Explicit Methods for Solving Diophantine Equations

Henri Cohen,
Laboratoire A2X, U.M.R. 5465 du C.N.R.S.,
Université Bordeaux I, 351 Cours de la Libération,
33405 TALENCE Cedex, FRANCE

March 17, 2006

Abstract

We give a survey of some classical and modern methods for solving Diophantine equations.

1 Introduction to Diophantine Equations

The study of *Diophantine equations* is the study of solutions of polynomial equations or systems of equations in integers, rational numbers, or sometimes more general number rings. It is one of the oldest branches of number theory, in fact of mathematics itself, since its origins can be found in texts of the ancient Babylonians, Chinese, Egyptians, Greeks,... One of the fascinations of the subject is that the problems are usually easy to state, but more often than not very difficult to solve, and when they can be solved sometimes involve extremely sophisticated mathematical tools.

Perhaps even more importantly, mathematicians must often invent or extensively develop entirely new tools to solve the number-theoretical problems, and these become in turn important branches of mathematics per se, which often have applications in completely different problems than the one from which they originate.

For many more details and examples, see Chapters 6 and 14 (pages 327 to 443 and 1011 to 1040) of the accompanying pdf file.

1.1 Examples of Diophantine Problems

Let me give four examples. The first and most famous is “Fermat’s last theorem” (FLT), stating that for $n \geq 3$, the curve $x^n + y^n = 1$ has no rational points other than the ones with x or y equal to 0 (this is of course equivalent to the usual statement). [1]

In the nineteenth century, thanks in particular to the work of E. Kummer and P.-G. Lejeune-Dirichlet, the theorem was proved for quite a large number of values of n, including all $n \leq 100$. Together with the theory of quadratic forms initiated by A.-M. Legendre and especially by C.-F. Gauss, one can without exaggeration say that this single problem gave rise to algebraic number theory (rings, ideals, prime ideals, principal ideals, class numbers, units, Dirichlet series, L-functions,...) As is well-known, although these methods were pushed to the extreme in the twentieth century, they did not succeed in solving the problem completely. The next progress on FLT came from algebraic geometry thanks to the work of G. Faltings who proved the so-called Mordell conjecture, which in particular implies that for a *fixed* $n \geq 3$ the number of solutions to the Fermat equation is finite. However it was only thanks to the work of several mathematicians starting with Y. Hellegouarch and G. Frey, and culminating with the work of K. Ribet, then finally of A. Wiles (helped for a crucial part by R. Taylor), that the problem was finally completely solved by using completely different tools from those of Kummer (and even Faltings): elliptic curves, Galois representations and modular forms. Although these subjects were not initiated by FLT, their development was certainly accelerated by the impetus given by FLT. In particular, thanks to the work of Wiles the complete proof of the Taniyama–Weil conjecture was obtained a few years later by C. Breuil, B. Conrad, F. Diamond and R. Taylor. This latter result can be considered in itself a more important (and certainly a more useful) theorem than FLT.

A second rather similar problem whose history is slightly different is *Catalan’s conjecture.* This states that when n and m are greater or equal to 2, the only solutions in nonzero integers x and y of the equation $x^m - y^n = 1$

[1] Incidentally, this is the place to destroy the legend concerning this statement, which has produced an enormous number of “Fermatists” claiming to have found an “elementary” proof that Fermat may have found himself: Fermat made this statement in the margin of his copy of the book by Diophantus on number theory (at the place where Diophantus discusses Pythagorean triples, see below), and claimed to have found a marvelous proof and so on. However, he wrote this statement when he was young, never claimed it publicly, and certainly never imagined that it would be made public, so he forgot about it. It *may* be possible that there does exist an elementary proof (although this is unlikely), but we can be positively sure that Fermat did not have it, otherwise he would at least have challenged his English colleagues as was the custom at that time.

come from the equality $3^2 - 2^3 = 1$. This problem can be naturally attacked by the standard methods of algebraic number theory originating in the work of Kummer. However, it came as a surprise that an elementary argument due to Cassels (see Theorem 3.11) shows that the "first case" is impossible, in other words that if $x^p - y^q = 1$ with p and q primes then $p \mid y$ and $q \mid x$. The next important result due to R. Tijdeman using Baker's theory of linear forms in logarithms of algebraic numbers was that the total number of quadruplets (m, n, x, y) satisfying the required conditions is finite. Note that the proof of this finiteness result is completely different from Faltings's proof of the corresponding one for FLT, and in fact in the latter his result did not imply the finiteness of the number of triples (x, y, n) with $n \geq 3$ and $xy \neq 0$ such that $x^n + y^n = 1$.

Until the end of the 1990's the situation was quite similar to that of FLT before Wiles: under suitable conditions on the nondivisibility of the class number of cyclotomic fields, the Catalan equation was known to have no nontrivial solutions. It thus came as a total surprise that in 1999 P. Mihăilescu proved that if Catalan's equation $x^p - y^q = 1$ with p and q odd primes has a solution then p and q must satisfy the so-called double Wieferich condition $p^{q-1} \equiv 1 \pmod{q^2}$ and $q^{p-1} \equiv 1 \pmod{p^2}$. These conditions were known before him, but he completely removed the conditions on class numbers. The last step was again taken by Mihăilescu in 2001, who finished the proof of Catalan's conjecture. His proof was improved and simplified by several people, including in particular Yu. Bilu and H. W. Lenstra.

The remarkable thing about the final proof is that it *only* uses algebraic number theory techniques on cyclotomic fields. However it uses a large part of the theory, including the relatively recent theorem of F. Thaine, which has had some very important applications elsewhere. It does not use any computer calculations, while the initial proof did.

A third example is the *congruent number problem*, stated by Diophantus in the fourth century A.D. The problem is to find all integers n (called congruent numbers) which are equal to the area of a *Pythagorean triangle*, i.e., a right-angled triangle with all three sides rational. Very simple algebraic transformations show that n is congruent if and only if the Diophantine equation $y^2 = x^3 - n^2x$ has rational solutions other than those with $y = 0$. The problem was in an "experimental" state until the 1970's, more precisely one knew the congruent or noncongruent nature of numbers n up to a few hundred (and of course of many other larger numbers). Remarkable progress was made on this problem by J. Tunnell in 1980 using the theory of modular forms, and especially of modular forms of half-integral weight. In effect, he completely solved the problem, by giving an easily checked criterion for n to be a congruent number, assuming a weak form of the Birch–Swinnerton-Dyer conjecture. This conjecture (for which a prize money of 1 million U.S. dollars has been offered by the Clay foundation) is probably one of the most important, and also one of the most beautiful conjectures in all of mathematics in the twenty-first century.

A fourth important example is the Weil conjectures. These have to do with the number of solutions of Diophantine equations *in finite fields*. Looking at Diophantine equations *locally*, and in particular over finite fields, is usually a first important step in its study. Let us give a simple example. Let $N(p)$ be the number of solutions modulo p of the equation $y^2 = x^5 - x$. Then $|N(p) - p|$ can never be very large compared to p, more precisely $|N(p) - p| < 4\sqrt{p}$, and the constant 4 is best possible. This result is already quite nontrivial, and the general study of the number of points on *curves* culminated with work of A. Weil in 1949 proving that this phenomenon occurs for all (nonsingular) curves and many other results besides. It was then natural to ask the question for surfaces, and more generally varieties of any dimension. This problem (in a very precise form, which in particular implied excellent bounds on the number of solutions) became known as the Weil conjectures. A general strategy for solving these conjectures was put forth by Weil himself, but the achievement of this goal was only made possible by an amazing amount of work by numerous people. It included the creation of modern algebraic geometry by A. Grothendieck and his students (the famous EGA and SGA treatises). The Weil conjectures were finally solved by P. Deligne in the early 1970's, exactly following Weil's strategy, but using all the tools developed since.

Note that for instance Waring's problem (given an integer $k \geq 2$, find the smallest integer $g(k)$ such that any nonnegative integer can be represented as a sum of $g(k)$ nonnegative k-th powers) or variations, will not be considered as Diophantine equations in this course since the equation is not fixed.

1.2 Introduction to Local Methods

As is explicit or implicit in all of the examples given above (and in fact in all Diophantine problems), it is essential to start by studying a Diophantine equation *locally*, in other words prime by prime (we will see later precisely what this means). Let p be a prime number, and let $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ be the prime finite field with p elements. We can begin by studying our problem in $\mathbb{F}_p$ (i.e., modulo p), and this can already be considered as the start of a local study. This is sometimes sufficient, but usually not, so we refine the study by considering the equation modulo p^2, p^3 and so on, i.e., by working in $\mathbb{Z}/p^2\mathbb{Z}$, $\mathbb{Z}/p^3\mathbb{Z}$... An important discovery, made by K. Hensel at the beginning of the twentieth century, is that it is possible to regroup all these rings with zero divisors into a single object, called the p-adic integers, and denoted by $\mathbb{Z}_p$, which is an integral domain. Not only do we have the benefit of being able to work conveniently with all the congruences modulo p, p^2, p^3,... simultaneously, but we have the added benefit of having *topological properties* which add a considerable number of tools that we may use, in particular *analytic methods* (note that this type of limiting construction is very frequent in mathematics, with the same type of benefits). When we say that we study our Diophantine problem locally at p, this means that we study it in $\mathbb{Z}_p$, or in the field of fractions $\mathbb{Q}_p$ of $\mathbb{Z}_p$.

Let us give simple but typical examples of all this. Consider first the Diophantine equation $x^2+y^2=3$ to be solved in rational numbers or, equivalently, the Diophantine equation $x^2+y^2=3z^2$ to be solved in rational integers. We may assume that x and y are coprime (exercise). Looking at the equation modulo 3, i.e., in the field $\mathbb{F}_3$, we see that it has no solution (x^2 and y^2 are congruent to 0 or 1 modulo 3, hence x^2+y^2 is congruent to 0 modulo 3 if and only if x and y are both divisible by 3, excluded by assumption). Thus, our initial Diophantine equation does not have any solution.

We are here in the case of a *quadratic* Diophantine equation. It is crucial to note that this type of equation can *always* be solved by local methods. In other words, either we can find a solution to the equation (often helped by the local conditions), or it is possible to prove that the equation does not have any solutions using positivity conditions together with congruences as above (or, equivalently, real and p-adic solubility). This is the so-called *Hasse principle*, a nontrivial theorem which is valid for a *single quadratic* Diophantine equation, but is in general not true for higher degree equations or for systems of equations.

Consider now the Diophantine equation $x^3+y^3=1$ to be solved in nonzero rational numbers or, equivalently, the Diophantine equation $x^3+y^3=z^3$ to be solved in nonzero rational integers. Once again we may assume that x, y, and z are pairwise coprime. It is natural to consider once more the problem modulo 3. Here, however, the equation has nonzero solutions (for example $1^3+1^3\equiv 2^3 \pmod 3$). We must go up one level, and consider the equation modulo $9=3^2$ to obtain a partial result: since it is easily checked that an integer cube is congruent to -1, 0 or 1 modulo 9, if we exclude the possibility that x, y, or z is divisible by 3 then we see immediately that the equation does not have any solution modulo 9, hence no solution at all. Thus we have proved that if $x^3+y^3=z^3$, then one of x, y, and z is divisible by 3. This is called solving the first case of FLT for the exponent 3. To show that the equation has no solutions at all, even with x, y, or z divisible by 3, is more difficult and *cannot* be shown by congruence conditions alone. Indeed it is easy to show that the equation $x^3 + y^3 = z^3$ has a solution with $xyz \neq 0$ in every p-adic field, hence modulo p^k for any prime number p and any exponent k (and it of course has real solutions). Thus, the Hasse principle clearly fails here since the equation does not have any solution in rational integers. In that case, it is necessary to use additional *global* arguments, whose main tools are those of algebraic number theory developed by Kummer et al. in the nineteenth century, and in particular class and unit groups, which are objects of a strictly *global* nature.

2 Use of Local Methods

2.1 A p-adic Reminder

In this section it would be useful for the reader to have some basic knowledge of the field of p-adic numbers $\mathbb{Q}_p$ and its ring of integers $\mathbb{Z}_p$. We briefly recall without proof what is needed:

- A homogeneous equation with integer coefficients has a nontrivial solution modulo p^n for all $n \geq 0$ if and only if it has a nontrivial solution in $\mathbb{Z}_p$ (or in $\mathbb{Q}_p$ by homogeneity).

- There is a canonical integer-valued valuation v_p on $\mathbb{Q}_p^*$ such that, if $x \in \mathbb{Q}$ then $v_p(x)$ is the unique integer such that $x/p^{v_p(x)}$ can be written as a rational number with denominator and numerator not divisible by p.

- The elements of $\mathbb{Q}_p$ such that $v_p(x) \geq 0$ are called p-adic integers, they form a local ring $\mathbb{Z}_p$ with maximal ideal $p\mathbb{Z}_p$, the invertible elements of $\mathbb{Z}_p$, called p-adic units, are those x such that $v_p(x) = 0$, and if $x \in \mathbb{Q}_p^*$ we have the canonical decomposition $x = p^{v_p(x)}y$ where y is a p-adic unit.

- If $a \in \mathbb{Q}$ is such that $v_p(a) \geq 0$ and if $v_p(x) \geq 1$ then the power series $(1+x)^a$ converges. On the other hand, if $v_p(a) < 0$ then the power series converges for $v_p(x) \geq |v_p(a)|+1$ when $p \geq 3$, and for $v_p(x) \geq |v_p(a)|+2$ when $p = 2$. In all cases, it converges to its "expected" value, for instance if $m \in \mathbb{Z} \setminus \{0\}$ then $y = (1+x)^{1/m}$ satisfies $y^m = 1 + x$.

- Hensel's lemma (which is nothing else than Newton's method). We will need only the following special case: let $f(X) \in \mathbb{Q}_p[X]$ be a polynomial, and assume that $\alpha \in \mathbb{Q}_p$ is such that $v_p(f(\alpha)) \geq 1$ and $v_p(f'(\alpha)) = 0$. Then there exists $\alpha^* \in \mathbb{Q}_p$ such that $f(\alpha^*) = 0$ and $v_p(\alpha^* - \alpha) \geq 1$, and α^* can easily be constructed algorithmically by using Newton's iteration.

If this is not the case, however, the reader can translate a statement such as $C(\mathbb{Q}_p) \neq \emptyset$ as meaning that $C(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset$ for all n (the equations that we will study here are homogeneous, so that there is no real difference between $C(\mathbb{Q}_p)$ and $C(\mathbb{Z}_p)$). Furthermore, consider the following statement (which will be used below): if $u \equiv 1 \pmod{16\mathbb{Z}_2}$ there exists $y \in \mathbb{Z}_2$ such that $u = y^4$. The proof is as follows: if we write $u = 1 + x$, then $y = (1 + x)^{1/4}$ is obtained by using the binomial expansion, and it converges 2-adically because $16 \mid x$. In "elementary" terms, this means that if we call $y_n \in \mathbb{Q}$ the truncation of the expansion of $(1+x)^{1/4}$ to n terms, then the 2-adic valuation of $u - y_n^4$ tends to infinity with n. All these statements are very easy to prove.

2.2 The Fermat Quartics $x^4 + y^4 = cz^4$

Although this is certainly not the simplest kind of Diophantine equation, we begin by studying in detail the so-called *Fermat quartics* $x^4 + y^4 = cz^4$ because they involve very interesting notions.

Thus, let $c \in \mathbb{Z}$, and denote by $\mathcal{C}_c$ the projective curve defined by the equation $x^4 + y^4 = cz^4$. To find all the integers satisfying this equation or, equivalently, the rational points on $\mathcal{C}_c$, we may clearly assume that $c > 0$ and that c is not divisible by a fourth power strictly greater than 1.

The general philosophy concerning local solubility is that it is in general possible to decide *algorithmically* whether a given equation is locally soluble or not, and even whether it is *everywhere* locally soluble, in other words soluble over $\mathbb{Q}_p$ for all p, and also over $\mathbb{R}$. For *families* of equations, such as the ones we have here, it is also usually possible to do this, as we illustrate in this subsection by giving a necessary and sufficient sufficient for local solubility.

Proposition 2.1 *1. $\mathcal{C}_c(\mathbb{Q}_2) \neq \emptyset$ if and only if $c \equiv 1$ or 2 modulo 16.*

2. If p is an odd prime divisor of c, then $\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset$ if and only if $p \equiv 1 \pmod 8$.

3. If $p \equiv 3 \pmod 4$ is a prime not dividing c then $\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset$.

4. If $p \geq 37$ is a prime not dividing c then $\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset$.

5. $\mathcal{C}_c(\mathbb{Q}_{17}) \neq \emptyset$.

6. *Let $p \in \{5, 13, 29\}$ be a prime not dividing c. Then*

   (a) *$\mathcal{C}_c(\mathbb{Q}_5) \neq \emptyset$ if and only if $c \not\equiv 3$ or 4 modulo 5.*

   (b) *$\mathcal{C}_c(\mathbb{Q}_{13}) \neq \emptyset$ if and only if $c \not\equiv 7$, 8 or 11 modulo 13.*

   (c) *$\mathcal{C}_c(\mathbb{Q}_{29}) \neq \emptyset$ if and only if $c \not\equiv 4$, 5, 6, 9, 13, 22 or 28 modulo 29.*

Proof. If $(x : y : z) \in \mathcal{C}_c(\mathbb{Q}_p)$, we may clearly assume that x, y and z are p-adic integers and that at least one is a p-adic unit (in other words with p-adic valuation equal to 0, hence invertible in $\mathbb{Z}_p$). If $p \nmid c$, reduction modulo p gives a projective curve $\overline{\mathcal{C}_c}$ over $\mathbb{F}_p$, which is smooth (nonsingular) if $p \neq 2$.

(1). Let u be a 2-adic unit. I claim that $u \in \mathbb{Q}_2^4$ if and only if $u \equiv 1 \pmod{16\mathbb{Z}_2}$. Indeed, if v is a 2-adic unit we can write $v = 1 + 2t$ with $t \in \mathbb{Z}_2$, and

$$v^4 = 1 + 8t + 24t^2 + 32t^3 + 16t^4 \equiv 1 + 8(t(3t+1)) \equiv 1 \pmod{16}\ .$$

Conversely, if $u \equiv 1 \pmod{16\mathbb{Z}_2}$ we write $u = 1 + x$ with $v_2(x) \geq 4$, and it is easy to check that the binomial expansion for $(1+x)^{1/4}$ converges for $v_2(x) \geq 4$.

Now assume that $x^4 + y^4 = cz^4$. Since $v_2(c) \leq 3$, either x or y is a 2-adic unit. It follows that $x^4 + y^4 \equiv 1$ or 2 modulo 16, hence z is a 2-adic unit, so that $c \equiv 1$ or 2 modulo 16 as claimed. Conversely, if $c \equiv 1 \pmod{16}$ then $c = t^4$ by my claim above, so that $(t : 0 : 1) \in \mathcal{C}_c(\mathbb{Q}_2)$, while if $c \equiv 2 \pmod{16}$, then $c - 1 = t^4$ for some t, hence $(t : 1 : 1) \in \mathcal{C}_c(\mathbb{Q}_2)$, proving (1).

(2). Assume that $p \mid c$ is odd. Since $v_p(c) \leq 3$, x and y are p-adic units, so that -1 is a fourth power in $\mathbb{F}_p$. If g is a generator of the cyclic group $\mathbb{F}_p^*$, then $-1 = g^{(p-1)/2}$, hence -1 is a fourth power in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 8$. If this is the case, let $x_0 \in \mathbb{Z}$ such that $x_0^4 \equiv -1 \pmod p$. By Hensel's lemma (which is trivial here since the derivative of $X^4 + 1$ at x_0 is a p-adic unit), there exists $x \in \mathbb{Z}_p$ such that $x^4 = -1$, so that $(x : 1 : 0) \in \mathcal{C}_c(\mathbb{Q}_p)$, proving (2).

The following lemma shows that for the remaining p it is sufficient to consider the equation in $\mathbb{F}_p$.

Lemma 2.2 *Let $p \nmid 2c$ be a prime number. Then $\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset$ if and only if $\overline{\mathcal{C}_c}(\mathbb{F}_p) \neq \emptyset$. In particular if $p \not\equiv 1 \pmod 8$ then*

$$\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset \quad \textit{if and only if} \quad c \bmod p \in \mathbb{F}_p^4 + \mathbb{F}_p^4\ .$$

Proof. One direction is clear. Conversely, assume that $\overline{\mathcal{C}_c}(\mathbb{F}_p) \neq \emptyset$, and let $(x_0 : y_0 : z_0)$ with x_0, y_0, and z_0 not all divisible by p such that $x_0^4 + y_0^4 \equiv cz_0^4$

(mod p). Since $p \nmid c$, either $p \nmid x_0$ or $p \nmid y_0$. Assume for instance that $p \nmid x_0$, and set $f(X) = X^4 + y_0^4 - cz_0^4$. Clearly $v_p(f'(x_0)) = 0$ and $v_p(f(x_0)) \geq 1$, so that by Hensel's lemma there exists $t \in \mathbb{Q}_p$ such that $f(t) = 0$, hence $(t : y_0 : z_0) \in \mathcal{C}_c(\mathbb{Q}_p)$, proving the converse.

Finally, assume that $p \not\equiv 1 \pmod{8}$. If $x^4 + y^4 \equiv cz^4 \pmod{p}$ with x or y not divisible by p, we cannot have $p \mid z$ otherwise $x^4 \equiv -y^4 \pmod{p}$ so that -1 is a fourth power modulo p, a contradiction. Thus $p \nmid z$, hence $(xz^{-1})^4 + (yz^{-1})^4 \equiv c \pmod{p}$, finishing the proof of the lemma. □

(3). Let $p \nmid c$, $p \equiv 3 \pmod{4}$. I claim that there exist x and y in $\mathbb{Z}$ such that $x^4 + y^4 \equiv c \pmod{p}$. Indeed, in a finite field $\mathbb{F}$ any element is a sum of two squares (in characteristic 2 any element is a square so the result is trivial, otherwise if $q = |\mathbb{F}|$ then there are $(q+1)/2$ squares hence $(q+1)/2$ elements of the form $c - y^2$, so the two sets have a nonempty intersection). Thus there exist u and v such that $c \equiv u^2 + v^2 \pmod{p}$. However, when $p \equiv 3 \pmod{4}$ we have $\mathbb{F}_p^{*2} = \mathbb{F}_p^{*4}$: indeed we have a trivial inclusion, and the kernel of the map $x \mapsto x^4$ from $\mathbb{F}_p^*$ into itself is ± 1, so that $|\mathbb{F}_p^{*4}| = (p-1)/2 = |\mathbb{F}_p^{*2}|$, proving the equality. Thus $c = x^4 + y^4$, as claimed, and the above lemma proves (3).

(4). If $p \nmid 2c$ the curve $\overline{\mathcal{C}_c}$ is smooth and absolutely irreducible. Its genus is at most equal to 3 (in fact equal), so that by the Weil bounds we know that $|\overline{\mathcal{C}_c}(\mathbb{F}_p)| \geq p + 1 - 6p^{1/2}$. This is strictly positive (for p prime) if and only if $p \geq 37$, so that (4) follows from the above lemma.

(5) and (6). Thanks to the above cases, it remains to consider the primes p not dividing c such that $3 \leq p \leq 31$ and $p \equiv 1 \pmod{4}$, in other words $p \in \{5, 13, 17, 29\}$. For such a p, -1 is a fourth power modulo p only for $p = 17$. In that case, Hensel's lemma as usual shows that there exists $t \in \mathbb{Q}_{17}^4$ such that $-1 = t^4$, proving (5) in this case. Otherwise, we compute that

$$\mathbb{F}_5^4 = \{0, 1\}, \quad \mathbb{F}_{13}^4 = \{0, 1, 3, 9\}, \quad \mathbb{F}_{29}^4 = \{0, 1, 7, 16, 20, 23, 24, 25\}\ ,$$

and we deduce the list of nonzero elements of $\mathbb{F}_p^4 + \mathbb{F}_p^4$, proving (6). □

Remark. In the above proof we have used the Weil bounds, which are not easy to prove, even for a curve. In the present case, however, the equations being diagonal it is not difficult to prove these bounds using *Jacobi sums.*

Corollary 2.3 *The curve $\mathcal{C}_c$ is everywhere locally soluble (i.e., has points in $\mathbb{R}$ and in every $\mathbb{Q}_p$) if and only if $c > 0$ and the following conditions are satisfied.*

1. $c \equiv 1$ *or* 2 *modulo* 16.

2. $p \mid c$, $p \neq 2$ *implies* $p \equiv 1 \pmod 8$.

3. $c \not\equiv 3$ *or* 4 *modulo* 5.

4. $c \not\equiv 7$, 8 *or* 11 *modulo* 13.

5. $c \not\equiv 4$, 5, 6, 9, 13, 22 *or* 28 *modulo* 29.

Proof. Clear. □

As an interesting consequence, we give the following.

Corollary 2.4 *For all primes* p *such that* $p \equiv 1 \pmod{1160}$ *the curve* $\mathcal{C}_{p^2}$ *is everywhere locally soluble, but is not globally soluble.*

Proof. It is clear that the above conditions are satisfied modulo 16, 5, and 29, and also modulo 13 since 7, 8, and 11 are nonquadratic residues modulo 13. On the other hand a classical and easy result of Fermat states that the equation $x^4 + y^4 = Z^2$ does not have any nontrivial solutions, so this is in particular the case for our equation $x^4 + y^4 = (pz^2)^2$. □

Since by Dirichlet's theorem on primes in arithmetic progressions there exist infinitely many primes $p \equiv 1 \pmod{1160}$ this corollary gives infinitely many examples where everywhere local solubility does *not* imply global solubility.

An equation (or system of equations) is said to satisfy the *Hasse principle* if everywhere local solubility implies global solubility. Important examples are given by *quadratic forms* thanks to the Hasse–Minkowski theorem which tells us that a quadratic form has nontrivial solutions over $\mathbb{Q}$ if and only if it is everywhere locally soluble. Unfortunately the Hasse principle is usually not valid, and the above result gives infinitely counterexamples.

The study of the global solubility of Fermat quartics is harder and will be considered later.

2.3 Fermat's Last Theorem (FLT)

Recall that FLT states that the equation $x^n+y^n = z^n$ has no integral solutions with xyz for $n \geq 3$, in other words that the curve $x^n + y^n = 1$ has no other rational points than those with x or y equal to 0. Note that, although these points are easy (!) to spot, they are *not* trivial, and this makes the problem more difficult than if there were none at all.

Thanks to Fermat's impossibility result on the equation $x^4 + y^4 = z^2$, it is immediate to see that we may reduce to equations of the form $x^p + y^p = z^p$ with $p \geq 3$ prime, and x, y, and z pairwise coprime integers. As we have seen in the introduction, it is convenient to separate FLT into two subproblems: FLT I deals with the case where $p \nmid xyz$, and FLT II with the case $p \mid xyz$. Intuitively FLT I should be simpler since the statement is now that there exist *no* solutions at all, and indeed this is the case. We will not embark on a study of FLT, but in this section we mention what can be said using only local methods. We begin by the following.

Proposition 2.5 *The following three conditions are equivalent.*

1. *There exists three p-adic units α, β, and γ such that $\alpha^p + \beta^p = \gamma^p$ (in other words FLT I is soluble p-adically).*

2. *There exists three integers a, b, c in $\mathbb{Z}$ such that $p \nmid abc$ with $a^p + b^p \equiv c^p \pmod{p^2}$.*

3. *There exists $a \in \mathbb{Z}$ such that a is not congruent to 0 or -1 modulo p with $(a+1)^p \equiv a^p + 1 \pmod{p^2}$.*

Proof. From the binomial theorem it is clear that if $u \equiv 1 \pmod{p\mathbb{Z}_p}$ then $u^p \equiv 1 \pmod{p^2\mathbb{Z}_p}$. Thus if $u \equiv v \pmod{p\mathbb{Z}_p}$ and u and v are p-adic units, then $u^p \equiv v^p \pmod{p^2\mathbb{Z}_p}$. We will use this several times without further mention. Taking a, b and c to be residues modulo p of α, β and γ thus shows that (1) implies (2). Conversely, assume (2). We would like to apply Hensel's lemma. However, the congruence is not quite good enough, so we have to do one step by hand. Let $a^p + b^p = c^p + kp^2$ for some $k \in \mathbb{Z}$, and set $d = c + kp$, so that $p \nmid d$. Then by the binomial theorem $d^p \equiv c^p + kp^2c^{p-1} \pmod{p^3}$, so that

$$a^p + b^p - d^p \equiv kp^2(1 - c^{p-1}) \equiv 0 \pmod{p^3}$$

since $p \nmid c$. We can now apply Hensel's lemma to the polynomial $f(X) = (X^p + b^p - d^p)/p$ and to $\alpha = a$: we have $v_p(f'(a)) = v_p(a^{p-1}) = 0$ since $p \nmid a$, while $v_p(f(a)) \geq 2$ by the above, so Hensel's lemma is applicable, proving (1).

Clearly (3) implies (2). Conversely, assume (2), i.e., that $c^p \equiv a^p + b^p \pmod{p^2}$ with $p \nmid abc$. In particular $c \equiv a + b \pmod{p}$. Thus, if we set $A = ba^{-1}$ modulo p, then by the above remark $A^p \equiv b^pa^{-p} \pmod{p^2}$ and $(A+1)^p \equiv c^pa^{-p} \pmod{p^2}$, so that $(A+1)^p \equiv A^p + 1 \pmod{p^2}$, proving (3) and the proposition. □

Corollary 2.6 *FLT I cannot be proved by congruence conditions (i.e., p-adically) if and only if condition (3) of the proposition is satisfied for some a such that* $1 \leq a \leq (p-1)/2$.

Proof. Indeed, condition (3) is invariant when we change a modulo p, and also under the change $a \mapsto p-1-a$, so the result is clear. □

Corollary 2.7 *If for all* $a \in \mathbb{Z}$ *such that* $1 \leq a \leq (p-1)/2$ *we have* $(a+1)^p - a^p - 1 \not\equiv 0 \pmod{p^2}$*, then the first case of FLT is true for* p.

Proof. Indeed, if $a^p + b^p = c^p$ with $p \nmid abc$ then condition (2) of the proposition is satisfied, hence by (3), as above there exists a such that $1 \leq a \leq (p-1)/2$ with $(a+1)^p - a^p - 1 \equiv 0 \pmod{p^2}$, proving the corollary. □

For instance, thanks to this corollary we can assert that FLT I is true for $p = 3$, 5, 11, 17, 23, 29, 41, 47, 53, 71, 89, 101, 107, 113, 131, 137, 149, 167, 173, 191, 197, which are the prime numbers less than 200 satisfying the condition of the corollary.

Using global methods, and in particular the Eisenstein reciprocity law, one can prove that it is sufficient to take $a = 1$ in the above corollary, in other words that FLT I is true as soon as $2^p - 2 \not\equiv 0 \mod p^2$. This result is due to Wieferich.

3 Naive Factorization over $\mathbb{Z}$

We now start our study of global (as opposed to local) methods, and begin by the most naive approach, which sometimes work: factorization of the equation over $\mathbb{Z}$. We give two important examples where the results are quite spectacular: once again a result on FLT I, called Wendt's criterion. What is remarkable about it, apart from the simplicity of its proof, is that it is highly probable that is applicable to *any* prime number p, and this would give an alternate proof of FLT I if this could be shown. Unfortunately, to *prove* that it is indeed applicable to all p would involve proving results in *analytic number theory* which are at present totally out of reach. The second example is the theorem of Cassels on Catalan's equation.

3.1 Wendt's Criterion for FLT I

Proposition 3.1 (Wendt) *Let* $p > 2$ *be an odd prime, and* $k \geq 1$ *be an integer. Assume that the following conditions are satisfied.*

1. *$k \equiv \pm 2 \pmod 6$.*

2. *$q = kp + 1$ is a prime number.*

3. *$q \nmid (k^k - 1)R(X^k - 1, (X+1)^k - 1)$, where $R(P, Q)$ denotes the resultant of the polynomials P and Q.*

Then FLT I is valid, in other words if $x^p + y^p + z^p = 0$ then $p \mid xyz$.

Proof. Assume that $x^p + y^p + z^p = 0$ with $p \nmid xyz$ and as usual x, y, and z pairwise coprime. We can write

$$-x^p = y^p + z^p = (y+z)(y^{p-1} - y^{p-2}z + \cdots + z^{p-1})\ .$$

Clearly the two factors are relatively prime: we cannot have $p \mid (y+z)$ otherwise $p \mid x$, and if $r \neq p$ is a prime dividing both factors then $y \equiv -z \pmod r$ hence the second factor is congruent to py^{p-1} modulo r, and since $r \neq p$ we have $r \mid y$, hence $r \mid z$ contradicting the fact that y and z are coprime. Since p is odd (otherwise we would have to include signs), it follows that there exist coprime integers a and s such that $y + z = a^p$ and $y^{p-1} - y^{p-2}z + \cdots + z^{p-1} = s^p$. By symmetry, there exist b and c such that $z + x = b^p$ and $x + y = c^p$.

Consider now the prime $q = kp + 1$. The Fermat equation implies that

$$x^{(q-1)/k} + y^{(q-1)/k} + z^{(q-1)/k} \equiv 0 \pmod q\ .$$

I claim that $q \mid xyz$. Indeed, assume by contradiction that $q \nmid xyz$, and let $u = (x/z)^{(q-1)/k} \bmod q$, which makes sense since $q \nmid z$. Since $q \nmid x$ we have $u^k - 1 \equiv 0 \pmod q$. On the other hand $u + 1 \equiv -(y/z)^{(q-1)/k} \pmod q$, and since k is even and $q \nmid y$ we deduce that $(u+1)^k - 1 \equiv 0 \pmod q$. It follows that the polynomials $X^k - 1$ and $(X+1)^k - 1$ have the common root u modulo q, contradicting the assumption that $q \nmid R(X^k - 1, (X+1)^k - 1)$.

Thus $q \mid xyz$, and by symmetry we may assume for instance that $q \mid x$. Thus

$$\begin{aligned}0 \equiv 2x = (x+y) + (z+x) - (y+z) &= c^p + b^p + (-a)^p \\ &= c^{(q-1)/k} + b^{(q-1)/k} + (-a)^{(q-1)/k} \pmod q\ .\end{aligned}$$

As above, it follows that $q \mid abc$. Since $q \mid x$ and x, y and z are pairwise coprime, we cannot have $q \mid b^p = z + x$ or $q \mid c^p = x + y$. Thus $q \mid a$. It follows that $y \equiv -z \pmod q$, hence $s^p \equiv py^{p-1} \pmod q$. On the other hand $y = (x+y) - x \equiv c^p \pmod q$, so that

$$s^{(q-1)/k} = s^p \equiv pc^{((q-1)/k)(p-1)} \pmod q\ ,$$

and since $q \nmid c$ we have $p \equiv d^{(q-1)/k} \pmod{q}$ with $d = s/c^{p-1}$ modulo q. Since a and s are coprime we have $q \nmid s$ hence $q \nmid d$, so $p^k \equiv 1 \pmod{q}$. Since k is even it follows that

$$1 = (-1)^k = (kp - q)^k \equiv k^k p^k \equiv k^k \pmod{q}\ ,$$

contradicting the assumption that $q \nmid k^k - 1$. □

Note that we have not used explicitly the assumption that $k \not\equiv 0 \pmod{6}$. However, if $k \equiv 0 \pmod{6}$ then $\exp(2i\pi/3)$ is a common root of $X^k - 1$ and $(X+1)^k - 1$ in $\mathbb{C}$, hence the resultant of these polynomials is equal to 0 (over $\mathbb{C}$, hence over any ring), so that the condition on q can never be satisfied. In other words (2) and (3) together imply (1).

A computer search shows that for every prime $p \geq 3$ up to very large bounds we can find an integer k satisfying the conditions of the proposition, and as mentioned at the beginning of this section it can reasonably be conjectured that such a k always exists, so that in practice FLT I can always be checked thanks to this criterion. Of course, thanks to the work of Wiles et al., this is not really necessary, but it shows how far one can go using very elementary methods.

A special case of Wendt's criterion due to S. Germain was stated and proved some years before:

Corollary 3.2 *Let $p > 2$ be an odd prime, and assume that $q = 2p + 1$ is also a prime. Then FLT I is valid, in other words if $x^p + y^p + z^p = 0$ then $p \mid xyz$.*

Proof. Since for $k = 2$ we have $(k^k - 1)R(X^k - 1, (X + 1)^k - 1) = -3^2$, the condition of the proposition is $q \neq 3$, which is always true. □

3.2 Special Cases of the Equation $y^2 = x^3 + t$

This subsection is meant to give additional examples, but should be considered as supplementary exercises, and skipped on first reading.

The equation $y^2 = x^3 + t$ is famous, and has been treated by a wide variety of methods. In the present subsection, we give two class of examples which can easily be solved by factoring over $\mathbb{Z}$.

Proposition 3.3 *Let a and b be odd integers such that $3 \nmid b$, and assume that $t = 8a^3 - b^2$ is squarefree but of any sign. Then the equation $y^2 = x^3 + t$ has no integral solution.*

Note that the case $t = 7$ of this proposition was already posed by Fermat to his English contemporaries.

Proof. We rewrite the equation as

$$y^2 + b^2 = (x + 2a)((x - a)^2 + 3a^2) \ .$$

Note that x must be odd otherwise $y^2 = x^3 + t \equiv t \equiv 7 \pmod 8$, which is absurd. Since a is also odd it follows that $(x - a)^2 + 3a^2 \equiv 3 \pmod 4$, and since this is a positive number (why is this needed?) this implies that there exists a prime $p \equiv 3 \pmod 4$ dividing it to an *odd* power. Thus $y^2 + b^2 \equiv 0 \pmod p$. Since -1 is not a square in $\mathbb{F}_p$ when $p \equiv 3 \pmod 4$, this implies that p divides b and y. I claim that $p \nmid x + 2a$. Indeed, since $(x-a)^2+3a^2 = (x+2a)(x-4a)+12a^2$ the condition $p \mid x+2a$ would imply $p \mid 12a^2$, hence either $p \mid a$ or $p = 3$ ($p = 2$ is impossible since $p \equiv 3 \pmod 4$). But $p \mid a$ implies $p^2 \mid t = 8a^3 - b^2$, a contradiction since t is squarefree, and $p = 3$ implies $3 \mid b$, which has been excluded, proving my claim. Thus the p-adic valuation of $y^2 + b^2$ is equal to that of $(x - a)^2 + 3a^2$ hence is odd, a contradiction since this would again imply that -1 is a square in $\mathbb{F}_p$. □

Another similar result is the following.

Proposition 3.4 *Let a be an odd integer, let b be an integer such that $3 \nmid b$, and assume that $t = a^3 - 4b^2$ is squarefree, not congruent to 1 modulo 8, but of any sign. Then the equation $y^2 = x^3 + t$ has no integral solution.*

Proof. I claim that x is odd. Indeed, otherwise, since t is odd, y would be odd, hence $y^2 \equiv 1 \pmod 8$, hence $t \equiv 1 \pmod 8$, contradicting our assumption. Thus x is odd and y is even. Writing $y = 2y_1$ we obtain

$$4(y_1^2 + b^2) = x^3 + a^3 = (x + a)(x(x - a) + a^2) \ .$$

Since $x-a$ is even and a is odd, it follows that $4 \mid x+a$. Writing $x+a = 4x_1$, we obtain

$$y_1^2 + b^2 = x_1((4x_1 - a)(4x_1 - 2a) + a^2) = x_1(16x_1^2 - 12ax_1 + 3a^2) \ .$$

Since a is odd we have $16x_1^2 - 12ax_1 + 3a^2 \equiv 3 \pmod 4$, hence as in the preceding proof there exists a prime $p \equiv 3 \pmod 4$ dividing it to an odd power. As above, this implies that p divides y_1 and b. I claim that $p \nmid x_1$. Indeed, otherwise $p \mid 3a^2$, hence either $p \mid a$ or $p = 3$. As above $p \mid a$ is impossible since it implies $p^2 \mid t$, a contradiction since t is squarefree, and $p = 3$ implies $3 \mid b$, which has been excluded. Thus the p-adic valuation of

$y_1^2 + b^2$ is odd, a contradiction since this would imply that -1 is a square in $\mathbb{F}_p$. □

A computer search shows that the squarefree values of t such that $|t| \leq 100$ which can be treated by these propositions are the following: -97, -91, -79, -73, -71, -65, -57, -55, -43, -41, -37, -33, -31, -17, -15, -5, -3, 7, 11, 13, 23, 39, 47, 53, 61, 67, 83, 87, and 95. Another computer search finds solutions for the following squarefree values of t such that $|t| \leq 100$: -95, -89, -87, -83, -79, -74, -71, -67, -61, -55, -53, -47, -39, -35, -26, -23, -19, -15, -13, -11, -7, -2, -1, 1, 2, 3, 5, 10, 15, 17, 19, 22, 26, 30, 31, 33, 35, 37, 38, 41, 43, 55, 57, 65, 71, 73, 79, 82, 89, 91, 94, and 97. This still leaves 45 squarefree values of t, which can all be treated by other methods.

3.3 Introduction to Catalan's Equation

Catalan's conjecture, now a theorem, is the following:

Theorem 3.5 (Mihăilescu) *If n and m are greater than or equal to 2 the only nonzero integral solutions to*

$$x^m - y^n = 1$$

are $m = 2$, $n = 3$, $x = \pm 3$, $y = 2$.

This conjecture was formulated by Catalan in 1844 and received much attention. It was finally solved in 2002 by P. Mihăilescu. Complete proofs are available on the Web (see in particular [4]), and at least two books are being written on the subject.

The goal of this section is to prove a result on this equation, due to Cassels, which has been crucial for the final proof.

The cases $m = 2$ or $n = 2$, which are *not* excluded, are treated separately. The proof of the case $n = 2$, in other words of the equation $x^m - y^2 = 1$, is due to V.-A. Lebesgue in 1850. It is not difficult, but uses the factoring of the equation over $\mathbb{Z}[i]$, and not over $\mathbb{Z}$. Knowing this, the reader can try his/her hand at it, perhaps after reading the section dealing with factoring over number fields.

On the other hand, quite surprisingly, the proof of the case $m = 2$, in other words of the equation $x^2 - y^n = 1$ is considerably more difficult, and was only obtained in the 1960's by Ko Chao. In retrospect, it could have been obtained much earlier, since it is an easy consequence of a theorem of

Nagell which only uses the structure of the unit group in a real quadratic *order*.

Once these two cases out of the way, it is clear that we are reduced to the equation $x^p - y^q = 1$, where p and q are odd primes. Before continuing, we make the trivial but crucial observation that this equation is now symmetrical in p and q, in that if (p, q, x, y) is a solution, then $(q, p, -y, -x)$ is also a solution, since p and q are odd.

Cassels's results, which we will prove in this section, involve factoring the equation over $\mathbb{Z}$, clever reasoning, and an analytic method called "Runge's method", which boils down to saying that if $x \in \mathbb{R}$ is such that $|x| < 1$ and $x \in \mathbb{Z}$ then $x = 0$. Even though this looks like a triviality, all proofs using Diophantine approximation techniques (of which Runge's method is one) boil down to that. As an exercise, find all integer solutions to $y^2 = x^4 + x^3 + x^2 + x+1$ by introducing the polynomial $P(x)$ such that $P(x)^2-(x^4+x^3+x^2+x+1)$ has lowest degree.

For the proof of Cassel's results we will need one arithmetic and two analytic lemmas.

Lemma 3.6 *Set $w(j) = j + v_q(j!)$. Then $q^{w(j)}\binom{p/q}{j}$ is an integer not divisible by q, and $w(j)$ is a strictly increasing function of j.*

Proof. If ℓ is a prime number different from q we know that $\binom{p/q}{j}$ is an ℓ-adic integer (note that this is *not* completely trivial), and it is an immediate exercise that its q-adic valuation is equal to $-w(j)$, proving the first assertion. Since $w(j+1)-w(j) = 1+v_q(j+1) \geq 1$ the second assertion is also clear. □

The first analytic result that we need is the following.

Lemma 3.7

1. *For all $x > 0$ we have $(x + 1)\log(x + 1) > x\log(x)$.*
2. *Let $b \in \mathbb{R}_{>1}$. The function $(b^t + 1)^{1/t}$ is a decreasing function of t from $\mathbb{R}_{>0}$ to $R_{>0}$ and the function $(b^t - 1)^{1/t}$ is an increasing function of t from $\mathbb{R}_{>0}$ to $R_{>0}$.*
3. *Assume that $q > p \in \mathbb{R}_{>0}$. If $a \in \mathbb{R}_{\geq 1}$ then $(a^q + 1)^p < (a^p + 1)^q$ and if $a \in \mathbb{R}_{>1}$ then $(a^q - 1)^p > (a^p - 1)^q$.*

Proof. Easy undergraduate exercise, left to the reader. □

The second analytic result that we need is more delicate.

Lemma 3.8 *Assume that $p > q$, set $F(t) = ((1+t)^p - t^p)^{1/q}$, let $m = \lfloor p/q \rfloor + 1$, and denote by $F_m(t)$ the sum of the terms of degree at most equal to m in the Taylor series expansion of $F(t)$ around $t = 0$. Then for all $t \in \mathbb{R}$ such that $|t| \le 1/2$ we have*

$$|F(t) - F_m(t)| \le \frac{|t|^{m+1}}{(1-|t|)^2}\ .$$

I could leave the proof as an exercise, but since it is not entirely trivial I prefer to give it explicitly. I am indebted to R. Schoof for it.

Proof. Set $G(t) = (1+t)^{p/q}$. It is clear that the Taylor coefficients of $F(t)$ and $G(t)$ around $t = 0$ are the same to order strictly less than p, and in particular to order m since $m \le p/3 + 1 < p$ (since $p \ge 5$). In what follows, assume that $|t| < 1$. By the Taylor–Lagrange formula applied to the functions $x^{1/q}$ and $G(x)$ respectively there exist t_1 and t_2 such that

$$\begin{aligned}|F(t) - F_m(t)| &\le |F(t) - G(t)| + |G(t) - F_m(t)|\\ &\le \frac{|t|^p}{q} t_1^{1/q-1} + |t|^{m+1}\frac{1}{(m+1)!}G^{(m+1)}(t_2)\\ &\le \frac{|t|^p}{q} t_1^{1/q-1} + |t|^{m+1}\binom{p/q}{m+1}(1+t_2)^{p/q-m-1}\ ,\end{aligned}$$

with t_1 between $(1+t)^p$ and $(1+t)^p - t^p$, and t_2 between 0 and t. Now note that $p/q < m \le p/q + 1$, so that $-1 \le p/q - m < 0$ and for all $j \ge 1$ $0 < p/q - (m-j) = j - (m - p/q) < j$ hence

$$0 < \prod_{1\le j\le m}(p/q - (m-j)) < \prod_{1\le j\le m} j = m!\ .$$

It follows that

$$\left|\binom{p/q}{m+1}\right| = \frac{(m-p/q)}{m+1}\frac{\prod_{1\le j\le m}(p/q-(m-j))}{m!} \le \frac{1}{m+1}\ .$$

Since $1/q - 1 < 0$ and $p/q - m - 1 < 0$ we must estimate t_1 and $1 + t_2$ from below. If $t > 0$ both $(1+t)^p$ and $(1+t)^p - t^p$ are greater than 1, so $t_1 > 1 > 1 - t^p$. If $t < 0$ then $(1+t)^p = (1-|t|)^p$ and $(1+t)^p - t^p = (1-|t|)^p + |t|^p > (1-|t|)^p$, so that $t_1 > (1-|t|)^p$ in all cases. On the other hand we have trivially $|1 + t_2| \ge 1 - |t|$. Putting everything together we obtain

$$|F(t) - F_m(t)| \le \frac{|t|^p}{q}(1-|t|)^{-p+p/q} + \frac{|t|^{m+1}}{m+1}(1-|t|)^{p/q-m-1}\ .$$

The above inequality is valid for all t such that $|t| < 1$. If we assume that $|t| \leq 1/2$ then $|t|^{p-m-1} \leq (1-|t|)^{p-m-1}$ (since $m \leq p-1$), hence $|t|^p(1-|t|)^{-p+p/q} \leq |t|^{m+1}(1-|t|)^{p/q-m-1}$. It follows that

$$|F(t) - F_m(t)| \leq \left(\frac{1}{q} + \frac{1}{m+1}\right) |t|^{m+1}(1-|t|)^{p/q-m-1} .$$

Since $p/q - m - 1 \geq -2$ and $1/q + 1/(m+1) \leq 1$ the lemma follows. □

3.4 Cassels's Results on Catalan's Equation

Lemma 3.9 *Let p be prime, let $x \in \mathbb{Z}$ be such that $x \neq 1$, and set $r_p(x) = (x^p - 1)/(x-1)$.*

1. *If p divides one of the numbers $(x-1)$ or $r_p(x)$ it divides both.*
2. *If $d = \gcd(x-1, r_p(x))$ then $d = 1$ or $d = p$.*
3. *If $d = p$ and $p > 2$, then $r_p(x) \equiv p \pmod{p^2}$.*

Proof. Expanding $r_p(x) = ((x-1+1)^p - 1)/(x-1)$ by the binomial theorem we can write

$$r_p(x) = (x-1)^{p-1} + p + (x-1)\sum_{k=1}^{p-2} \binom{p}{k+1} (x-1)^{k-1}$$

and all three results of the lemma immediately follow from this and the fact that $p \mid \binom{p}{k+1}$ for $1 \leq k \leq p-2$. Note that (3) is trivially false for $p = 2$. □

Corollary 3.10 *Let (x, y, p, q) be such that $x^p - y^q = 1$. Then $\gcd(r_p(x), x-1) = p$ if $p \mid y$ and $\gcd(r_p(x), x-1) = 1$ otherwise.*

Proof. Since $y^q = (x-1)r_p(x)$ it follows that $p \mid y$ if and only if p divides either $x-1$ or $r_p(x)$, hence by the above lemma, if and only if $\gcd(r_p(x), x-1) = p$. □

We can now state and prove Cassels's results.

Theorem 3.11 (Cassels) *Let p and q be primes, and let x and y be nonzero integers such that $x^p - y^q = 1$. Then $p \mid y$ and $q \mid x$.*

Before proving this theorem, we state and prove its most important corollary.

Corollary 3.12 *If x and y are nonzero integers and p and q are odd primes such that $x^p - y^q = 1$ there exist nonzero integers a and b, and positive integers u and v with $q \nmid u$ and $p \nmid v$ such that*

$$x = qbu,\ x - 1 = p^{q-1}a^q,\ \frac{x^p - 1}{x - 1} = pv^q,$$
$$y = pav,\ y + 1 = q^{p-1}b^p,\ \frac{y^q + 1}{y + 1} = qu^p\ .$$

Proof. Since $p \mid y$, by the above corollary we have $\gcd(r_p(x), x-1) = p$, so by Lemma 3.9 (3) we have $r_p(x) \equiv p \pmod{p^2}$, and in particular $v_p(r_p(x)) = 1$. Thus the relation $y^q = (x-1)r_p(x)$ implies that there exist integers a and v with $p \nmid v$ such that $x - 1 = p^{q-1}a^q$, $r_p(x) = pv^q$, hence $y = pav$, and since $r_p(x) > 0$, we also have $v > 0$. This shows half of the relations of the theorem, and the other half follow by symmetry, changing (x, y, p, q) into $(-y, -x, q, p)$ and noting that p and q are odd. □

The proof of Cassels's Theorem 3.11 is split in two, according to whether $p < q$ or $p > q$. We begin with the case $p < q$ which is considerably simpler.

Proposition 3.13 *Let x and y be nonzero integers and p and q be odd primes such that $x^p - y^q = 1$. Then if $p < q$ we have $p \mid y$.*

Proof. Assume on the contrary that $p \nmid y$. It follows from Corollary 3.10 that $x - 1$ and $r_p(x)$ are coprime, and since their product is a q-th power, they both are. We can thus write $x - 1 = a^q$ for some integer a, and $a \neq 0$ (otherwise $y = 0$) and $a \neq -1$ (otherwise $x = 0$), hence $(a^q + 1)^p - y^q = 1$. Consider the function $f(z) = (a^q+1)^p - z^q - 1$, which is trivially a decreasing function of z. Assume first that $a \geq 1$. Then $f(a^p) = (a^q + 1)^p - a^{pq} - 1 > 0$ by the binomial expansion, while $f(a^p + 1) = (a^q + 1)^p - (a^p + 1)^q - 1 < 0$ by (3) of Lemma 3.7. Since f is strictly decreasing it follows that y which is such that $f(y) = 0$ is not an integer, a contradiction. Similarly, assume that $a < 0$, so that in fact $a \leq -2$, and set $b = -a$. Then since p and q are odd $f(a^p) = (a^q+1)^p - a^{pq} - 1 = -((b^q-1)^p - b^{pq} + 1) > 0$ by the binomial expansion, while $f(a^p + 1) = (a^q + 1)^p - (a^p + 1)^q - 1 = -((b^q - 1)^p - (b^p - 1)^q + 1) < 0$ again by (3) of the Lemma 3.7 since $b > 1$. Once again we obtain a contradiction, proving the proposition. □

The following corollary, essentially due to S. Hyyrö, will be used for the case $p > q$.

Corollary 3.14 *With the same assumptions as above* (*and in particular $p < q$*) *we have $|y| \geq p^{q-1} + p$.*

Proof. Since by the above proposition we have $p \mid y$, as in Corollary 3.12 we deduce that there exist integers a and v with $a \neq 0$ and $v > 0$ such that $x-1 = p^{q-1}a^p$, $(x^p-1)/(x-1) = pv^q$ and $y = pav$. Set $P(X) = X^p - 1 - p(X-1)$. Since $P(1) = P'(1) = 0$, it follows that $(X-1)^2 \mid P(X)$, hence that $(x-1) \mid (x^p-1)/(x-1) - p = p(v^q-1)$. Since $p^{q-1} \mid x-1$ it follows that $v^q \equiv 1 \pmod{p^{q-2}}$. However the order of the multiplicative group modulo p^{q-2} is equal to $p^{q-3}(p-1)$, and since $q > p$ this is coprime to q. As usual this implies that $v \equiv 1 \pmod{p^{q-2}}$.

On the other hand, I claim that $v > 1$. Indeed, assume otherwise that $v = 1$, in other words $x^{p-1} + \cdots + x + 1 = p$. If $x > 1$ then $2^{p-1} > p$ so this is impossible. Since p and q are odd primes and $a \neq 0$ we have $|x-1| = p^{q-1}|a|^p \geq 9$, hence when $x \leq 1$ we must have in fact $z = -x \geq 8$. But then since $p-1$ is even we have

$$p = z^{p-1} - z^{p-2} + \cdots + 1 \geq z^{p-1}(z-1) \geq z^{p-1} \geq 2^{p-1} \ ,$$

a contradiction which proves my claim. Since $v \equiv 1 \pmod{p^{q-2}}$, it follows that $v \geq p^{q-2}+1$, hence $|y| = pav \geq pv \geq p^{q-1}+p$, proving the corollary. □

We now prove the more difficult case $p > q$ of Cassels's theorem.

Proposition 3.15 *Let x and y be nonzero integers and p and q be odd primes such that $x^p - y^q = 1$. Then if $p > q$ we have $p \mid y$.*

Proof. We keep all the notation of Lemma 3.8 and begin as for the case $p < q$ (Proposition 3.13): assuming by contradiction that $p \nmid y$ and using Corollary 3.10, we deduce that there exists $a \in \mathbb{Z} \setminus \{0\}$ such that $x - 1 = a^q$, hence $y^q = (a^q+1)^p - 1$, so that $y = a^p F(1/a^q)$. Thus if we set $z = a^{mq-p}y - a^{mq}F_m(1/a^q)$ we have $z = a^{mq}(F(1/a^q) - F_m(1/a^q))$. Applying Lemma 3.8 to $t = 1/a^q$ (which satisfies $|t| \leq 1/2$ since $a \neq \pm 1$) we obtain

$$|z| \leq \frac{|a|^q}{(|a|^q-1)^2} \leq \frac{1}{|a|^q-2} \leq \frac{1}{|x|-3} \ .$$

By Taylor's theorem we have $t^m F_m(1/t) = \sum_{0 \leq j \leq m} \binom{p/q}{j} t^{m-j}$, and by Lemma 3.6 $D = q^{m+v_q(m!)}$ is a common denominator of all the $\binom{p/q}{j}$ for $0 \leq j \leq m$. It follows that $Da^{mq}F_m(1/a^q) \in \mathbb{Z}$, and since $mq \geq p$ that $Dz \in \mathbb{Z}$. We now estimate the size of Dz. By Hyyrö's Corollary 3.14 (with (p,q,x,y) replaced by $(q,p,-y,-x)$) we have $|x| \geq q^{p-1}+q \geq q^{p-1}+3$, so by the above estimate for $|z|$ we have

$$|Dz| \leq \frac{D}{|x|-3} \leq q^{m+v_q(m!)-(p-1)} \ .$$

Now for $m \geq 1$ we have $v_q(m!) < m/(q-1)$, and since $m < p/q + 1$ we have

$$m + v_q(m!) - (p-1) < m\frac{q}{q-1} - (p-1) = \frac{3-(p-2)(q-2)}{q-1} \leq 0$$

since $q \geq 3$ and $p \geq 5$ (note that it is essential that the above inequality be strict). Thus $|Dz| < 1$, and since $Dz \in \mathbb{Z}$, it follows that $Dz = 0$. However note that

$$Dz = Da^{mq-p}y - \sum_{0 \leq j \leq m} D\binom{p/q}{j} a^{q(m-j)} ,$$

and by Lemma 3.6 we have

$$v_q\left(\binom{p/q}{j}\right) < v_q\left(\binom{p/q}{m}\right) = v_q(D)$$

for $0 \leq j \leq m-1$, so that $0 = Dz \equiv D\binom{p/q}{m} \not\equiv 0 \pmod{q}$ by the same lemma. This contradiction finishes the proof of the proposition hence of Cassels's theorem. □

4 Factorization over Number Fields

Although factorization over $\mathbb{Z}$ can sometimes give interesting results, it is in general much more fruitful to factor over a *number field*. In fact, as already mentioned, the theory of number fields, essentially algebraic number theory, arose mainly from the necessity of inventing the tools necessary to solve Diophantine equations such as FLT.

4.1 An Algebraic Reminder

The prerequisites for this section is any classical course on algebraic number theory. We briefly review what we will need.

- A number field K is a finite extension of $\mathbb{Q}$. By the primitive element theorem it can always be given as $K = \mathbb{Q}(\alpha)$, where α is a root of some nonzero polynomial $A \in \mathbb{Q}[X]$.
- An algebraic *integer* is a root of a *monic* polynomial with integer coefficients. The element α such that $K = \mathbb{Q}(\alpha)$ can always be chosen to be an algebraic integer. The set of algebraic integers of K forms a ring, which we will denote by $\mathbb{Z}_K$, which contains (with finite index) $\mathbb{Z}[\alpha]$, when α is chosen to be an algebraic integer. It is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, and a $\mathbb{Z}$-basis of $\mathbb{Z}_K$ is called an integral basis.

- The ring $\mathbb{Z}_K$ is a Dedekind domain. Whatever that means, the main implication for us is that any fractional ideal can be decomposed uniquely into a power product of prime ideals. This is in fact the main motivation. Note the crucial fact that $\mathbb{Z}[\alpha]$ is *never* a Dedekind domain when it is not equal to $\mathbb{Z}_K$, so that prime ideal decomposition does not work in $\mathbb{Z}[\alpha]$.

- If p is a prime number, let $p\mathbb{Z}_K = \prod_{1\le i\le g} \mathfrak{p}_i^{e_i}$ be the prime power decomposition of the principal ideal $p\mathbb{Z}_K$. The ideals $\mathfrak{p}_i$ are exactly the prime ideals "above" (in other words containing) p, the e_i are called the ramification indexes, the field $\mathbb{Z}_K/\mathfrak{p}_i$ is a finite field containing $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and the degree of the finite field extension is denoted by f_i. Finally we have the important relation $\sum_{1\le i\le g} e_i f_i = n = [K : \mathbb{Q}]$.

- The class group $Cl(K)$ defined as the quotient of the group of fractional ideals by the group of principal ideals, is a finite group whose cardinality is often denoted $h(K)$.

- The unit group $U(K)$, in other words the group of invertible elements of $\mathbb{Z}_K$, or again the group of algebraic integers of norm equal to ± 1, is a finitely generated abelian group of rank $r_1 + r_2 - 1$, where r_1 and $2r_2$ are the number of real and complex embeddings, respectively. Its torsion subgroup is finite and equal to the group $\mu(K)$ of roots of unity contained in K.

- A quadratic field is of the form $\mathbb{Q}(\sqrt{t})$, where t is a squarefree integer different from 1. Its ring of integers is either equal to $\mathbb{Z}[\sqrt{t}] = \{a + b\sqrt{t},\ a, b \in \mathbb{Z}\}$ when $t \equiv 2$ or 3 modulo 4, or is the set of $(a + b\sqrt{t})/2$, where a and b are integers having the same parity.

- A cyclotomic field is a number field of the form $K = \mathbb{Q}(\zeta_\ell)$, where ζ_ℓ is a primitive m-th root of unity for some m. The main result that we will need is that the ring of integers of a cyclotomic field is equal to $\mathbb{Z}[\zeta_\ell]$, and no larger.

4.2 FLT I

We begin by the historically most important example, that of FLT I. In retrospect, Kummer's criterion that we will prove below does not seem to be very interesting since it has infinitely many exceptions, while the much more elementary criterion of Wendt has probably none. However congruence methods or approaches a la Wendt are totally useless for the *second case* of FLT, and in that case Kummer's methods can be adapted, with some difficulty, and in fact Kummer's initial criterion remains valid.

In the sequel, we let $\zeta_\ell = \zeta_p$ be a primitive p-th root of unity in $\mathbb{C}$, we let $K = \mathbb{Q}(\zeta_\ell)$, and we recall that the ring of integers of K is equal to $\mathbb{Z}[\zeta_\ell]$. We set $\pi = 1 - \zeta_\ell$, and recall that the ideal $\pi\mathbb{Z}_K$ is a prime ideal such that $(\pi\mathbb{Z}_K)^{p-1} = p\mathbb{Z}_K$, and p is the only prime number ramified in K. The first successful attacks on FLT were based on the possibility of unique factorization in $\mathbb{Z}[\zeta_\ell]$. Unfortunately this is true for only a limited number of small values of p. With the work of E. Kummer it was realized that one could achieve the same result with the much weaker hypothesis that p does not divide the class number h_p of $\mathbb{Z}_K$. Such a prime is called a *regular* prime. Note that it is known that there are infinitely many irregular (i.e., nonregular) primes, but that it is unknown (although widely believed) that there are infinitely many regular primes. In fact, there should be a positive density equal to $1 - 1/e$ of regular primes among all prime numbers. The irregular primes below 100 are $p = 37$, 59, and 67.

Let us begin by considering the case where there is unique factorization in $\mathbb{Z}[\zeta_\ell]$, so as to see below the "magic" of ideals. We prove the following lemma.

Lemma 4.1 *Assume that $\mathbb{Z}[\zeta_\ell]$ has unique factorization, in other words that it is a principal ideal domain. If $x^p + y^p = z^p$ with $p \nmid xyz$ then there exists $\alpha \in \mathbb{Z}[\zeta_\ell]$ and a unit u of $\mathbb{Z}[\zeta_\ell]$ such that*

$$x + y\zeta_\ell = u\alpha^p \ .$$

Proof. As usual we may assume that x, y, and z are pairwise coprime. The equation $x^p + y^p = z^p$ can be written

$$(x + y)(x + y\zeta_\ell) \cdots (x + y{\zeta_\ell}^{p-1}) = z^p \ .$$

I claim that the factors on the left are pairwise coprime (this makes sense, since $\mathbb{Z}[\zeta_\ell]$ is a PID): indeed, if some prime element ω divides $x + y{\zeta_\ell}^i$ and $x + y{\zeta_\ell}^j$ for $i \neq j$, it divides also $y({\zeta_\ell}^i - {\zeta_\ell}^j)$ and $x({\zeta_\ell}^j - {\zeta_\ell}^i)$, hence ${\zeta_\ell}^i - {\zeta_\ell}^j$ since x and y are coprime. Since the norm of ${\zeta_\ell}^i - {\zeta_\ell}^j$ is equal to p it follows that $\omega \mid p$, so that $\omega \mid z$, hence $p \mid z$, contrary to our hypothesis. We thus have a product of pairwise coprime elements in $\mathbb{Z}[\zeta_\ell]$ which is equal to a p-th power. Since $\mathbb{Z}[\zeta_\ell]$ is a PID, it follows that each of them is a p-th power, up to multiplication by a unit, proving the lemma. □

Unfortunately this lemma is not of much use since $\mathbb{Z}[\zeta_\ell]$ is a PID for only a small finite number of primes p. This is where *ideals* come in handy, since in the ring of integers of a number field there is always unique factorization of ideals into prime ideals:

Lemma 4.2 *The result of the above lemma is still true if we only assume that $p \nmid h_p$, in other words that p is a regular prime.*

Proof. The above proof is valid verbatim if we replace "prime element" by "prime ideal", so each ideal $\mathfrak{a}_i = (x + y{\zeta_\ell}^i)\mathbb{Z}_K$ is equal to the pth power of an ideal, say $\mathfrak{a}_i = \mathfrak{b}_i^p$. Now comes the crucial additional step: since the class number h_p is finite, we know that any ideal raised to the h_pth power is a principal ideal. Thus, both $\mathfrak{b}_i^p = (x + y{\zeta_\ell}^i)\mathbb{Z}_K$ and $\mathfrak{b}_i^{h_p}$ are principal ideals. Since $p \nmid h_p$ there exists integers u and v such that $up + vh_p = 1$, so that $\mathfrak{b}_i = (\mathfrak{b}_i^p)^u(\mathfrak{b}_i^{h_p})^v$ is also a principal ideal. Thus, if we write $\mathfrak{b}_1 = \alpha\mathbb{Z}_K$, we have

$$\mathfrak{a}_1 = (x + y\zeta_\ell)\mathbb{Z}_K = \alpha^p\mathbb{Z}_K = \mathfrak{b}_1^p\ .$$

Since two generators of a principal ideal differ multiplicatively by a unit, it follows that $x + y\zeta_\ell = u\alpha^p$ for some unit u. □

Proposition 4.3 *If $p \geq 3$ is a regular prime then FLT I holds.*

Proof. First note that if $p = 3$ and $p \nmid xyz$ we have x^3, y^3, and z^3 congruent to ± 1 modulo 9, which is impossible if $x^3 + y^3 = z^3$, so we may assume that $p \geq 5$. By the above lemma, there exists $\alpha \in \mathbb{Z}[\zeta_\ell]$ and a unit u such that $x + y\zeta_\ell = u\alpha^p$. Denote complex conjugation by $\bar{\ }$. An elementary but crucial lemma on cyclotomic fields asserts that if u is a unit of $\mathbb{Z}[\zeta_\ell]$, then $u/\overline{u}$ is a root of unity, and since the only roots of unity are $\pm{\zeta_\ell}^m$ for some m, we have $u/\overline{u} = \eta = \pm z^m$. Recall that we have set $\pi = 1 - \zeta_\ell$. Thus $\pi \mid ({\zeta_\ell}^j - {\zeta_\ell}^{-j})$ for all j, so that for any $\beta \in \mathbb{Z}[\zeta_\ell]$ we have $\overline{\beta} \equiv \beta \pmod{\pi}$, hence $\overline{\alpha} \equiv \alpha \pmod{\pi}$. Since $\pi \nmid z$, it follows that $\pi \nmid \alpha$, hence $\overline{\alpha}/\alpha \equiv 1 \pmod{\pi}$. Using the binomial expansion and the fact that $\pi^{(p-1)} \mid p\mathbb{Z}_K$, we deduce that $(\overline{\alpha}/\alpha)^p \equiv 1 \pmod{\pi^p}$. Dividing $x + \zeta_\ell y$ by its complex conjugate (and remembering that both are coprime to π), we obtain $(x+\zeta_\ell y)/(x+{\zeta_\ell}^{-1}y) \equiv \eta \pmod{\pi^p}$, in other words

$$x + \zeta_\ell y - \eta(x + {\zeta_\ell}^{-1}y) \equiv 0 \pmod{\pi^p}\ .$$

I claim that $m = 1$. Indeed, assume otherwise. If $m = 0$ we multiply the above congruence by ζ_ℓ, and if $m = p - 1$ we multiply it by ${\zeta_\ell}^2$, otherwise we do nothing. Thus we see that there exists a polynomial $f(T) \in \mathbb{Z}[T]$ of degree at most equal to $p-2 \geq 3$ (since we have assumed $p \geq 5$), not divisible by p, and such that $f(\zeta_\ell) \equiv 0 \pmod{\pi^p}$. Set $g(X) = f(1 - X)$. It is also of degree at most equal to $p-2$ and not divisible by p, and $g(\pi) \equiv 0 \pmod{\pi^p}$. However it is clear that different monomials in $g(\pi)$ have valuations which are noncongruent modulo $p-1$, hence are distinct, a contradiction. It follows that $m = 1$, proving my claim. Thus $\eta = \pm\zeta_\ell$, and our congruence reads $x + \zeta_\ell y \mp (x\zeta_\ell + y) = (x \mp y)(1 \mp \zeta_\ell) \equiv 0 \pmod{\pi^p}$ hence $x \mp y \equiv 0 \pmod{p}$. We cannot have $x + y \equiv 0 \pmod{p}$, otherwise $p \mid z$. Thus $y \equiv x \pmod{p}$. We may now apply the same reasoning to the equation $(-x)^p + z^p = y^p$ and deduce that $-z \equiv x \pmod{p}$. It follows that $0 = x^p + y^p - z^p \equiv 3x^p \pmod{p}$, and since $p \nmid x$, we obtain $p = 3$ which has been excluded and treated directly, finishing the proof of FLT I when p is a regular prime. $\square$

For instance, the irregular primes less than or equal to 200 are $p = 37$, 59, 67, 101, 103, 131, 149, 157, so that FLT I is true up to $p = 200$ for all but those primes. This of course also follows (for all primes) from Wendt's criterion.

Asymptotically, it is conjectured that the proportion of regular prime numbers is equal to $\exp(-1/2) = 0.607\ldots$, although it is not even known that there are infinitely of them, while it is easy to show that there are infinitely many irregular primes.

To finish this section on FLT, note that with more work it is possible to extend Kummer's theorem verbatim to FLT II.

4.3 The Equation $y^2 = x^3 + t$ Revisited

We come back to this equation which we have already solved in many cases above, but now using the techniques of algebraic number theory. Note that most of what we are going to say also applies to the more general equations $y^2 = x^p + t$ with $p \geq 3$ prime.

Proposition 4.4 *Let t be a squarefree negative integer not congruent to 1 modulo 8 and such that 3 does not divide the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{t})$.*

1. *When $t \equiv 2$ or 3 modulo 4 then if t is not of the form $t = -(3a^2 \pm 1)$ the equation $y^2 = x^3 + t$ has no integral solutions. If $t = -(3a^2 + \varepsilon)$ with $\varepsilon = \pm 1$, the integral solutions are $x = 4a^2 + \varepsilon$, $y = \pm(8a^3 + 3\varepsilon a)$.*

2. *When $t \equiv 5 \pmod{8}$ then if t is not of the form $t = -(12a^2 - 1)$ or $-(3a^2 \pm 8)$, both with a odd, the equation $y^2 = x^3 + t$ has no integral solutions. If $t = -(12a^2 - 1)$ with a odd, the integral solutions are $x = 16a^2 - 1$, $y = \pm(64a^3 - 6a)$. If $t = -(3a^2 + 8\varepsilon)$ with $\varepsilon = \pm 1$ and a odd, the integral solutions are $x = a^2 + 2\varepsilon$, $y = \pm(a^3 + 3a\varepsilon)$.*

Note that the case $t = -2$ of the above equation was already solved by Fermat, who also posed it as a challenge problem to his English contemporaries.

Proof. Let (x, y) be a solution to the equation $y^2 = x^3 + t$. I first claim that x is odd. Indeed, is x is even then y is odd (since otherwise $4 \mid t$, contradicting the fact that t is squarefree), hence $t = y^2 - x^3 \equiv 1 \pmod 8$, contradicting the assumption of the proposition. In the quadratic field $K = \mathbb{Q}(\sqrt{t})$ we factor our equation as $(y - \sqrt{t})(y + \sqrt{t}) = x^3$. I claim that the ideals generated by the two factors on the left are coprime. Indeed, assume otherwise, and let $\mathfrak{q}$ be a prime ideal of $\mathbb{Z}_K$ dividing both factors. It thus divides their sum and difference, hence if q is the prime number below $\mathfrak{q}$ we have $q \mid 2y$ and $q \mid 2t$. Since we have seen that x is odd $\mathfrak{q}$ cannot be above 2, so $q \mid \gcd(y, t)$, hence $q \mid x$ so $q^2 \mid t$, contradicting the fact that t is squarefree and proving my claim. Since the product of the two coprime ideals $(y - \sqrt{t})\mathbb{Z}_K$ and $(y + \sqrt{t})\mathbb{Z}_K$ is a cube, it follows that $(y + \sqrt{t})\mathbb{Z}_K = \mathfrak{a}^3$ for some ideal $\mathfrak{a}$ of $\mathbb{Z}_K$. As in the proof of FLT I for regular primes, since we have assumed that 3 does not divide the class number of K it follows that $\mathfrak{a}$ itself is a principal ideal, hence that there exists a unit $u \in K$ such that $y + \sqrt{t} = u\alpha^3$. However, since K is an *imaginary* quadratic field, there are not many units, and more precisely the group of units is $\{\pm 1\}$ except for $t = -1$ and $t = -3$ for which it has order 4 and 6 respectively. Thus the apart from the case $t = -3$, the order of the group of units not divisible by 3, hence any unit is a cube, so in these cases we are reduced to the equation $y + \sqrt{t} = \alpha^3$ with $\alpha \in \mathbb{Z}_K$. We postpone for later the special case $t = -3$. Since the ring of integers of a quadratic field is well known, we can write $\alpha = (a + b\sqrt{t})/d$ with a and b integral, where either $d = 1$, or, only in the case $t \equiv 5 \pmod 8$, also $d = 2$ and a and b odd. Expanding the relation $y + \sqrt{t} = \alpha^3$ gives the two equations

$$d^3 y = a(a^2 + 3b^2 t) \quad \text{and} \quad d^3 = b(3a^2 + b^2 t)\ .$$

Note that we may assume $a \geq 0$ since changing a into $-a$ does not change the second equation, and changes y into $-y$ in the first. From the second equation we deduce that $b \mid d^3$, and since b is coprime to d this means that $b = \pm 1$. It follows that $d^3 = \pm(3a^2 + t)$ and $d^3 y = a(a^2 + 3t)$. Separating the cases $d = 1$ and $d = 2$ (in which case a must be odd), and using the formula $x = \mathcal{N}_{K/\mathbb{Q}}(\alpha) = (a^2 - b^2 t)/d^2 = (a^2 - t)/d^2$ proves the proposition for $t \neq -3$.

Consider now the case $t = -3$. We have seen above that $y + \sqrt{t} = u\alpha^3$ for some unit u. Thus either we are led to the equations of the proposition (if $u = \pm 1$), or there exists $\varepsilon = \pm 1$ such that $y + \sqrt{t} = ((a + b\sqrt{t})/2)^3(-1 + \varepsilon\sqrt{t})/2$.

Equating coefficients of $\sqrt{t}$ gives

$$16 = \varepsilon(a^3 - 9b^2a) - 3b(a^2 - b^2) \ .$$

If $a \equiv 0 \pmod{3}$, the right hand side is divisible by 3, a contradiction. If $b \equiv 0 \pmod{3}$, the right hand side is congruent to ± 1 modulo 9 since a cube is such, again a contradiction. Thus neither a nor b is divisible by 3, hence $a^2 \equiv b^2 \equiv 1 \pmod{3}$, so the right hand side is still congruent to ± 1 modulo 9, a contradiction once again, so there are no solutions for $t = -3$. □

Remarks.

1. When t is not squarefree, it not difficult to obtain similar, but more complicated results.

2. In the other cases that we have not treated ($t \equiv 1 \pmod{8}$, $t > 0$, or 3 dividing the class number of $\mathbb{Q}(\sqrt{t})$) the problem is considerably more difficult but can be solved for a *given* value of t by the use of so-called Thue equations.

5 The Super-Fermat Equation

An equation of the form $x^p + y^q = z^r$, where p, q, and r are given positive exponents (greater than or equal to 2, otherwise there is no problem) is called a super-Fermat equation, and we search for integral solutions. Note that the equation is not homogeneous, so some new phenomena appear. In particular, it is now reasonable to *add* the supplementary condition that x, y, and z be pairwise coprime (in the homogeneous case this could be assumed without loss of generality). Indeed, as an easy but important exercise, the reader is invited to show that for instance if the exponents p, q, and r are pairwise coprime, there exist an infinity of solutions to the equation. We thus make the coprimeness assumption from now on.

A detailed study of what is known on these equations is fascinating, but we will have to restrict to a few facts. The behavior of the solution set depends in an essential way on the quantity $\chi = 1/p + 1/q + 1/r$ associated to the equation. It can be shown that if $\chi > 1$ there exist infinitely many (coprime) solutions, which can be given by a finite number of explicitly given disjoint parametric families. For $\chi = 1$ there are only finitely many (known) solutions, although if we had taken different coefficients in front of x^p, y^q, and z^r, there could be infinitely many. Finally, for $\chi < 1$ it is known that there are finitely many solutions, but not effectively. For instance it is widely believed that the equation $x^3 + y^5 = z^7$ has no coprime solutions, but this problem seems presently out of reach.

We will give a few examples of complete parametric solutions, and an example for $\chi < 1$ where it is not too difficult to give the solution set, using tools that we will only introduce later.

5.1 The Equations $x^2 + y^2 = z^2$ and $x^2 + 3y^2 = z^2$

We begin by a very simple and classical result.

Proposition 5.1 *The general coprime integer solution to the equation $x^2 + y^2 = z^2$ is given by the two disjoint parametrizations*

$$(x, y, z) = (2st, s^2 - t^2, \pm(s^2 + t^2)) \quad \textit{and} \quad (x, y, z) = (s^2 - t^2, 2st, \pm(s^2 + t^2)) \ ,$$

where s and t are two coprime integers of opposite parity.

Proof. Exchanging if necessary x and y, we may assume that x is even, hence y and z are odd. Also, changing signs if necessary we may assume that x, y, and z are nonnegative. Since z and y are coprime, so are $(z - y)/2$ and $(z + y)/2$ (consider the sum and difference), hence from the equation $(x/2)^2 = ((z - y)/2)((z + y)/2)$ we deduce that $(z - y)/2$ and $(z + y)/2$ are both squares (since they are nonnegative). The proposition follows by setting $(z - y)/2 = t^2$ and $(z + y)/2 = s^2$, which are coprime and of opposite parity. □

Note that the change of signs of x and/or y are accounted for by a change of sign of s or the exchange of s and t.

Proposition 5.2 *The general coprime integer solution of the equation $x^2 + 3y^2 = z^2$ is given by the two disjoint parametrizations*

$$(x, y, z) = (\pm(s^2 - 3t^2), 2st, \pm(s^2 + 3t^2)) \ ,$$

where s and t are coprime integers of opposite parity such that $3 \nmid s$, and

$$(x, y, z) = (\pm(s^2 + 4st + t^2), s^2 - t^2, \pm 2(s^2 + st + t^2)) \ ,$$

where s and t are coprime integers of opposite parity such that $s \not\equiv t \pmod 3$.

Proof. I first claim that x is odd. Indeed, if x is even y and z are odd, so that $x^2 = z^2 - 3y^2 \equiv 6 \pmod 8$, which is absurd. We write $3y^2 = (z - x)(z + x)$. Since x and z are coprime the GCD of $z - x$ and $z + x$ is either equal to 1 (when z is even) or to 2 (when z is odd). Assume first that $\gcd(z-x, z+x) = 1$, so that z is even. Changing x into $-x$ and z into $-z$ if necessary, there exist integers a and b, necessarily coprime, such that $z+x = 3a^2$, $z-x = b^2$, and $y = ab$. Since z is even and x odd, a and b are both odd, so that if we write $s = (a+b)/2$ and $t = (a-b)/2$ we obtain $z = 2(s^2+st+t^2)$ and $x = s^2+4st+t^2$, giving the second parametrization. Since a and b are odd, s and t have opposite parity, and since $z+x$ and $z-x$ are coprime we have $3 \nmid b = s-t$. Assume now that $\gcd(z-x, z+x) = 2$, so that z is odd and y is even. Writing $3(y/2)^2 = ((z-x)/2)((z+x)/2)$ and changing once again the signs of x and z, there exist coprime integers s and t such that $(z+x)/2 = s^2$ and $(z-x)/2 = 3t^2$, giving the first parametrization. Since x and z are odd s and t have opposite parity, and since $(z+x)/2$ and $(z-x)/2$ are coprime we have $3 \nmid s$. □

5.2 The Equation $x^3 + y^2 = z^2$ and $x^2 + y^2 = z^3$

Proposition 5.3 *The general coprime integer solution of the equation $x^3 + y^2 = z^2$ is given by the two disjoint parametrizations*

$$(x, y, z) = (s(s^2+3t^2), t(3s^2+t^2), (s-t)(s+t)) ,$$

where $s \not\equiv t \pmod{2}$, and

$$(x, y, z) = (\pm(2s^3+t^3), 2s^3-t^3, 2ts) ,$$

where $2 \nmid t$.

Proof. Here we simply write $(z-y)(z+y) = x^3$, and separate the cases where z and y have opposite or the same parity. The details are left as an exercise for the reader. □

Proposition 5.4 *The general coprime integer solution of the equation $x^2 + y^2 = z^3$ is given by the parametrization*

$$(x, y, z) = (s(s^2-3t^2), t(3s^2-t^2), s^2+t^2) ,$$

where s and t are coprime integers of opposite parity.

Proof. Here we work in the PID $\mathbb{Z}[i]$. Set $a = x+iy$, $b = x-iy$ so that $ab = z^3$. If we had $x \equiv y \equiv 1 \pmod{2}$, we would have $z^3 \equiv 2 \pmod{8}$, which is impossible. Since x and y are coprime it follows that x and y have opposite parity and a and b are coprime in the PID $\mathbb{Z}[i]$. It follows that there exist $\alpha = s+it \in \mathbb{Z}[i]$ and some unit u of $\mathbb{Z}[i]$ such that $x+iy = u\alpha^3$.

Since the unit group has order 4 every unit is a cube, so that, changing α if necessary we can write $x+iy=\alpha^3$, hence $x-iy=\overline{\alpha}^3$, $z=\alpha\overline{\alpha}$, giving the parametrization of the proposition. It is immediate to see that the condition that x and y be coprime is equivalent to s and t being coprime of opposite parity. □

5.3 The Equation $x^2+y^4=z^3$

We note that here we cannot have x and y both odd, otherwise $z^3 \equiv 2 \pmod 8$, absurd. We work in $\mathbb{Z}[i]$ and factor the equation as $(x+iy^2)(x-iy^2)=z^3$. Since x and y are coprime and not both odd, $x+iy^2$ and $x-iy^2$ are coprime in $\mathbb{Z}[i]$. Thus there exists $\alpha \in \mathbb{Z}[i]$ such that $x+iy^2=\alpha^3$, hence $x-iy^2=\overline{\alpha}^3$, $z=\alpha\overline{\alpha}$, where the possible power of i can be absorbed in α. We write $\alpha=u+iv$, so that $z=u^2+v^2$, $x=u^3-3uv^2$, and $y^2=3u^2v-v^3$. Thus, we must solve this equation. Note that since x and y are coprime, we have $\gcd(u,v)=1$ and u and v have opposite parity. We write $y^2=v(3u^2-v^2)$ and consider two cases.

Case 1: $3 \nmid v$

Then v and $3u^2-v^2$ are coprime, hence $v=\varepsilon a^2$, $3u^2-v^2=\varepsilon b^2$, $y=\pm ab$ with $\varepsilon=\pm 1$, and then a and b are coprime, b is odd, and $3 \nmid ab$. We note that $3u^2-v^2 \equiv -(u^2+v^2) \equiv -1 \pmod 4$ since u and v have opposite parity, hence we must have $\varepsilon=-1$, so the equations to be solved are $v=-a^2$ and $3u^2=v^2-b^2$. Since $3 \nmid v$ and $3 \nmid b$, changing if necessary b into $-b$, we may assume that $3 \mid v-b$, so the second equation is $u^2=((v-b)/3)(v+b)$. Note that v and b are coprime. I claim that v is odd. Indeed, otherwise a is even, hence $4 \mid v=-a^2$, hence $v^2-b^2 \equiv 7 \pmod 8$, while $3u^2 \equiv 3 \pmod 8$, a contradiction. Thus v is indeed odd, so u is even and $v-b$ and $v+b$ are even with $(v-b)/2$ and $(v+b)/2$ coprime. Thus we can write $v-b=6\varepsilon_1 c^2$, $v+b=2\varepsilon_1 d^2$, $u=2cd$ (where the sign of u can be removed by changing c into $-c$) with c and d coprime, and $3 \nmid d$. Thus $v=\varepsilon_1(3c^2+d^2)$, $b=\varepsilon_1(d^2-3c^2)$, and since $v=-a^2$ we have $\varepsilon_1=-1$, the last remaining equation to be solved is the second degree equation $d^2+3c^2=a^2$. Proposition 5.2 gives us à priori the two parametrizations $d=\pm(s^2-3t^2)$, $c=2st$, $a=\pm(s^2+3t^2)$ with coprime integers s and t of opposite parity such that $3 \nmid s$, and $d=\pm(s^2+4st+t^2)$, $c=s^2-t^2$, $a=\pm 2(s^2+st+t^2)$, with coprime integers s and t of opposite parity such that $s \not\equiv t \pmod 3$. However, since $v=-a^2$ is odd, a is odd hence this second parametrization is impossible. Thus there only remains the first one, so replacing everywhere gives the first parametrization

$$\begin{cases} x = 4ts(s^2 - 3t^2)(s^4 + 6t^2s^2 + 81t^4)(3s^4 + 2t^2s^2 + 3t^4) \\ y = \pm(s^2 + 3t^2)(s^4 - 18t^2s^2 + 9t^4) \\ z = (s^4 - 2t^2s^2 + 9t^4)(s^4 + 30t^2s^2 + 9t^4) \ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $3 \nmid s$.

Case 2: $3 \mid v$

Set $w = v/3$. Then $3 \nmid u$, w and $u^2 - 3w^2$ are coprime, hence $v = \varepsilon 3a^2$, $u^2 - 3w^2 = \varepsilon b^2$, $y = \pm 3ab$ with $\varepsilon = \pm 1$, and then a and b are coprime and b is odd. Since u and v (hence w) have opposite parity, we have $u^2 - 3w^2 \equiv u^2 + w^2 \equiv 1 \pmod 4$, hence we must have $\varepsilon = 1$, so the equations to be solved are $w = a^2$ and $u^2 - 3w^2 = b^2$. Proposition 5.2 tells us that there exist coprime integers c and d of opposite parity such that either $u = c^2 + 3d^2$, $w = 2cd$, $b = c^2 - 3d^2$ with $3 \nmid c$, or $u = 2(c^2 + cd + d^2)$, $w = c^2 - d^2$, $b = c^2 + 4cd + d^2$ with $c \not\equiv d \pmod 3$, where the signs can be absorbed as usual either by changing x into $-x$ or b into $-b$. Thus in the first case the final equation to be solved is $2cd = a^2$, so that there exists coprime s and t with $3 \nmid s$ such that either $c = 2s^2$, $d = t^2$, $a = \pm 2st$ and t odd, or $c = s^2$, $d = 2t^2$, $a = \pm 2st$ and s odd. Replacing everywhere gives the second and third parametrizations:

$$\begin{cases} x = \pm(4s^4 + 3t^4)(16s^8 - 408t^4s^4 + 9t^8) \\ y = 6ts(4s^4 - 3t^4) \\ z = 16s^8 + 168t^4s^4 + 9t^8 \ , \end{cases}$$

where t is odd and $3 \nmid s$.

$$\begin{cases} x = \pm(s^4 + 12t^4)(s^8 - 408t^4s^4 + 144t^8) \\ y = 6ts(s^4 - 12t^4) \\ z = s^8 + 168t^4s^4 + 144t^8 \ , \end{cases}$$

where s is odd and $3 \nmid s$.

In the second case the final equation to be solved is $c^2 - d^2 = a^2$ with c and d of opposite parity, hence with a odd, so that by the solution to the Pythagorean equation there exists coprime integers s and t of opposite parity such that $c = s^2 + t^2$, $d = 2st$, $a = s^2 - t^2$ with $s \not\equiv t \pmod 3$ Replacing everywhere gives the fourth and final parametrization:

$$\begin{cases} x = \pm 2(s^4+2ts^3+6t^2s^2+2t^3s+t^4)(23s^8-16ts^7-172t^2s^6-112t^3s^5 \\ \qquad\qquad -22t^4s^4-112t^5s^3-172t^6s^2-16t^7s+23t^8) \\ y = 3(s-t)(s+t)(s^4+8ts^3+6t^2s^2+8t^3s+t^4) \\ z = 13s^8+16ts^7+28t^2s^6+112t^3s^5+238t^4s^4 \\ \qquad\qquad +112t^5s^3+28t^6s^2+16t^7s+13t^8\ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $s \not\equiv t \pmod 3$.

We have thus shown the following theorem:

Theorem 5.5 *The equation $x^2+y^4=z^3$ in integers x, y, z with $\gcd(x,y)=1$ can be parametrized by one of the above four parametrizations, where s and t denote coprime integers with the indicated congruence conditions modulo 2 and 3. In addition these parametrizations are disjoint, in that any solution to our equation belongs to a single parametrization.*

5.4 An Example with $1/p+1/q+1/r<1$: the Equation $x^6-y^4=z^2$

As already mentioned, the cases $1/p+1/q+1/r<1$ are considerably more difficult, essentially because they can be reduced to finding rational points on curves of genus 1 or higher. We give one example of this. To treat it, we will need to find all the rational points on two elliptic curves. In the cases that we will consider this can be done using 2-*descent* methods. All this is implemented in an extremely useful program `mwrank` of J. Cremona, that we will therefore use as a black box. We will see later a sketch of how it works.

Proposition 5.6 *The equation $x^6-y^4=z^2$ has no solution in nonzero coprime integers x, y, z.*

Proof. Thanks to Proposition 5.4, we see that $x^6-y^4=z^2$ is equivalent to $x^2=s^2+t^2$, $y^2=s(s^2-3t^2)$, $z=t(3s^2-t^2)$ where s and t are coprime integers of opposite parity. By Proposition 5.1, up to exchange of s and t the first equation is equivalent to $s=2uv$, $t=u^2-v^2$, $x=\pm(u^2+v^2)$, where u and v are coprime integers of opposite parity. We consider both cases.

Case 1: $2 \mid s$

Set $a=u+v$, $b=u-v$, which are coprime and both odd. Then $s=(a^2-b^2)/2$ and $t=ab$, so the last equation to be solved can be written $8y^2=(a^2-b^2)(a^4-14a^2b^2+b^4)$. Since b is odd, we can set $Y=y/b^3$, $X=a^2/b^2$, and we obtain the equation $8Y^2=(X-1)(X^2-14X+1)$

or, equivalently $Y_1^2 = (X_1 - 2)(X_1^2 - 28X_1 + 4)$ after multiplying by 8 and setting $Y_1 = 8Y$ and $X_1 = 2X$. This is the equation of an elliptic curve in Weierstrass form, and the `mwrank` program or 2-descent methods tell us that the only rational point has $Y_1 = 0$, which does not correspond to a solution of our equation.

Case 2: $2 \nmid s$

Here $s = u^2 - v^2$, $t = 2uv$, so that the last equation to be solved can be written $y^2 = (u^2 - v^2)(u^4 - 14u^2v^2 + v^4)$. We cannot have $v = 0$, otherwise $t = 0$ hence $z = 0$, which is impossible. Thus, we can set $Y = y/v^3$, $X = u^2/v^2$ and we obtain the elliptic curve $Y^2 = (X - 1)(X^2 - 14X + 1)$. The `mwrank` program again tells us that the only rational point has $y = 0$, which does not correspond to a solution of our equation. □

6 Introduction to Elliptic Curves

It is of course out of the question in this short text to explain the incredibly rich theory of elliptic curves. As we have done above with p-adic numbers and with algebraic number theory, we simply recall without proof a number of basic definitions and facts.

For many more details and examples, see Chapter 8 (pages 495 to 587) of the accompanying pdf file.

6.1 An Elliptic Curve Reminder

- The "abstract" definition of an elliptic curve is a curve of genus 1 together with a point defined on the base field. In practice, an elliptic curve can be given in a number of ways: the simplest is as a simple Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$, or as a generalized Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (the numbering is canonical!), together with the condition that the curve be nonsingular, condition which is understood in the subsequent examples. More generally it can be given as a nonsingular plane cubic, as a hyperelliptic quartic $y^2 = a^2x^4 + bx^3 + cx^2 + dx + e$, as the intersection of two quadrics, and so on. All these other realizations can algorithmically be transformed into Weierstrass form, so we will assume from now on that this is the case.

- The set of projective points of an elliptic curve (in the case of $y^2 = x^3 + ax^2 + bx + c$, these are the affine points plus the point at infinity $\emptyset$ with projective coordinates $(0 : 1 : 0)$) form an abelian *group* under the secant and tangent method of Fermat (if you do not know what this is, here is a brief explanation: if P and Q are distinct points on the curve, draw the line joining P and Q; it meets the curve in a third point R, and we define $P+Q$ to be the symmetrical point of R with respect to the x-axis. If $P=Q$, do the same with the tangent).

- If the base field is $\mathbb{C}$ the group $E(\mathbb{C})$ of complex points of an elliptic curve E is in canonical bijection with the quotient $\mathbb{C}/\Lambda$, where Λ is a *lattice* of $\mathbb{C}$, thanks to the Weierstrass $\wp$ function and its derivative.

- If the base field is a finite field $\mathbb{F}_q$, we have the important Hasse bound $|E(\mathbb{F}_q)-(q+1)|\le 2\sqrt{q}$.

- If the base field is equal to $\mathbb{Q}_p$ (or more generally to a finite extension of $\mathbb{Q}_p$), we have a good understanding of $E(\mathbb{Q}_p)$.

The reader will of course have noticed that I do not mention the most interesting case where the base field is equal to $\mathbb{Q}$, or more generally a number field. Indeed, this deserves a theorem:

Theorem 6.1 (Mordell–Weil) *Let K be a number field. The group $E(K)$ is a finitely generated abelian group, called the Mordell–Weil group of E (over K).*

Thus $E(K)\simeq E(K)_{\text{tors}}\oplus\mathbb{Z}^r$, where $E(K)_{\text{tors}}$ is a finite group, and r is of course called the rank of $E(K)$. The finite group $E(K)_{\text{tors}}$ can be computed algorithmically (and there are only a finite number of possibilities for it, which are known for instance for $K=\mathbb{Q}$). On the other hand, one of the major unsolved problems on elliptic curves is to compute algorithmically the rank r, together with a system of generators.

The goal of the next sections is to explain some methods which can be used to compute the Mordell–Weil group over $\mathbb{Q}$, either rigorously in certain cases, or heuristically. Keep in mind that there is no general algorithm, but only partial ones, which luckily work in "most" cases. We will mention the 2 and 3-descent techniques, the use of L-functions, and finish with the beautiful Heegner point method, one of the most amazing and useful tools in the theory, both for the theory and in practice.

7 2-Descent with Rational 2-Torsion

See Section 8.2, pages 510–525.

8 General 2-Descent

See Section 8.3, pages 526–534.

9 3-Descent with Rational 3-Torsion Subgroup

See Section 8.4, pages 534–544.

Look in particular at the beautiful application to $ax^3 + by^3 + cz^3 = 0$ in Section 8.4.5, pages 542–544.

10 Use of $L(E, s)$

See Section 8.5, pages 544–560.

11 The Heegner Point Method

See Section 8.6, pages 560–573.

12 Computation of Integral Points

See Section 8.7, pages 573–580.

References

[1] J. Cremona, *Computing the degree of the modular parametrization of a modular elliptic curve*, Math. Comp. **64** (1995), 1235–1250.

[2] H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Math. **101** (2004), American Math. Soc., also available on the author's web page.

[3] B. Gross, *Heegner points on $X_0(N)$*, in Modular forms, edited by R. Rankin (1984), 87–105.

[4] M. Mischler, *La conjecture de Catalan racontée à un ami qui a le temps*, preprint available on the web at the URL `http://arxiv.org/pdf/math.NT/0502350`.

[5] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), 372–384.