--$ $+++$	1	1	2	2
$31-37t+t^3$	(3,0)	$-5+5\theta+\theta^2$ $-10+13\theta-2\theta^2$	$+++$ $---$	3	2	8	4

Proof. Something of a proof here... □

3. Ternary cubic forms from cubic number fields

In the quadratic case, the correspondence between ideals and quadratic forms goes as follows. Let $\mathfrak{a}$ be an ideal in $K = \mathbb{Q}(\sqrt{d})$, and let $[\alpha_1, \alpha_2]$ be a $\mathbb{Z}$-basis for $\mathfrak{a}$. One has that

$$\det(\sigma_i(\alpha_j))^2 = N(\mathfrak{a})^2 \Delta_K \,,$$

where σ_i are all the embeddings $K \to \mathbb{R}$ or $\mathbb{C}$. Call the basis *normalised* if $\det(\sigma_i(\alpha_j)) = N(\mathfrak{a})^2\sqrt{\Delta_K}$, where $\sqrt{\cdot}$ is the principal branch of the square root function. If $[\alpha_1, \alpha_2]$ is a normalised basis for $\mathfrak{a}$, the map

$$\mathcal{Q} \colon \mathfrak{a} \mapsto \frac{1}{N_K(\mathfrak{a})} N_K(\alpha_1 x + \alpha_2 y)$$

gives a bijective correspondence between narrow ideal classes in $\mathbb{Q}(\sqrt{d})$ and equivalence classes of quadratic forms of discriminant $4d$. Moreover, the quadratic form $\mathcal{Q}(\mathfrak{a})(x, y)$ represents an integer m if and only if there is an ideal of norm m in the narrow ideal class $[\mathfrak{a}]$.

More precisely, it is if and only if there is an ideal of norm m in the narrow ideal class $[\mathfrak{a}]^{-1}$. But the forms arising from $\mathfrak{a}$ and $\widetilde{\mathfrak{a}}$ represent the same integers since $\mathcal{Q}(\mathfrak{a})(x, y) = \mathcal{Q}(\widetilde{\mathfrak{a}})(x, -y)$ and $[\mathfrak{a}]^{-1} = [\widetilde{\mathfrak{a}}]$.

A similar map can be defined from the ideal class group of a cubic number field to ternary cubic forms. Let $\mathfrak{a}$ be an ideal of cubic number field K, and let $[\alpha, \beta, \gamma]$ be a normalised basis for $\mathfrak{a}$. Then

$$\mathcal{C} \colon \mathfrak{a} \mapsto \frac{1}{N_K(\mathfrak{a})} N_K(\alpha x + \beta y + \gamma z)$$

associates an equivalence class of ternary cubic forms to the ideal class $[\mathfrak{a}]$.

Essentially the proof goes through as in the quadratic case. The change of basis of an ideal, gives an action of $\mathrm{SL}(3,\mathbb{Z})$ on the cubic form converting it to an equivalent form. Ideals $\mathfrak{a}$ and $\mathfrak{b}$ in the came class can be related to multiplication by principal ideal (λ). By changing to $(-\lambda)$ we can force $N(\lambda)>0$, and go pick up normalised basis for $\mathfrak{b}$ as a multiple of the normalised basis for $\mathfrak{a}$. (If we go this for an even degree field, we must have some non-totally-positive unit in order to be able to do this, so we will have to deal with the narrow class group.)

It still remains to check injectivity. The method for the quadratic case heavily relies on computing roots of a single variable version of the form in order to produce a principal ideal relating the two ideals. One might also want surjectivity, but this also is problematic.

But we do have a representation result. The cubic form $\mathcal{C}(\mathfrak{a})(x,y,z)$ represents a positive integer m if and only if there is an integral ideal of norm m in the ideal class $[\mathfrak{a}]^{-1}$. Since $C(-x,-y,-z)=-C(x,y,z)$ an integer m is represented if and only if $|m|$ is represented, so we may restrict to positive integers without loss of generality.

Say $\mathfrak{b}$ is an ideal of norm m in the class $[\mathfrak{a}]^{-1}$. Then we have $(\lambda)=\mathfrak{a}\mathfrak{b}\subset\mathfrak{a}$ for some λ. We can assume $N(\lambda)>0$ by multiplying by -1. We thus have $\lambda\in\mathfrak{a}$ and can therefore be expressed in terms of the basis $[\alpha_1,\alpha_2,\alpha_3]$ of $\mathfrak{a}$. Also $N(\lambda)=N(\mathfrak{a})m$, we can be get $m=N(\lambda)/N(\mathfrak{a})=\mathcal{C}(\mathfrak{a})(x_0,y_0,z_0)$ where $\lambda=x_0\alpha_1+y_0\alpha_2+z_0\alpha_3$.

Suppose that $m=\mathcal{C}(\mathfrak{a})(x_0,y_0,z_0)$, then let $\lambda=x_0\alpha_1+y_0\alpha_2+z_0\alpha_3\in\mathfrak{a}$. So $m=N(\lambda)/N(\mathfrak{a})=N(\lambda\mathfrak{a}^{-1})$. Therefore $\mathfrak{b}=(\lambda)\mathfrak{a}^{-1}$ is an ideal of norm m in the class of $[\mathfrak{a}]^{-1}$. It remains to check that this is an integral ideal. But we have that $\mathfrak{b}\mathfrak{a}=(\lambda)\subset\mathfrak{a}$, so multiplying by $\mathfrak{a}^{-1}$ shows that $\mathfrak{b}\subset(1)=\mathcal{O}_K$, and is therefore an integral ideal.

3.1. Group structure on ternary cubic forms.

Knowing that the ternary cubic forms arise from the class group of the number fields means that there should be some composition law which makes them into a group too. As in the quadratic case the composition law is as follows. The form $C(x,y,z)$ is the composition of the two forms $A(x,y,z)$ and $B(x,y,z)$, written $C=A\circ B$, provides there are bilinear forms

$$b_i(x_1,y_1,z_1;x_2,y_2,z_2) := \sum_j\sum_k a_{ijk}x_jx_k\,,$$

such that

$$C(b_1(x_1,y_1,z_1;x_2,y_2,z_2),b_2(x_1,y_1,z_1;x_2,y_2,z_2),b_3(x_1,y_1,z_1;x_2,y_2,z_2)) \\ = A(x_1,y_1,z_1)B(x_2,y_2,z_2)\,.$$

To obtain this, let $\mathfrak{a}$ correspond to A, $\mathfrak{b}$ correspond to B and $\mathfrak{c}$ correspond to C. Then firstly we must have $[\mathfrak{a}][\mathfrak{b}]=[\mathfrak{c}]$ for this to be the composition. Then take bases of $\mathfrak{a}$ and $\mathfrak{b}$ and express the products in terms of the basis of $\mathfrak{c}$ (up to some principal ideal (λ)). Applying the construction $\mathcal{Q}$ will give the bilinear forms in the composition law.

4. Ternary cubic forms from $\mathbb{Q}(\sqrt[3]{11})$

We can apply this construction to the field $K=\mathbb{Q}(\sqrt[3]{11})$. This field has class number $h_K=2$, so there are two ideal classes, and two classes of ternary cubic forms. The prototypical instance of a principal ideal is obtained by $\mathcal{O}_K$ itself, with basis $[1,\sqrt[3]{11},\sqrt[3]{11^2}]$. This corresponds to the norm form on $\mathcal{O}_K$, giving

$$\mathcal{O}_K\mapsto P(x,y,z):=x^3+11y^3+121z^2-33xyz\,.$$

A representative of the non-principal ideal class is obtained by the prime decomposition $2\mathcal{O}_K=\mathfrak{p}_2\mathfrak{q}_2$, where $\mathfrak{p}_2$ has norm 2, and $\mathfrak{q}_2$ has norm 4. Both of these ideals are non-principal. The ideal

$\mathfrak{q}_2$ has basis $[2, 2\sqrt[3]{11}, 1 + \sqrt[3]{11} + \sqrt[3]{11^2}]$, and this gives rise to the ternary cubic form

$$\mathfrak{q}_2 \mapsto Q(x,y,z) \coloneqq 2x^3 + 22y^3 + 3x^2z - 33xyz + 33y^2z - 15xz^2 + 25z^3\,.$$

In order to determine which primes P and Q represent, we need to determine which ideal classes contain integral ideals of norm p. This is determined by which ideal classes appear in the factorisation of the ideal $p\mathcal{O}_K$, since an ideal contains its norm. Let us analyse the situation using the standard techniques of the Hilbert class field. The number field K is defined by the polynomial $f_K(t) = t^3 - 11$. The Hilbert class field H is defined over $\mathbb{Q}$ by the polynomial $f_H(t) = t^6 - 9t^4 + 60t^2 - 16$.

If we assume p is an odd prime, not dividing the discriminant of f_K or f_H, then we can relate ideal factorisation to factorisation of these polynomials. This excludes the primes $p = 2, 3, 11$.

$p\mathcal{O}_K$ inert: Then $p\mathcal{O}_K$ is an ideal of norm p^3. Therefore there is no ideal of norm p, and so neither P nor Q represents p. In this case modulo p, the polynomial f_K factors into irreducibles with degrees (3), and f_H factors into irreducibles with degrees $(3,3)$.

$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{q}_1$: In this case $\mathfrak{p}_1$ has norm p, and $\mathfrak{q}_1$ has norm p^2. Modulo p the polynomial f_K factors as degrees $(1,2)$.

If $\mathfrak{p}_1$ is principal, then P represents p, and $\mathfrak{q}_1$ is also principal. The polynomial f_H factors as degrees $(1,1,2,2)$.

Otherwise $\mathfrak{p}_1$ is non-princpal, then Q represents p and $\mathfrak{q}_1$ is also non-principal. The polynomial f_H factors as degrees $(2,4)$.

$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_2$: In this case each $\mathfrak{p}_i$ has norm p. The polynomial f_K factors as degrees $(1,1,1)$.

If all $\mathfrak{p}_i$ are principal, then only P represents p. And f_H factors as degree $(1,1,1,1,1,1)$.

Otherwise at least one $\mathfrak{p}_i$ is non-principal. It is not possible for all to be non-principal (the class group is $\mathbb{Z}_2$ and $1+1+1 = 1 \neq 0$), one of the $\mathfrak{p}_i$ is principal. More precisely one is principal, and two are non-principal. So we see both(!) P and Q represent p. The polynomial f_K factors as degrees $(1,1,2,2)$.

In K	Subcases	f_K degrees	f_H degrees	P reps p	Q reps p
$p\mathcal{O}_K$ prime	$p\mathcal{O}_K$ principal	(3)	(3,3)		
$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{q}_1$	$\mathfrak{p}_1$, $\mathfrak{q}_1$ principal	(1,2)	(1,1,2,2)	✓	
	$\mathfrak{p}_1$, $\mathfrak{q}_1$ non-principal	(1,2)	(2,4)		✓
$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_i$ all principal	(1,1,1)	(1,1,1,1,1,1)	✓	
	$\mathfrak{p}_i$ both classes	(1,1,1)	(1,1,2,2)	✓	✓

The upshot of this discussion is the the following.

Theorem 4.1. *For $p \neq 2, 3, 11$ the form*

$$P(x,y,z) \coloneqq x^3 + 11y^3 + 121z^3 - 33xyz$$

represents p, if and only if

- *$f_K(t) \pmod p$ factors as degrees $(1,2)$ and $f_H(t) \pmod p$ factors as degrees $(1,1,2,2)$, or*
- *$f_K(t) \pmod p$ factors as degrees $(1,1,1)$*

where

$$f_K(t) = t^3 - 11 \text{ and } f_H(t) = t^6 - 9t^4 + 60t^2 - 16$$

are the polynomials defining $K = \mathbb{Q}(\sqrt[3]{11})/\mathbb{Q}$ and $H/\mathbb{Q}$ the Hilbert class field of K.

Notice this is equivalent to $f_H(t) \pmod p$ has a linear factor, which is turn is equivalent to having a root.

Theorem 4.2. *For $p \neq 2, 3, 11$ the form*

$$Q(x,y,z) := 2x^3 + 22y^3 + 3x^2z - 33xyz + 33y^2z - 15xz^2 + 25z^3$$

represents p, if and only if

- *$f_K(t) \pmod p$ factors as degrees $(1,2)$ and $f_H(t) \pmod p$ factors as degrees $(2,4)$, or*
- *$f_K(t) \pmod p$ factors as degrees $(1,1,1)$, and $f_H(t)$ factors as degrees $(1,1,2,2)$.*

where

$$f_K(t) = t^3 - 11 \text{ and } f_H(t) = t^6 - 9t^4 + 60t^2 - 16$$

are the polynomials defining $K = \mathbb{Q}(\sqrt[3]{11})/\mathbb{Q}$ and $H/\mathbb{Q}$ the Hilbert class field of K.

Theorem 4.3. *For $p \neq 2, 3, 11$ the forms*

$$P(x,y,z) := x^3 + 11y^3 + 121z^3 - 33xyz \text{ and}$$
$$Q(x,y,z) := 2x^3 + 22y^3 + 3x^2z - 33xyz + 33y^2z - 15xz^2 + 25z^3$$

simultaneously represent p if and only if

- *$f_K(t) \pmod p$ factors as degrees $(1,1,1)$, and $f_H(t)$ factors as degrees $(1,1,2,2)$*

where

$$f_K(t) = t^3 - 11 \text{ and } f_H(t) = t^6 - 9t^4 + 60t^2 - 16$$

are the polynomials defining $K = \mathbb{Q}(\sqrt[3]{11})/\mathbb{Q}$ and $H/\mathbb{Q}$ the Hilbert class field of K.

With these criteria we can produce the following lists of primes represented by the various forms.

List 4.4. *For $p \neq 2, 3, 11$, the primes ≤ 1000 which are represented by*

$$P(x,y,z) := x^3 + 11y^3 + 121z^3 - 33xyz$$

are

19, 29, 37, 43, 53, 61, 71, 83, 89, 107, 113, 131, 167, 173, 179, 193, 199, 211, 227, 229, 233, 239, 281, 293, 311, 337, 349, 353, 389, 409, 431, 457, 461, 467, 509, 521, 523, 569, 577, 617, 641, 677, 719, 727, 733, 761, 773, 809, 823, 829, 859, 863, 877, 907, 911, 929, 941, 947, 967, 977, 983

List 4.5. *For $p \neq 2, 3, 11$, the primes ≤ 1000 which are represented by*

$$Q(x,y,z) := 2x^3 + 22y^3 + 3x^2z - 33xyz + 33y^2z - 15xz^2 + 25z^3$$

are

5, 17, 19, 23, 37, 41, 43, 47, 59, 61, 101, 137, 149, 191, 197, 199, 211, 229, 251, 257, 263, 269, 317, 347, 349, 359, 383, 401, 409, 419, 443, 449, 457, 479, 491, 503, 557, 563, 577, 587, 593, 599, 647, 653, 659, 683, 701, 727, 733, 743, 797, 821, 823, 827, 839, 857, 859, 877, 881, 887, 907, 953, 971

List 4.6. *For $p \neq 2, 3, 11$, the primes ≤ 1000 which are represented simultaneously by both*

$$P(x,y,z) := x^3 + 11y^3 + 121z^3 - 33xyz$$

and by

$$Q(x,y,z) := 2x^3 + 22y^3 + 3x^2z - 33xyz + 33y^2z - 15xz^2 + 25z^3$$

are

19, 37, 43, 61, 199, 211, 229, 349, 409, 457, 577, 727, 733, 823, 859, 877, 907

4.1. **Example of the composition.** In the case of $\mathbb{Q}(\sqrt[3]{11})$, the class group is $\mathbb{Z}/2$, and we have the following correspondences $P \leftrightarrow \overline{0} = [\mathcal{O}_K]$, and $Q \leftrightarrow \overline{1} = [\mathfrak{q}_2]$. This means we should expect that $Q \circ Q = P$. Here is an outline of how to show this.

Recall $\mathfrak{q}_2$ has basis given by $[\alpha_1, \alpha_2, \alpha_3] = [2, 2\sqrt[3]{11}, 1 + \sqrt[3]{11} + \sqrt[3]{11^2}]$. From the class group, we know that $\mathfrak{q}_2^2$ is principal. We find that $\mathfrak{q}_2^2 = (3 + \sqrt[3]{11} - \sqrt[3]{11^2}) = (3 + \sqrt[3]{11} - \sqrt[3]{11^2})\mathcal{O}_K$, with basis given by $[\lambda_1, \lambda_2, \lambda_3] = (3 + \sqrt[3]{11} - \sqrt[3]{11^2})[1, \sqrt[3]{11}, \sqrt[3]{11^2}]$.

Now decompose the elements $\alpha_i\alpha_j$ into the λ-basis. For example $\alpha_1\alpha_2 = 11\lambda_1 + 5\lambda_2 + 2\lambda_3$. Using this we can write $N(x\alpha_1 + y\alpha_2 + z\alpha_3)N(u\alpha_2 + v\alpha_2 + w\alpha_3) = N(b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3)$, where b_i is a bilinear form in x, y, z and u, v, w. From there we can divide through by the ideal norms to get the composition on cubic forms, as follow.

$$\begin{aligned}
&Q(x, y, z)Q(u, v, w) = \\
&\quad P(5ux + 11vx + 19wx + 11uy + 22vy + 44wy + 19uz + 44vz + 81wz, \\
&\quad 2ux + 5vx + 9wx + 5uy + 11vy + 19wy + 9uz + 19vz + 36wz, \\
&\quad ux + 2vx + 4wx + 2uy + 5vy + 9wy + 4uz + 9vz + 16wz)
\end{aligned}$$

5. Orders in $\mathbb{Q}(\sqrt[3]{11})$

Like in the quadratic case, we can consider *orders* in the ring of integers, which allows us to deal with cubic forms of 'non-primitive' discriminant. That is, forms which do not arise directly from ideals in number fields.

An order in a number field K is a subring $\mathcal{O} \subset K$ which contains 1, and is a free $\mathbb{Z}$-module of rank $\deg(K)$. (So rank 2 for quadratic fields, and rank 3 for cubic fields.)

5.1. **Order $\mathbb{Z}\langle 1, 2\sqrt[3]{11}, 2\sqrt[3]{11^2}\rangle$ and $\mathbb{Z}\langle 1, 2\sqrt[3]{11}, 4\sqrt[3]{11^2}\rangle$.** The first order has index 4, and the second has index 8. Both are contained in the ideal (2) of $\mathcal{O}_K$. We compute the abelian extension A of K associated to this ideal to defined by the polynomial

$$\begin{aligned}
f_A(t) = t^{18} &+ 3t^{17} - 6t^{16} - 28t^{15} - 15t^{14} + 57t^{13} + \\
&+ 107t^{12} + 9t^{11} - 165t^{10} - 75t^9 + 207t^8 + 372t^7 + \\
&+ 275t^6 + 150t^5 + 57t^4 - t^3 - 3t^2 - 3t - 1\,.
\end{aligned}$$

This has discriminant $2^8 \cdot 3^{36} \cdot 11^{12} \cdot 19^2 \cdot 37^2 \cdot 179^2 \cdot 193^2 \cdot 188857^2$.

For the order $\mathcal{O}_1 = \mathbb{Z}\langle 1, 2\sqrt[3]{11}, 2\sqrt[3]{11^2}\rangle$, the principal ideal class has basis $[1, 2\sqrt[3]{11}, 2\sqrt[3]{11^2}]$, so gives rise to the ternary cubic form

$$R(x, y, z) := \frac{1}{N_{\mathcal{O}_1}(\mathcal{O}_1)} N(x + 2\sqrt[3]{11}y + 2\sqrt[3]{11^2}z) = x^3 + 88y^3 + 968z^3 - 132xyz\,.$$

For the order $\mathcal{O}_2 = \mathbb{Z}\langle 1, 2\sqrt[3]{11}, 2\sqrt[3]{11^2}\rangle$, the principal ideal class has basis $[1, 2\sqrt[3]{11}, 4\sqrt[3]{11^2}]$, so gives rise to the ternary cubic form

$$S(x, y, z) := \frac{1}{N_{\mathcal{O}_2}(\mathcal{O}_2)} N(x + 2\sqrt[3]{11}y + 4\sqrt[3]{11^2}z) = x^3 + 88y^3 + 7744z^3 - 264xyz\,.$$

Observe that $R(x, y, z) = P(x, 2y, 2z)$ and $S(x, y, z) = P(x, 2y, 4z)$. So we are in fact going to determine which primes p are represented by P with some divisibility condition on the parameters y and z.

It turns out that the *ring class field* associated to both of these orders is exactly the field A. (*** Check *** It should contain the Hilbert class field since the Hilbert class field is unramified at all primes, so inp particular those dividing the conductor (2). This shows that $3 \times 2 = 6$ divides the degree of the ring class field. Moreover, it can be shown that $R(x, y, z)$ does not represent 29, so the degree must be at least $6 \times 2 = 12$. But the only subfields with degree ≥ 12 is A itself.)

We therefore obtain

Theorem 5.1. *For $p \neq 2, 3, 11, 19, 37, 179, 193, 188857$, the form*

$$R(x, y, z) := x^3 + 88y^3 + 968z^3 - 132xyz$$

represents p if and only if

$$\begin{aligned} f_A(t) = t^{18} + 3t^{17} - 6t^{16} - 28t^{15} - 15t^{14} + 57t^{13} + \\ + 107t^{12} + 9t^{11} - 165t^{10} - 75t^9 + 207t^8 + 372t^7 + \\ + 275t^6 + 150t^5 + 57t^4 - t^3 - 3t^2 - 3t - 1 \end{aligned}$$

has a root modulo p.

The same result also holds for the form

$$S(x, y, z) := x^3 + 88y^3 + 7744z^3 - 264xyz\,.$$

List 5.2. *For $p \neq 2, 3, 11, 19, 37, 179, 193, 188857$, the primes ≤ 2000 which are represented by*

$$R(x, y, z) := x^3 + 88y^3 + 968z^3 - 132xyz$$

are

61, 89, 167, 239, 337, 431, 457, 461, 509, 521, 523, 641, 677, 719, 829, 907, 911, 941, 967, 1013, 1087, 1093, 1181, 1187, 1193, 1217, 1229, 1279, 1283, 1303, 1373, 1409, 1433, 1489, 1493, 1559, 1613, 1637, 1697, 1709, 1747, 1931, 1933

The same result also holds for the form

$$S(x, y, z) := x^3 + 88y^3 + 7744z^3 - 264xyz\,.$$

Since the ring class field A/K has order 6, and $\mathrm{Gal}(A/K)$ isomorphic to the ideal class group of the order, we see that $\mathcal{C}(\mathcal{O}_1) \cong \mathbb{Z}_6$. Similarly $\mathcal{C}(\mathcal{O}_2) \cong \mathbb{Z}_6$. Therefore we obtain 6 classes of ternary cubic forms from these orders. We might ask what primes these represent?

References

[Cox11] David A Cox. *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication.* Vol. 34. John Wiley & Sons, 2011.