Fermat's last theorem for regular primes

Dinesh S. Thakur

The so-called Fermat's last theorem (FLT for short) that 'there are no integral solutions to $x^n + y^n = z^n$, with $n > 2$ and $xyz \neq 0$ (a non-triviality condition)' is now proved by Wiles. The proof is outside the scope of this summer school, though we will sketch some ideas in the later lectures.

Now we will prove the so-called 'regular prime case' of FLT, following Kummer in essence, but connecting with later ideas and simplifications by other mathematicians.

It may be advisable to first learn the proof for $n = 3$ from Hardy and Wright or from Ireland-Rosen pp. 285-286, which prove even stronger result, using only the basics of quadratic fields that we have seen.

Since FLT for the exponent n implies FLT for multiples of n and since we proved it for $n = 4$, it is enough to prove FLT for $n = p$ an odd prime. The basic strategy is the same as before: try to get an infinite descent and thus a contradiction starting with an assumed non-trivial solution. We have a factorization $z^p = \prod(x + \zeta_p^i y)$ and we try to conclude that each factor (apart from GCD) is a p-th power. This conclusion is justified in the case of unique factorization domains. But since we only have unique factorization in ideals in general, we can conclude that each factor is a p-th power of an ideal, which can be further assumed to be principal, if p does not divide h, the class number of $\mathbf{Q}(\zeta_p)$. Such a (odd) prime is called a *regular prime*. But we want more. If a principal ideal is known to be a p-th power, its generator is of the form $u\alpha^p$, for some unit u and we would like to know when u itself can be concluded to be a p-th power. Since $(\sum a_i\zeta_p^i)^p \equiv \sum a_i^p(\zeta_p^p)^i \equiv \sum a_i$ modulo p, we know that the p-th powers are congruent to rational integers modulo p.

Kummer's lemma: If p is a regular prime and u is a unit of $\mathbf{Z}[\zeta_p]$ congruent to a rational integer modulo p, then u is a p-th power.

This is the hard part of the proof. This and characterization of regularity in terms of divisibility properties of Bernoulli numbers (essentially the special zeta values) are the great achievements of Kummer regarding the theorem. We will first prove FLT for regular p, assuming the Kummer lemma and then prove the Kummer's lemma.

What do we know about the regular primes? There are only three irregular primes less than hundred: 37, 59 and 67. Numerical data and heuristics

(see Washington) suggest that approximately 61 % of the primes are regular, but it is not even proved that there are infinitely many. On the other hand, it is known that (see Katre's article) there are infinitely many irregular primes!

FLT for regular primes. If p is a regular prime, then $x^p + y^p = z^p$ has no non-trivial integral solutions.

In fact, there are no non-trivial solutions, even in $\mathbf{Z}[\zeta_p]$, but we will not prove this.

From what we have seen earlier, we might want to try to show there are no local solutions. But indeed there are local and global solutions, namely the trivial ones. So the next natural try is to see whether there are any local non-trivial solutions or even non-trivial solutions modulo a prime. If we look at the prime p itself, this leads naturally the so-called *first case*: p does not divide xyz. Indeed, $x^p + y^p = z^p$ has no non-trivial solutions modulo 9, if $p = 3$ and modulo 25, if $p = 5$. So the first case for $p = 3$ and $p = 5$ follows. For $p = 7$, there is even a 7-adic non-trivial solution (exercise). So we follow a different path. If p divides xyz, it is called the *second case* and then we need Kummer's lemma, which we do not need for the first case.

It should be noted though that (i) Terjanian gave a short, elementary proof of the first case for exponent $2p$ instead, (ii) Sophie Germain gave an elementary proof of the first case, for odd prime p such that $2p + 1$ is also a prime, and combining her ideas with sieve techniques, it was proved by Adleman, Heath-Brown and Fouvry that the first case holds for infinitely many primes p, (iii) Eichler proved the first case, under much weaker hypothesis that $p^{\lfloor\sqrt{p}\rfloor-2}$ does not divide h. There are even some easy, non-trivial conditions, for which no counter-example is known and under which the first case is proved. For these and more results, see Ribenboim's book on FLT.

Proof for the first case: For the rest of the chapter, let p be a prime greater than 3, $\zeta := \zeta_p$, $K := \mathbf{Q}(\zeta)$, $\mathcal{O} := \mathbf{Z}[\zeta]$, h be the class number of $\mathcal{O}$ and $\lambda := 1 - \zeta$.

Suppose $x^p + y^p = z^p$, with x, y and z relatively prime (without loss of generality, as we can just take out the common factors: note that if x, y , z were to be cyclotomic integers, we can not do this, as there may be non-principal ideal common factor) and with p not dividing xyz. We want to get a contradiction.

If $x \equiv y \equiv -z$ modulo p, then $-2z^p \equiv z^p$ modulo p which is a contradiction, since $p > 3$. Hence, changing signs and labelling of x, y and z if necessary, we can assume that $x \not\equiv y$ modulo p. We have $z^p = \prod(x + \zeta^i y)$.

Lemma 1: Ideals $(x + \zeta^i y)$ are relatively prime: Otherwise a prime $\wp$ divides two of them. By eliminating x, we see that $\wp$ divides λ or y, whereas eliminating y, we see that $\wp$ divides λ or x. So $\wp = \lambda$. But then $x + y \equiv$

$x + \zeta^i y \equiv 0$ modulo λ, hence $z^p \equiv x + y \equiv 0$ modulo λ, which leads to the contradiction p divides z.

So by the unique factorization of ideals, each factor is a p-th power of an ideal which is principal by regularity. Hence $x + \zeta^i y = \epsilon_i \alpha_i^p$, where ϵ_i are units and $\alpha_i \in \mathcal{O}$.

Lemma 2: Any unit ϵ of $\mathcal{O}$ is a power of ζ times a real unit: Since $\epsilon/\overline{\epsilon}$ is an algebraic integer with all its absolute values 1, it is a root of unity, so can be written as $\pm\zeta^{2r}$. If the sign is positive, $\zeta^{-r}\epsilon$ is invariant under the complex conjugation and is thus real and we are done. Now we have modulo λ, $\epsilon = \sum a_i \zeta^i \equiv \sum a_i \equiv \overline{\epsilon}$, whereas the negative sign would lead to $\epsilon \equiv -\overline{\epsilon}$, a contradiction. (Note that the first half of the argument is a special case of what we have seen before in much more general situation).

So, since a p-th power is congruent to a rational integer modulo p, we get $x + \zeta y = \zeta^r \epsilon_1 \alpha^p \equiv \zeta^r \epsilon_1 a$ modulo p, with rational integer a and a real unit ϵ_1. Conjugation gives $x + \zeta^{-1} y \equiv \zeta^{-r} \epsilon_1 a$ modulo p. Hence $\zeta^{-r}(x + \zeta y) \equiv \zeta^r (x + \zeta^{-1} y)$ i.e., $x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0$ modulo p. If the ζ powers occurring here are distinct, then since they form a part of a basis, we get p divides x and y, which is a contradiction. Otherwise, we break into the following cases, each leading to an easy contradiction listed: (i) $1 = \zeta^{2r}$, then p divides y, (ii) $1 = \zeta^{2r-1}$, then p divides $x - y$ and (iii) $\zeta = \zeta^{2r-1}$, then p divides x. This finishes the proof of the first case.

Proof of the second case: Suppose there is a second case non-trivial solution, then taking out the common λ factors, if any, we have $\alpha^p + \beta^p = \epsilon \delta^p \lambda^{mp}$, with m least positive such, $\alpha, \beta, \gamma \in \mathcal{O}$ not divisible by λ and ϵ a unit. Writing $\alpha^p + \beta^p = \prod(\alpha + \zeta^i \beta)$ we analyze the GCD:

Lemma 3: Changing β by $\zeta^i \beta$ if necessary, we have $\alpha + \beta = \lambda^{p(m-1)+1} I' J_0^p$ and $\alpha + \zeta^k \beta = \lambda I' J_k^p$, where $I' = (\alpha, \beta)$, J_i are pairwise prime and not multiples of λ and $m > 1$.

Assuming this for now, we have $(\alpha + \zeta^k \beta)/(\alpha + \beta) = \lambda^{-p(m-1)} (J_k/J_0)^p$, so again by regularity assumption on p, we know that J_k/J_0 is principal generated by μ_k/n_k say, with $\mu_k \in \mathcal{O}$ and $n_k \in \mathbf{Z}$ both not divisible by λ. Hence $(\alpha + \zeta^k \beta)\lambda^{p(m-1)} = \epsilon_k (\alpha + \beta)(\mu_k/n_k)^p$. Subtracting the resulting equation for $k = 2$ from $(1 + \zeta)$ times the equation resulting for $k = 1$, we get $\zeta(\alpha + \beta)\lambda^{p(m-1)} = (\alpha + \beta)[(\mu_1/n_1)^p \epsilon_1 (1 + \zeta) - (\mu_2/n_2)^p \epsilon_2]$ implying $(\mu_1 n_2)^p - (\epsilon_2 (\mu_2 n_1)^p)/(\epsilon_1(1 + \zeta)) = \lambda^{p(m-1)} (n_1 n_2)^p \zeta/(\epsilon_1(1 + \zeta))$.

Now $1 + \zeta = (1 - \zeta^2)/(1 - \zeta)$ is a unit. Hence we get an equation of the form $\alpha_1^p + \epsilon' \beta_1^p = \epsilon'' \delta_1^p \lambda^{p(m-1)}$, with α_1 and β_1 not multiples of λ. This would contradict the minimality of m above, if we can show that the unit ϵ' is a p-th power. This we do using Kummer's lemma: By Lemma 3, we have $m > 1$, so λ^p divides $\alpha_1^p + \epsilon' \beta_1^p$. Now $\beta_1 = \mu_2 n_1$ is prime to λ, so ϵ' is

a p-th power modulo λ^p and hence modulo p, so it is congruent to rational integer modulo p. Kummer lemma then provides the contradiction we need. This finishes the proof of the Theorem, modulo the proof of Lemma 3 and Kummer's lemma, which we now proceed to prove.

Proof of Lemma 3: Since α is not divisible by λ, we have $\alpha \equiv a + d\lambda$ modulo λ^2, with a not divisible by p. Let $ca \equiv d$ modulo p.

Then $(\zeta^c\alpha - a)/(1-\zeta) \equiv -a(1-\zeta^c)/(1-\zeta) + d\zeta^c \equiv -ac + d \equiv 0$ modulo λ, i.e., $\zeta^c\alpha \equiv a$, a rational integer, modulo λ^2.

So multiplying α and β by appropriate ζ powers, we can assume that $\alpha \equiv a$ and $\beta \equiv b$ modulo λ^2. Since $(p) = (\lambda^{p-1})$, we have $\alpha^p \equiv a^p$ and $\beta^p \equiv b^p$ modulo $\lambda^{p+1} = p\lambda^2$, as the p-th binomial coefficients are divisible by p. If m were 1, $a^p + b^p = \alpha^p + \beta^p + \rho\lambda^{p+1} = \epsilon\lambda^p(\delta^p + \epsilon^{-1}\rho\lambda)$. But if $a^p + b^p$ has valuation e at p, then it has valuation $e(p-1)$ at λ, whereas the right side has valuation p, a contradiction proving $m > 1$.

Now $\epsilon\delta^p\lambda^{mp} = \prod(\alpha + \zeta^k\beta)$. So λ divides some term of the product, but the difference in i-th and j-th term is $\zeta^j(\zeta^{i-j} - 1)\beta$ which is divisible by λ to the exactly first power. Hence λ divides each term and only one term, say one corresponding to j_0, can be divisible by higher power of λ. Hence the λ powers are as claimed in the lemma. Now $I' = (\alpha, \beta)$ divides each term and is not divisible by λ, so we see that J_i' are relatively prime. (If $\wp$ divides two of them, then $\lambda I'\wp$ divides the difference and hence divides $\lambda\beta$ and similarly divides $\lambda\alpha$. This implies $I'\wp$ divides $(\alpha, \beta) = I'$, a contradiction). Hence, each is a p-th power, as claimed. This proves lemma 3.

Proof of Kummer's lemma: First proof: The first proof is the simplest, assuming the following fact from the class field theory, for the special case $F = K := \mathbf{Q}(\zeta)$.

Fact: Given any number field F, its maximal abelian unramified extension H_F (called the Hilbert class field of F) has degree h_F, the class number of F.

Suppose u is as in the hypothesis, but not a p-th power, then $K(u^{1/p})$ is (a Kummer extension) an abelian extension of degree p of K. We will get a contradiction to the regularity of p, once we show that this extension is unramified everywhere:

Without loss of generality, we can assume that $u \equiv 1$ modulo p (replace u by u^{p-1}, if necessary). We then claim that, in fact, $u \equiv 1$ modulo λ^p: Write $u = 1 + \kappa p$. Now κ is congruent to some rational integer k modulo λ, as its residue field is $\mathbf{Z}/p\mathbf{Z}$. Hence $u \equiv 1 + kp$, a rational integer modulo λ^p. But conjugate of u is also congruent to the same integer modulo λ^p, as λ is its own conjugate. Hence $1 = Norm(u) \equiv (1 + kp)^{p-1} \equiv 1 - kp$, which implies $k \equiv 0$ modulo p proving the claim.

Now let w be a p-th root of u. Then $(1-w)/\lambda$ is a root of $((\lambda x - 1)^p + u)/\lambda^p$, which is a monic polynomial with algebraic integer coefficients by the claim above. Hence $(1-w)/\lambda$, which generates the same extension as w, is an algebraic integer. But the other roots are $(1-\zeta^i w)/\lambda$ and hence the differences of the roots are $(\zeta^i - \zeta^j)w/\lambda$ which are units. Hence the relative field discriminant is a unit, as it divides the product of these differences. Hence the extension is everywhere unramified (including at the infinite places, which are complex, so there is nothing to check there) as claimed. This finishes the first proof.

See also Washington pp. 80-81 for a couple of variations on this proof.

Kummer's lemma: Second proof: This proof again uses what we proved above that if the Kummer's lemma is false for u, then the Kummer extension we thus get is everywhere unramified, but rather than using the fact about Hilbert class field to get a contradiction, we get immediate contradiction by applying the following theorem to $K = \mathbf{Q}(\zeta)$ and $L = K(u^{1/p})$.

Hilbert theorem 94: Let K be a number field and let L be its cyclic extension of degree p, an odd prime and with relative discriminant 1. Then there is a non-principal ideal J of $\mathcal{O}_K$ such that $I = J\mathcal{O}_L$ is principal. Further, J^p is principal, so that p divides the class number of K.

Proof: We use the following theorem:

Theorem: Let L be a cyclic extension of a number field K of degree p, an odd prime. Let $Gal(L/K) = \langle\sigma\rangle$. Then there is $U \in \mathcal{O}_L^*$ of relative norm 1 which is not $(1-\sigma)$-th power of a unit (in $\mathcal{O}_L^*$).

This says that $H^1(Gal(L/K), \mathcal{O}_L^*) \neq 0$ and follows by easy Herbrand quotient argument, if you know that technology. We will give a classical proof (see Hilbert chapter 15) based on construction of a 'relative units basis'. But first let us see how it implies the theorem: By Hilbert 90, proved in Narlikar lectures, (i.e, $H^1(Gal, L^*) = 0$), we can write $U = \alpha^{1-\sigma}$, with $\alpha \in L^*$. Multiplying by suitable rational integer, we can assume that $\alpha \in \mathcal{O}_L^*$.

Let $I = (\alpha)$. Then $I^\sigma = (U\alpha) = I$. Consider a prime factor $\wp$, if any, which does not lie in K (i.e., is not inert). If $\wp^\sigma \neq \wp$, so that $\wp$ splits, then the relative norm of $\wp$, which is a prime ideal in K divides I. If $\wp^\sigma = \wp$, then $\wp$ is ramified, which contradicts the discriminant hypothesis. Hence I comes from an ideal J of $\mathcal{O}_K$.

If J were principal, then $\alpha = \overline{U}\alpha_1$ for some unit $\overline{U} \in \mathcal{O}_L^*$ and $\alpha_1 \in \mathcal{O}_K$. Now $\alpha^{1-\sigma} = \overline{U}^{1-\sigma}$, a contradiction. Finally, J^p is the relative norm of I, so is principal generated by relative norm of α. This finishes the proof of Hilbert theorem 94 modulo the proof of the Theorem.

Proof of the Theorem: To construct the U we want, we have to get a

good control on the units with respect to the Galois action. Let $\epsilon_i \in \mathcal{O}_K^*$, $1 \leq i \leq r = r_K = r_1 + r_2 - 1$ be independent units. By the Dirichlet theorem, they form a finite index subgroup of $\mathcal{O}_K^*$. Since our extension is cyclic of odd degree p, the real primes cannot ramify and we have $r_L = p(r_1 + r_2) - 1$. If we choose a unit $U_1 \in \mathcal{O}_L^*$ independent of ϵ_i, then $r + p - 1$ units ϵ_j, $U_1^{\sigma^i}$ $(0 \leq i < p - 1)$ are independent: Otherwise we have a (non-zero) polynomial $F(\sigma)$ of degree $\leq p - 2$ and with integral coefficients such that $U_1^{F(\sigma)} \in \mathcal{O}_K^*$, with obvious meaning attached to this exponentiation. Since (the norm) $1 + \sigma + \cdots + \sigma^{p-1}$ is irreducible of degree $p - 1$, expressing the GCD as a linear combination and clearing the denominators, we get $Fg_1 + (1 + \sigma + \cdots + \sigma^{p-1})g_2 = a \in \mathbf{Z} - \{0\}$, with some polynomials g_1 and g_2 with integral coefficients. This would lead to a contradiction $U_1^a \in \mathcal{O}_K^*$ to the choice of U_1. Similarly, if we choose U_2 independent from the previous list, then $U_2^{\sigma^i}$, $0 \leq i \leq p-2$ are also independent and so on. Continuing this way, we get a set of $(r + 1)(p - 1) + r = r_L$ independent units consisting of ϵ_i's and $r + 1$ blocks of $U_i^{\sigma^j}$.

We can do even better.

Theorem: Units $\overline{U_1}, \cdots, \overline{U_{r+1}} \in \mathcal{O}_L^*$ exist such that if $\prod \overline{U_i}^{F_i(\sigma)} = U^{1-\sigma}\epsilon$, where $U \in \mathcal{O}_L^*$ and where $\epsilon \in \mathcal{O}_K^*$ or $\epsilon \in \mathcal{O}_L^*$ with $\epsilon^p \in \mathcal{O}_K^*$, then p divides $F_i(1)$, for all i.

Such a system $\overline{U_i}$ is called a *fundamental system of relative units*. Note that p divides $F_i(1)$ is equivalent to λ dividing $F_i(\zeta)$ or $1 - \sigma$ dividing $F_i(\sigma)$, since $\zeta^i \equiv 1$ modulo λ. Let us write $[\epsilon]$ as a short-hand for an arbitrary unit of K or a unit of L with its p-th power belonging to K.

Proof: We have found a nice subset of units generating a finite index subgroup of $\mathcal{O}_L^*$. Hence, for large enough p^m, $\prod U_i^{F_i(\sigma)}[\epsilon]$ cannot be a p^m-th power of a unit, unless all the coefficients of $F_i(\sigma)$ (of degree $\leq p - 2$) are divisible by p.

Now $(1 - \sigma)^p = 1 - \sigma^p + pg(\sigma)$, so that $(1 - \sigma)^{pm}$-th symbolic power is actually p^m-th power. So let e_1 be the largest non-negative integer such that $\prod_1^{r+1} U_i^{F_i(\sigma)}[\epsilon] = \overline{U_1}^{(1-\sigma)^{e_1}}$, with $\overline{U_1} \in \mathcal{O}_L^*$ and without having all $F_i(\zeta)$ divisible by λ, say $F_1(\zeta)$ is not divisible by λ. Next, let e_2 be the largest non-negative integer such that $\prod_2^{r+1} U_i^{F_i(\sigma)}[\epsilon] = \overline{U_2}^{(1-\sigma)^{e_2}}$, with $F_2(\zeta)$ not divisible by λ and so on.

Now suppose there are $g_i(\sigma)$ such that $\prod_1^{r+1} \overline{U_i}^{g_\sigma}[\epsilon]$ is $1 - \sigma$-th power of a unit, but with not all $g_i(\sigma)$ being divisible by $1 - \sigma$, say with g_h being first such, so that we can drop the first $h - 1$ terms in the product above without loosing the property. Raise the two sides to $(1 - \sigma)^{e_h}$-th power, so that it is now $(1 - \sigma)^{e_h+1}$-th power, so substituting the definitions of $\overline{U_i}$ in terms of

U_i, we get that all the exponents are divisible by p, which is a contradiction as U_h has exponent $F_h(1)g_h(1)$ not divisible by p. This proves the Theorem.

Now we construct U as claimed: First note that given $\eta_1, \cdots, \eta_{r+2} \in \mathcal{O}_K^*$, there are integers a_i not all divisible by p such that $\prod \eta_i^{a_i} = 1$ (Since any $r+1$ units are dependent by the Dirichlet theorem, we have $\prod_1^{r+1} \eta_i^{d_i} = 1$. Taking out common p factors if any, we have $\prod_1^{r+1} \eta_i^{c_i} = \zeta^c$. (Here we make a simplifying assumption $\zeta_{p^2} \notin K$, which is true in our case $K = \mathbf{Q}(\zeta_p)$. Without it, we need an additional easy induction argument). Similarly, $\prod_2^{r+2} \eta_i^{b_i} = \zeta^b$, where without loss of generality p does not divide bc. Then the product of the b-th power of the first combination with $-c$-th power of the second is the combination we want).

Now relative norm of ζ is $\zeta^p = 1$, so by Hilbert 90, $\zeta = E^{1-\sigma}$, where without loss of generality E is a unit. (Otherwise, put $U = \zeta$). Now $(E^p)^{1-\sigma} = 1$, so $E^p =: \epsilon \in \mathcal{O}_K^*$ and clearly $E \notin K$. Note that by definition of E, its relative norm is $E^p = \epsilon$.

For $1 \leq i \leq r+1$, let η_i be the relative norm of $\overline{U_i}$ and let $\eta_{r+2} = \epsilon$. Find the integers a_i as above and put $U := \prod \overline{U_i}^{a_i} E^{a_{r+2}}$, so that its relative norm is 1. If it were a $1-\sigma$-th power, by the definition of the fundamental set, p divides a_i for $1 \leq i \leq r+1$. So we can express the norm of U as $1 = (\prod \eta_i^{a_i/p} E^{a_{r+2}})^p$ implying that the bracketed quantity is ζ^b and hence $E^{a_{r+2}} \in K$. This would give a contradiction $E \in K$, since p does not divide a_{r+2}. Hence U has the property we want and the Theorem and the second proof of Kummer's lemma is complete.

Since the class number is difficult to calculate, Kummer gave an easy *criterion for checking regularity*. He proved (1) If p divides h^+, the class number of $\mathbf{Q}(\zeta)^+$, then p divides $h^- := h/h^+$ and (2) The prime p divides h^- if and only if p divides one of the Bernoulli numbers B_j for some even j between 2 and $p-3$. By (1), this condition holds if and only if p is irregular.

For (1), we will see an algebraic proof in Sujatha's lecture, which is based on the Spiegelgungsatz or the reflection theorem (see also Washington 10.2 or Lang) obtained by comparing the class field theory information with Kummer theory information, giving switch of the parity (sign) of the characters. A proof involving p-adic class number formula and another proof (apparently close to Kummer's original proof) of Kummer's lemma based on similar considerations were presented in the workshop and can be found in Washington 5.6 (pp. 77-81).

For (2), again we have seen an algebraic proof as a corollary to Stickelbeger-Herbrand theorem in Katre's lectures. Another way is to note that the units of K and K^+ being closely related, the regulators are essentially the same

so taking the ratio of analytic class number formulas for K and K^+, we get a formula for h^- in terms of special values of L-functions, which are Bernoulii numbers, as explained in Raghunathan's lectures. Thus we get $h^- = 2p\prod_{\chi \text{ odd}}(-B_{1,\chi}/2)$ which is congruent to $\prod(-B_j/2j)$ modulo p, where j runs through even integers between 2 and $p-3$. For details, see Washington Theorem 4.17.

We end by making some *miscellaneous comments*: For $n = 2$, we had a *parametric solution*, in fact. This is possible, since the corresponding curve is of genus zero. Since for $n > 2$, the equation represents a curve of *genus* $(n-1)(n-2)/2 > 0$, the parametric solutions are impossible. Hard part is to show that not a single non-trivial solution is possible.

More than 10 years before Wiles, Faltings proved *Mordell conjecture* that non-singular curves of genus more than one over a number field can have only finitely many solutions in a number field. This proves that for each $n > 3$, the Fermat equation with the exponent n can have only finitely many solutions up to scaling (as we have to dehomogenize), but in any number field. So in some respects, it is a stronger result.

In fact, even before Faltings proved this, Arizona undergraduate Filaseta noticed that as an easy consequence of Mordell conjecture, given any n, there is M_n such that Fermat equation for exponent nk with $k > M_n$ has no non-trivial integral solutions (Exercise: Note that a solution for exponent nk gives a solution for exponent n). This, coupled with careful counting, led Heath-Brown and Granville to conclude from Faltings result that for almost all (i.e., density 1) exponents n, FLT has no non-trivial integral solutions.

My colleague Bill McCallum has given another proof of the second case of Fermat for regular primes p, by using geometric and p-adic techniques (so-called Coleman-Chabauty method), which seem to have more potential. Interestingly, the techniques only imply existence of at most $p-3$ primitive solutions in the first case, the case which is supposed to be easier.

The *abc conjecture* states that given $\epsilon > 0$, there is $C_\epsilon > 0$, such that for any non-zero relatively prime integers a, b, c with $a + b = c$, we have $\max(|a|, |b|, |c|) \leq C_\epsilon(\prod_{p|abc} p)^{1+\epsilon}$. This is believed because of analogies with function fields (See Lang's Algebra) and is stronger than Mordell conjecture (this implication was proved by Elkies). It is easy to see that it implies FLT for large enough n.

Fermat's false proof?: It is well-known that Fermat wrote in the margin that he had a 'truly marvelous' proof, but in public only repeated weaker claims. So most probably he quickly found a mistake in his original false argument. Can it be the following infinite descent method attempt (the method that he was so fond of and used successfully for $n = 4$)?

Consider $a^n + b^n = c^n$, where $n \geq 3$ odd and $c \neq 0$ is even. Set $x + y = a^n$, $x - y = b^n$. Then $(x^2 - y^2)/(4x^2) = (ab/c^2)^n =: (z/x)^n$ and we get $x(x^n - 4z^n) = x^{n+1} - 4xz^n = x^{n-1}y^2$, which is a square.

Let d be a GCD of x and z, let $x' = x/d$, $z' = z/d$, so that $d^{n+1}x'(x'^n - 4z'^n)$ and so $x'(x'^n - 4z'^n)$ are squares. The last two factors are coprime, so $x' = p^2$, $x'^n - 4z'^n = q^2$ and now $p^{2n} - q^2 = (p^n + q)(p^n - q) = 4z'^n$.

The GCD of p^n+q and p^n-q is 2. Therefore $p^n+q = 2r^n$ and $p^n-q = 2s^n$, so that $p^n = r^n + s^n$ is another solution!

It seems we can apply descent (or even ascent, thanks to Faltings), but the problem is that the 'new' solution is one we started with!

This argument, attributed to Lexell, appears in Euler, Opera Postuma Math. et Physica (1862), vol. 1, 231-232.

Acknowledgements: I thank Andrew Granville for faxing me a copy of this argument from Euler dug out by Bombieri. I thank Pavlos Tzermias for carefully going through the manuscript. We have borrowed from many books which discuss Fermat for regular primes, e.g., those by Washington, Edwards, Lang, Landau, Hilbert, Borevich-Shafarevich, Ribenboim. See also Rosen's article in 'Modular forms and Fermat's last theorem' volume.

Dinesh Thakur
Department of Mathematics
University of Arizona
Tucson, AZ 85721
USA
e-mail: thakur@math.arizona.edu