Using this theorem, it is immediate to check that the values of d given in Corollary 6.4.31 are the *only* positive cubefree values of d less than or equal to 100 for which Skolem's equation has a solution with $y \neq 0$. The only additional such values for $d \leqslant 1000$ are $d = 124$, 126, 182, 215, 217, 254, 342, 422, 511, 614, 635, 651, 730, and 813. Let us show how we can prove that there are no nontrivial solutions in the particular case $d = 11$.

Proposition 6.4.34. *The only integral solution to* $x^3+11y^3 = 1$ *is the trivial solution* $(x, y) = (1, 0)$.

Proof. We work in the number field $\mathbb{Q}(\theta)$ with $\theta = 11^{1/3}$. A fundamental unit is $\varepsilon = 1 + 4\theta - 2\theta^2$, with $\mathcal{N}_{K/\mathbb{Q}}(\varepsilon) = 1$. Since our Diophantine equation is equivalent to $\mathcal{N}_{K/\mathbb{Q}}(x + y\theta) = 1$, Dirichlet's unit theorem tells us that $x + y\theta = \varepsilon^n$ for some $n \in \mathbb{Z}$.

The smallest prime p in which $X^3 - 11$ splits completely is $p = 19$, sox we work in $\mathbb{Q}_{19}$, in which the three roots are $c_1 \equiv -3 + 5 \cdot 19 \pmod{19^2}$, $c_2 \equiv -2+8\cdot 19 \pmod{19^2}$, and $c_3 \equiv 5+6\cdot 19 \pmod{19^2}$. The corresponding values of the embeddings of ε are $e_1 \equiv 9+2\cdot 19 \pmod{19^2}$, $e_2 \equiv 4 \pmod{19^2}$, $e_3 \equiv 9 + 16 \cdot 19 \pmod{19^2}$, and for $j = 1$, 2, and 3 we have $x + yc_j = e_j^n$. Since $\mathrm{Tr}_{K/\mathbb{Q}}(\theta) = \mathrm{Tr}_{K/\mathbb{Q}}(\theta^2) = 0$, we have $\sum_j c_j = \sum_j c_j^2 = 0$, so that $c_1e_1^n + c_2e_2^n + c_3e_3^n = 0$. On the other hand, since $\mathcal{N}_{K/\mathbb{Q}}(\varepsilon) = 1$ we have $e_1e_2e_3 = 1$, so replacing e_1 by $(e_2e_3)^{-1}$ and multiplying by $(e_2e_3)^n$ we obtain

$$c_1 + c_2e_2^{2n}e_3^n + c_3e_2^ne_3^{2n} = 0\ .$$

We first consider this equation modulo 19. We obtain $16 + 17 \cdot 11^n + 5 \equiv 0 \pmod{19}$, in other words $11^n \equiv 1 \pmod{19}$, or equivalently, since the order of 11 modulo 19 is equal to 3, $n \equiv 0 \pmod 3$. Thus, we must have $n = 3m$ for some $m \in \mathbb{Z}$. But then we have $(e_2^2e_3)^3 \equiv 1 + 7 \cdot 19 \pmod{19^2}$ and $(e_2e_3^2)^3 \equiv 1 + 11 \cdot 19 \pmod{19^2}$. Thus, with the notation of Corollary 4.2.18, we have $(e_2^2e_3)^n = \phi_a(m)$ and $(e_2e_3^2)^n = \phi_b(m)$ for $a = e_2^2e_3 - 1$ and $b = e_2e_3^2 - 1$. We immediately see that $\phi_a(X) = 1+7\cdot 19\,X \pmod{19^2}$ and $\phi_b(X) = 1+11\cdot 19\,X \pmod{19^2}$, and since $c_1 + c_2 + c_3 = 0$, our equation has the form $\phi(m) = 0$ with $\phi(X) \equiv 3 \cdot 19\,X \pmod{19^2}$. In the notation of Strassmann's theorem we thus have $N = 1$, so there exists only one solution $m = 0$ corresponding to $(x, y) = (1, 0)$, as claimed. □

6.4.9 The Equations $y^2 = x^3 \pm 1$ in Rational Numbers

In Corollary 6.4.32 we have found all *integral* solutions to the equation $y^2 = x^3+1$. It is instructive to see how to find all *rational* solutions to this equation. The method that we use is not related to Skolem's, but is an example of a *descent* method that we will explore in more detail in Section 8.2. This proof is essentially due to L. Euler. I would like to thank B. de Weger and R. Schoof for showing me their versions, and the one below is a (slight) blend of the two. We slightly simplify Euler's argument by using the following lemma.

Lemma 6.4.35. *Let $K = \mathbb{Q}(\sqrt{-3})$ and $\alpha \in \mathbb{Z}_K$. Then $\alpha\overline{\alpha}$ is a square in $\mathbb{Z}$ if and only if there exist $n \in \mathbb{Z}$ and $\beta \in \mathbb{Z}_K$ such that $\alpha = n\beta^2$.*

Proof. Since $\mathbb{Z}_K$ is a principal ideal domain, simply decompose α into a product of a root of unity and a product of powers of prime elements of $\mathbb{Z}_K$. The details are left to the reader (Exercise 22). □

The key descent result of Euler is the following.

Proposition 6.4.36. *Let $\varepsilon = \pm 1$. The only nonzero integral solutions to the Diophantine equations $Y^2 = XZ(X^2 - 3\varepsilon XZ + 3Z^2)$ with $\gcd(X, Z) = 1$ are for $\varepsilon = 1$, with $(X, Z) = \pm(1, 1)$ (hence $Y = \pm 1$) or $\pm(3, 1)$ (hence $Y = \pm 3$).*

Proof. Since the discriminant of $X^2 - 3\varepsilon X + 3$ is negative it follows that $XZ > 0$, so X and Z have the same sign. Thus if necessary changing (X, Z) into $(-X, -Z)$ we may assume they are both positive.

Assume first that $3 \nmid X$, and consider a solution to our equation where $|Y| > 1$ is *minimal*. As always in descent arguments we are going to construct another solution with a strictly smaller value of $|Y|$, hence giving a contradiction. Thus X, Z, and $X^2 - 3\varepsilon XZ + 3Z^2$ are pairwise coprime, and since they are all positive they are all three squares, so we write $X = x^2$, $Z = z^2$, and $X^2 - 3\varepsilon XZ + 3Z^2 = a^2$, say. If we set $\alpha = X + Z(-3\varepsilon + \sqrt{-3})/2 \in \mathbb{Z}_K$, we see that $\alpha\overline{\alpha} = a^2$, so that by the above lemma we have $\alpha = n\beta^2$ with $n \in \mathbb{Z}$ and $\beta \in \mathbb{Z}_K$. Since $(1, (-3\varepsilon + \sqrt{-3})/2)$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, we write $\beta = u + v(-3\varepsilon + \sqrt{-3})/2$, and equating coefficients we obtain $X = n(u^2 - 3v^2)$, $Z = n(2uv - 3\varepsilon v^2)$. Since X and Z are coprime, it follows that $n = \pm 1$, that u and v are coprime, and $3 \nmid u$. Since X is a square and $3 \nmid u$ we have $X \equiv nu^2 \equiv n \pmod 3$, hence $n \equiv 1 \pmod 3$, so in fact $n = 1$. We thus obtain the system of equations $u^2 = x^2 + 3v^2$, $z^2 = v(2u - 3\varepsilon v)$. If $\alpha_1 = x + v\sqrt{-3}$ we have $\alpha_1\overline{\alpha_1} = u^2$, so again by the above lemma there exists $\beta_1 = (s + t\sqrt{-3})/2 \in \mathbb{Z}_K$ (thus, with $s \equiv t \pmod 2$) and $n_1 \in \mathbb{Z}$ such that $\alpha_1 = n_1\beta_1^2$, which gives by equating coefficients $x = n_1(s^2 - 3t^2)/4$, $v = n_1 st/2$, hence $u = n_1(s^2 + 3t^2)/4$. Replacing in the formula for z^2, we obtain $z^2 = (n_1/2)^2 st(s^2 - 3\varepsilon st + 3t^2)$. It follows that $Y_1 = z/(n_1/2)$ is an integer such that $Y_1^2 = st(s^2 - 3\varepsilon st + 3t^2)$, so we have obtained a new solution to our Diophantine equation. Evidently s and t are nonzero (otherwise v, hence Z, is zero). If $g = \gcd(s, t)$ (equal in fact to 1 or 2), replacing (s, t, Y_1) by $(s/g, t/g, Y_1/g^2)$ we may assume that s and t are coprime. Let us show that $|Y_1| < |Y|$. Indeed, we have

$$\frac{Y^2}{Y_1^2} = \frac{XZ(X^2 - 3\varepsilon XZ + 3Z^2)}{4z^2/n_1^2} \geqslant \frac{X(X^2 - 3\varepsilon XZ + 3Z^2)}{4} .$$

Now $X^2 - 3\varepsilon XZ + 3Z^2 \geqslant 7$ for $\varepsilon = -1$. For $\varepsilon = 1$, since $Z = z^2$ we have $X^2 - 3XZ + 3Z^2 = (X - 3Z/2)^2 + 3Z^2/4 \geqslant 3z^4/4 > 1$ for $|z| \geqslant 2$. For $\varepsilon = Z = 1$, since $X = x^2$ we have $X(X^2 - 3\varepsilon X + 3) \geqslant x^2(x^4 - 3x^2 + 3) > 4$

for $|x| > 1$. It follows from all this that $|Y| > |Y_1|$ unless $\varepsilon = X = Z = 1$. But in that case we have $|Y| = 1$, and since we have initially assumed that $|Y| > 1$, this gives the desired contradiction showing that when $3 \nmid X$ the only possible solution has $|Y| = 1$, which is indeed possible with $\varepsilon = 1$ and $X = Z = 1$, but not possible if $\varepsilon = -1$.

If $3 \mid X$ then $3 \mid Y$, so $(Y/3)^2 = Z(X/3)(Z^2 - 3\varepsilon Z(X/3) + 3(X/3)^2)$, and since $\gcd(X, Z) = 1$ we have $3 \nmid Z$, so by what we have just proved we have $\varepsilon = 1$, $(Z, X/3) = \pm(1, 1)$, hence $(X, Z) = \pm(3, 1)$. □

Corollary 6.4.37. *The only* rational *solution to the equation* $y^2 = x^3 - 1$ *is* $(x, y) = (1, 0)$*, and the only rational solutions to the equation* $y^2 = x^3 + 1$ *are* $(x, y) = (-1, 0)$*,* $(0, \pm 1)$*, and* $(2, \pm 3)$*.*

As already mentioned we will later give a similar proof of this result (Proposition 8.2.14), this time using 2-descent explicitly.

Proof. Write $x = m/n$ with $\gcd(m, n) = 1$. Multiplying the equation $y^2 = x^3 + \varepsilon$ by n^4 we see that $n(m^3 + \varepsilon n^3)$ is a square, and if we set $c = m + \varepsilon n$ this means that $nc(m^2 - \varepsilon mn + n^2) = nc(c^2 - 3\varepsilon nc + 3n^2)$ is a square. Clearly $\gcd(c, n) = \gcd(m, n) = 1$, $n \neq 0$, and $c \neq 0$ except if $m = -\varepsilon n$, i.e., $x = -\varepsilon$. Thus by the above proposition we deduce that otherwise we have $\varepsilon = 1$, and $(c, n) = \pm(1, 1)$ or $\pm(3, 1)$, giving $x = 0$ or $x = 2$ respectively, and proving the corollary. □

6.5 The Equations $ax^4 + by^4 + cz^2 = 0$ and $ax^6 + by^3 + cz^2 = 0$

Equations of the type $ax^p + by^q + cz^r = 0$ are called super-Fermat equations, and we will devote a special chapter to them (Chapter 14). Simple heuristic reasoning shows that if $1/p + 1/q + 1/r < 1$, we expect only a finite number of solutions up to a reasonable notion of equivalence, and if $1/p + 1/q + 1/r > 1$ we expect infinitely many solutions (see Chapter 14 for details). The intermediate case $1/p + 1/q + 1/r = 1$ reduces to the study of elliptic curves, and the existence or not of solutions essentially depends on the *rank* of the curve. It is clear that up to permutation of p, q, and r we have $(p, q, r) = (3, 3, 3)$, $(4, 4, 2)$, or $(6, 3, 2)$. We have studied in great detail the case $(p, q, r) = (3, 3, 3)$ in Section 6.4. It is thus natural to study the other two cases here, and in fact we are going to see that the $(4, 4, 2)$ case is very similar to the $(3, 3, 3)$ case, although the equation is not homogeneous.

6.5.1 The Equation $ax^4 + by^4 + cz^2 = 0$: Local Solubility

The question of local solubility is answered by the following proposition.

Proposition 6.5.1. *Let* a*,* b*, and* c *be nonzero integers such that* a *and* b *are* 4*th power-free and* c *is squarefree, and such that* $\gcd(a, b, c) = 1$*.*