Diophantine equations are polynomial equations with integer coefficients, where one typically looks for solutions in the integers or rational numbers. One of the problems with studying such equations is that analytic techniques are not directly applicable: for example, if we are just looking for the existence of real solutions then we might be able to use the intermediate value theorem but the fact that the field of rational numbers is not complete precludes this line of attack.

Analysis can, on the other hand, give another idea by looking at an analogy between $\mathbb{Q}$ and the field $\mathbb{C}(x)$ of rational functions with complex coefficients. Any function in $\mathbb{C}(x)$ defines a meromorphic function on the complex plane so, from complex analysis, is determined by its “local behaviour” – that is, from its Laurent series expansion $\sum_{n \geq n_0} a_n (x-z_0)^n$ in a neighbourhood of any $z_0 \in \mathbb{C}$. Now $(x-z_0)$ generates a maximal ideal in the polynomial ring $\mathbb{C}[x]$ and, by truncation, the coefficients in the Laurent series expansion are describing the behaviour of the function “modulo $(x-z_0)^n$”.

The analogue of this for the rational numbers is to take a maximal ideal in $\mathbb{Z}$, which is generated by a prime number $p$, and to look modulo powers of $p$. Thus the idea of the local-global principle in number theory is to try to derive implications on (the existence of) solutions to a diophantine equation from (the existence of) solutions modulo $p^n$, for each prime $p$ and positive integer $n$. One might also ask whether one can have an analogue of a Laurent series expansion and, if so, where this would live – the answer being a suitable completion of $\mathbb{Q}$.

In these lectures we will first look at the local-global principle in number theory first at the level of congruences (if a diophantine equation has solutions modulo $n$ for all $n$ then does it have an integral/rational solution), then introduce the $p$-adic numbers as a way of understanding the local behaviour “at a prime number $p$”, and finally look at some examples of the success/failure of the local-global principle in number theory.

**Recommended literature**


Exercises

How to use these exercises. Some of the exercises are elementary, aimed at those for whom the basic material was new – if it was all familiar to you, then you should skip these. Some of the exercises are filling in proofs omitted from the lectures – again, if you have seen these before, or if you are happy that you could complete the proof if you took the time, then you should skip these. The rest of the questions are the interesting ones. There is one that is really quite hard (question 10(ii)) and I would also omit this one and keep it for later when you have more time – it is there so that you can use it in the following question.

1. (i) Find a primitive root \((\mod p)\), for each odd prime \(p \leq 11\).
   (ii) Find a primitive root \((\mod p^2)\), for each odd prime \(p \leq 11\).
   (iii) Find all quadratic residues \((\mod p)\), for each odd prime \(p \leq 11\).
   (iv) Prove that \(X^2 + 2Y^2 - 5Z^2\) has no solutions in \(\mathbb{Z}\).

2. The purpose of this exercise is to prove Proposition 1.1(i) and (iii).
   (i) Let \(F\) be a field and let \(G \subseteq F^\times\) be a multiplicative subgroup of order \(n\).
      (a) Let \(f(X) \in F[X]\). Prove that \(f\) has at most \(\deg(f)\) distinct roots in \(F\).
      (b) Prove that \(X^n - 1\) has exactly \(n\) distinct roots in \(F\) and deduce that, for any divisor \(d\) of \(n\), the polynomial \(X^d - 1\) has exactly \(d\) distinct roots in \(F\).
      (c) Let \(p\) be a prime and suppose \(p^d \mid n\) and \(p^{d+1} \nmid n\). Prove that \(G\) contains an element of order \(p^d\).
      (d) Use the prime factorization of \(n\) and the previous part to prove that \(G\) contains an element of order \(n\).
   (ii) Deduce that \((\mathbb{Z}/p\mathbb{Z})^\times\) is cyclic.
   (iii) Imitating the proof of Proposition 1.1(ii), prove that \((\mathbb{Z}/2^f\mathbb{Z})^\times = \langle -1 \rangle \times \langle 5 \rangle \simeq C_2 \times C_{2^{f-2}}\).

3. Imitate the proofs of Corollary 1.3(i) to give two proofs of: for odd \(a \in \mathbb{Z}\) and \(t \geq 3\),
   \[x^2 \equiv a \pmod{2^t}\] is soluble \(\iff a \equiv 1 \pmod{8}\).

4. (i) Prove that \((X^2 - 5)(X^2 - 29)(X^2 - 145)\) has a root \((\mod n)\) for all \(n \in \mathbb{N}\), but none in \(\mathbb{Z}\).
   (ii) Let \(p, q\) be odd primes and set \(f(X) = (X^2 - p)(X^2 - q)(X^2 - pq)\). Find the best sufficient conditions you can so that \(f\) has a root \((\mod n)\) for every \(n \in \mathbb{N}\) but no root in \(\mathbb{Z}\).

5. (i) For each prime \(p \leq 11\), determine whether \(p\) is a square \((\mod 1009)\) and/or \((\mod 1001)\).
   (ii) Prove that, for \(p > 3\) prime,
      \[\left( \frac{-3}{p} \right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{3}, \\ -1 & \text{if } p \equiv 2 \pmod{3}. \end{cases}\]
   (iii) Find similar formulae for \(\left( \frac{2}{p} \right), \left( \frac{3}{p} \right), \left( \frac{-5}{p} \right), \ldots\).

6. (i) Let \(p \equiv 2 \pmod{3}\) be a prime. Prove that every element of \((\mathbb{Z}/p\mathbb{Z})^\times\) is a cube. What changes if \(p \equiv 1 \pmod{3}\)?
   (ii) Let \(b \in \mathbb{Z}\) and \(r \geq 2\) an integer. Let \(p \neq 3\) be a prime number such that \(p \nmid b\).
      (a) Prove that \(x^3 \equiv b \pmod{p^r}\) is soluble if and only if \(x^3 \equiv b \pmod{p}\) is soluble.
      (b) Prove that, if \(3 \nmid b\), then \(x^3 \equiv b \pmod{3^r}\) is soluble if and only if \(b \equiv \pm 1 \pmod{9}\).
7. (i) Let \( q, p_1, \ldots, p_r \) be distinct odd prime numbers. Prove that there is a prime number \( \ell \) such that

\[
\ell \equiv 1 \pmod{8}, \quad \left( \frac{q}{\ell} \right) = -1, \quad \text{and} \quad \left( \frac{p_i}{\ell} \right) = 1, \quad \text{for} \ i = 1, \ldots, r.
\]

[You should assume Dirichlet’s Theorem on primes in arithmetic progression: if \( a, n \) are coprime natural numbers then there are infinitely many primes \( \ell \) such that \( \ell \equiv a \pmod{n} \).]

(ii) Let \( n \) be an integer. Use 7(i) to prove that \( n \) is a quadratic residue modulo \( \ell \) for all but finitely many primes \( \ell \), if and only if \( n \) is a perfect square.

8. (i) Let \( f \) be a monic quadratic polynomial with integer coefficients. Prove that: \( f \mod n \) has a root for all natural numbers \( n \), if and only if \( f \) has a root in \( \mathbb{Z} \).

(ii) What changes in 8(i) if we do not require \( f \) to be monic?

9. Let \( b \in \mathbb{Z} \) and put \( f(X) = (X^2 + 3)(X^3 - b) \). Find a sufficient condition on \( b \) so that \( f \mod n \) has a root, for all natural numbers \( n \), but \( f \) has no root in \( \mathbb{Q} \). Give some examples of values for \( b \) satisfying the condition.

[You will need to use questions 5(ii) and 6 for this question.]

10. (i) Prove that the polynomial \( f(X) = X^4 + 1 \) is irreducible in \( \mathbb{Z}[X] \) but that \( f \mod p \) is reducible for all primes \( p \).

(ii)* Prove the following:

Let \( f \in \mathbb{Z}[X] \) be a monic irreducible polynomial. Then there is a prime \( p \) such that \( f \mod p \) has no roots.

This is hard and requires both Galois Theory and Algebraic Number Theory. You should omit it for now but a good account of the required background is given in some notes by Hendrik Lenstra: websites.math.leidenuniv.nl/algebra/Lenstra-Chebotarev.pdf.

11. Read the statement of question 10(ii) and assume it has been proved.

(i) Show that, if \( f \in \mathbb{Z}[X] \) is a monic polynomial and \( \deg(f) \leq 4 \) then, \( f \mod n \) has a root for all natural numbers \( n \) if and only if \( f \) has a root in \( \mathbb{Z} \).

(ii) What changes in 11(i) if we do not require \( f \) to be monic?
12. (i) Pick some rational numbers $q_1, \ldots, q_n$ and, for each one, compute its $p$-adic valuation for each prime $p \leq 11$.
(ii) Prove that $|xy|_p = |x|_p|y|_p$, for $x, y \in \mathbb{Q}$.
(iii) Let $x, y_1, \ldots, y_r \in \mathbb{Q}$ such that $|x|_p > \max\{|y_1|_p, \ldots, |y_r|_p\}$. Prove that $x+y_1+\cdots+y_r \neq 0$.

13. (i) Let $p$ be a prime number and $a$ a positive integer. Show that $a|a|_p \geq 1$. When is there equality?
(ii) Let $q$ be a non-zero rational number. Show that $|q|_\infty \prod_p |q|_p = 1$, where $|q|_\infty$ is the usual absolute value.

14. The purpose of this question is to sketch the proof of the existence of the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ with respect to $|\cdot|_p$. I suggest you read the question but then don’t actually write down the proof.

(i) Prove that $\mathcal{R} = \{\text{Cauchy sequences } (x_n) \text{ w.r.t. } \| \cdot \|_p \text{ in } \mathbb{Q} \}$, with coordinate-wise addition and multiplication, is a ring.
(ii) For $(x_n) \in \mathcal{R}$, explain why $\lim_{n \to \infty} |x_n|_p$ exists. Define $\| \cdot \|_p : \mathcal{R} \to \mathbb{R}_{\geq 0}$ by

$$\|(x_n)\|_p = \lim_{n \to \infty} |x_n|_p$$

and show that $\|(x_n)(y_n)\|_p = \|(x_n)\|_p\|(y_n)\|_p$ and $\|(x_n) + (y_n)\|_p \leq \max\{\|(x_n)\|_p,\|(y_n)\|_p\}$, for all $(x_n), (y_n) \in \mathcal{R}$.
(iii) Prove that $\mathcal{N} = \{(x_n) \in \mathcal{R} : \|(x_n)\|_p = 0\}$ is an ideal of $\mathcal{R}$ and, moreover, that it is the unique maximal ideal of $\mathcal{R}$ and every element of $\mathcal{R} \setminus \mathcal{N}$ is a unit.
(iv) Deduce that $\mathbb{Q}_p := \mathcal{R}/\mathcal{N}$ is a field, that $\| \cdot \|_p$ induces a nonarchimedean valuation on $\mathbb{Q}_p$, and that the canonical map $\mathbb{Q} \hookrightarrow \mathcal{R}$ mapping $x \in \mathbb{Q}$ to the constant sequence $(x)$ induces an injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.
(v) Finally, perform the long and complicated checks to show that $\mathbb{Q}_p$ is complete and that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

15. (i) Prove that $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is a subring of $\mathbb{Q}_p$ and that every ideal of $\mathbb{Z}_p$ is of the form $p^n\mathbb{Z}_p$, for some $n \geq 0$.
(ii) Prove that the natural map $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ induces an isomorphism $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$.

16. (i) Prove Hensel’s Lemma.
(ii) Deduce from Hensel’s Lemma the following special case: Suppose $f(X) \in \mathbb{Z}_p[X]$ and suppose its reduction $f \pmod{p}$ has a simple root $\alpha$; then $\alpha$ can be lifted uniquely to a root of $f$ in $\mathbb{Z}_p$ – that is, $f$ has a unique root $a \in \mathbb{Z}_p$ such that $a \pmod{p} = \alpha$.

17. Let $p$ be a prime and $n$ a natural number such that $p \nmid n$.

(i) Use Hensel’s Lemma to prove that every root of $X^n - 1 \pmod{p}$ can be lifted uniquely to a root of $X^n - 1$ in $\mathbb{Q}_p$.
(ii) Prove that the group of roots of unity of order coprime to $p$ in $\mathbb{Q}_p$ is cyclic of order $p - 1$.
(iii) Determine the full group of roots of unity in $\mathbb{Q}_p$. 

18. Let \( n \) be a natural number and \( q \in \mathbb{Q} \). Prove that \( q \) is an \( n \)th power in \( \mathbb{Q} \) if and only if it is an \( n \)th power in \( \mathbb{Q}_p \) for all primes \( p \).

19. Describe the group \( \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^3 \) in the same way that we described \( \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \) in lectures.

20. In this question, we show that the equation \( X^2 - 68Y^4 + 1 = 0 \) does not satisfy the local-global principle.

(i) Use finite field arguments, Hensel’s lemma etc. to show that there is a solution in \( \mathbb{R} \) and in each \( \mathbb{Q}_p \).

(ii) Show that there exist solutions \( x, y \in \mathbb{Q} \) if and only if there are integers \( r, s, t \), not all zero, such that

\[
\begin{align*}
s^2 + 4t^4 &= 17r^4, \quad \gcd(r, t) = 1. \\
\end{align*}
\]

\(*\)

(iii) Now suppose we have a solution to \( (*) \). Show that \( \alpha \beta = 17\gamma^2 \), where

\[
\alpha = 17r^2 + 8t^2 + s, \quad \beta = 17r^2 + 8t^2 - s, \quad \gamma = 4r^2 + 2t^2.
\]

Show also that \( \gcd(\alpha, \beta) \) divides 2 so we have one of

(a) \( (\alpha, \beta, \gamma) = (17u^2, v^2, uv) \) or \( (v^2, 17y^2, uv) \),

(b) \( (\alpha, \beta, \gamma) = (34u^2, 2v^2, 2uv) \) or \( (2v^2, 34u^2, 2uv) \),

where \( u, v \) are coprime integers. By eliminating \( s \) and looking modulo 8, derive a contradiction.