MA3H1
Topics in Number Theory

Samir Siksek

Samir Siksek, Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: samir.siksek@gmail.com

Contents

Do you subscribe to the illustrious Warwick tradition of setting the same exam every year? I am not going to answer that question, except to point out that this is only the second time the module is being offered, so there's no way for you to guess what I'm going to do, and you'll just have to work hard for the exam.

The exam is tomorrow/next week/within six months. I'm running around like a headless chicken and stressing all my friends because I can't do a homework question. Can I knock on your door and ask you about it? Don't worry, I've already branched out into agony-aunting. Yes come and ask, and I promise not to set the dogs on you.

IS THIS IT? I've spent two whole quid from my beer money on your notes and they're only 70 odd pages. Do you call that value for money? I'm gutted to see you upset. I was just about to offer you your two pounds back but I've had a better idea. I'll go through many sleepless nights to write more notes and make them available via `mathstuff`. Do you forgive me now?

After this year is over, I'm going to devote my life to drunkeness and antisocial behaviour. This year however is my last year in mathematics and I want to enjoy it to the full. Can you pleeeeeease set us lots of homework? *We must be careful.* If I give you too much homework then you'll suffer severe withdrawl symptoms once the term is over, and there's no telling what you might do to yourself. I simply can't have that on my conscience. I'll therefore limit the homework to one sheet per week. It cuts me deep to be so hard on you, but sometimes you have to be tough to be kind.

CHAPTER -1

FAQ

Why is this FAQ upside down? This is to increase the probability that you will notice it and read it, but you should already know this if you took Vectors and Matrices with me.

I have/haven't done MA246 Number Theory. Am I allowed to take this module? Yes. This module has nothing to do with MA246 Number Theory.

How is this module related to Algebra II? In my humble opinion, this module should have been a prerequiste to Algebra II. On the other hand, Algebra II is not needed to follow this module.

I got massacred in second year algebra. Is it total suicide for me to take your module? No. This module relies on common sense, not algebra.

How is this course assessed? 15% for a yet undetermined number of homework assignments and 85% for the final exam.

Are past exam papers available? This course has been offered only once before. Last year's paper is at the end of these notes.

Can we have solutions to last year's paper? I want you to answer last year's paper on your own; it will be good practice. However, if you email me two weeks before the final exam solemnly swearing that you have done the paper and only want to check your answers I'll be happy to oblige you.

Are we required to know the proofs taken during the lectures or found in the lecture notes? Yes, theorems, definitions, proofs and homework questions. I love bookwork.

CHAPTER 0

Prologue

1. What's This?

These are my lecture notes for MA3H1 Topics in Number Theory, with the usual Siksek trademarks. Thanks go to Jenny Cooley, Samantha Pilgram and Vandita (Ditz) Patel for corrections. Please send comments, misprints and corrections to samir.siksek@gmail.com.

2. The Queen of Mathematics

Gauss wrote that "mathematics is the queen of sciences and number theory is the queen of mathematics". In this module we hope to cover some fascinating but fairly elementary aspects of the subject, to ensure **maximal enjoyment with minimal prerequisites**. Topics covered should include:

(1) A review of the number theory you met in the first year Foundations module (primes, unique factorisation, greatest common divisors, modular arithmetic, Chinese Remainder Theorem).
(2) Structure of $\mathbb{Z}/m\mathbb{Z}$ and U_m.
(3) p-adic numbers.
(4) Geometry of Numbers.
(5) Diophantine equations.
(6) The Hasse Principle for ternary quadratic forms.
(7) Counterexamples to the Hasse Principle.
(8) Irrationality and transcendence.

CHAPTER 1

Review

You've spent the last two or three years thinking about rings, topological spaces, manifolds, and so on. This chapter reminds you of the heros of your mathematical childhood: the integers. We review some of their properties which you have seen before, but perhaps not for a long time.

1. Divisibility

Definition. Let a, b be integers. We say that a *divides* b and write $a \mid b$ if there exists an integer c such that $b = ac$.

The following lemma gives easy properties of divisibility; all have one-line proofs from the definition.

Lemma 1.1. *(***Easy Properties of Divisibility***) For all integers a, b, c and k:*

(1) $a \mid 0$;
(2) *if* $a \mid b$ *then* $a \mid kb$;
(3) *if* $a \mid b$ *and* $a \mid c$ *then* $a \mid (b \pm c)$;
(4) *if* $a \mid b$ *and* $b \mid c$ *then* $a \mid c$;
(5) *if* $a \mid b$ *and* $b \mid a$ *then* $a = \pm b$.
(6) *if* $a \mid b$ *and* $b \neq 0$ *then* $|a| \leq |b|$;
(7) $(\pm 1) \mid a$ *for all integers* a;
(8) *if* $a \mid (\pm 1)$ *then* $a = \pm 1$.

Example 1.1. Show that $42 \mid (7^n - 7)$ for all positive integers n.
Answer. This is easy to do using congruences (have a go). But let us try to do it from the definition of divisibility using induction on n. It is obvious for $n = 1$. Suppose it is true for $n = k$. That is, suppose that $42 \mid (7^k - 7)$. In other words, $7^k - 7 = 42c$ for some integer c. Then

$$7^{k+1} - 7^2 = 7 \times 42c$$

so

$$7^{k+1} - 7 = 7 \times 42c + 42 = 42(7c + 1).$$

As c is an integer, $7c + 1$ is an integer, so $42 \mid (7^{k+1} - 7)$.

Theorem 1.2. *(Division with remainder) Let a, b be integers with b positive. Then there are* **unique** *integers q, r satisfying $a = qb + r$ and $0 \leq r \leq b - 1$.*

Here q is called the *quotient* and r the *remainder* on dividing a by b. The uniqueness is certainly needed to say '**the** quotient' and '**the** remainder'.

PROOF. Let us prove uniqueness first. Suppose that

$$a = qb + r, \qquad a = q'b + r'$$

where q, q', r, r' are integers and $0 \leq r$, $r' \leq b - 1$. Without loss of generality, we can suppose that $r < r'$. Subtracting we see that

$$(q - q')b + r - r' = 0$$

so

$$(q - q')b = r' - r.$$

Hence $0 \leq r' - r \leq b - 1$ and $r' - r$ is a multiple of b. Therefore $r' - r = 0$, so $r = r'$ and $q = q'$. This proves uniqueness.

Let us now prove the existence of q and r. Suppose first that $a \geq 0$. In Foundations you have done this case using the well-ordering principle. Keep b fixed and let a be the least non-negative counterexample to the statement of the theorem. If $0 \leq a \leq b - 1$ then we can take $q = 0$ and $r = a$. So $a \geq b$. Now let $a_1 = a - b$. Then $0 \leq a_1 < a$. Hence $a_1 = q_1 b + r_1$ where q_1 and r_1 are integers and $0 \leq r_1 \leq b - 1$. Now just let $q = q_1 + 1$ and $r = r_1$, and so $a = qb + r$.

The proof is complete for $a \geq 0$. What about for $a < 0$? □

2. Ideals

Definition. An *ideal* in $\mathbb{Z}$ is a subset I satisfying the following three properties:

(i) $0 \in I$,
(ii) if a, $b \in I$ then $a + b \in I$,
(iii) if $a \in I$ and $r \in \mathbb{Z}$ then $ra \in I$.

The *principal ideal* of $\mathbb{Z}$ generated by a is the subset

$$(a) = a\mathbb{Z} = \{ka \quad | \quad k \in \mathbb{Z}\}.$$

In other words, (a) is the set of multiples of a.

It is very easy to check that every principal ideal is an ideal [1].

[1] If you have done Algebra II then you will know that the converse is not true in every ring, but is true for $\mathbb{Z}$.

Proposition 1.3. *Let I be an ideal in $\mathbb{Z}$. Then I is principal. Moreover, there is a unique non-negative integer a such that $I = (a)$.*

PROOF. Let I be an ideal of $\mathbb{Z}$; we want to show that I is principal. If $I = \{0\}$ then $I = (0)$ and we're finished, so suppose $I \neq \{0\}$. Then I must contain a non-zero element. From (iii) in the definition, we know that if $a \in I$ then $-a \in I$. Thus I must have a positive element. Let a be the least positive element of I. Again by (iii) we have that $(a) \subseteq I$. We want to show that $I = (a)$. Suppose otherwise. Then there is some $b \in I \backslash (a)$. By Theorem 1.2 we can write $b = qa + r$ where $0 \leq r < a$. If $r = 0$ then $b \in (a)$ giving a contradiction. Hence $0 < r < a$. Moreover $r = b - qa \in I$ using (iii) and (ii). This contradicts the fact that a is the smallest positive element of I. Hence $I = (a)$.

Finally we want to show that a is the unique non-negative element satisfying $I = (a)$. Suppose $I = (b)$ with b non-negative. Then $a \mid b$ and $b \mid a$ so $a = \pm b$, and so $a = b$. □

3. Greatest Common Divisors

Theorem 1.4. *Let $a_1, \ldots, a_n$ be a finite set of elements of $\mathbb{Z}$.*

1. *There exists a unique integer d satisfying*
   (i) *d divides a_i for $i = 1, \ldots, n$;*
   (ii) *if c divides a_i for $i = 1, \ldots, n$ then c divides d;*
   (iii) *$d \geq 0$.*
2. *The integer d can be expressed in the form $d = u_1 a_1 + u_2 a_2 + \cdots + u_n a_n$ where $u_1, \ldots, u_n \in \mathbb{Z}$.*

Definition. For $a_1, \ldots, a_n \in \mathbb{Z}$ we define their *greatest common divisor* (or GCD) to be the integer d satisfying properties (i–iii) of Theorem 1.4. Some books and lecturers call this the *highest common factor*. We shall denote the GCD of $a_1, \ldots, a_n$ by $\gcd(a_1, \ldots, a_n)$. Again some books and lecturers used the notation $(a_1, \ldots, a_n)$.

PROOF OF THEOREM 1.4. Let

$$I = \left\{ \sum_{i=1}^{n} x_i a_i \quad : \quad x_1, \ldots, x_n \in \mathbb{Z} \right\}.$$

In other words I is the set of all linear combinations of the a_i with integer coefficients. It is very easy to see that I is an ideal (use the definition of ideal). By Proposition 1.3 we know that $I = (d)$ for some unique non-negative integer d; in other words, every element of I is a multiple of d and d is non-negative. We will prove that d satisfies the statement of Theorem 1.4. It certainly satisfies (iii) and moreover since

it is an element of I and I is the set of integral linear combinations of the a_i, it satisfies 2.

Clearly $a_1, \ldots, a_n \in I$ so the a_i are multiples of d. This proves (i). Let us prove (ii). Suppose c divides all the a_i. Thus $a_i = k_i c$ for integers k_i for $i = 1, \ldots, n$. Moreover as $d \in I$,

$$d = u_1 a_1 + \cdots + u_n a_n,$$

with $u_i \in \mathbb{Z}$. So

$$d = (u_1 k_1 + \cdots + u_n k_n)c.$$

Hence $c \mid d$. This proves (ii) and completes the proof of Theorem 1.4. □

4. Euler's Lemma

The fact that the gcd can expressed as a linear combination is used again and again. For example, in the proof of the following crucial lemma.

Lemma 1.5. *(Euler's Lemma) If* $u \mid vw$ *and* $\gcd(u, v) = 1$ *then* $u \mid w$.

Proof. Since $\gcd(u, v) = 1$ we can, using Theorem 1.4, write $1 = au + bv$ for some a, $b \in \mathbb{Z}$. Multiply by w to obtain $w = auw + bvw$. Now since $u \mid vw$ we can write $vw = cu$ for some $c \in \mathbb{Z}$, hence $w = auw + bvw = (aw + bc)u$, so $u \mid w$ as required. □

5. The Euclidean Algorithm

Lemma 1.6. *If* $a = qb + r$ *then* $\gcd(a, b) = \gcd(b, r)$.

Proof. Note that for any integer c

$$c \mid a \text{ and } c \mid b \iff c \mid b \text{ and } c \mid r.$$

Hence $\gcd(a, b) \mid \gcd(b, r)$ and $\gcd(b, r) \mid \gcd(a, b)$, and so $\gcd(a, b) = \pm \gcd(b, r)$. As both are non-negative, they must be equal. □

Lemma 1.6 is the basis for the Euclidean Algorithm for computing the GCD, which you did in Foundations. Here is an example.

Example 5.1. To find the greatest common divisor of 1890 and 909 using the Euclidean Algorithm you would write

$$\begin{aligned} 1890 &= 2 \times 909 + 72, \\ 909 &= 12 \times 72 + 45, \\ 72 &= 1 \times 45 + 27, \\ 45 &= 1 \times 27 + 18, \\ 27 &= 1 \times 18 + 9, \\ 18 &= 2 \times 9 + 0, \end{aligned}$$

therefore

$$\begin{aligned} \gcd(1890, 909) &= \gcd(909, 72) = \gcd(72, 45) = \gcd(45, 27) \\ &= \gcd(27, 18) = \gcd(18, 9) = \gcd(9, 0) = 9. \end{aligned}$$

You also know, or should know, how to use the above to express the GCD, in this case 9, as a linear combination of 1890 and 909:

$$\begin{aligned} 9 &= 27 - 18 \\ &= 27 - (45 - 27) = -45 + 2 \times 27 \\ &= -45 + 2(72 - 45) = 2 \times 72 - 3 \times 45 \\ &= 2 \times 72 - 3(909 - 12 \times 72) = -3 \times 909 + 38 \times 72 \\ &= -3 \times 909 + 38(1890 - 2 \times 909) = 38 \times 1890 - 79 \times 909. \end{aligned}$$

6. Primes and Irreducibles

Definition. An integer $p > 1$ is a *prime* if it satisfies the property: for all integers a, b, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

An integer $p > 1$ is *irreducible* if its only factors are ± 1 and $\pm p$.

Of course, you will immediately say that primes and irreducibles are the same thing, which is true but we have to prove it. If you think the proof should be trivial, put these notes down and try it yourself.

Theorem 1.7. *(irreducibles and primes are the same) $p > 1$ is irreducible if and only if it is prime.*

Proof. Let $p > 1$ be a prime. We want to show that p is irreducible; i.e. that the only factors of p are ± 1 and $\pm p$. Suppose $a \in \mathbb{Z}$ is a factor of p. Then we can write $p = ab$ where $b \in \mathbb{Z}$. Then $p \mid ab$. Since p is a prime, by definition, we have $p \mid a$ or $p \mid b$. Let's look at these possibilities separately:

(a) Suppose first that $p \mid a$. Then $a \mid p$ and $p \mid a$ so $a = \pm p$.
(b) Suppose that $p \mid b$. Then $b = pc$ for some $c \in \mathbb{Z}$. Hence $p = ab = apc$, so $ac = 1$ and so $a = \pm 1$.

In other words, the only factors of p are ± 1 and $\pm p$, so p is irreducible.

Now we have to do the converse direction. Let $p > 1$ be irreducible. We want to show that p is prime. So suppose that $p \mid ab$ and we want to show that $p \mid a$ or $p \mid b$. Let $d = \gcd(a, p)$. Then $d \mid p$. As p is irreducible, $d = \pm 1$ or $d = \pm p$, but GCDs are non-negative, so $d = 1$ or $d = p$. If $d = p$ then $p \mid a$ (as $d = p$ is the GCD of a and p). Suppose $d = 1$; i.e. $\gcd(a, p) = 1$. Using $p \mid ab$ and Euler's Lemma (Lemma 1.5) we obtain that $p \mid b$. Hence either $p \mid a$ or $p \mid b$, and so p must be prime. □

From now on we will not mention the word irreducible again, as irreducibles are the same as primes. But what is vital is to know that the two definitions are equivalent. A positive integer $m > 1$ which is not a prime is called a *composite*. Note that $m > 1$ is a composite iff we can write $m = ab$ with $1 < a, b < m$.

You'll have no trouble seeing why the following lemma is true.

Lemma 1.8. *If $p \mid a_1 \dots a_n$ where p is a prime then $p \mid a_i$ for some $i = 1, \dots, n$.*

Theorem 1.9. *(The Fundamental Theorem of Arithmetic) Every positive integer n can be written as a product of prime numbers, this factorisation into primes is unique up to the order of the factors.*

Proof. Let us prove the existence of factorisation into primes first and then the uniquenss. The proof is by induction. Note that $n = 1$ is regarded as the 'empty' product of primes. If n is a prime then there is nothing to prove. Suppose that $n > 1$ is composite. Then we can write $n = ab$ with $1 < a, b < n$. By the inductive hypothesis, a, b can be written as products of primes and so $n = ab$ is a product of primes. This proves the existence.

Now let us prove the uniqueness. Again we do this by induction. This is clear for $n = 1$. Suppose $n > 1$ and uniquness is established for $m < n$. Suppose

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

where the p_i and the q_j are primes. We want to show that $r = s$ and the p_i and q_j are the same up to ordering. Now $p_r \mid q_1 \cdots q_s$ and so $p_r \mid q_j$ for some j. By reordering the qs we may assume that $p_r \mid q_s$ and so $p_r = q_s$. Cancelling we obtain

$$p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}.$$

By the inductive hypothesis, $r - 1 = s - 1$ and $q_1, \cdots, q_{s-1}$ are a rearrangement of $p_1, \cdots, p_{r-1}$. Hence $r = s$ and $q_1, \cdots, q_s$ is a rearrangement of $p_1, \cdots, p_r$. □

You should have no trouble remembering the following theorem or its proof from Foundations.

Theorem 1.10. (Euclid) *There are infinitely many primes.*

PROOF. Suppose that there are finitely many and let them be $p_1, \ldots, p_n$. Let $N = p_1 p_2 \cdots p_n + 1$. Then $N \geq 2$ and so by the Fundamental Theorem of Arithmetic must have a prime divisor. This must be one of $p_1, \ldots, p_n$; say it's p_i. Then $p_i \mid N$ and $p_i \mid p_1 p_1 \cdots p_n$. Hence p_i divides $N - p_1 p_1 \cdots p_n = 1$ giving a contradiction. □

This proof is a model for many other proofs. For example, we'll show later that there are infinitely many primes $p \equiv 1 \pmod 4$, $p \equiv 3 \pmod 4$, $p \equiv 1 \pmod 3$ etc.

7. Coprimality

Definition. We say that integers $m_1, m_2, \ldots, m_n$ are *coprime* if

$$\gcd(m_1, m_2, \ldots, m_n) = 1.$$

We say that integers $m_1, \ldots, m_n$ are *pairwise coprime* if $\gcd(m_i, m_j) = 1$ whenever $i \neq j$.

Lemma 1.11. *Let $m_1, \ldots, m_n$ be pairwise coprime integers and suppose $m_i \mid x$ for all i. Then $M \mid x$ where $M = \prod m_i$.*

PROOF. Let us prove it for $n = 2$. The general case then follows by induction. So $m_1 \mid x$ and $m_2 \mid x$ where $\gcd(m_1, m_2) = 1$. We can write $x = km_1$ for some integer k. So $m_2 \mid km_1$ and by Euler's Lemma (Lemma 1.5) we have that $m_2 \mid k$. So $k = cm_2$ for some integer c. Hence $x = km_1 = cm_1 m_2 = cM$, which gives the desired $M \mid x$.

□

8. ord_p

Let p be a prime, and let n be a non-zero integer. We define $\mathrm{ord}_p(n)$ by the property

$$e = \mathrm{ord}_p(n) \text{ if and only if } p^e \mid n \text{ and } p^{e+1} \nmid n.$$

In a sense, $\mathrm{ord}_p(n)$ measures how divisible n is by powers of p. We define $\mathrm{ord}_p(0) = \infty$.

Example 8.1. If $n = 2^3 \times 3^2 \times 7$, then $\mathrm{ord}_2(n) = 3$, $\mathrm{ord}_3(n) = 2$, $\mathrm{ord}_7(n) = 1$ and $\mathrm{ord}_p(n) = 0$ for all primes $p \neq 2, 3, 7$.

We extend ord_p to a function $\mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ by defining

$$\mathrm{ord}_p\left(\frac{a}{b}\right) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$$

for any non-zero integers a, b.

Exercise 8.2. Check that ord_p is well-defined on $\mathbb{Q}^*$. In other words, if a, b, c, d are integers and $a/b = c/d$ then $\mathrm{ord}_p(a/b) = \mathrm{ord}_p(c/d)$.

Theorem 1.12. *(Another formulation of the Fundamental Theorem of Arithmetic) Every non-zero rational number α can be expressed uniquely in the form*

$$\alpha = \pm \prod_{p \in \mathbb{P}} p^{\mathrm{ord}_p(\alpha)}$$

where $\mathbb{P}$ is the set of all primes.

Note the following obvious corollary.

Corollary 1.13. *Let α, β be non-zero rationals.*

(i) *$\alpha = \pm\beta$ if and only if $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta)$ for all primes p.*
(ii) *$\alpha = \pm 1$ if and only if $\mathrm{ord}_p(\alpha) = 0$ for all primes p.*
(iii) *α is a square of some other rational if and only if $\mathrm{ord}_p(\alpha)$ is even for all primes p.*

The following is the fundamental theorem about ord_p.

Theorem 1.14. *(Properties of ord_p) Let p be a prime, and α, β rational numbers. Then,*

(1) $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$.
(2) $\mathrm{ord}_p(\alpha+\beta) \geq \min\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\}$ *with equality if* $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$.

Before proving Theorem 1.14 we need the following observation whose proof is an easy exercise.

Lemma 1.15. *Any non-zero rational α can be written as*

$$\alpha = p^{\mathrm{ord}_p(\alpha)} \frac{a}{b}$$

where a, b are integers and $p \nmid a$, b.

Proof of Theorem 1.14. Part (1) is obvious from Lemma 1.15. Let's prove part (2). Write

$$\alpha = p^u \frac{a}{b}, \qquad \beta = p^v \frac{c}{d}$$

where p does not divide a, b, c, d. Here $u = \mathrm{ord}_p(\alpha)$ and $v = \mathrm{ord}_p(\beta)$. Without loss of generality, we suppose that $u \leq v$. Then

$$\alpha + \beta = p^u \left(\frac{a}{b} + p^{v-u} \frac{c}{d} \right) = p^u \frac{ad + p^{v-u}bc}{bd}.$$

Note that $p \nmid bd$. However, we don't know if the integer $ad + p^{v-u}bc$ is divisible by p, so let's write $ad + p^{v-u}bc = p^w e$, where $p \nmid e$ and $w \geq 0$, and write $f = bd$. Hence

$$\alpha + \beta = p^{u+w} \frac{e}{f}$$

and so

$$\mathrm{ord}_p(\alpha + \beta) = u + w \geq u = \min(u, v) = \min(\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)).$$

To complete the proof, suppose that $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$, or in other words, $u \neq v$. Since we are assuming $u \leq v$ we have $u < v$ and so $v - u > 0$. Now if $p \mid (ad + p^{v-u}bc)$ then $p \mid ad$ which contradicts $p \nmid a$, d. Hence $p \nmid (ad + p^{v-u}bc)$ which says that $w = 0$. We obtain the desired equality

$$\mathrm{ord}_p(\alpha + \beta) = u + w = u = \min(u, v) = \min(\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)).$$

□

9. Congruences

We are still revising the material you have met in the first year Foundations module.

Definition. Let a, b and m be integers with m positive. We say a is congruent to b modulo m and write $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$.

Lemma 1.16. *Congruence modulo a fixed positive integer m is an equivalence relation:*

- **Reflexive:** *$a \equiv a \pmod{m}$ for all integers a;*
- **Symmetric:** *if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$;*
- **Transitive:** *if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.*

The equivalence classes are represented by $0, 1, \ldots, m-1$. In other words, every integer is congruent to precisely one of $0, 1, \ldots, m-1$ modulo m.

Lemma 1.17. (a) *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.*

(b) *If $a \equiv b \pmod{m}$ and $d \mid m$ then $a \equiv b \pmod{d}$.*

(c) *If* $a \equiv b \pmod{m}$ *then* $na \equiv nb \pmod{nm}$.
(d) *If* $ac \equiv bc \pmod{m}$ *then* $a \equiv b \pmod{m'}$ *where* $m' = \frac{m}{\gcd(c,m)}$. *In particular, if* $\gcd(c, m) = 1$ *and* $ac \equiv bc \pmod{m}$ *then* $a \equiv b \pmod{m}$.

PROOF. Parts (a), (b), (c) are easy consequences of the definition and the properties of divisibility. Let us prove (d), so suppose $ac \equiv bc \pmod{m}$. Suppose first that $\gcd(c, m) = 1$ which is easier. Then $m \mid c(a-b)$ and so by Euler's Lemma (Lemma 1.5), $m \mid (a-b)$ which gives $a \equiv b \pmod{m}$.

Now let's do the general case. Let $d = \gcd(c, m)$ and let $c' = c/d$ and $m' = m/d$. Observe that $\gcd(c', m') = 1$. From $ac \equiv bc \pmod{m}$, we know that $m \mid (ac - bc)$ which means

$$(a-b)c = km$$

for some integer k. Dividing both sides by d we obtain

$$(a-b)c' = km'$$

and so $m' \mid (a-b)c'$. As $\gcd(c', m') = 1$, Euler's Lemma tells us that $m' \mid (a-b)$. Hence $a \equiv b \pmod{m'}$ as required. □

Example 9.1. You should be very careful with cancellation where congruences are involved. For example, $100 \equiv 60 \pmod{8}$, but $10 \not\equiv 6 \pmod{8}$. However, using part (d) of the above lemma to cancel the factor of 10, we get $10 \equiv 6 \pmod{8/\gcd(8, 10)}$ which means $10 \equiv 6 \pmod{4}$ and this is true.

9.1. Inverses modulo m.

Lemma 1.18. *Suppose that* a, m *are integers with* $m \geq 1$. *Then there exists an integer* b *such that* $ab \equiv 1 \pmod{m}$ *if and only if* $\gcd(a, m) = 1$.

PROOF. Suppose $\gcd(a, m) = 1$. We know from Euclid's algorithm that there are integers b, c such that $ab + cm = 1$. Reducing modulo m we obtain $ab \equiv 1 \pmod{m}$ as required.

To prove the converse, suppose $ab \equiv 1 \pmod{m}$. Thus $ab - 1 = km$ for some integer k. Write $g = \gcd(a, m)$. Now $g \mid a$ and $g \mid m$, so $g \mid ab$ and $g \mid km$. Hence $g \mid (ab - km) = 1$. Thus $\gcd(a, m) = g = 1$ completing the proof. □

You should pay special attention to the above proof as it gives us a practical way of inverting elements modulo m; see the following example.

Example 9.2. Let us find the inverse of 502 modulo 2001. One way of doing this is to try all the numbers $b = 0, 1, \cdots, 2000$ and see which one satisfies $502b \equiv 1 \pmod{2001}$. Using Euclid's algorithm is much faster!

$$\begin{aligned} 2001 &= 3 \times 502 + 495, \\ 502 &= 1 \times 495 + 7, \\ 495 &= 70 \times 7 + 5, \\ 7 &= 1 \times 5 + 2, \\ 5 &= 2 \times 2 + 1. \end{aligned}$$

Therefore $\gcd(502, 2001) = 1$. Moreover,

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2(7 - 5) = -2 \times 7 + 3 \times 5 \\ &= -2 \times 7 + 3(495 - 70 \times 7) = 3 \times 495 - 212 \times 7 \\ &= 3 \times 495 - 212(502 - 495) = -212 \times 502 + 215 \times 495 \\ &= -212 \times 502 + 215(2001 - 3 \times 502) = 215 \times 2001 - 857 \times 502. \end{aligned}$$

Reducing $215 \times 2001 - 857 \times 502 = 1$ modulo 2001 we obtain $-857 \times 502 \equiv 1 \pmod{2001}$, so the inverse of 502 is $-857 \equiv 2001 - 857 \equiv 1144 \pmod{2001}$.

9.2. Complete Residue Systems. A *complete residue system modulo* m is a set of m integers $\{a_1, a_2, \ldots, a_m\}$ such that $a_i \not\equiv a_j \pmod{m}$ whenever $i \neq j$.

Example 9.3. The set $\{0, 1, 2, 4\}$ isn't a complete residue system modulo 5, since it has too few elements. The set $\{0, 1, 2, 3, 6\}$ also isn't a complete residue system since $6 \equiv 1 \pmod{5}$. However, $\{0, 1, 2, 3, 4\}$ is a complete residue system modulo 5 and so is $\{2, 3, 4, 5, 6\}$ and so is $\{0, 6, -3, 13, 24\}$.

Lemma 1.19. (a) *Let $\{a_1, \ldots, a_m\}$ be a complete residue system modulo m, then every integer is congruent to precisely one a_i modulo m.*

(b) *Let $\{a_1, \ldots, a_m\}$ and $\{b_1, \ldots, b_m\}$ be complete residue systems modulo m. Then, after reordering the b_i if necessary, $a_i \equiv b_i \pmod{m}$ for all i.*

PROOF. Let c_i be the unique integer in $\{0, 1, \ldots, m-1\}$ satisfying $c_i \equiv a_i \pmod{m}$. Since $a_i \not\equiv a_j \pmod{m}$ whenever $i \neq j$, we have $c_i \not\equiv c_j \pmod{m}$ and so $c_i \neq c_j$. Hence $c_1, c_2, \ldots, c_m$ are m distinct elements of the set $\{0, 1, \ldots, m-1\}$, which itself has precisely m distinct

elements. Hence $c_1, c_2, \ldots, c_m$ is a rearrangment of $\{0, 1, \ldots, m-1\}$. This quickly proves parts (a) and (b). □

9.3. Reduced Residue Systems.

Definition. We define *Euler's φ-function* as follows. Let $m \geq 1$. Let $\varphi(m)$ be the number of integers a in the set $\{0, 1, \ldots, m-1\}$ satisfying $\gcd(a, m) = 1$. If you like symbols,

$$\varphi(m) = \#\{a \mid 0 \leq a \leq m-1 \text{ and } \gcd(a, m) = 1\}.$$

Example 9.4. You'll have no trouble seeing, for example, that $\varphi(5) = 4$ and $\varphi(24) = 8$.

Definition. A *reduced residue system modulo m* is a set $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ of $\varphi(m)$ elements such that $\gcd(a_i, m) = 1$ for all i and $a_i \not\equiv a_j \pmod{m}$ whenever $i \neq j$.

Example 9.5. $\{1, 3, 5, 7\}$ is a reduced residue system modulo 8, and so is $\{7, 5, 9, -5\}$. However $\{2, 3, 5, 7\}$ isn't, nor is $\{1, 3, 5\}$ nor is $\{1, 3, 5, 13\}$.

There are no prizes for guessing what comes next.

Lemma 1.20. (a) *Let $\{a_1, \ldots, a_{\varphi(m)}\}$ be a reduced residue system modulo m, then every integer a satisfying $\gcd(a, m) = 1$ is congruent to precisely one a_i modulo m.*

(b) *Let $\{a_1, \ldots, a_{\varphi(m)}\}$ and $\{b_1, \ldots, b_{\varphi(m)}\}$ be reduced residue systems modulo m. Then, after reordering the b_i if necessary, $a_i \equiv b_i \pmod{m}$ for all i.*

The proof is left as an exercise. You have to follow the same steps as in the proof of Lemma 1.19, but you'll need the following lemma, whose proof is also an exercise.

Lemma 1.21. *If $a \equiv b \pmod{m}$ then $\gcd(a, m) = \gcd(b, m)$.*

Lemma 1.22. *If $\{a_1, \ldots, a_{\varphi(m)}\}$ is a reduced residue system modulo m, and $\gcd(c, m) = 1$ then $\{ca_1, ca_2, \ldots, ca_{\varphi(m)}\}$ is also a reduced residue system modulo m.*

Proof. Note that the set $\{ca_1, ca_2, \ldots, ca_{\varphi(m)}\}$ has precisely $\varphi(m)$ elements and that all are coprime to m. Suppose $i \neq j$. We want to show that $ca_i \not\equiv ca_j \pmod{m}$, so suppose that $ca_i \equiv ca_j \pmod{m}$. Since $\gcd(c, m) = 1$ we obtain that $a_i \equiv a_j \pmod{m}$ by part (d) of Lemma 1.17; this contradicts the fact that $\{a_1, \ldots, a_{\varphi(m)}\}$ is a reduced residue system modulo m. □

9.4. The Theorems of Fermat and Euler.

Theorem 1.23. (Euler's Theorem) *If* $\gcd(c, m) = 1$ *then* $c^{\varphi(m)} \equiv 1 \pmod{m}$.

PROOF. Suppose first that $\{a_1, \ldots, a_{\varphi(m)}\}$ and $\{b_1, \ldots, b_{\varphi(m)}\}$ are reduced residue systems modulo m. By part (b) of Lemma 1.20 we have

$$\prod_{i=1}^{\varphi(m)} a_i \equiv \prod_{i=1}^{\varphi(m)} b_i \pmod{m}.$$

Now let $\{a_1, \ldots, a_{\varphi(m)}\}$ be any reduced residue system and observe that $\{ca_1, ca_2, \ldots, ca_{\varphi(m)}\}$ is also a reduced residue system by Lemma 1.22. Hence

$$\prod_{i=1}^{\varphi(m)} a_i \equiv \prod_{i=1}^{\varphi(m)} ca_i \pmod{m}.$$

We may rewrite this as $A \equiv c^{\varphi(m)} A \pmod{m}$ where $A = \prod a_i$. Clearly $\gcd(A, m) = 1$, and by part (d) of Lemma 1.17 we obtain $c^{\varphi(m)} \equiv 1 \pmod{m}$. □

Corollary 1.24. (Fermat's Little Theorem)

(i) *If* p *is a prime and* $p \nmid a$ *then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

(ii) *If* p *is a prime and* a *is any integer then*

$$a^p \equiv a \pmod{p}.$$

PROOF. Let p be a prime. Note that the only integer in the set $\{0, 1, \ldots, p-1\}$ that is not coprime with p is 0. Hence, by definition of φ, we have $\varphi(p) = p - 1$. Now (i) follows from Euler's Theorem. Let us prove (ii). If $p \nmid a$ then (ii) follows from (i) on multiplying both sides by a. If $p \mid a$ then (ii) is obvious since both sides are congruent to 0 modulo p. □

10. The Chinese Remainder Theorem

Theorem 1.25. (The Chinese Remainder Theorem) *Let* $a_1, \ldots, a_n$ *and* $m_1, \ldots, m_n$ *be integers with* m_i *positive and* $\gcd(m_i, m_j) = 1$ *whenever* $i \neq j$. *Write* $M = \prod m_i$. *Then there exists a unique integer* x *such that* $x \equiv a_i \pmod{m_i}$ *for* $i = 1, 2, \ldots, n$ *and* $0 \leq x \leq M - 1$. *Moreover, if* x' *also satisfies* $x' \equiv a_i \pmod{m_i}$ *then* $x' \equiv x \pmod{M}$.

For the proof we need a the following lemma.

Lemma 1.26. *With notation as in the Chinese Remainder Theorem, there exists integers $u_1, u_2, \ldots, u_n$ such that*

$$u_i \equiv \begin{cases} 1 \pmod{m_i} \\ 0 \pmod{m_j} \quad \textit{whenever } j \neq i. \end{cases} \tag{1}$$

PROOF. Let us prove this for u_1. Put $M_1 = \prod_{j \neq 1} m_j$. Then $\gcd(m_1, M_1) = 1$ and by Euclid's Algorithm there are integers r_1 and s_1 such that $r_1 m_1 + s_1 M_1 = 1$. Let $u_1 = s_1 M_1$. Clearly u_1 satisfies (1). □

Now the proof of the Chinese Remainder Theorem is easy.

PROOF OF THE CHINESE REMAINDER THEOREM. Let the u_i be as in Lemma 1.26. Write

$$y = a_1 u_1 + a_2 u_2 + \cdots + a_n u_n.$$

From (1) we see that $y \equiv a_i \pmod{m_i}$. Now let x satisfy $0 \leq x \leq M-1$ and $x \equiv y \pmod{M}$. Clearly $x \equiv y \pmod{m_i}$ for all i and so $x \equiv a_i \pmod{m_i}$ for all i. The uniqueness of x follows from the second part of the Chinese Remainder Theorem that we're about to prove.

Suppose also that $x' \equiv a_i \pmod{m_i}$ for all i. Then $m_i \mid (x' - x)$ for all i. By Lemma 1.11, as the m_i are coprime, $M \mid (x' - x)$ where $M = \prod m_i$. □

You should pay particular attention to the proof of the Chinese Remainder Theorem. It's constructive; this means that it gives us a practical method of solving a system of simultaneous congruences. Once again it is the Euclidean Algorithm that does the work, and so you must make sure that you know how to use it to express the gcd as a linear combination. See the following example.

Example 10.1. Solve the simultaneous congruences

$$x \equiv 3 \pmod{4}, \qquad x \equiv 5 \pmod{7}.$$

Answer: Using Euclid's Algorithm you will see that

$$2 \times 4 - 1 \times 7 = 1.$$

Let $u_1 = -1 \times 7 = -7$ and $u_2 = 2 \times 4 = 8$. Note that

$$u_1 \equiv \begin{cases} 1 \pmod{4}, \\ 0 \pmod{7}, \end{cases} \qquad u_2 \equiv \begin{cases} 0 \pmod{4}, \\ 1 \pmod{7}. \end{cases}$$

Now let $y = 3 \times u_1 + 5 \times u_2 = -21 + 40 = 19$. Then the solutions to the simultaneous congruences are precisely those values of x such that $x \equiv 19 \pmod{28}$.

CHAPTER 2

Multiplicative Structure Modulo m

1. Euler's φ Revisited

With the help of the Chinese Remainder Theorem we will derive a convenient formula for φ. For this we have to revisit reduced residue systems.

Lemma 2.1. *If* $\gcd(m_1, m_2) = 1$ *then* $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.

PROOF. For a positive integer m define

$$U(m) = \{a \mid 0 \leq a \leq m-1 \text{ and } \gcd(a, m) = 1\}.$$

Note that $\varphi(m) = \#U(m)$. Now let m_1, m_2 be coprime and write $M = m_1 m_2$. We will shortly define a bijection

$$f : U(m_1) \times U(m_2) \to U(M).$$

You know if two finite sets are related by a bijection then they have the same number of elements. Assuming the existence of the bijection f we obtain

$$\begin{aligned}\varphi(m_1 m_2) = \varphi(M) = \#U(M) &= \#\left(U(m_1) \times U(m_2)\right) \\ &= \#U(m_1) \times \#U(m_2) = \varphi(m_1)\varphi(m_2).\end{aligned}$$

So to complete the proof all we have to do is to define f and show that it's a bijection. Now let $a_i \in U(m_i)$ for $i = 1, 2$. Let $f(a_1, a_2)$ be the unique x satisfying $0 \leq x \leq M-1$ and $x \equiv a_i \pmod{m_i}$ whose existence is guaranteed by the Chinese Remainder Theorem. For the map f to be well-defined, we have to show that $\gcd(x, M) = 1$. However, $\gcd(x, m_i) = \gcd(a_i, m_i) = 1$ and as $M = m_1 m_2$ we obtain that $\gcd(x, M) = 1$ as required. Thus $f(a_1, a_2) = x$ is in $U(M)$. Now let us show that f is $1-1$. Suppose that $x = f(a_1, a_2) = f(b_1, b_2)$. Then $x \equiv a_i \pmod{m_i}$ and $x \equiv b_i \pmod{m_i}$ and so $a_i \equiv b_i \pmod{m_i}$. As $0 \leq a_i,\ b_i \leq m_i - 1$, we have $a_i = b_i$ for $i = 1,\ 2$, so that f is $1-1$. Finally let us show that f is onto. Let $c \in U(M)$. Let a_i be the unique integer satisfying $0 \leq a_i \leq m_i - 1$ and $c \equiv a_i \pmod{m_i}$. Then $\gcd(a_i, m_i) = \gcd(c, m_i)$ and this divides $\gcd(c, M) = 1$. Hence $\gcd(a_i, m_i) = 1$ so $a_i \in U(m_i)$. Now $f(a_1, a_2) = x$ is the unique integer

satisfying $x \equiv a_i \pmod{m_i}$ and $0 \leq x \leq m_i - 1$. But c satisfies these properties, so $c = x = f(a_1, a_2)$. This shows that f is onto, and so is a bijection. □

Theorem 2.2. *Let $m \geq 2$ be an integer and let*

$$m = \prod_{i=1}^{n} p_i^{r_i}$$

be its factorisation into prime powers with $r_i \geq 1$. Then

$$\varphi(m) = \prod_{i=1}^{n} p_i^{r_i - 1}(p_i - 1).$$

PROOF. We will prove that if p is a prime and $r \geq 1$ then $\varphi(p^r) = p^{r-1}(p-1)$. The theorem follows from this and Lemma 2.1.

By definition, $\varphi(p^r)$ is the number of integers m in the interval $0 \leq m \leq p^r - 1$ that are coprime with p^r; in otherwords not divisible by p. There are p^r integers in the interval, and the ones divisible by p are

$$0,\ p,\ 2p,\ 3p, \ldots, (p^{r-1} - 1)p.$$

Clearly there are p^{r-1} integers in the interval that are divisible by p, so $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$ as required. □

2. Orders Modulo m

Definition. Let $\gcd(a, m) = 1$. We define the *order of a modulo m* to be the least positive integer d such that $a^d \equiv 1 \pmod{m}$.

Lemma 2.3. *Suppose*

$$a^u \equiv a^v \equiv 1 \pmod{m}.$$

and let $w = \gcd(u, v)$. Then $a^w \equiv 1 \pmod{m}$.

PROOF. By Euclid's Algorithm, there are r, s such that $w = ru + sv$. So that

$$a^w = (a^u)^r (a^v)^s \equiv 1 \pmod{m}.$$

□

Theorem 2.4. *Let $\gcd(a, m) = 1$, and let d be the order of a modulo m.*

(i) *If $a^e \equiv 1 \pmod{m}$ then $d \mid e$.*
(ii) *$d \mid \varphi(m)$. In particular, if $m = p$ is prime then $d \mid (p-1)$.*

PROOF. Let d be the order of a modulo m. Then $a^d \equiv 1 \pmod{m}$ by definition of order. Suppose that $a^e \equiv 1 \pmod{m}$. By Lemma 2.3, $a^{d'} \equiv 1 \pmod{m}$ where $d' = \gcd(d, e)$. Note that $d' \mid d$ and so $d' \leq d$. But by definition of order, d is the least positive integer satisfying $a^d \equiv 1 \pmod{m}$. Hence $d \leq d'$ and so $d = d'$. As $d' \mid e$ we have $d \mid e$. This proves (i).

Part (ii) follows from (i) and Euler's Theorem. □

Lemma 2.5. *Let* $\gcd(g_i, m) = 1$ *for* $i = 1, 2$ *and suppose that* g_i *has order* d_i *modulo* m. *Suppose that* $\gcd(d_1, d_2) = 1$. *Then* $g_1 g_2$ *has order* $d_1 d_2$ *modulo* m.

PROOF. Let d be the order of $g = g_1 g_2$ modulo m. Note that

$$g^{d_1 d_2} = (g_1^{d_1})^{d_2} (g_2^{d_2})^{d_1} \equiv 1 \pmod{m}.$$

Hence by Theorem 2.4, $d \mid d_1 d_2$.

From $g^d \equiv 1 \pmod{m}$ we obtain

$$g_1^d g_2^d \equiv 1 \pmod{m}$$

and raising both sides to d_2 we have that

$$g_1^{dd_2} (g_2^{d_2})^d \equiv 1 \pmod{m}.$$

But $g_2^{d_2} \equiv 1 \pmod{m}$, so $g_1^{dd_2} \equiv 1 \pmod{m}$. By Theorem 2.4, $d_1 \mid dd_2$. Since $\gcd(d_1, d_2) = 1$, Euler's Lemma tells us that $d_1 \mid d$. Likewise $d_2 \mid d$. So $d_1 d_2 \mid d$. As we've already observed that $d \mid d_1 d_2$ we obtain that $d = d_1 d_2$. □

3. Primitive Roots

Lemma 2.6. *Let* p *be a prime and* X *an indeterminate. Then*

$$X^{p-1} - 1 \equiv (X-1)(X-2)\cdots(X-(p-1)) \pmod{p}.$$

PROOF. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$ for $a = 1, 2, \ldots, p-1$. So $X^{p-1} - 1$ must have $a = 1, 2, \cdots, p-1$ as roots modulo p. Thus, modulo p, the polynomial $(X-1)(X-2)\cdots(X-(p-1))$ is a factor of $X^{p-1} - 1$. But both are monic of degree $p-1$, so they must be the same modulo p. □

Lemma 2.7. *Let* p *be a prime. If* $n \mid (p-1)$ *then* $x^n \equiv 1 \pmod{p}$ *has exactly* n *incongruent solutions modulo* p.

PROOF. Let $p - 1 = nd$. Recall the factorization

$$X^{p-1} - 1 = X^{nd} - 1 = (X^n - 1)(X^{n(d-1)} + X^{n(d-2)} + \cdots + 1).$$

By Lemma 2.6, $X^{p-1}-1$ factors completely modulo p and has distinct roots. Since X^n-1 is a factor of $X^{p-1}-1$, it must also factor completely and have distinct roots modulo p. This proves the lemma. □

Definition. A primitive root modulo p is a number g such that $p \nmid g$ and g has order $p-1$.

Theorem 2.8. *If g is a primitive root modulo p then $1, g, g^2, \ldots, g^{p-2}$ is a reduced residue system modulo p. In particular, for every integer $a \not\equiv 0 \pmod{p}$, there is a unique $0 \leq r \leq p-2$ such that $a \equiv g^r \pmod{p}$.*

Proof. The second part follows from the first and the definition of a reduced residue system. Let us prove the first part. Note that every element of $1, g, g^2, \ldots, g^{p-2}$ is coprime to p and the set has $p-1 = \varphi(p)$ elements. All we have to do is to show that no two elements of this set are congruent modulo p. Now suppose $g^r \equiv g^s \pmod{p}$ where $0 \leq r \leq s \leq p-2$. Then $g^{s-r} \equiv 1 \pmod{p}$. By definition of primitive root, g has order $p-1$ and so $(p-1) \mid (s-r)$. This is impossible unless $s = r$. □

Theorem 2.9. *If p is prime, there exists a primitive root modulo p.*

Proof. Want to find an integer g such that $p \nmid g$ and has order $p-1$ modulo p. Let the prime-power factorization of $p-1$ be

$$p - 1 = q_1^{e_1} q_2^{e_2} \ldots q_r^{e_r}.$$

By Lemma 2.7,

- $x^{q_i^{e_i}} \equiv 1 \pmod{p}$ has $q_i^{e_i}$ incongruent solutions modulo p, and
- $x^{q_i^{e_i-1}} \equiv 1 \pmod{p}$ has $q_i^{e_i-1}$ incongruent solutions modulo p.

So there must be some integer g_i with

$$g_i^{q_i^{e_i}} \equiv 1 \pmod{p}, \qquad g_i^{q_i^{e_i-1}} \not\equiv 1 \pmod{p}.$$

Thus g_i has exact order $q_i^{e_i}$ modulo p. Let $g = g_1 g_2 \ldots g_r$. By Lemma 2.5, g has order $p-1$ modulo p, and so g is a primitive root. □

Here is a past exam question.

Example 3.1. Find a primitive root for 149. You may use the following observations:

$$149 = 2^2 \times 37 + 1, \qquad 5^{37} \equiv 44^4 \equiv 1 \pmod{149}, \qquad 44^2 \not\equiv 1 \pmod{149}.$$

Answer. The order of 5 modulo 149 divides 37. But the only positive divisors of 37 are 1 and 37. Moreover, $5^1 \not\equiv 1 \pmod{149}$, so 5 has order 37 modulo 149.

The order of 44 modulo 149 divides 4 and so is 1, 2 or 4. But $44^1 \not\equiv 1 \pmod{149}$, and $44^2 = 1936 \equiv 148 \not\equiv 1 \pmod{149}$. Hence the order of 44 is 4.

Now we use Lemma 2.5. Since $\gcd(37, 4) = 1$, we find that the order of $20 = 5 \times 4$ modulo 149 is $37 \times 4 = 149 - 1$. Hence 20 is a primitive root modulo 149.

CHAPTER 3

Quadratic Reciprocity

1. Quadratic Residues and Non-Residues

Definition. Let $\gcd(a, m) = 1$. We say that a is a quadratic residue modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution. Otherwise we say that a is a quadratic non-residue.

Example 1.1. Note that

$$1^2 \equiv 6^2 \equiv 1, \quad 2^2 \equiv 5^2 \equiv 4, \quad 3^2 \equiv 4^2 \equiv 2 \pmod{7}.$$

Hence the quadratic residues modulo 7 are 1, 2 and 4. The quadratic non-residues modulo 7 are 3, 5 and 6.

Definition. Let p be an odd prime. Let

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \\ 0 & \text{if } p \mid a. \end{cases}$$

The symbol $\left(\frac{a}{p}\right)$ is called a *Legendre symbol*.

The Legendre symbol is extremely convenient for discussing quadratic residues.

Example 1.2. From Example 1.1 we have

$$\left(\frac{0}{7}\right) = 0, \qquad \left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1,$$

and

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

We will focus on quadratic residues modulo primes and return to quadratic residues modulo arbitrary positive integers later.

2. Quadratic Residues and Primitive Roots

Lemma 3.1. *Let p be an odd prime and let g be a primitive root modulo p.*

- *The quadratic residues modulo p are of the form g^r where $0 \leq r \leq p-2$ and r is even.*
- *The quadratic non-residues are of the form g^r where $0 \leq r \leq p-2$ and r is odd.*

In particular, exactly half the non-zero residues are quadratic residues modulo p and the other half are quadratic non-residues.

PROOF. Let g be a primitive root modulo p. Modulo p, the integers $1 \leq a \leq p-1$ are a rearrangement of the integers $1, g, \ldots, g^{p-2}$, since both lists are reduced residue systems. Note that g^r is certainly a quadratic residue modulo p for all even integers r. Let us prove the converse. Suppose that $g^r \equiv x^2 \pmod{p}$. Then we can write $x \equiv g^s \pmod{p}$ for some $0 \leq s \leq p-2$. Thus $g^{r-2s} \equiv 1 \pmod{p}$. As g is a primitive root, $p-1$ divides $r-2s$. But $p-1$ is even so $r-2s$ is even and so r is even. Thus we know that g^r is a quadratic residue modulo p if and only if r is even. Hence the quadratic residues modulo p are $1, g^2, g^4, \ldots, g^{p-3}$ and the quadratic non-residues are $g, g^3, g^5, \ldots, g^{p-2}$. This proves the lemma. □

Before we start proving properties of the Legendre symbol, we need another important fact about primitive roots.

Lemma 3.2. *Let p be an odd prime and g a primitive root modulo p. Then*

$$g^{(p-1)/2} \equiv -1 \pmod{p}.$$

PROOF. Let $h = g^{(p-1)/2}$. Then $h^2 = g^{p-1} \equiv 1 \pmod{p}$. So $p \mid (h^2-1) = (h+1)(h-1)$. Hence $h \equiv \pm 1 \pmod{p}$. If $h \equiv 1 \pmod{p}$ then $g^{(p-1)/2} \equiv 1 \pmod{p}$ contradicting the fact that the order of g (a primitive root) is exactly $p-1$. Hence $h \equiv -1 \pmod{p}$ which is what we want. □

3. First Properties of the Legendre Symbol

Proposition 3.3. *Let p be an odd prime, and a, b integers.*

(i) *If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(ii) **(Euler's Criterion)** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

(iii) *For integers a, b we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

PROOF. (i) follows straightaway from the definition, and (iii) follows from (ii). Let's prove (ii). Let a be an integer. If $p \mid a$ then

$$\left(\frac{a}{p}\right) = 0 \equiv a^{(p-1)/2} \pmod{p}.$$

Hence suppose that $p \nmid a$. Let g be a primitive root modulo p. We know from Lemma 3.1 that $a \equiv g^r \pmod{p}$ for some $0 \leq r \leq p-2$ and that r is even if and only if a is a quadratic residue. Hence

$$a^{(p-1)/2} \equiv \left(g^{(p-1)/2}\right)^r \equiv (-1)^r \pmod{p}$$

by Lemma 3.2. This proves (ii). □

4. The Law of Quadratic Reciprocity

The main theorem on quadratic reciprocity is the Law of Quadratic Reciprocity.

Theorem 3.4. *Let p and q be distinct odd primes. Then*

(a) **(Law of Quadratic Reciprocity)** $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$.

(b) **(First Supplement to the Law of Quadratic Reciprocity)** $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$

(c) **(Second Supplement to the Law of Quadratic Reciprocity)** $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$

Remark. Note that we can rephrase the Law of Quadratic Reciprocity as follows:

$$\begin{cases} \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod 4 \end{cases}$$

Example 4.1. Is 94 a square modulo 257? One way to decide this is to run through the integers $x = 0, 1, \ldots, 256$ and see if $94 \equiv x^2 \pmod{257}$. It is much quicker to use Proposition 3.3 and the Law of

Quadratic Reciprocity.

$$\begin{aligned}
\left(\frac{94}{257}\right) &= \left(\frac{2}{257}\right)\left(\frac{47}{257}\right) && \text{by Proposition 3.3}\\
&= \left(\frac{47}{257}\right) && \text{using the second supplement}\\
&= \left(\frac{257}{47}\right) && \text{since } 257 \equiv 1 \pmod 4\\
&= \left(\frac{22}{47}\right) && 257 \equiv 22 \pmod{47}\\
&= \left(\frac{2}{47}\right)\left(\frac{11}{47}\right)\\
&= \left(\frac{11}{47}\right)\\
&= -\left(\frac{47}{11}\right) && 11 \equiv 47 \equiv 3 \pmod 4\\
&= -\left(\frac{3}{11}\right)\\
&= \left(\frac{11}{3}\right) && 3 \equiv 11 \equiv 3 \pmod 4\\
&= \left(\frac{2}{3}\right) && 11 \equiv 2 \pmod 3\\
&= -1 && \text{using the second supplement.}
\end{aligned}$$

Hence 94 is not a square modulo 47.

Actually the proof of the first supplement is straightforward.

Proof of the First Supplement. By Euler's Criterion (Proposition 3.3),

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p.$$

Thus $\left(\frac{-1}{p}\right) = 1$ if and only if $(p-1)/2$ is even. This is the case if and only if $p \equiv 1 \pmod 4$. □

To prove the Law of Quadratic Reciprocity we need Gauss' Lemma.

Theorem 3.5. (Gauss' Lemma) *Let p be an odd prime and write*

$$S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

For integer n let $\widehat{n}$ be the unique integer satisfying $\widehat{n} \equiv n \pmod{p}$ and $-p/2 < \widehat{n} < p/2$. Let $p \nmid a$ and let

$$\widehat{aS} = \{\widehat{as} : s \in S\}.$$

Define $\mu(a)$ to be the number of **negative** *members of the set $\widehat{aS}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a)}.$$

Example 4.2. Let us determine $\left(\frac{3}{11}\right)$ using Gauss' Lemma. Note that

$$S = \{1, 2, 3, 4, 5\}$$

and

$$\widehat{3S} = \{\widehat{3}, \widehat{6}, \widehat{9}, \widehat{12}, \widehat{15}\} = \{3, -5, -2, 1, 4\}.$$

Thus $\mu(3) = 2$ and so $\left(\frac{3}{11}\right) = 1$.

Proof of Gauss' Lemma. We will show that $(-1)^{\mu(a)} a^{(p-1)/2} \equiv 1 \pmod{p}$. Gauss' Lemma will then follow from Euler's Criterion.

By definition, $\mu(a)$ is the number of negative elements in $\widehat{aS}$. Let $|\widehat{aS}| = \{|\widehat{as}| : s \in S\}$. We **claim** that $|\widehat{aS}| = S$. Let's assume this for the moment and use it to complete the proof. We will return to prove the claim later on. Now

$$\begin{aligned}
\prod_{s\in S} s &= \prod_{t\in|\widehat{aS}|} t && \text{as } S = |\widehat{aS}| \\
&= \prod_{s\in S} |\widehat{as}| && \text{by definition of } |\widehat{aS}| \\
&= (-1)^{\mu(a)} \prod_{s\in S} \widehat{as} && \widehat{as} = -|\widehat{as}| \text{ for precisely } \mu(a) \text{ values of } s \in S \\
&\equiv (-1)^{\mu(a)} \prod_{s\in S} as && \text{since } as \equiv \widehat{as} \pmod{p} \\
&\equiv (-1)^{\mu(a)} a^{(p-1)/2} \prod_{s\in S} s \pmod{p} && \text{since } \#S = (p-1)/2.
\end{aligned}$$

Cancelling $\prod_{s\in S} s$ we obtain the desired conclusion that $(-1)^{\mu(a)} a^{(p-1)/2} \equiv 1 \pmod{p}$.

It remains to prove our claim that $|\widehat{aS}| = S$. Suppose $s \in S$. Then $-p/2 < \widehat{as} < p/2$ so $0 \le |\widehat{as}| < p/2$. But $\widehat{as} \neq 0$ since $p \nmid a$ and $p \nmid s$. Hence $\widehat{as} \in S$. This shows that $|\widehat{aS}| \subseteq S$. To show that the two sets are equal, we must show that the have the same number of elements. Suppose that $s,\ t \in S$ satisfy $|\widehat{as}| = |\widehat{at}|$. Then $as \equiv \pm at \pmod p$ and so $s \equiv \pm t \pmod p$. But $-p/2 < s, \pm t < p/2$, so their difference can't be divisible by p unless it is 0. Thus $s = \pm t$. But $s,\ t \in S$ so $s = t$. This shows that $|\widehat{aS}|$ has as many elements as S, completing the proof. □

Gauss' Lemma enables us to prove the second supplement to the Law of Quadratic Reciprocity.

Proof of the Second Supplement. We want to show that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Consider the case $p \equiv 1 \pmod 8$; the other cases are similar and are left as an exercise. Then $p = 8m + 1$ for some integer m. Here $(p-1)/2 = 4m$. We will apply Gauss' Lemma to determine $\left(\frac{2}{p}\right)$. For this we need to compute $\widehat{2x}$ where $x = 1, 2, \ldots, 4m$. Now for $x = 1, 2, \ldots, 2m$ we have $0 < 2x < p/2$ and so $\widehat{2x} = 2x$ which is positive. However, for $x = 2m+1, 2m+2, \ldots, 4m$ we have $p/2 < 2x < p$ and $\widehat{2x} = 2x - p$ which is negative. Hence $\mu(2) = 2m$, so by Gauss' Lemma

$$\left(\frac{2}{p}\right) = 1.$$

□

Proof of the Law of Quadratic Reciprocity. The original proof is due to Gauss. Gauss altogether gave eight different proofs of LQR, and there are hundreds of published proofs. The proof we give is due to Eisenstein. It starts with the following trigonometric identity which everyone knows. Let m be an odd positive integer and let

$$S_m = \left\{1, 2, 3, \ldots, \frac{m-1}{2}\right\}.$$

Then

$$\frac{\sin mx}{\sin x} = (-4)^{(m-1)/2} \prod_{t \in S_m} \left(\sin^2 x - \sin^2 \frac{2\pi t}{m}\right). \tag{2}$$

Observe that if $u \equiv v \pmod p$ then $2\pi u/p$ and $2\pi v/p$ differ by a multiple of 2π and so $\sin(2\pi u/p) = \sin(2\pi v/p)$. Let $\operatorname{sgn}(u)$ denote the

sign of u so that $u = \operatorname{sgn}(u)|u|$. Then $\sin(2\pi u/p) = \operatorname{sgn}(u)\sin(2\pi|u|/p)$. Now for $s \in S_p$,

$$qs \equiv \widehat{qs} \equiv \operatorname{sgn}(\widehat{qs})|\widehat{qs}| \pmod{p}.$$

Thus

$$\sin\frac{2\pi qs}{p} = \operatorname{sgn}(\widehat{qs})\sin\frac{2\pi|\widehat{qs}|}{p}.$$

In the notation of Gauss' Lemma, exactly $\mu(q)$ of the $\widehat{qs}$ are negative. Hence

$$\left(\frac{q}{p}\right) = \prod_{s\in S_p}\operatorname{sgn}(\widehat{qs}).$$

From the last two equations,

$$\prod_{s\in S_p}\sin\frac{2\pi qs}{p} = \left(\frac{q}{p}\right)\prod_{s\in S_p}\sin\frac{2\pi|\widehat{qs}|}{p}.$$

However, from the proof of Gauss's Lemma, $\{|\widehat{qs}| : s \in S_p\} = \widehat{|qS_p|} = S_p$. Hence

$$\prod_{s\in S_p}\sin\frac{2\pi qs}{p} = \left(\frac{q}{p}\right)\prod_{s\in S_p}\sin\frac{2\pi s}{p},$$

which can be rewritten as

$$\left(\frac{q}{p}\right) = \prod_{s\in S_p}\frac{\sin(2\pi qs/p)}{\sin(2\pi s/p)}.$$

Using the identity (2) with $m = q$ and $x = 2\pi s/p$ we obtain

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{s\in S_p}(-4)^{(q-1)/2}\prod_{t\in S_q}\left(\sin^2(2\pi s/p) - \sin^2(2\pi t/q)\right)\\ &= (-4)^{(p-1)(q-1)/4}\prod_{s\in S_p,t\in S_q}\left(\sin^2(2\pi s/p) - \sin^2(2\pi t/q)\right),\end{aligned}$$

as S_p has $(p-1)/2$ members. Now interchanging p and q we have

$$\left(\frac{p}{q}\right) = (-4)^{(q-1)(p-1)/4}\prod_{s\in S_p,t\in S_q}\left(\sin^2(2\pi t/q) - \sin^2(2\pi s/p)\right).$$

The right-hand sides of the last two equations are identical except for a minus sign for each term in the product. But there are $(\#S_p)(\#S_q) = \dfrac{(p-1)}{2}\dfrac{(q-1)}{2}$ terms in the product. Thus

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}},$$

completing the proof. □

5. The Sheer Pleasure of Quadratic Reciprocity

Did you enjoy the proof of the Law of Quadratic Reciprocity? Or did the flicker of light at the end of the long, dark tunnel not seem worth it? If you're having doubts prepare to dispel them: we're going to exhilarate ourselves with several applications of LQR.

5.1. Mersenne Numbers. You have met the Mersenne numbers $M_n = 2^n - 1$ in the homework, and know that if n is composite then so is M_n. What if $n = q$ is prime; is M_q necessarily prime? Computing the first few we find

$$M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127,$$

which are all prime numbers. Now $M_{11} = 2047$ which is already not entirely trivial to factor by hand. The following theorem gives us a large supply of Mersenne numbers M_q where q is prime but M_q is composite.

Theorem 3.6. *Let $q \equiv 3 \pmod 4$ be a prime such that $p = 2q + 1$ is also prime. Then p divides M_q. In particular, for $q > 3$, M_q is composite.*

Before proving Theorem 3.6 let us apply it with $q = 11$. Note that $q \equiv 3 \pmod 4$ and $p = 2q + 1 = 23$ is prime. Then according to the Theorem 3.6, p divides M_q and indeed we find that $M_{11} = 2047 = 23 \times 89$. You can use the same argument to find a factor of M_q for

$$q = 11, 23, 83, 131, 179, 191, 239, 251, 359, 419, 431, 443, 491, 659, \ldots$$

Proof of Theorem 3.6. Since $q \equiv 3 \pmod 4$, we have that $p = 2q + 1 \equiv 7 \pmod 8$. Hence

$$\left(\frac{2}{p}\right) = 1.$$

But by Euler's Criterion

$$2^q = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) = 1 \pmod p.$$

Hence $M_q = 2^q - 1$ is divisible by p. To prove the last statement in Theorem 3.6, observe that M_q is composite if $M_q > p$. This is the same as $2^q - 1 > 2q + 1$ which is satisfied if $q > 3$. □

5.2. A Diophantine Equation. A Diophantine equation is one where we are interested in integer solutions. It can be very hard to determine all the solutions of a Diophantine equations (e.g. Fermat's Last Theorem). However, quadratic reciprocity can sometimes be used to show that there are no solutions. Here is an example.

Theorem 3.7. *The equation*

$$y^2 = x^3 - 5$$

has no solutions with x, $y \in \mathbb{Z}$.

PROOF. We proceed by contradiction. Suppose that x, $y \in \mathbb{Z}$ satisfy $y^2 = x^3 - 5$. If x is even then $y^2 \equiv -5 \equiv 3 \pmod 8$ which is impossible as the squares modulo 8 are 0, 1 and 4. Thus x is odd. Now rewrite the equation as

$$y^2 + 4 = x^3 - 1 = (x-1)(x^2 + x + 1).$$

Note that $x^2 + x + 1 = \text{odd} + \text{odd} + \text{odd}$ and so is odd. Moreover $x^2 + x + 1$ is positive (e.g. by completing the square). Let p be a prime divisor of $x^2 + x + 1$. Then $p \mid (y^2 + 4)$ and so $y^2 \equiv -4 \pmod p$. Hence

$$\left(\frac{-1}{p}\right) = 1.$$

Thus $p \equiv 1 \pmod 4$. As this is true of all prime divisors of $x^2 + x + 1$ we have

$$x^2 + x + 1 \equiv 1 \pmod 4.$$

If $x \equiv 1 \pmod 4$ then $x^2 + x + 1 \equiv 3 \pmod 4$ giving a contradiction. Hence $x \equiv 3 \pmod 4$. Hence $y^2 \equiv x^3 - 5 \equiv 3 - 5 \equiv 2 \pmod 4$, which is impossible. □

CHAPTER 4

p-adic Numbers

1. Congruences Modulo p^m

In quadratic reciprocity we studied congruences of the form $x^2 \equiv a \pmod{p}$. We now turn our attention to situations where p is replaced by a power of p.

We shall need the following lemma whose proof is an easy exercise, but try out a few examples first to convince yourself that it is true.

Lemma 4.1. *Let $f(X) \in \mathbb{Z}[X]$ and let $n > 0$ be an integer. Then $f^{(n)}(X)/n!$ has integer coefficients.*

Next is Hensel's Lemma which is the main result of this section.

Theorem 4.2. (Hensel's Lemma) *Let $f(X) \in \mathbb{Z}[X]$. Let p be a prime and $m \geq 1$. Suppose $a \in \mathbb{Z}$ satisfies*

$$f(a) \equiv 0 \pmod{p^m}, \qquad f'(a) \not\equiv 0 \pmod{p}.$$

Then there exists some $b \in \mathbb{Z}$ such that

$$b \equiv a \pmod{p^m}, \qquad f(b) \equiv 0 \pmod{p^{m+1}}. \tag{3}$$

We say that we **lift** a to a solution modulo p^{m+1}.

Proof of Hensel's Lemma. By Taylor's Theorem

$$f(a+x) = f(a) + f'(a)x + \frac{f^{(2)}(a)}{2!}x^2 + \cdots + \frac{f^{(n)}(a)}{n!}x^n$$

where n is the degree of f (note that all higher derivatives vanish). We want b to satisfy two conditions, one of them that $b \equiv a \pmod{p^m}$. Let us write $b = a + p^m y$ where the integer y will be determined later. Then

$$f(b) = f(a) + p^m f'(a)y + p^{2m}(\text{integer}).$$

Since $f(a) \equiv 0 \pmod{p^m}$ we have $f(a) = p^m c$ where c is an integer. Thus

$$f(b) = p^m(c + f'(a)y) + p^{2m}(\text{integer}).$$

Note that $p^{m+1} \mid p^{2m}$. To make $f(b) \equiv 0 \pmod{p^{m+1}}$ it is enough to choose y so that $p \mid (c + f'(a)y)$. In otherwords, we want y so that $f'(a)y \equiv -c \pmod{p}$. But $f'(a) \not\equiv 0 \pmod{p}$ and so is invertible

modulo p. Let h satisfy $hf'(a) \equiv 1 \pmod{p}$. Then we choose $y = -hc$ and take $b = a - hcp^m$ and then both congruences in (3) are satisfied. □

The proof of Hensel's Lemma is constructive; this means that it can be used to solve congruences modulo prime powers. You need to practice Hensel's Lemma a few times to get the hang of it. The following example will help show you how.

Example 1.1. Solve the congruence $x^2 \equiv 2 \pmod{7^3}$.
Answer: It is easy to solve $x^2 \equiv 2 \pmod{7}$ by trying all the values modulo 7. We get that $x \equiv 3, 4 \pmod{7}$. Note that obviously if u is a solution then $-u$ is also a solution.

Next we solve $x^2 \equiv 2 \pmod{7^2}$. Note that any solution must also satisfy $x^2 \equiv 2 \pmod{7}$ and so $x \equiv 3, 4 \pmod{7}$. Suppose first that $x \equiv 3 \pmod{7}$. Then $x = 3 + 7y$ where y is an integer. Substituting in $x^2 \equiv 2 \pmod{7^2}$ we obtain

$$9 + 42y + 49y^2 \equiv 2 \pmod{7^2}$$

or equivalently

$$7(1 + 6y) \equiv 0 \pmod{7^2}$$

or equivalently $1 + 6y \equiv 0 \pmod{7}$, so $y \equiv 1 \pmod{7}$, so we obtain that $x = 3 + 7y \equiv 3 + 7 = 10 \pmod{7^2}$. Similarly, if $x \equiv 4 \pmod{7}$ then $x \equiv 39 \pmod{49}$ (which is the same as -10 modulo 49).

Now let us solve $x^2 \equiv 2 \pmod{7^3}$. Then $x \equiv 10, 39 \pmod{7^2}$. Suppose first $x \equiv 10 \pmod{7^2}$. Then $x = 10 + 7^2 z$ for some integer z. Hence

$$100 + 2 \times 10 \times 7^2 z + 7^4 z^2 \equiv 2 \pmod{7^3}.$$

Note $100 - 2 = 98 = 2 \times 7^2$. Thus

$$7^2 \times 2(1 + 10z) \equiv 0 \pmod{7^3}.$$

This is equivalent to $1 + 10z \equiv 0 \pmod{7}$ which gives $z \equiv 2 \pmod{7}$. Hence $x = 10 + 7^2 z = 108 \pmod{7^3}$. Similarly starting from $x \equiv 39 \pmod{7^2}$ would give $x \equiv 235 \pmod{7^3}$.

In the above example, we note that to obtain a solution modulo 7^2 we had to add $7y = 1 \times 7$ and to obtain a solution modulo 7^3 we had to add a $7^2 z = 2 \times 7^2$. We can continue this calculation and write up our solutions in the following suggestive manner:

m	solutions to $x^2 \equiv 2 \pmod{7^m}$
1	± 3
2	$\pm(3+7)$
3	$\pm(3+7+2\times 7^2)$
4	$\pm(3+7+2\times 7^2+6\times 7^3)$
5	$\pm(3+7+2\times 7^2+6\times 7^3+7^4)$

We are writing solutions as a series in powers of 7 with coefficients between 0 and 6. This suggests very much an analogy with decimal expansions. We immediately begin to wonder if the series converges in any sense. Of course it does not converge in the sense of 1st year analysis as the powers of 7 are tending to infinity. However we will change our notion of large and small to make it converge.

2. p-Adic Absolute Value

Before we define the p-adic absolute value, it is worth recalling ord_p and its properties. Remember that if p is a prime and α is a non-zero rational, then $\operatorname{ord}_p(\alpha)$ is the unique integer such that

$$\alpha = p^{\operatorname{ord}_p(\alpha)} \cdot \frac{a}{b}, \qquad a, b \in \mathbb{Z}, \quad p \nmid a, b.$$

We defined $\operatorname{ord}_p(0) = +\infty$. Recall also that one formulation of the Unique Factorization Theorem says that any non-zero rational α can be written as

$$\alpha = \pm \prod_{p \in \mathbb{P}} p^{\operatorname{ord}_p(\alpha)}, \tag{4}$$

where $\mathbb{P}$ is the set of all primes. Of course only finitely many of the exponents $\operatorname{ord}_p(\alpha)$ are non-zero, so the product makes sense.

Definition. Let p be a prime and α a non-zero rational number. We define the **p-adic absolute value** of α to be

$$|\alpha|_p = p^{-\operatorname{ord}_p(\alpha)}.$$

We define $|0|_p = 0$ which is consistent with our convention that $\operatorname{ord}_p(0) = +\infty$.

Example 2.1. Let $\alpha = -50/27$. Then

$$|\alpha|_p = \begin{cases} 2^{-1} & p = 2 \\ 3^3 & p = 3 \\ 5^{-2} & p = 5 \\ 1 & p \neq 2, 3, 5. \end{cases}$$

Now evaluate $\prod_{p \in \mathbb{P}} |\alpha|_p$. What do you notice.

Example 2.2. Notice that $|p^r|_p = p^{-r}$, so powers of p with positive exponent are actually 'small'. It now looks likely that the series where we seem to be expanding $\sqrt{2}$ as a 'powerseries' in 7 does converge. We will come to that soon, but first we need some properties of the p-adic absolute value.

Theorem 4.3. *Let p be a prime and α, $\beta \in \mathbb{Q}$. Then*

(i) $|\alpha|_p \geq 0$. *Moreover,* $|\alpha|_p = 0$ *iff* $\alpha = 0$.
(ii) $|\alpha\beta|_p = |\alpha|_p|\beta|_p$.
(iii) $|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}$, *with equality if* $|\alpha|_p \neq |\beta|_p$.

Inequality (iii) is called the **ultrametric inequality**. Notice that it implies the triangle inequality $|\alpha + \beta|_p \leq |\alpha|_p + |\beta|_p$ but is actually much stronger.

Proof of Theorem 4.3. We'll leave (i) and (ii) as exercises. Let's do (iii). Recall the following property of ord_p:

$$\mathrm{ord}_p(\alpha + \beta) \geq \min\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\} \tag{5}$$

with equality if $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$. Write

$$r = \mathrm{ord}_p(\alpha), \qquad s = \mathrm{ord}_p(\beta), \qquad t = \mathrm{ord}_p(\alpha + \beta),$$

and suppose that $r \leq s$. Then $t \geq \min(r, s) = r$. Hence

$$|\alpha + \beta|_p = p^{-t} \leq p^{-r} = \max\{p^{-r}, p^{-s}\} = \max\{|\alpha|_p, |\beta|_p\}.$$

Now suppose that $|\alpha|_p \neq |\beta|_p$. Then $p^{-r} \neq p^{-s}$ which means that $r \neq s$. Hence $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$ and we have equality in (5). Hence $t = r$ and so

$$|\alpha + \beta|_p = p^{-t} = p^{-r} = \max\{p^{-r}, p^{-s}\} = \max\{|\alpha|_p, |\beta|_p\}.$$

□

Example 2.3. The triangle inequality is true for the p-adic absolute value, so everything you proved previously for the ordinary absolute value using the triangle inequality also holds for the p-adic absolute value. But the ultrametric inequality is much stronger. Notice the following striking consequence of the ultrametric inequality. Let C be a constant and p a prime. Consider the set

$$\{\alpha \in \mathbb{Q} : |\alpha|_p \leq C\}.$$

This is a 'disc centred at the origin'. However, the ultrametric inequality tells us that if we add two elements in this 'disc', we stay inside it. Compare this with what happens if you add two elements of the disc in the complex plane

$$\{\alpha \in \mathbb{C} : |\alpha| \leq C\}.$$

Here it is easy to add two elements in the disc so that you leave the disc. The triangle inequality for the usual absolute value will tell you that if $|\alpha| \leq C$ and $|\beta| \leq C$ then $|\alpha + \beta| \leq 2C$, so you can see that the ultrametric inequality is much stronger than the triangle inequality.

Theorem 4.4. *(The Product Formula) Let α be a non-zero rational number. Then*

$$|\alpha| \prod_{p \in \mathbb{P}} |\alpha|_p = 1,$$

where $\mathbb{P}$ is the set of primes.

PROOF. Prove this using (4). Notice that all but finitely many terms in the product are 1, so the product makes sense. □

3. Convergence

Definition. We say that the series of rational numbers $\{a_n\}_{n=1}^{\infty}$ **converges p-adically** to $a \in \mathbb{Q}$ if

$$\lim_{n \to \infty} |a_n - a|_p = 0.$$

We can also express this in terms of epsilons: the series $\{a_n\}_{n=1}^{\infty}$ converges to $a \in \mathbb{Q}$ if for every $\epsilon > 0$, there is some N such that for all $n \geq N$, we have $|a_n - a|_p < \epsilon$. A series $\sum_{j=1}^{\infty} a_j$ converges p-adically if the sequence of partial sums $s_n = \sum_{j=1}^{n} a_j$ converges p-adically.

Example 3.1. Let $a \in \mathbb{Q}$. It is easy to see that the constant sequence $\{a\}_{n=1}^{\infty}$ converges p-adically to a.

Example 3.2. The sequence $\{p^n\}_{n=1}^{\infty}$ converges to 0 p-adically since

$$|p^n - 0|_p = p^{-n} \to 0 \qquad \text{as } n \to \infty.$$

Example 3.3. Consider 5-adically the series

$$1 + 5 + 5^2 + 5^3 + \cdots .$$

The n-th partial sum is

$$s_n = 1 + 5 + \cdots + 5^{n-1} = \frac{5^n - 1}{5 - 1} = \frac{5^n}{4} - \frac{1}{4}.$$

As $5^n \to 0$, it seems that the sequence of partial sums is converging to $-1/4$. Let's check this:

$$|s_n - (-1/4)|_5 = |5^n/4|_5 = 5^{-n} \to 0 \qquad \text{as } n \to \infty.$$

Hence $\{s_n\}_{n=1}^{\infty}$ converges 5-adically to $-1/4$ and we can write

$$1 + 5 + 5^2 + \cdots = \frac{-1}{4}.$$

Example 3.4. Now consider 7-adically the same series

$$1 + 5 + 5^2 + 5^3 + \cdots .$$

Now the partial sums are exactly the same as before, and find that

$$|s_n - (-1/4)|_7 = |5^n/4|_7 = 1 \to 1 \qquad \text{as } n \to \infty.$$

This shows that the series does not 7-adically converge to $-1/4$. Does it converge to something else, or not converge at all? We'll answer this question shortly.

Definition. A sequence $\{a_n\}_{n=1}^{\infty}$ of rational numbers is **p-adically null** if it p-adically converges to 0. A sequence $\{a_n\}_{n=1}^{\infty}$ of rational numbers is **p-adically Cauchy** if

$$\lim_{m,n\to\infty} |a_m - a_n|_p = 0.$$

Example 3.5. As we saw previously, the sequences $\{0\}_{n=1}^{\infty}$ and $\{p^n\}_{n=1}^{\infty}$ converge p-adically to 0 and so are both null.

The following lemma will give us lots of examples of Cauchy sequences.

Lemma 4.5. *If the sequence of rational numbers $\{a_n\}_{n=1}^{\infty}$ converges p-adically then it is p-adically Cauchy.*

PROOF. Suppose $\{a_n\}$ converges p-adically to $a \in \mathbb{Q}$. Then $\lim_{n\to\infty}|a_n - a|_p = 0$. Now

$$|a_m - a_n|_p = |(a_m - a) - (a_n - a)|_p \leq \max\{|a_m - a|_p, |a_n - a|_p\}$$

using the ultrametric inequality. Hence

$$|a_m - a_n|_p \to 0 \qquad \text{as } m, n \to \infty,$$

which is what we wanted to prove. Notice that the proof is almost the same as the proof you saw in first-year analysis with the usual absolute value. The only difference is that the triangle inequality is replaced by the ultrametric inequality. □

What about the converse of Lemma 4.5. Does every p-adically Cauchy sequence of rationals converge to a rational number? If you recall our earlier example where we were solving $x^2 \equiv 2 \pmod{7^n}$, we seemed to be constructing a 7-adically Cauchy sequence that converges to $\sqrt{2}$ which is not rational. So it seems that the converse of Lemma 4.5 does not hold unless we replace the rationals by something bigger. We know that with the usual absolute value a sequence is Cauchy if and

only if it converges; but here we are talking about real numbers, not just rational numbers. For example, you know that the sequence

$$a_n = \left(1 + \frac{1}{n}\right)^n$$

is a Cauchy sequence of rational numbers that converges to e which is not rational but real. But what is a real number? The best way to define real numbers is to say that a real number is simply a Cauchy sequence of rational numbers! Think about it. This motivates our next definition.

Definition. A p-adic number α is a p-adically Cauchy sequence $\{a_n\}_{n=1}^{\infty}$ of rational numbers. We write $\mathbb{Q}_p$ for the set of p-adic numbers. We identify $\mathbb{Q}$ as a subset of $\mathbb{Q}_p$ via the map

$$\mathbb{Q} \to \mathbb{Q}_p, \qquad a \mapsto \{a\}_{n=1}^{\infty}. \tag{6}$$

Let's go back to the reals for a moment to make sure that our definition makes sense. We said that a real number is simply a Cauchy sequence of rationals. So e is just the sequence $(1 + 1/n)^n$. But there are other sequences converging to e. For example, take the partial sums of the series

$$1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots .$$

So to say that a real number is a Cauchy sequence seems an ambiguous way to define real numbers. However, the ambiguity disappears as soon as we adopt the convention that two Cauchy sequences define the same real number if their difference is a null sequence. We do the same in the p-adic setting.

Definition. We say that two p-adic numbers $\{a_n\}$ and $\{b_n\}$ are **equal** if the difference $\{a_n - b_n\}$ is p-adically null.

Example 3.6. Via the identification (6) we think of $0 \in \mathbb{Q}$ to be the same as the zero sequence $\{0\}$ in $\mathbb{Q}_p$. Now the $\{p^n\}$ and $\{0\}$ are both p-adically null sequences and we have that

$$0 = \{0\} = \{p^n\} = \text{any null sequence of rationl numbers.}$$

Lemma 4.6. *Suppose that the sequence of rational numbers $\{a_n\}$ converges p-adically to $a \in \mathbb{Q}$. Then in $\mathbb{Q}_p$*

$$\lim_{n\to\infty} a_n = a = \{a_n\}_{n=1}^{\infty}.$$

Proof. What is the lemma saying? There is no doubt that $\lim_{n\to\infty} a_n = a$. Now $a \in \mathbb{Q}$ and via the identification (6) we can write $a = \{a\}_{n=1}^{\infty}$. So what we're asked to prove that the sequences $\{a_n\}_{n=1}^{\infty}$ and $\{a\}_{n=1}^{\infty}$

are the same in $\mathbb{Q}_p$. In other words, they differ by a p-adically null sequence. But this true: $\lim_{n\to\infty}|a_n - a|_p = 0$ as $\{a_n\}_{n=1}^{\infty}$ converges to a p-adically. This completes the proof. □

Lemma 4.6 gives a hint of how to define limits of p-adically Cauchy sequences that don't seem to have a rational limit.

Definition. Suppose that $\{a_n\}_{n=1}^{\infty}$ is a p-adically Cauchy sequence of rational numbers. We define the **limit**

$$\lim_{n\to\infty} a_n = \{a_n\}_{n=1}^{\infty}.$$

There is **no** misprint in this definition! A p-adically Cauchy sequence converges to a p-adic number that happens to be the sequence itself. This solves the convergence problem and, by Lemma 4.6, is consistent with the case where the sequence does converge to a rational number.

It might be said that this is a cowardly way of solving the issue of p-adically Cauchy sequences for which there is no rational limits. But mathematics is full of such cowardice. For example, to square-root 2 we introduce the symbol $\sqrt{2}$ and work with it. Everytime we square this symbol we replace it with 2. This does not tell us what the square-root of 2 is, but is a convenient psychological way of avoiding answering the question. Likewise, the only difficulties with accepting the above definition are purely psychological, and at any rate, it is rather late in the term to drop MA3H1 and take up something else.

4. Operations on $\mathbb{Q}_p$

Of course $\mathbb{Q}_p$ would not be very interesting if it was a set with no additional structure. In fact we can define addition and multiplication on $\mathbb{Q}_p$ in a natural way:

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}$$

and

$$\{a_n\} \cdot \{b_n\} = \{a_n b_n\}.$$

One must check that these operations are well-defined. For a start we want to make sure that the sequences $\{a_n + b_n\}$ and $\{a_n b_n\}$ are p-adically Cauchy so that we are staying in $\mathbb{Q}_p$. We also want to check that if $\{a_n\}$ and $\{a'_n\}$ differ by a p-adically null sequence and if $\{b_n\}$ and $\{b'_n\}$ differ by a p-adically null sequence then $\{a_n + b_n\}$ and $\{a'_n + b'_n\}$ differ by a p-adically null sequence and $\{a_n b_n\}$ and $\{a'_n b'_n\}$ differ by a p-adically null sequence. These we'll leave as relatively easy exercises. We also want to check that the usual properties of addition

and multiplication hold (commutativity, associativity, distributivity of multiplication over addition); again these are easy exercises.

What about division? Here there is a slight difficulty. We might want to define $\{a_n\}/\{b_n\} = \{a_n/b_n\}$. Of course we will exclude the case when $\{b_n\}$ is p-adically null. But even if $\{b_n\}$ is not null, it might contain some zeros. We might then say, ignore them, after all ignoring finitely many terms in a sequence is not going to affect its limit. But what if $\{b_n\}$ has infinitely many zeros? Well that can't happen and to show that we need a lemma.

Lemma 4.7. *Let $\{a_n\}$ be a sequence of rational numbers that is p-adically Cauchy. Then the sequence $\{|a_n|_p\}$ converges to some element in the set $\{0\} \cup \{p^r : r \in \mathbb{Z}\}$.*

PROOF. Note that the convergence we're talking about in the second sentence of the lemma is covergence with respect to the usual absolute value. Now certainly $|a_n|_p$ is in the set $\{0\} \cup \{p^r : r \in \mathbb{Z}\}$, and it's easy to see that any Cauchy subsequence of $\{0\} \cup \{p^r : r \in \mathbb{Z}\}$ must actually converge to some element of this set. Thus all we have to show is that $\{|a_n|_p\}$ is Cauchy with respect to the usual absolute value. Now it is an easy exercise to check that

$$\big|\, |a|_p - |b|_p \big| \leq |a - b|_p.$$

Hence

$$0 \leq \big|\, |a_m|_p - |a_n|_p \big| \leq |a_m - a_n|_p.$$

As $\{a_n\}$ is p-adically Cauchy, $\lim_{m,n\to\infty} |a_m - a_n|_p = 0$. Hence by the Sandwich Theorem,

$$\lim_{m,n\to\infty} \big|\, |a_m|_p - |a_n|_p \big| = 0.$$

This shows that the sequence $\{|a_n|_p\}$ is Cauchy with respect to the usual absolute value and completes the proof. □

Lemma 4.8. *Let $\{b_n\}$ be a p-adically Cauchy sequence of rational numbers that is non-null. Then the sequence contains at most finitely many zero elements.*

PROOF. By the previous lemma, $|b_n|_p$ has a limit, which is either zero, or a power of p. However, as $\{b_n\}$ is non-null, this limit must be non-zero. Now if the sequence contains infinitely many zeros then $\{|b_n|_p\}$ contains infinitely many zeros and hence a subsequence converging to zero. This contradicts that fact that $\{|b_n|_p\}$ converges to a non-zero limit. □

The above lemma allows us to define division. If $\{a_n\}$ and $\{b_n\}$ are elements of $\mathbb{Q}_p$ and $\{b_n\} \neq 0$ (i.e. non-null) then there is some N such that for $n \geq N$, $b_n \neq 0$ and we define $\{c_n\} = \{a_n\}/\{b_n\}$ by assigning c_n randomly for $n < N$ and letting $c_n = a_n/b_n$ for $n \geq N$. Note that $\{c_n\} \cdot \{b_n\}$ agrees with $\{a_n\}$ except for finitely many terms and so their difference is null; in other words $\{c_n\} \cdot \{b_n\} = \{a_n\}$ in $\mathbb{Q}_p$.

Theorem 4.9. *$\mathbb{Q}_p$ is a field containing $\mathbb{Q}$ as a subfield.*

PROOF. The proof is an easy but slightly lengthy verification which we leave as an exercise. □

We can extend the p-adic absolute value to $\mathbb{Q}_p$ as follows.

Definition. Let $\alpha \in \mathbb{Q}_p$ be represented by the p-adically Cauchy sequence of rationals $\{a_n\}$. We define the p-adic absolute value of α by

$$|\alpha|_p = \lim_{n\to\infty} |a_n|_p.$$

Note that the limit exists by Lemma 4.7 and is equal to some element of the set $\{0\} \cup \{p^r : r \in \mathbb{Z}\}$, but we still need to show that $|\alpha|_p$ is well-defined in the sense that if $\{a_n\} = \{b_n\}$ in $\mathbb{Q}_p$ then

$$\lim_{n\to\infty} |a_n|_p = \lim_{n\to\infty} |b_n|_p.$$

The assumption that $\{a_n\} = \{b_n\}$ in $\mathbb{Q}_p$ means that the difference $\{a_n - b_n\}$ is p-adically null. Now by the triangle inequality

$$|a_n|_p = |(a_n - b_n) + b_n|_p \leq |a_n - b_n|_p + |b_n|_p.$$

Hence

$$\lim_{n\to\infty} |a_n|_p \leq \lim_{n\to\infty} |a_n - b_n|_p + \lim_{n\to\infty} |b_n|_p.$$

As $\{a_n - b_n\}$ is null, $\lim_{n\to\infty} |a_n - b_n|_p = 0$, so

$$\lim_{n\to\infty} |a_n|_p \leq \lim_{n\to\infty} |b_n|_p.$$

Swapping the rôles of the as and bs in the above argument gives

$$\lim_{n\to\infty} |b_n|_p \leq \lim_{n\to\infty} |a_n|_p.$$

Hence

$$\lim_{n\to\infty} |b_n|_p = \lim_{n\to\infty} |a_n|_p,$$

which shows that $|\alpha|_p$ is well-defined for $\alpha \in \mathbb{Q}_p$.

4.1. Properties of p-adic absolute value. Now that we have defined the p-adic absolute value on $\mathbb{Q}_p$, it is natural to ask if it has the same properties it had on $\mathbb{Q}$, and it does.

Theorem 4.10. *Let p be a prime and α, $\beta \in \mathbb{Q}_p$. Then*

(i) $|\alpha|_p \geq 0$. *Moreover,* $|\alpha|_p = 0$ *iff* $\alpha = 0$.
(ii) $|\alpha\beta|_p = |\alpha|_p|\beta|_p$.
(iii) $|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}$, *with equality if* $|\alpha|_p \neq |\beta|_p$.

PROOF. The proof follows by choosing p-adically Cauchy sequences of rationals representing α and β and then using the definition of $|\cdot|_p$ in terms of these sequences and Theorem 4.3. We leave this as an exercise. □

5. Convergence of Series

The ultrametric inequality has a dramatic effect of making the convergence of series very easy to check.

Theorem 4.11. *Let p be a prime. The series $\sum_{j=1}^{\infty} a_j$ converges p-adically if and only if $\lim_{j\to\infty}|a_j|_p = 0$.*

We know that with the usual absolute value the theorem is true only in the left to right direction. The famous counterexample being the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots,$$

which diverges even though $\lim_{j\to\infty} 1/j = 0$. Working p-adically, we don't need any of the complicated convergence tests of first-year analysis—the theorem makes it all very easy!

PROOF OF THEOREM 4.11. Suppose that $\lim_{n\to\infty}|a_n|_p = 0$. All we have to do is to show the the sequence of partial sums $s_n = \sum_{j=1}^{n} a_j$ is Cauchy. A Cauchy sequence converges to some element of $\mathbb{Q}_p$ (which happens to equal the sequence itself). Now suppose $m > n$. Then

$$|s_m - s_n|_p = |a_{n+1} + a_{n+2} + \cdots + a_m|_p = \max_{n+1\leq j\leq m}|a_j|_p,$$

by the ultrametric inequality. For any $\epsilon > 0$, there is some N such that if $j \geq N$ then $|a_j|_p < \epsilon$. Hence if $m, n \geq N$ then $|s_m - s_n|_p < \epsilon$, proving that the sequence $\{s_n\}$ is p-adically Cauchy. □

6. p-adic Integers

Definition. The set of p-adic integers $\mathbb{Z}_p$ is defined by

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \ : \ |\alpha|_p \leq 1\}.$$

So $\mathbb{Z}_p$ 'looks' like a disc of radius 1 centred at the origin. In this sense, the following theorem is striking.

Theorem 4.12. *$\mathbb{Z}_p$ is a ring and contains $\mathbb{Z}$ as a subring.*

PROOF. Note first that if $a \in \mathbb{Z}$ then $\operatorname{ord}_p(a) \geq 0$ and so $|a|_p = p^{-\operatorname{ord}_p(a)} \leq 1$. Hence $\mathbb{Z} \subset \mathbb{Z}_p$.

To complete the proof we must show that $\mathbb{Z}_p$ is a ring. You don't have to know anything about rings except the definition. Note that $\mathbb{Z}_p \subset \mathbb{Q}_p$ and $\mathbb{Q}_p$ is already a field. So we have to show that $\mathbb{Z}_p$ is closed under addition and multiplication (it already contains 0 and 1). But if α, $\beta \in \mathbb{Z}_p$ then

$$|\alpha\beta|_p = |\alpha|_p|\beta|_p \leq 1 \cdot 1 = 1,$$

and

$$|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\} \leq \max\{1, 1\} = 1.$$

Hence $\alpha\beta$, $\alpha + \beta \in \mathbb{Z}_p$. □

Lemma 4.13. *If $\{a_n\}$ is a p-adically Cauchy sequence with $a_n \in \mathbb{Z}$ then $\lim_{n\to\infty} a_n$ is in $\mathbb{Z}_p$. Conversely, any $\alpha \in \mathbb{Z}_p$ is the limit of such a sequence.*

PROOF. Suppose $\{a_n\}$ is a p-adically Cauchy sequence with $a_n \in \mathbb{Z}$ and let $\alpha = \lim_{n\to\infty} a_n$. Then $|a_n|_p \leq 1$ and so

$$|\alpha|_p = \lim_{n\to\infty} |a_n|_p \leq 1$$

which shows that $\alpha \in \mathbb{Z}_p$. The converse is harder. Suppose $\alpha \in \mathbb{Z}_p$. Now $\mathbb{Z}_p \subset \mathbb{Q}_p$ and so $\alpha = \lim_{n\to\infty} a_n$ where $\{a_n\}$ is a p-adically Cauchy sequence of rational numbers, but there is *a priori* no reason for the a_n be integral. We will construct a p-adically Cauchy sequence $\{b_n\}$ where the b_n are in $\mathbb{Z}$ and $\{a_n - b_n\}$ is a p-adically null sequence. Then $\alpha = \lim_{n\to\infty} b_n$ as required. Now

$$\lim_{n\to\infty} |a_n|_p = |\alpha|_p \leq 1.$$

Consider $\operatorname{ord}_p(a_n)$. If there are infinitely many n such that $\operatorname{ord}_p(a_n) \leq -1$ then there are infinitely many n such that $|a_n|_p \geq p$ and this contradicts the above. Hence there is some N such that $\operatorname{ord}_p(a_n) \geq 0$ for all $n \geq N$. So we can write

$$a_n = \frac{u_n}{v_n}$$

where u_n, $v_n \in \mathbb{Z}$, with $p \nmid v_n$. Since $p \nmid v_n$, we know that v_n is invertible modulo p^n. Let $v_n w_n \equiv 1 \pmod{p^n}$, where $w_n \in \mathbb{Z}$ and write $b_n = u_n w_n \in \mathbb{Z}$. Then $a_n = u_n/v_n \equiv u_n w_n = b_n \pmod{p^n}$ and so $|a_n - b_n|_p \leq p^{-n}$. This completes the proof. □

7. Hensel's Lemma Revisited

Corollary 4.14. *Let p be a prime. Let $f(X)$ be a polynomial with integer coefficients. Suppose that there is an integer a such that*

$$f(a) \equiv 0 \pmod{p}, \qquad f'(a) \not\equiv 0 \pmod{p}.$$

(i) *Then there is a sequence $\{a_m\}_{m=1}^{\infty}$ such that $a_1 = a$, and*

$$f(a_m) \equiv 0 \pmod{p^m}, \qquad a_{m+1} \equiv a_m \pmod{p^m}. \tag{7}$$

(ii) *The sequence $\{a_m\}_{m=1}^{\infty}$ converges to $\alpha \in \mathbb{Z}_p$ and α satisfies $f(\alpha) = 0$.*

Proof. We start with $a_1 = a$ and apply Hensel's Lemma (Theorem 4.2) with $m = 1$. We obtain an a_2 such that

$$f(a_2) \equiv 0 \pmod{p}, \qquad a_2 \equiv a_1 \pmod{p}.$$

Suppose now we have constructed $a_1, a_2, \ldots, a_k$ to satisfy (7). Note that

$$a_k \equiv a_{k-1} \pmod{p^k}, \quad a_{k-1} \equiv a_{k-2} \pmod{p^{k-1}}, \ldots, a_2 \equiv a_1 \pmod{p}.$$

Then certainly $a_k \equiv a_1 = a \pmod{p}$ and so $f'(a_k) \equiv f'(a) \not\equiv 0 \pmod{p}$. We can now apply Hensel to obtain a_{k+1}. This completes the proof of (i).

Let us prove (ii). We want to prove that $\{a_n\}$ converges p-adically. Write

$$b_1 = a_1, \qquad b_2 = a_2 - a_1, \qquad b_3 = a_3 - a_2, \ldots.$$

Then $a_n = b_1 + b_2 + \cdots + b_n$. Hence the sequence $\{a_n\}$ converges p-adically iff the series $\sum b_m$ converges p-adically. But

$$|b_m|_p = |a_m - a_{m-1}|_p \leq p^{-(m-1)},$$

since $a_m \equiv a_{m-1} \pmod{p^{m-1}}$. Thus $\{a_n\}$ converges in $\mathbb{Q}_p$. As $a_n \in \mathbb{Z}$, we know from the previous lemma that $\{a_n\}$ converges to some $\alpha \in \mathbb{Z}_p$. Now [1]

$$f(\alpha) = f\left(\lim_{n\to\infty} a_n\right) = \lim_{n\to\infty} f(a_n) = 0,$$

since $|f(a_n)|_p \leq p^{-n}$. □

Corollary 4.15. *Let $b \in \mathbb{Z}$ be non-zero and p an odd prime. Then b is a square in $\mathbb{Z}_p$ if and only if $b = p^{2r}c$ where $r \in \mathbb{Z}$ and $\left(\frac{c}{p}\right) = 1$.*

---

[1] For a polynomial f, the equality

$$f\left(\lim_{n\to\infty} a_n\right) = \lim_{n\to\infty} f(a_n)$$

is an easy exercise.

PROOF. Suppose $b = p^{2r}c$ where $r \in \mathbb{Z}$ and $\left(\frac{c}{p}\right) = 1$. All we have to show is that c is a square in $\mathbb{Z}_p$. Let $f(X) = X^2 - c$. Since $\left(\frac{c}{p}\right) = 1$, there is some $a \not\equiv 0 \pmod{p}$ such that $c \equiv a^2 \pmod{p}$. Hence

$$f(a) \equiv 0 \pmod{p}, \qquad f'(a) = 2a \not\equiv 0 \pmod{p}.$$

By the above corollary to Hensel's Lemma, there is some $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$, so $\alpha^2 = c$ as required.

Let us prove the converse. Suppose b is a square in $\mathbb{Z}_p$, say $b = \beta^2$ where $\beta \in \mathbb{Z}_p$. Write $b = p^s c$ where $p \nmid c$. Then

$$p^{-s} = |b|_p = |\beta|_p^2.$$

Now $|\beta|_p$ is a power of p, so s is even, say $s = 2r$. So $b = p^{2r}c$ is a square in $\mathbb{Z}_p$. Hence c is a square in $\mathbb{Q}_p$. Say $c = \gamma^2$ with $\gamma \in \mathbb{Q}_p$. But $1 = |c|_p = |\gamma|_p^2$, so $\gamma \in \mathbb{Z}_p$. Let $\{a_n\}$ be a Cauchy sequence of integers converging to γ. Then $\{a_n^2\}$ coverges to c. Hence there is some N such that for $n \geq N$,

$$|a_n^2 - c|_p \leq p^{-1},$$

which can be rewritten as

$$c \equiv a_n^2 \pmod{p}.$$

This shows that $\left(\frac{c}{p}\right) = 1$. □

Deciding which integers are squares in $\mathbb{Z}_2$ is a little more tricky, and needs a stronger version of Hensel's Lemma.

Theorem 4.16. (Hensel's Lemma—Strong Version) *Let $f(X) \in \mathbb{Z}[X]$. Let p be a prime and $m \geq 0$. Suppose $a \in \mathbb{Z}$ and write*

$$k = \operatorname{ord}_p(f'(a)).$$

Suppose that $m \geq 1$ and

$$f(a) \equiv 0 \pmod{p^{m+2k}}.$$

Then there exists $b \in \mathbb{Z}$ such that

$$b \equiv a \pmod{p^{m+k}}, \qquad f(b) \equiv 0 \pmod{p^{m+1+2k}}.$$

PROOF. Write $b = a + p^{m+k}y$ where $y \in \mathbb{Z}$ is yet to be determined. By Taylor's Theorem,

$$f(b) = f(a) + p^{m+k}y \cdot f'(a) + p^{2m+2k}(\text{integer}).$$

We can write

$$f(a) = p^{m+2k}c, \qquad f'(a) = p^k d$$

where c, $d \in \mathbb{Z}$ and $p \nmid d$. Then

$$f(b) = p^{m+2k}(c + dy) + p^{2m+2k}(\text{integer}).$$

To complete the proof of the theorem, all we have to do is to choose $y \in \mathbb{Z}$ so that $p \mid (c + dy)$. In other words we want $dy \equiv -c \pmod{p}$, and we can do this as d is invertible modulo p; this is where we use the fact that $p \nmid d$. □

We can now improve on Corollary 4.14 as follows.

Corollary 4.17. *Let p be a prime. Let $f(X)$ be a polynomial with integer coefficients, and $k \geq 0$ an integer. Suppose that there is an integer a such that*

$$f(a) \equiv 0 \pmod{p^{2k+1}}, \qquad \operatorname{ord}_p(f'(a)) = k.$$

(i) *Then there is a sequence $\{a_m\}_{m=1}^{\infty}$ such that $a_1 = a$, and*

$$f(a_m) \equiv 0 \pmod{p^{m+2k}}, \qquad a_{m+1} \equiv a_m \pmod{p^{m+k}}.$$

(ii) *The sequence $\{a_m\}_{m=1}^{\infty}$ converges to $\alpha \in \mathbb{Z}_p$ and α satisfies $f(\alpha) = 0$.*

The proof is an easy modification of the proof of Corollary 4.14 using the strong version of Hensel's Lemma and we leave it as an exercise.

Corollary 4.18. *Let $b \in \mathbb{Z}$ be non-zero. Then b is a square in $\mathbb{Z}_2$ if and only if $b = 2^{2r}c$ where $c \equiv 1 \pmod{8}$.*

Proof. The proof is almost the same as the proof of Corollary 4.15 but uses Corollary 4.17 instead. Let us show that if $c \equiv 1 \pmod{8}$ then c is a square in $\mathbb{Z}_2$. Let $f(X) = X^2 - c$. Then

$$f(1) \equiv 0 \pmod{2^3}, \qquad \operatorname{ord}_2(f'(1)) = 1,$$

so taking $k = 1$ in Corollary 4.17 shows that there is some $\alpha \in \mathbb{Z}_2$ such that $f(\alpha) = 0$. Then $c = \alpha^2$ as required.

The rest of the proof is an exercise. □

8. The Hasse Principle

Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$. We want to know if the equation $f(X_1, \ldots, X_n) = 0$ has a solution in integers. As $\mathbb{Z} \subseteq \mathbb{Z}_p$ for all primes p and as $\mathbb{Z} \subseteq \mathbb{R}$ we know the following:

$$f = 0 \text{ has a solution in } \mathbb{Z}^n \implies \begin{cases} f = 0 \text{ has a solution in } \mathbb{Z}_p^n \text{ for all primes } p & \text{and} \\ f = 0 \text{ has a solution in } \mathbb{R}^n. \end{cases}$$

Is the converse statement true? The converse statement is called the 'Hasse Principle'. It is true for many classes of polynomials, and for

these classes of polynomials we say that the Hasse Principle holds. But it is false for many other classes of polynomials and for those we say that the Hasse principle fails. Here is a counterexample to the Hasse principle for polynomials in 1 variable.

Example 8.1. Let $f(X) = (X^2 - 2)(X^2 - 17)(X^2 - 34)$. Show that $f(X) = 0$ is a counterexample to the Hasse principle.
Answer: Basically we are asked to show that $f(X) = 0$ has solutions in $\mathbb{Z}_p$ for all primes p and in $\mathbb{R}$, but has no solutions in $\mathbb{Z}$. It clearly has solutions in $\mathbb{R}$, which are $\pm\sqrt{2}$, $\pm\sqrt{17}$, $\pm\sqrt{34}$, and clearly it has no solutions in $\mathbb{Z}$ as none of these roots are integral.

Now $17 \equiv 1 \pmod 8$ and so by Corollary 4.18 $17 = \alpha^2$ for some $\alpha \in \mathbb{Z}_2$. Then $f(\alpha) = 0$, so $f(X) = 0$ has a solution in $\mathbb{Z}_2$. Also $\left(\frac{2}{17}\right) = 1$, so 2 is a square in $\mathbb{Z}_{17}$ by Corollary 4.15, and so $f(X) = 0$ has a solution in $\mathbb{Z}_{17}$. Suppose that $p \neq 2, 17$. We want to show that $f(X) = 0$ has a solution in $\mathbb{Z}_p$. Equivalently, we want to show that at least one of 2, 17, 34 is a square in $\mathbb{Z}_p$. Suppose that 2, 17 are not squares in $\mathbb{Z}_p$. By Corollary 4.15,

$$\left(\frac{2}{p}\right) = -1, \qquad \left(\frac{17}{p}\right) = -1.$$

But multiplying we obtain

$$\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = 1.$$

Hence 34 is a square in $\mathbb{Z}_p$ and so $f(X)$ has a solution in $\mathbb{Z}_p$. This completes the proof.

8.1. A Bivariate Counterexample to the Hasse Principle. Let $f(X, Y) = 2Y^2 - X^4 + 17$. We claim that $f(X, Y) = 0$ is a counterexample to the Hasse Principle. Clearly $f(X, Y) = 0$ has solutions in $\mathbb{R}$; for example $(X, Y) = (\sqrt[4]{17}, 0)$. The standard proof that $f(X, Y) = 0$ has solutions in $\mathbb{Z}_p$ for all primes p uses some advanced results and we shall omit it. How do we show that $f(X, Y) = 0$ has no solutions in $\mathbb{Z}$? Suppose x, $y \in \mathbb{Z}$ such that $f(x, y) = 0$. Clearly $y \neq 0$, and $f(x, -y) = f(x, y)$, so we can assume that $y > 0$. Moreover, from $2y^2 = x^4 - 17$, if $17 \mid x$ or $17 \mid y$ then 17 divides both and $17^2 \mid 17$ which is impossible. Thus $17 \nmid x$, $17 \nmid y$.

Suppose p is an odd prime divisor of y. Then

$$x^4 \equiv 17 \pmod p.$$

So certainly 17 is a square modulo p, and we can write

$$\left(\frac{17}{p}\right) = 1.$$

By the Law of Quadratic Reciprocity (as $17 \equiv 1 \pmod 4$),

$$\left(\frac{p}{17}\right) = 1.$$

Write $y = 2^r \prod p_i^{r_i}$ where the p_i are distinct odd prime divisors of y. Then

$$\left(\frac{p_i}{17}\right) = 1$$

by the above, and

$$\left(\frac{2}{17}\right) = 1,$$

as $17 \equiv 1 \pmod 8$. Thus

$$\left(\frac{y}{17}\right) = \left(\frac{2}{17}\right)^r \prod \left(\frac{p_i}{17}\right)^{r_i} = 1.$$

Hence $y \equiv z^2 \pmod{17}$. From $2y^2 = x^4 - 17$ we obtain that

$$2z^4 \equiv x^4 \pmod{17}.$$

We said earlier that $17 \nmid x, y$, so $z \not\equiv 0 \pmod{17}$. Thus z is invertible modulo 17. Let $w \equiv xz^{-1} \pmod{17}$. Then $w^4 \equiv 2 \pmod{17}$. However, by trying the values $w = 0, 1, \ldots, 16$ we find that the congruence $w^4 \equiv 2 \pmod{17}$ does not have any solutions, giving us a contradiction.

CHAPTER 5

Geometry of Numbers

We now come to the **Geometry of Numbers**, a branch of number theory that will enable us to prove several interesting results, including the Hasse Principle for conics. There are only two theorems from the Geometry of Numbers that we need: Blichfeldt's Theorem and Minkowski's Theorem.

Definition. By a **sublattice** of $\mathbb{Z}^n$ we simply mean a subgroup of $\mathbb{Z}^n$ of finite index.

A subset $C \subset \mathbb{R}^n$ is said to be **symmetric** if for every $\mathbf{x}$ in C, $-\mathbf{x}$ is also in C. We say C is **convex** if for every pair of points $\mathbf{x}$ and $\mathbf{y}$ in C, the entire line segment joining $\mathbf{x}$ and $\mathbf{y}$ is contained in C. If you like symbols you can write this as, for all $\mathbf{x}$, $\mathbf{y} \in C$ and all $0 \leq \lambda \leq 1$, we have

$$\lambda\mathbf{x} + (1-\lambda)\mathbf{y} \in C.$$

Theorem 5.1. (Minkowski's Theorem) *Let Λ be a sublattice of $\mathbb{Z}^n$ of index m. Let C be a convex symmetric subset of $\mathbb{R}^n$ having volume $V(C)$ satisfying*

$$V(C) > 2^n m.$$

Then C and Λ have a common point other than $\mathbf{0}$.

For the proof of Minkowski's Theorem we will need Blichfeldt's Theorem. So we'll delay Minkowski's proof until we've seen some of it's beautiful consequences.

1. The Two Squares Theorem

Theorem 5.2. *Every prime $p \equiv 1 \pmod 4$ can be written in the form $p = x^2 + y^2$ for some integers x, y.*

Proof. Since $p \equiv 1 \pmod 4$ we know that $\left(\frac{-1}{p}\right) = 1$. Hence there is an integer $\ell \in \mathbb{Z}$ such that

$$\ell^2 \equiv -1 \pmod p. \tag{8}$$

Let

$$\Lambda = \{(x,y) \in \mathbb{Z}^2 : x \equiv \ell y \pmod p\}.$$

Common sense dictates that Λ is a subgroup of $\mathbb{Z}^2$ of index p. But if you're not a fan of common sense we can also prove this using the First Isomorphism Theorem. Write $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \ldots, \overline{p-1}\}$ for the group of integers modulo p. Let

$$\phi : \mathbb{Z}^2 \to \mathbb{Z}/p\mathbb{Z}, \qquad \phi(x, y) = \overline{x - \ell y}.$$

It's easy to check that ϕ is a homomorphism and that Λ is the kernel of ϕ. Hence Λ is a subgroup of $\mathbb{Z}^2$. If $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ then $\phi(a, 0) = \overline{a}$, so ϕ is surjective. In other words, the image of ϕ is $\mathbb{Z}/p\mathbb{Z}$. The First Isomorphism Theorem tells us that

$$\mathbb{Z}^2/\Lambda \cong \mathbb{Z}/p\mathbb{Z}.$$

Hence the index of Λ in $\mathbb{Z}^2$ is the cardinality of $\mathbb{Z}^2/\Lambda$ which is the cardinality of $\mathbb{Z}/p\mathbb{Z}$ which is p. We have now completely circumvented common sense to show that the index is p and can with clear conscience return to the proof of the Two Squares Theorem.

Let

$$C = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 2p\}.$$

This is clearly convex and symmetric with volume(=area)

$$V(C) = 2\pi p > 2^2 p.$$

You're probably reading this in the privacy of your own room, so feel free to jump up and down from excitement now that we have satisfied all the conditions of Minkowski's Theorem. Minkowski tells us that C and Λ have some common point other than $(0, 0)$. Let this be (x, y). As $(x, y) \in \Lambda$, we have that x, $y \in \mathbb{Z}$ and $x \equiv \ell y \pmod{p}$. Hence

$$x^2 + y^2 \equiv \ell^2 y^2 + y^2 \equiv (\ell^2 + 1)y^2 \equiv 0 \pmod{p};$$

here we made use of (8). Also (x, y) is a non-zero point of C, so

$$0 < x^2 + y^2 < 2p.$$

To sum up, $x^2 + y^2$ is an integer strictly between 0 and $2p$ that is divisible by p. Hence $x^2 + y^2 = p$, as required. □

The Two Squares Theorem is due to Fermat who proved it using the a technique called **infinite descent**.

2. Areas of Ellipses and Volumes of Ellipsoids

To be able to do the homework you need formulae for the area of the ellipse

$$E_{a,b} = \left\{(x, y) \in \mathbb{R}^2 : \frac{x^2}{a^2} + \frac{y^2}{b^2} < 1\right\},$$

and the volume of the ellipsoid

$$\mathcal{E}_{a,b,c} = \left\{(x,y,z) \in \mathbb{R}^3 : \frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} < 1\right\}.$$

Here a, b and c are positive constants.

You know of course that the area of the ellipse is going to be given by the double integral

$$V(E_{a,b}) = \iint_{E_{a,b}} 1 dxdy.$$

To evaluate this double integral we'll use a substitution. Let $u = x/a$ and $v = y/b$. Then the ellipse $E_{a,b}$ in the xy-plane becomes the unit disc

$$D = \{(u,v) \in \mathbb{R}^2 : u^2 + v^2 < 1\}$$

in the uv-plane. Moreover $dx = d(au) = adu$ and $dy = d(bv) = bdv$. Hence

$$V(E_{a,b}) = \iint_D abdudv = ab \iint_D 1 dudv = abV(D),$$

and $V(D) = \pi$ is the area of the unit disc D. We obtain

$$V(E_{a,b}) = \pi ab,$$

and similarly you can prove that

$$V(\mathcal{E}_{a,b,c}) = \frac{4\pi}{3} abc.$$

2.1. Volume of the Ball in 4-Dimensions. For our next treat, the Four Squares Theorem, we will need the volume of the Ball of radius r in 4-dimensions:

$$\mathcal{B}_r = \{(x,y,z,w) \in \mathbb{R}^4 : x^2 + y^2 + z^2 + w^2 < r^2\}.$$

This is given by the quadruple integral

$$V(\mathcal{B}_r) = \iiiint_{x^2+y^2+z^2+w^2<r^2} dxdydzdw.$$

Note that $-r < w < r$, so we can rewrite the quadruple integral as

$$V(\mathcal{B}_r) = \int_{w=-r}^{w=r} \left(\iiint_{x^2+y^2+z^2<r^2-w^2} dxdydz \right) dw.$$

However $x^2 + y^2 + z^2 < r^2 - w^2$ is a ball (sphere) in xyz-space of radius $\sqrt{r^2 - w^2}$, so

$$\iiint_{x^2+y^2+z^2<r^2-w^2} dxdydz = \frac{4\pi}{3}(r^2 - w^2)^{3/2}.$$

Hence

$$V(\mathcal{B}_r) = \frac{4\pi}{3}\int_{w=-r}^{w=r}(r^2-w^2)^{3/2}dw = \frac{8\pi}{3}\int_{w=0}^{w=r}(r^2-w^2)^{3/2}dw.$$

You immediately say to yourself that this needs are trigonometric substitution, and you're right: let $w = r\sin\theta$, so $dw = r\cos\theta d\theta$, and so

$$V(\mathcal{B}_r) = \frac{8\pi}{3}\int_{\theta=0}^{\theta=\pi/2} r^3(1-\sin^2\theta)^{3/2}r\cos\theta d\theta = \frac{8\pi r^4}{3}\int_0^{\pi/2}\cos^4\theta d\theta.$$

We need to integrate $\cos^4$, and one way of doing this is using multiple-angle formulae. See your Vectors and Matrices lecture notes if you haven't ceremoniously incinerated them at the end of your first year. But just in case, here is how it works. Write

$$\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2}.$$

Taking fourth powers we get

$$\cos^4\theta = \frac{1}{16}\left(e^{4i\theta}+4e^{2i\theta}+6+4e^{-2i\theta}+e^{-4i\theta}\right)$$

which we can rewrite as

$$\cos^4\theta = \frac{1}{8}\cos 4\theta + \frac{1}{2}\cos 2\theta + \frac{3}{8}.$$

Hence

$$\int_0^{\pi/2}\cos^4\theta d\theta = \frac{3\pi}{16}.$$

We deduce that the volume of the ball of radius r in 4-space is

$$V(\mathcal{B}_r) = \frac{\pi^2 r^4}{2}. \tag{9}$$

3. The Four Squares Theorem

Theorem 5.3. *Every positive integer n can be written as the sum of four integer squares.*

This is a statement that your non-mathematical parents would understand. If they ask you what you've learned in three or four years on a maths degree you can mention this, and they'll be very impressed and think that your education has been worthwhile. Most of your other modules give you statements that are pure gobbledygook to the uninitiated. Galois Theory gives a few statements that your parents might understand but they're all negative: you can't solve a quintic, or construct a heptagon, or trisect an angle. Number Theory gives positive

assertions that broaden your horizons, and expand the frontiers of your knowledge ...

If you've survived reading the previous paragraph without vomiting then you have strong constitution and is ready for the proof of the Four Squares Theorem.

PROOF OF THE FOUR SQUARES THEOREM. First we prove the statement of the theorem for primes. If $p = 2$ then we can write $p = 1^2 + 1^2 + 0^2 + 0^2$, so assume that p is an odd prime. By one of the exercises on the early homework assignments—unassessed due to lack of foresight on my part—you know that there integers a, b such that

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

Let

$$\Lambda = \{(x, y, z, w) \in \mathbb{Z}^4 : x \equiv az+bw \pmod{p}, \qquad y \equiv bz-aw \pmod{p}\}.$$

This common-sensically is a sublattice of $\mathbb{Z}^4$ of index p^2.

We also take

$$C = \{(x, y, z, w) \in \mathbb{R}^4 : x^2 + y^2 + z^2 + w^2 < 2p\}.$$

This is a ball of radius $\sqrt{2p}$, so is convex and symmetric and by (9) we have

$$V(C) = \frac{\pi^2}{2}(\sqrt{2p})^4 = 2\pi^2 p^2 > 2^4 p^2.$$

Hence the hypotheses of Minkowski are satisfied. So we have a point (x, y, z, w) common to both Λ and C that is not $(0, 0, 0, 0)$. As (x, y, z, w) is in Λ, the coordinates are integers and

$$\begin{aligned} x^2 + y^2 + z^2 + w^2 &\equiv (az + bw)^2 + (bz - aw)^2 + z^2 + w^2 \\ &= (a^2 + b^2 + 1)(z^2 + w^2) \equiv 0 \pmod{p}. \end{aligned}$$

However, as (x, y, z, w) is a non-zero point of C,

$$0 < x^2 + y^2 + z^2 + w^2 < 2p,$$

so $x^2 + y^2 + z^2 + w^2$ is an integer strictly between 0 and $2p$ that is divisible by p. The inescapable conclusion is $x^2 + y^2 + z^2 + w^2 = p$.

This proves the theorem for primes. To complete the proof we need the identity

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) = \tag{10}$$
$$(ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+(az-bw+cx+dy)^2+(aw+bz-cy+dx)^2$$

Now if $n > 1$ is a positive integer then you can write as a product of primes and use the identity repeatedly to write n as a sum of four squares. □

Notes:

- The Four Squares Theorem was proved by Joseph Louis Lagrange in 1770, though the theorem appears–without proof– in the Arithmetica of Diophantus (probably written around 250AD). We have followed Davenport's proof of the Four Squares Theorem (1941).
- Another fascinating question is, in how many ways can we write a positive integer n as the sum of four squares? This was answered in 1834 by Carl Jacobi. He showed that this number is eight times the sum of the divisors of n if n is odd, and 24 times the sum of the odd divisors of n if n is even. Jacobi's theorem has remarkable proof using modular forms.
- Where does identity in (10) come from? You are surely familiar with the multiplicative property of norms of Gaussian integers. If $\alpha = a + bi \in \mathbb{Z}[i]$ then the norm of α is defined by $N(\alpha) = a^2 + b^2$, and you know $N(\alpha\beta) = N(\alpha)N(\beta)$. The identity in (10) is the corresponding identity for quaternion norms.

4. Proof of Minkowski's Theorem

Now that you've seen these 'wicked' applications of Minkowski's Theorem, you're obviously dying to see its proof. But that has to wait (I know I'm cruel) until after Blichfeldt's Theorem.

Theorem 5.4. (Blichfeldt's Theorem) *Let $m \geq 1$ be an integer. Let S be a subset of $\mathbb{R}^n$ with volume $V(S)$ satisfying*

$$V(S) > m.$$

There exists $m+1$ distinct points $\mathbf{x}_0, \ldots, \mathbf{x}_m \in S$ such that

$$\mathbf{x}_j - \mathbf{x}_i \in \mathbb{Z}^n, \qquad \text{for } 0 \leq i, j \leq m.$$

Proof. Let χ_S be the characteristic function of S; thus

$$\chi_S(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{x} \in S \\ 0 & \text{if } \mathbf{x} \notin S. \end{cases}$$

Then

$$V(S) = \int_{\mathbb{R}^n} \chi_S(\mathbf{x})\, d\mathbf{x}. \tag{11}$$

Let W be the unit cube:

$$W = \{(x_1, \ldots, x_n) : 0 \leq x_i < 1\}.$$

Then every vector $\mathbf{x} \in \mathbb{R}^n$ can be decomposed uniquely [1] as $\mathbf{x} = \mathbf{z} + \mathbf{w}$ where $\mathbf{z} \in \mathbb{Z}^n$ and $\mathbf{w} \in W$. Thus

$$\mathbb{R}^n = \bigcup_{\mathbf{z} \in \mathbb{Z}^n} (\mathbf{z} + W),$$

where

$$\mathbf{z} + W = \{\mathbf{z} + \mathbf{w} : \mathbf{w} \in W\}.$$

Thus we can rewrite (11) as

$$V(S) = \sum_{\mathbf{z} \in \mathbb{Z}^n} \int_{\mathbf{w} \in W} \chi_S(\mathbf{z} + \mathbf{w})\, d\mathbf{w}.$$

Interchanging the summation and integration signs we obtain [2]

$$V(S) = \int_{\mathbf{w} \in W} \left(\sum_{\mathbf{z} \in \mathbb{Z}} \chi_S(\mathbf{z} + \mathbf{w}) \right) d\mathbf{w}.$$

Write $f(\mathbf{w}) = \sum_{\mathbf{z} \in \mathbb{Z}} \chi_S(\mathbf{z} + \mathbf{w})$, and recall that $V(S) > m$ is a hypothesis of the theorem. Hence

$$\int_{\mathbf{w} \in W} f(\mathbf{w}) d\mathbf{w} > m.$$

But W has volume 1. Hence there is some point $\mathbf{w} \in W$ such that $f(\mathbf{w}) > m$; i.e. $\sum_{\mathbf{z} \in \mathbb{Z}} \chi_S(\mathbf{z} + \mathbf{w}) > m$ for that particular $\mathbf{w}$. But the $\chi_S(\mathbf{z}+\mathbf{w})$ are ones and zeros, so there are $m+1$ distinct $\mathbf{z}_0, \ldots, \mathbf{z}_m \in \mathbb{Z}^n$ such that $\chi_S(\mathbf{z}_i + \mathbf{w}) = 1$. Write $\mathbf{x}_i = \mathbf{z}_i + \mathbf{w}$, so the $\mathbf{x}_i$ are distinct. Now note that $\chi_S(\mathbf{x}_i) = 1$, so by definition of χ_S, the $\mathbf{x}_i$ are in S. Finally

$$\mathbf{x}_j - \mathbf{x}_i = (\mathbf{z}_j + \mathbf{w}) - (\mathbf{z}_i + \mathbf{w}) = \mathbf{z}_j - \mathbf{z}_i \in \mathbb{Z}^n,$$

which completes the proof. □

Here is the statement of Minkowski again, with proof.

Theorem 5.5. (Minkowski's Theorem) *Let Λ be a sublattice of $\mathbb{Z}^n$ of index m. Let C be a convex symmetric subset of $\mathbb{R}^n$ having volume $V(C)$ satisfying*

$$V(C) > 2^n m.$$

Then C and Λ have a common point other than $\mathbf{0}$.

---

[1] For example in $\mathbb{R}^2$, we write $(1.7, 5.9) = (1, 5) + (0.7, 0.9)$ where we note that $(1, 5) \in \mathbb{Z}^2$ and $(0.7, 0.9) \in W$.

[2] To justify interchanging integration with infinite summation one needs rather delicate theorems in Lebesgue Integration. Fortunately/unfortunately for you, I've forgotten my Lebesgue and so I can't tell you about it. But **beware**, Analysis lecturers with no sense of humour don't like to see this sort of thing without justification; they would regard my lecture notes as mathematical pornography.

PROOF. Let

$$S = \frac{1}{2}C = \left\{ \frac{1}{2}\mathbf{x} : \mathbf{x} \in C \right\}.$$

The volume of S is

$$V(S) = \frac{1}{2^n}V(C) > m.$$

By Blichfeldt's Theorem, there are $m+1$ distinct points $\mathbf{x}_0, \ldots, \mathbf{x}_m \in S$ such that

$$\mathbf{x}_j - \mathbf{x}_i \in \mathbb{Z}^n, \qquad \text{for } 0 \leq i, j \leq m.$$

Let $\mathbf{y}_j = \mathbf{x}_j - \mathbf{x}_0 \in \mathbb{Z}^n$ for $j = 0, \ldots, m$. These are $m+1$ distinct points $\mathbf{y}_j$ in $\mathbb{Z}^n$ and Λ has m cosets in $\mathbb{Z}^n$. So two distinct $\mathbf{y}_i$, $\mathbf{y}_j$ lie in the same coset of Λ. Thus, $\mathbf{x}_j - \mathbf{x}_i = \mathbf{y}_j - \mathbf{y}_i$ is a non-zero element of Λ. Now we can write $\mathbf{x}_j = \mathbf{c}/2$ and $\mathbf{x}_i = \mathbf{c}'/2$ where $\mathbf{c}$ and $\mathbf{c}'$ are in C. Hence

$$\frac{\mathbf{c} - \mathbf{c}'}{2}$$

is a non-zero element of Λ. Now C is symmetric so, $-\mathbf{c}' \in C$ as well as $\mathbf{c} \in C$. Finally C is convex and $(\mathbf{c} - \mathbf{c}')/2$ is the mid-point between $\mathbf{c}$ and $-\mathbf{c}'$, so it must be in C as well as being a non-zero element of Λ. This is the point whose existence is asserted in the statement of the theorem. □

CHAPTER 6

Irrationality and Transcendence

1. Irrationality: First Steps

A number in $\mathbb{C}$ is called **irrational** if it does not belong to $\mathbb{Q}$. You of course recall the proof that $\sqrt{2}$ is irrational which you did in Foundations. Let's go through it again as it is the model for Gauss' Theorem below.

Theorem 6.1. *$\sqrt{2}$ is irrational.*

PROOF. The proof is by contradiction. Suppose $\sqrt{2}$ is rational, and write it as $\sqrt{2} = a/b$ where a, b are coprime integers with $b \neq 0$. Then $a^2 = 2b^2$, so a^2 is even and hence a is even. We write $a = 2c$ where c is an integer. Thus $b^2 = 2c^2$. Hence b^2 is even and therefore b is even. Since a, b are both even they're not coprime; this is the desired contradiction. □

Theorem 6.2. *(Gauss) Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ be a monic polynomial with integer coefficients and degree $n \geq 1$. The only possible rational roots of f are integers which divide a_0.*

PROOF. Let λ be a rational root and write $\lambda = c/d$ where c, d are coprime integers with $d > 0$. Thus

$$a_0 + a_1\frac{c}{d} + \cdots + a_{n-1}\frac{c^{n-1}}{d^{n-1}} + \frac{c^n}{d^n} = 0. \tag{12}$$

Multiplying by d^n and rearranging we have

$$d(-a_0 d^{n-1} - a_1 c d^{n-2} - \cdots - a_{n-1}c^{n-1}) = c^n.$$

Thus $d \mid c^n$. We argue that $d = 1$. Suppose $d > 1$ and let p be a prime factor of d. Then $p \mid d$ so $p \mid c^n$ and hence $p \mid c$, contradicting the fact that c and d are coprime. Hence $d = 1$. Therefore $\lambda = c \in \mathbb{Z}$. Moreover, by (12) we have

$$c(-a_1 - a_2 c - \cdots - a_{n-1}c^{n-2}) = a_0,$$

hence $c \mid a_0$. In otherwords, any rational root of f must be an integer dividing a_0. □

From Gauss' Theorem it is easy to deduce the following generalization of the irrationality of $\sqrt{2}$.

Corollary 6.3. *Let $n > 1$ be a positive integer. Suppose that d is a positive integer that is not an n-th power. Then $\sqrt[n]{d}$ is irrational.*

PROOF. Let $f(x) = x^n - d$. Suppose $\sqrt[n]{d}$ is rational. By Gauss' Theorem, $\sqrt[n]{d}$ is an integer, say $\sqrt[n]{d} = c \in \mathbb{Z}$. Then $d = c^n$ is a square, giving a contradiction. □

2. The irrationality of e

So far the only irrational numbers we've seen are roots of polynomials. It is natural to wonder about the irrationality of naturally occuring numbers such as $e = \exp(1)$. In fact Euler proved that e is irrational.

Theorem 6.4. *(Euler) $e = \exp(1)$ is irrational.*

PROOF. The proof starts with the familiar power series expansion

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Thus

$$e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots.$$

Suppose that e is rational, and write $e = a/b$ where a, b are positive coprime integers. Now

$$\begin{aligned}(b-1)!a = b!e &= b!\left(1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots\right) \\ &= b!\left(1 + 1 + \frac{1}{2!} + \cdots + \frac{1}{b!}\right) + b!\left(\frac{1}{(b+1)!} + \frac{1}{(b+2)!} + \cdots\right).\end{aligned}$$

Write

$$\alpha = b!\left(1 + 1 + \frac{1}{2!} + \cdots + \frac{1}{b!}\right)$$

and note that α is an integer. Thus $(b-1)!a - \alpha$ is an integer. Write $\beta = (b-1)!a - \alpha \in \mathbb{Z}$. We see that

$$\beta = b!\left(\frac{1}{(b+1)!} + \frac{1}{(b+2)!} + \cdots\right).$$

It is clear from this that $\beta > 0$. However,

$$\begin{aligned}
\beta &= \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+2)(b+3)} + \cdots \\
&= \frac{1}{b+1}\left(1 + \frac{1}{b+2} + \frac{1}{(b+2)(b+3)} + \frac{1}{(b+2)(b+3)(b+4)} + \cdots\right) \\
&< \frac{1}{b+1}\left(1 + \frac{1}{b+1} + \frac{1}{(b+1)^2} + \frac{1}{(b+1)^3} + \cdots\right) \\
&= \frac{1}{(b+1)}\left(\frac{1}{1-\frac{1}{b+1}}\right) \qquad \text{(by the formula for geometric series)} \\
&= \frac{1}{b} < 1.
\end{aligned}$$

Summing up, β is an integer and $0 < \beta < 1$. This is impossible! Hence e is irrational. □

You can see from the proof why Euler was such a hero.

3. What about Transcendental Numbers?

Definition. A number $\alpha \in \mathbb{C}$ is *algebraic* if there is some $n \geq 1$ and integers $a_0, a_1, \ldots, a_n$, not all zero, such that α is a root of the polynomial

$$a_0 + a_1 x + \cdots + a_n x^n.$$

A number $\alpha \in \mathbb{C}$ is *transcendental* if it is not algebraic.

It is easy to come up with examples of algebraic numbers.

Example 3.1. 1 is algebraic because it is a root of $x - 1$ which has integer coefficients. The number $-5/17$ is algebraic because it is a root of $17x + 5$ which has integer coefficients. Also $\sqrt{2}$ is algebraic because it is a root of $x^2 - 2$ which has integer coefficients.

By now you must have formulated and proved in your head the following lemma.

Lemma 6.5. *Every rational number is algebraic.*

3.1. Hocus Pocus. It is not so easy to give examples of transcendental numbers. But there is a magic way to show that there are plenty of transcendental numbers. If you remember your Foundations, it isn't hard to show that algebraic numbers are countable, whilst you know that real and complex numbers are uncountable. This shows that 'almost all' numbers are transcendental. If you're a set-theorist then you'd satisfied with this; no need for examples. But if you're a normal person, you'd no doubt be dying to see one.

3.2. More on algebraic numbers.

Definition. Let α be an algebraic number. The *degree* of α is the smallest positive integer d such that there is a polynomial $f \in \mathbb{Z}[x]$ of degree d with $f(\alpha) = 0$.

Lemma 6.6. *Let α be an algebraic number of degree d. Then it is a root of an irreducible polynomial $f \in \mathbb{Z}[x]$ with degree d.*

PROOF. All we're adding to the definition is the specification that f is irreducible. If it isn't, then we can write $f(x) = g(x)h(x)$ with $g(x)$, $h(x) \in \mathbb{Z}[x]$ having degree smaller than d and either $g(\alpha) = 0$ or $h(\alpha) = 0$. This contradicts the mimimality of d. □

Theorem 6.7. *(Liouville's Theorem) Let $\alpha \in \mathbb{R}$ be an algebraic number of degree d. Then there is a constant $C > 0$, depending on α, so that for all rational numbers p/q,*

$$\textit{either} \quad \alpha = \frac{p}{q}, \qquad \textit{or} \quad \left|\frac{p}{q} - \alpha\right| \geq \frac{C}{q^d}.$$

PROOF. We know that $f(\alpha) = 0$ for some irreducible polynomial $f \in \mathbb{Z}[x]$ of degree $d \geq 1$. Write

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d.$$

Then

$$\begin{aligned} f\left(\frac{p}{q}\right) &= a_0 + a_1 \frac{p}{q} + \cdots a_d \frac{p^d}{q^d} \\ &= \frac{N}{q^d} \end{aligned}$$

where $N = a_0 q^d + a_1 p q^{d-1} + \cdots + a_d p^d$. Clearly $N \in \mathbb{Z}$. Can $N = 0$? Let's suppose it is. Then $f(p/q) = 0$, so $qx - p$ is a factor of the irreducible polynomial f. Hence f has degree 1 and is equal to $qx - p$ up to multiplication by a non-zero constant. By $f(\alpha) = 0$. Hence $q\alpha - p = 0$ so $\alpha = p/q$.

What happens if $\alpha \neq p/q$. Well, for a start $N \neq 0$. As N is an integer, $|N| \geq 1$. So

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}.$$

Now we note that

$$\begin{aligned} \frac{1}{q^d} &\le \left| f\left(\frac{p}{q}\right) \right| \\ &= \left| f(\alpha) - f\left(\frac{p}{q}\right) \right| \qquad \text{since } f(\alpha) = 0 \\ &= f'(\eta) \left| \alpha - \frac{p}{q} \right|, \end{aligned} \tag{13}$$

by the Mean Value Theorem, where η is some number between α and p/q.

Let

$$C' = \sup \left\{ |f'(t)| : \alpha - 1 \le t \le \alpha + 1. \right\}.$$

Let

$$C = \min \left\{ 1, \frac{1}{C'} \right\}.$$

We shall show that

$$\left| \alpha - \frac{p}{q} \right| \ge \frac{C}{q^d},$$

which proves the theorem. If $\alpha - 1 \le p/q \le \alpha + 1$, then η is also in the interval $[\alpha - 1, \alpha + 1]$. So $f'(\eta) \le C'$. Hence by (13),

$$\left| \alpha - \frac{p}{q} \right| \ge \frac{1}{C'} \frac{1}{q^d} \ge \frac{C}{q^d},$$

which is what we want. Now all we have to worry about is the case when p/q is outside the interval $[\alpha - 1, \alpha + 1]$. But this is easy:

$$\left| \alpha - \frac{p}{q} \right| \ge 1 \ge \frac{1}{q^d} \ge \frac{C}{q^d},$$

which completes the proof. □

3.3. Transcendentals at last. Now at last we can see some transcendental numbers. Joseph Liouville was the first to construct them in 1844. Here is his example.

Corollary 6.8. *Let*

$$\alpha = \sum_{i=0}^{\infty} \frac{1}{10^{i!}}.$$

Then α is transcendental.

PROOF. We do this using contradiction. Suppose that α is algebraic of degree d. Let $n \geq 1$ and let $q = 10^{n!}$. Let

$$p = q \cdot \sum_{i=0}^{n} \frac{1}{10^{i!}}.$$

Note that p, q are positive integers, and that

$$\begin{aligned}
0 &< \alpha - \frac{p}{q} \\
&= \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+2)!}} + \cdots \\
&= \frac{1}{10^{(n+1)!}} \left(1 + \frac{1}{10^{(n+2)!-(n+1)!}} + + \frac{1}{10^{(n+3)!-(n+1)!}} + \cdots \right) \\
&< \frac{1}{10^{(n+1)!}} \left(1 + \frac{1}{10} + \frac{1}{10^2} + \cdots \right) \\
&= \frac{10}{9 \cdot 10^{(n+1)!}}.
\end{aligned}$$

By the first inequality $\alpha \neq p/q$. So we know by Liouville's Theorem that, for some positive constant C

$$\frac{10}{9 \cdot 10^{(n+1)!}} > \frac{C}{q^d} = \frac{C}{10^{d \cdot n!}}.$$

Hence

$$\frac{10}{9C} > 10^{(n+1)!-d \cdot n!}.$$

Note here that d and C are fixed, where as we can choose n as large as we like. Making n very large gives a contradiction. □

Perhaps you're not impressed. Maybe you think that Lioville's number is a little artificial? What about naturally occuring numbers like e and π? Are they transcendental? Perhaps you should check out Wikipedia.

APPENDIX X

Last Year's Exam

THE UNIVERSITY OF WARWICK

THIRD YEAR EXAMINATION : April 2010

TOPICS IN NUMBER THEORY

Time Allowed: **3 hours**

Read carefully the instructions on the answer book and make sure that the particulars required are entered on each answer book.

Calculators are not needed and are not permitted in this examination.

ANSWER 4 QUESTIONS.

If you have answered more than the required 4 questions in this examination, you will only be given credit for your 4 best answers. The numbers in the margin indicate approximately how many marks are available for each part of a question.

---

1) Let p be a prime.

a) What does it mean for an integer g to have order d modulo p? **[2]**

b) Show that if g has order d modulo p and if $g^m \equiv 1 \pmod{p}$ then $d \mid m$. **[6]**

c) Suppose g_1 and g_2 respectively have orders d_1, d_2 modulo p. Suppose moreover that $\gcd(d_1, d_2) = 1$. Show that $g_1 g_2$ has order $d_1 d_2$ modulo p. **[6]**

d) What does it mean for g to be a primitive root modulo p? **[2]**

e) Show that p must have a primitive root. You may assume that if q^e is a prime power dividing $p-1$ then $x^{q^e} \equiv 1 \pmod{p}$ has precisely q^e incongruent solutions modulo p. **[6]**

f) Find a primitive root for 149. You may use the following observations: **[3]**

$149 = 2^2 \times 37 + 1$, $\quad 5^{37} \equiv 44^4 \equiv 1 \pmod{149}$, $\quad 44^2 \not\equiv 1 \pmod{149}$.

2)

a) Let a be an integer and p an odd prime. Show that

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

You may assume standard facts about primitive roots. **[7]**

b) State without proof the two supplements to the law of quadratic reciprocity. **[4]**

c) Let x be an even integer. Show that every prime divisor p of $x^4 + 1$ satisfies

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1,$$

and hence $p \equiv 1 \pmod{8}$. **Hint:** You might find it helpful to observe that $x^4 + 1 = (x^2 + 1)^2 - 2x^2$. **[7]**

d) Deduce that there are infinitely many primes $p \equiv 1 \pmod{8}$. **[7]**

3)

a) State Blichfeldt's Theorem and Minkowski's Theorem. **[6]**

b) Give a proof of Minkowski's Theorem assuming Blichfeldt's Theorem. **[6]**

c) Let a, $b > 0$. Show that the area of the ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} < 1$$

is πab. You may assume the formula for the area of a circle. **[6]**

d) Suppose λ and N are coprime positive integers satisfying

$$\lambda^2 \equiv 2 \pmod{N}.$$

Show that there are integers x, y such that **[7]**

$$x^2 - 2y^2 = \pm N.$$

Hint: In Minkowski's Theorem, take the convex symmetric set to be

$$C = \{(x, y) \in \mathbb{R}^2 : x^2 + 2y^2 < 2N\}.$$

4)

a) Let $f(X) \in \mathbb{Z}[X]$, $a \in \mathbb{Z}$ and n a positive integer. Show that $f^{(n)}(a)/n!$ is an integer. **[4]**

b) Let $f(X) \in \mathbb{Z}[X]$. Let p be a prime and $m \geq 1$. Suppose $a \in \mathbb{Z}$ satisfies

$$f(a) \equiv 0 \pmod{p^m}, \qquad f'(a) \not\equiv 0 \pmod{p}.$$

Show that there exists some $b \in \mathbb{Z}$ such that **[8]**

$$b \equiv a \pmod{p^m}, \qquad f(b) \equiv 0 \pmod{p^{m+1}}.$$

c) Solve the following simultaneous system of congruences **[4]**

$$x^2 \equiv 3 \pmod{5^3}, \qquad x^2 \equiv 6 \pmod{7}.$$

d) Solve the following simultaneous system of congruences **[9]**

$$y^3 \equiv 3 \pmod{5^3}, \qquad y \equiv 1 \pmod{4}.$$

5) Let p be a prime.

a) Let α be a rational number. Define $\mathrm{ord}_p(\alpha)$ and $|\alpha|_p$. **[2]**

b) Let α, β be rational numbers. Prove that

$$\mathrm{ord}_p(\alpha+\beta) \geq \min\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\},$$

and **[8]**

$$|\alpha+\beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}.$$

c) Prove that the series of rational numbers $\sum_{n=1}^{\infty} a_n$ converges in $\mathbb{Q}_p$ if and only if $\lim_{n\to\infty}|a_n|_p = 0$. You may assume that a sequence converges in $\mathbb{Q}_p$ if and only if it is p-adically Cauchy. **[7]**

d) State—with proof—for which primes p do the following series converge in $\mathbb{Q}_p$?

(i) $1 + (21/2)^2 + (21/2)^4 + (21/2)^8 + \cdots$. **[4]**

(ii) $1^1 + 2^2 + 3^3 + 4^4 + \cdots$. **[4]**

APPENDIX Y

Mathematical Pornography

After I wrote the footnote on page 63 in last year's lecture notes, I was inundated with requests for more explicit examples of mathematical pornography. Being an obliging and generous person, I'll share with you couple of my favourites. They are due to Leonhard Euler, the greatest mathematician (and mathematical pornographer) of his age. Needless to say the material in this appendix is **not examinable** and is merely for your own personal gratification.

Euler defines

$$e^x = \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n$$

and wants to deduce the well-known power series expansion for e^x. So he introduces *infinite* numbers, and reasons that if i is an infinite number then obviously

$$\frac{i}{i} = 1, \qquad \frac{i(i-1)}{i^2} = 1, \qquad \frac{i(i-1)(i-2)}{i^3} = 1, \ldots.$$

Thus

$$\begin{aligned} e^x &= \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n \\ &= \left(1 + \frac{x}{i}\right)^i \qquad i \text{ infinite} \\ &= 1 + i\frac{x}{i} + \frac{i(i-1)}{2!}\frac{x^2}{i^2} + \cdots \qquad \text{using the binomial theorem} \\ &= 1 + x + \frac{x^2}{2!} + \cdots \end{aligned}$$

Next Euler wants to derive the power series expansion for $\log(1+t)$. To do this he defines the *infinitesimal* $\epsilon = 1/i$. This infinitesimal is so small that

$$\epsilon^2 = \epsilon^3 = \cdots = 0. \tag{14}$$

Now to get the power series expansion for $\log(1+t)$, write $x = 1 + t$, and $y = \log x$. Thus

$$x = e^y = \left(1 + \frac{y}{i}\right)^i.$$

Hence

$$x^\epsilon = x^{1/i} = 1 + \frac{y}{i} = 1 + \epsilon y.$$

Rearranging we get

$$\log(1+t) = \log x = y = \frac{1}{\epsilon}(x^\epsilon - 1) = \frac{1}{\epsilon}\left(-1 + (1+t)^\epsilon\right). \tag{15}$$

Now by the Binomail Theorem

$$(1+t)^\epsilon = 1+\epsilon t+\frac{\epsilon(\epsilon-1)}{2!}t^2+\frac{\epsilon(\epsilon-1)(\epsilon-2)}{3!}t^3+\frac{\epsilon(\epsilon-1)(\epsilon-2)(\epsilon-3)}{4!}t^4+\cdots$$

However, by (14) we can eliminate all higher powers of ϵ. Thus

$$\begin{aligned}(1+t)^\epsilon &= 1 + \epsilon t + \frac{-\epsilon}{2!}t^2 + \frac{2!\epsilon}{3!}t^3 + \frac{-3!\epsilon}{4!}t^4 + \cdots \\ &= 1 + \epsilon t - \frac{\epsilon}{2}t^2 + \frac{\epsilon}{3}t^3 - \frac{\epsilon}{4}t^4 + \cdots\end{aligned}$$

Substituting into (15) we obtain

$$\begin{aligned}\log(1+t) &= \frac{1}{\epsilon}\left(\epsilon t - \frac{\epsilon}{2}t^2 + \frac{\epsilon}{3}t^3 - \frac{\epsilon}{4}t^4 + \cdots\right) \\ &= t - \frac{t^2}{2} + \frac{t^3}{3} - \frac{t^4}{4} + \cdots\end{aligned}$$

1. An Integral Equation

Here is an beautiful example I found on `mathoverflow.org`. Let "$\int = \int_0^x$". We want to solve the integral equation

$$f - \int f = 1.$$

Factoring out the f we have

$$\left(1 - \int\right) f = 1.$$

Hence

$$\begin{aligned}f &= \left(1 - \int\right)^{-1} 1 \\ &= \left(1 + \int + \iint + \iiint + \cdots\right) 1 \\ &= 1 + \int_0^x 1 + \int_0^x \int_0^x 1 + \int_0^x \int_0^x \int_0^x 1 + \cdots \\ &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \\ &= e^x.\end{aligned}$$