Number Theory

Martina Tscheckl

November 8, 2015

Please send feedback to martina@tscheckl.eu.

Contents

Organizatorial stuff

Dates (in TUGrazOnline):

Mon	14:15–15:45	C208	Exercises (starting 19.10. first exercise class)
Tue	14:15–15:45	C307	Lecture (starting 20.10. first (real) lecture)
Wed	08:15–09:45	C208	Lecture

From now until 15.12. lectures by Martin Widmer. Then C. Frei.
End: oral exams
Exercises: Find details on website of the instructor Dijana Kreso. math.tugraz.at/~kreso

0 Basics

$$\mathbb{N} = \{1, 2, \dots\} \tag{1}$$
$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} \tag{2}$$
$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \tag{3}$$

0.1 Divisibility

Definition 0.1.1. *Let $a, b \in \mathbb{Z}$. a divides b (written $a \mid b$) if $\exists q \in \mathbb{Z} : b = qa$. Some properties: Let $a, b, c \in \mathbb{Z}$. Then the following statements hold:*

$$a \mid b \Rightarrow ac \mid bc \tag{4}$$
$$a \mid b \wedge b \mid c \Rightarrow a \mid c \tag{5}$$
$$a \mid b \wedge b \mid a \Leftrightarrow a = b \tag{6}$$
$$a \mid b \wedge a \mid c \Rightarrow a \mid (b + c) \tag{7}$$

Definition 0.1.2 (Remainder)**.** *Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Then there are unique $q, r \in \mathbb{Z}$ such that*

$$a = qb + r \text{ and } 0 \le r < b.$$

Remark 1. *1. $b \mid a \Leftrightarrow r = 0$*

2. $q = \lfloor \frac{a}{b} \rfloor$ (largest integer $\le \frac{q}{b}$)

3. we will somtimes write: $a \mod b := c$

Definition 0.1.3. *Let $a_1, a_2, \dots, a_n, d \in \mathbb{Z}$. d is a greatest common divisor (gcd) of $a_1, \dots, a_n$ if $d \mid a_i$ $\forall 1 \le i \le n$, and for every $e \in \mathbb{Z}$ with $e \mid a_i$ $\forall 1 \le i \le n$, $e \mid d$.*

Remark 2. *1. a $\gcd$ of $a_1, \dots, a_n$ is unique up to sign*

2. we write $d = \gcd(a_1, \dots, a_n)$ if d is a $\gcd$ of $a_1, \dots, a_n$

3. for $a_1, \dots, a_n \in \mathbb{Z}$, a $\gcd$ exists and can be written as a linear combination of $a_1, \dots, a_n$, i.e., $\exists x_1, \dots, x_n \in \mathbb{Z}$ such that

$$\gcd(a_1, \dots, a_n) = x_1 a_1 + \dots + x_n a_n$$

4. $\gcd(a_1, \dots, a_n) = \gcd(\gcd(a_1, \dots, a_{n-1}), a_n)$

5. if $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

6. let $a' := \frac{a}{\gcd(a,b)}$, $b' = \frac{b}{\gcd(a,b)}$. Then $\gcd(a', b') = 1$

The algorithm is correct, since $\gcd(a, b) = \gcd(b, a \mod b)$.
The algorithm terminates because b decreases in each step.
The algorithm is fast: $(\mathcal{O}(\log b))$

Hier verwendest du :=, sonst aber nur =, evtl. einheitlich machen für alle Definitionen?

The Euclidean algorithm also allows us to find x, y such that $\gcd(a, b) = ax + by$ by doing all computations backwards.

sollte ausgebessert werden, 1. $O(logn)$ steps, 2. stimmt nur wenn $|r| \le b/2$

Algorithm 1 Compute the gcd of two integers: Euclidean algorithm

Given: $a, b \in \mathbb{Z}$. $|a| \geq |b|$
Find: $a := \gcd(a, b)$

replace a by $|a|$, b by $|b|$
while $b \neq 0$ **do**
  write $a = qb + r$, $0 \leq r < b$
  $a := b$
  $b := r$
end while
return a

Example 1. $\gcd(56, 22) = ?$

$$\begin{aligned}
a &= 56, b = 22 \\
56 &= 2 \cdot 22 + 12 \\
a &= 22, b = 12 \neq 0 \\
22 &= 1 \cdot 12 + 10 \\
a &= 12, b = 10 \neq 0 \\
12 &= 1 \cdot 10 + 2 \\
a &= 10, b = 2 \neq 0 \\
10 &= 5 \cdot 2 + 0 \\
a &= 2, b = 0 && \Rightarrow \gcd(56, 22) = 2
\end{aligned}$$

Doing the computations backwards:

$$2 = 12 - 10 = 12 - (22 - 12) = -22 + 2 \cdot 12 = -22 + 2(56 - 2 \cdot 22) = 2 \cdot 56 - 5 \cdot 22$$
$$x = 2, y = -5$$

Application (linear diophantine equations)**.** *Let* $a, b, c \in \mathbb{Z}$*,* $a, b, c \neq 0$*. Find all* $(x, y) \in \mathbb{Z}^2$ *which satisfy*

$$ax + by = c. \tag{8}$$

Existence of solution let $d = \gcd(a, b)$.

$$(d \mid a \Rightarrow d \mid xa) \wedge (d \mid b \Rightarrow d \mid yb)$$
$$\Rightarrow d \mid xa + yb = c$$
$$\Rightarrow eq. (8)$$

can have solutions only if $d \mid c$.

Solution in case $d = 1$ Let $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = 1$ using the Euclidean algorithm. Then from $acx_0 + bcy_0 = c$ the solution (cx_0, cy_0) of (eq. (8)) follows: for all $n \in \mathbb{Z} : (x, y) := (cx_0 + nb, cy_0 + na)$ is a solution.

Indeed,

$$ax + by = acx_0 + anb + bcy_0 - bna = c \qquad \checkmark$$

These (x,y) are all solutions: let (x,y) be a solution. Then

$$
\begin{aligned}
ax + by &= c \\
acx_0 + bcy_0 &= c \\
\Rightarrow a(x - cx_0) &= b(cy_0 - y)
\end{aligned}
$$

$$
\begin{gathered}
\gcd(a,b) = 1 \;\Rightarrow\; b \mid x - cx_0 \;\Rightarrow\; x = cx_0 + nb, n \in \mathbb{Z} \\
\Rightarrow\; a \mid cy_0 - y \;\Rightarrow\; y = cy_0 + ma, m \in \mathbb{Z} \\
c = ax + by = acx_0 + anb + bcy_0 + bma \\
= c + (n+m)ab \Rightarrow (n+m)ab = 0 \Rightarrow m = -n
\end{gathered}
$$

Solutions in the general case Assume $d = \gcd(a,b)$ and $d \mid c$, let

$$a' = \frac{a}{d} \qquad b' = \frac{b}{d} \qquad c' := \frac{c}{d}$$

Then $\gcd(a',b') = 1$ and the solution to (eq. (8)) is exactly the solution of $a'x + b'y = c'$.

0.2 Primes

1. Beistriche für bessere Lesbarkeit
2. faustregel, vor und nach "i.e." gehört eigentlich beistrich

Definition 0.2.1. *$p \in \mathbb{N}$, $p > 1$ is a* prime number *if the only positive divisors of p are 1 and p, i.e., $a \in \mathbb{N}$, $a \mid p \Rightarrow a \in \{1,p\}$. $\mathbb{P} := \{primes\} \subset \mathbb{N}, \mathbb{P} = \{2,3,5,7,11,13,\dots\}$. p prime and $p \mid ab \Rightarrow p \mid a$ or $p \mid b$*

Theorem 0.2.2 (Fundamental theorem of arithmetic)**.** *Every $n \in \mathbb{N}$ can be written uniquely (up to reordering) as a product of primes. i.e. there are distinct primes $p_1,\dots,p_l$, and $\alpha_1,\dots,\alpha_l \in \mathbb{N}$ such that $n = p_1^{\alpha_1}\dots p_l^{\alpha_l}$*

Sketch.

Existence let $p_0 > 1$ be the smallest divisor > 1 of n. Then p_0 is prime. $n = p_0 n_0$, induction ✓

Uniqueness let $p_1 \dots p_m = q_1 \dots q_l = n$, p_i, q_j primes. $p_1 \mid q_1 \dots q_l \Rightarrow \exists i : p_1 \mid q_i$, both prime $\Rightarrow p_1 = q_i$, wlog: $i = 1$. $p_1 \dots p_m = q_1 \dots q_l$, induction ✓

□

Theorem 0.2.3 (Euclid)**.** *There are ∞-many primes.*

Proof. Given primes $p_1,\dots,p_n \in \mathbb{P}$. We construct one more prime

$$N := p_1 \cdot \dots \cdot p_n + 1.$$

Assume P is a prime factor of N. If $P \in \{p_1,\dots,p_n\}$ then $P \mid N$ and $P \mid p_1 \dots p_n \Rightarrow P \mid 1$ ↯ □

Remark 3 (prime factors and gcds)**.** *Let $a_1,\dots,a_n \in \mathbb{Z}$, write*

$$a_i = \prod_{p \in \mathbb{P}} p^{\alpha_{p,i}},\ \alpha_{p,i} \in \mathbb{N}_0,$$

almost all $a_i = 0$, then

$$\gcd(a_1,\dots,a_n) = \prod_{p \in \mathbb{P}} p^{\min_{1 \le i \le n}\{\alpha_{p,i}\}}$$

0.3 Congruences

All rings are commutative with 1.

Definition 0.3.1. *Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Then a* is congruent to $b \pmod{n}$, $a \equiv b \pmod{n}$, *if $n \mid a - b$. We write $\bar{a} = [a]_n := \{b \in \mathbb{Z} : b \equiv a(\mod n)\}$*

Remark 4. 1. *Congruence* $\bmod n$ *is an* equivalence relation

2. *$\bar{0}, \bar{1}, \dots, \overline{n-1}$ is a partition of $\mathbb{Z}$.*

3. *if $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, then $-a \equiv -b \pmod{n}$, $a \overset{+}{\underset{-}{\cdot}} d \pmod{n}$.*

Definition 0.3.2. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n := \{[a]_n : a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ *residue class ring modulo n*

Remark 5. *$\mathbb{Z}_n$ is a ring with operation $\bar{a} \overset{+}{\underset{-}{\cdot}} \bar{b} := \overline{a \overset{+}{\underset{-}{\cdot}} b}$ (well defined due to item 3 of Remark 4) $\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n : \exists \bar{b} \in \mathbb{Z}_n : \bar{a}\bar{b} = \bar{1}\}$ ... group of units* $\bmod n$

Lemma 0.3.3. *Let $a \in \mathbb{Z}$. Then $\bar{a} \in \mathbb{Z}_n^\times \Leftrightarrow$* $\gcd(a, n) = 1$.

Proof.

"$\Rightarrow$" $\bar{a}\bar{b} = \bar{1} \Leftrightarrow ab \equiv 1 \pmod{n} \Leftrightarrow n \mid ab - 1$
$\Rightarrow$ no prime factor of n divides a
$\Rightarrow \gcd(a, n) = 1$.

"$\Leftarrow$" $1 = \gcd(a, n) = ax + ny \Rightarrow \bar{1} = \bar{a}\bar{x}$

□

Remark 6. *The inverse of $\bar{a}$ can be computed by the Euclidean algorithm.*

Example 2 (Simultaneous congruences). *Find $x \in \mathbb{Z}$ such that*

$$x \equiv 2 \pmod{3} \tag{9}$$
$$x \equiv 1 \pmod{5} \tag{10}$$
$$x \equiv 0 \pmod{7} \tag{11}$$

Theorem 0.3.4 (Chinese remainder theorem (CRT)). *Let*

$$n_1, \dots, n_l \in \mathbb{N} \text{ subject to } \gcd(n_i, n_j) = 1 \ \forall i \neq j$$

$$x_1, \dots, x_l \in \mathbb{Z}.$$

Then

$$\exists x \in \mathbb{Z} \text{ such that } x \equiv x_i \pmod{n_i} \ \forall 1 \leq i \leq l$$

where x is unique modulo $n_1 \cdot \dots \cdot n_l$.

Proof. How to compute x? For $i \in \{1, \dots, l\}$, let

$$N_i := \prod_{j \neq i} n_j = n_1 \dots n_{i-1} n_{n+1} \dots n_l$$

and let

$$N := \prod_i n_i = n_1 N_1 = n_2 N_2 = \dots = n_l N_l$$

because $\gcd(n_i, N_i) = 1 \Rightarrow N_i$ in invertible modn_i. Let

$$m_i N_i \equiv 1 \pmod{n_i}$$

and let

$$x := N_1 m_1 x_1 + \cdots + N_l m_l x_l.$$

We have $N_i m_i x_i \equiv 0 \pmod{n_j, j \neq i}$ □

Example 3.

$$n_1 = 3, \qquad n_2 = 5, \qquad n_3 = 7$$

$$x_1 = 2, \qquad x_2 = 1, \qquad x_3 = 0$$

$$N_1 = 35, \qquad N_2 = 21, \qquad N_3 = ?$$

$$\overline{m}_1 = \overline{35}^{-1} \pmod 3 = \overline{2}^{-1} \pmod 3 = \overline{2} \pmod 3 \Rightarrow m_1 = 2$$

$$\overline{m}_2 = \overline{21}^{-1} \pmod 5 = \overline{1}^{-1} \pmod 5 = \overline{1} \pmod 5 \Rightarrow m_2 = 1$$

$$\begin{aligned} x &= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 1 + 0 \\ &= 140 + 21 \\ &= 161 \\ &\equiv 56 \pmod{105} \end{aligned}$$

Example 4 (more abstract CRT)**.** *Let $n_1, \dots, n_l \in \mathbb{N}$, with* $\gcd(n_i, n_j) = 1$ $\forall i \neq j$. *There is a ring isomorphism $f : \mathbb{Z}_{n_1 \dots n_l} \overset{\cong}{\mapsto} \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_l}$ that satisfies $f([a]_{n_1 \dots n_l}) = ([a]_{n_1}, \dots, [a]_{n_l})$ $\forall a \in \mathbb{Z}$. In particular: $\mathbb{Z}^\times_{n_1 \dots n_l} \cong \mathbb{Z}^\times_{n_1} \times \cdots \times \mathbb{Z}^\times_{n_l}$ (restrict f to $\mathbb{Z}^\times_{n_1 \dots n_l}$)*

0.4 Arithmetic functions

Definition 0.4.1. *$f : \mathbb{N} \to \mathbb{C}$ is an* arithmetic function. *f is* multiplicative *if $\forall m, n$ it holds that* $\gcd(m, n) = 1$. *We have $f(mn) = f(m)f(n)$. f is* completely multiplicative *if $\forall m, n : f(mn) = f(m)f(n)$. Let $f : \mathbb{N} \to \mathbb{C}$. Its* summatory function *is $S_f(n) := \sum_{d|n} f(d)$.*

Proof. If $\gcd(m, n) = 1$ and $d \mid mn$, then $\exists$ unique d_1, d_2 such that $d = d_1 \cdot d_2$ with $d_1 \mid m$, $d_2 \mid n$.

$$S_f(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = S_f(m) S_f(n)$$

□

Example 5.

$$\tau(n) := S_1(n) = \sum_{d|n} 1 \qquad \textit{\dots number of divisors of } n$$

$$\sigma(n) := S_{id}(n) = \sum_{d|n} d \qquad \textit{\dots divisor sum of } n$$

Definition 0.4.2. *The function $\phi(n) := |\mathbb{Z}_n^\times|$ is called* Euler's ϕ-function.

Remark 7. *1.* $\phi(n) = |\{0 \leq a < n : \gcd(a, n) = 1\}|$

2. ϕ *is multiplicative (CRT:* $\gcd(m,n) = 1$*.* $\mathbb{Z}_{nm}^{\times} \cong \mathbb{Z}_n^{\times} \times \mathbb{Z}_m^{\times}$*)*

3. $\phi(p) = p - 1$ *(*$\mathbb{Z}_p$ *is a field)*

Lemma 0.4.3. $\phi(p^n) = p^n - p^{n-1}$

Proof.

$$\begin{aligned}\phi(p^n) &= |\{0 \le a < p^n\}| - |\{0 \le a < p^n : \gcd(a, p^n) \ne 1\}| \\ &= p^n - |\{0 \le a < p^n : p|a\}| \\ &= p^n - p^{n-1}\end{aligned}$$

□

Proposition 0.4.4. *If* $n = p_1^{\alpha_1} \dots p_l^{\alpha_l}$ *with* $p_i \ne p_j$ *primes,* $\alpha_i \in \mathbb{N}$*. Then*

$$\phi(n) = \prod_{i=1}^{l} p_i^{\alpha_i}(1 - \frac{1}{p_i}) = n \prod_{p|n}(1 - \frac{1}{p})$$

Theorem 0.4.5 (Euler-Fermat)**.** *Then* $a^{\phi(n)} \equiv 1 \mod n$*. In particular:* $a^{p-1} \equiv 1 \mod p \ \forall p \nmid a$ *(little Fermat).*

Proof 1. Lagrange's Theorem, $G = \mathbb{Z}_n^{\times}, \bar{a} \in G \Rightarrow \bar{a}^{|G|} = \bar{1}, |G| = \phi(n)$. □

Proof 2. $\prod_{x \in \mathbb{Z}_n^{\times}} x = \prod_{x \in \mathbb{Z}_n^{\times}} (\bar{a}x) = \bar{a}^{\phi(n)} \prod_{x \in \mathbb{Z}_n^{\times}} x \Rightarrow a^{\phi(n)} \equiv 1 \mod n$ □

Definition 0.4.6. *The Möbius function* $\mu : \mathbb{N} \to \{-1, 0, +1\}$ *is defined as*

$$\mu(n) = \begin{cases} (-1)^l & n = p_1 \dots p_l, p_i \ne p_j, i \ne j, p_i \text{ primes} \\ 0 & \text{otherwise i.e. if } \exists p : p^2 \mid n \end{cases}$$

Remark 8.

1. $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, ...

2. μ *is* multiplicative

Lemma 0.4.7.

$$S_\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 0 \end{cases}$$

Proof.

$$S_\mu(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$$

By multiplicativity, it suffices to prove $S_\mu(p^n) = 0 \ \forall p, n$.

$$\begin{aligned}S_\mu(p^n) &= \sum_{d|p^n} \mu(d) \\ &= \sum_{i=0}^{n} \mu(p^i) \\ &= \mu(1) + \mu(p) + 0 + \dots + 0 \\ &= 0\end{aligned}$$

□

Theorem 0.4.8 (Möbius inversion formula)**.** *Let $f : \mathbb{N} \to \mathbb{C}$. Then*

$$f(n) = \sum_{d \mid n} \mu(d) S_f(\frac{n}{d}).$$

Proof.

$$\begin{aligned}\sum_{d \mid n} \mu(d) S_f\left(\frac{n}{d}\right) &= \sum_{d \mid n} \mu(d) \sum_{e \mid \frac{n}{d}} f(e) \\ &= \sum_{e \mid n} f(e) \sum_{\substack{d \mid n \\ s.t. e \mid \frac{n}{d}}} \mu(d)\end{aligned}$$

For the next step we use $d \mid n \wedge e \mid \dfrac{n}{d} \Leftrightarrow ed \mid n \Leftrightarrow e \mid n \wedge d \mid \dfrac{n}{e}$

$$\begin{aligned}&= \sum_{e \mid n} f(e) \sum_{d \mid \frac{n}{e}} \mu(d) \\ &= f(n)\end{aligned}$$

since $\displaystyle\sum_{d \mid \frac{n}{e}} \mu(d) = \begin{cases} 1 & \frac{n}{e} = 1 \\ 0 & \text{otherwise} \end{cases}$

□

0.5 Structure of $\mathbb{Z}_n^\times$

$$n = p_1^{\alpha_1} \dots p_l^{\alpha_l} \text{ with } p_i \neq p_j, i \neq j, \alpha_i \in \mathbb{N} \text{ where } p_i \text{ are primes}$$

From the CRT it follows that $\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{\alpha_1}}^\times \times \dots \times \mathbb{Z}_{p_l^{\alpha_l}}^\times$. So we only consider prime powers p^α, $p \in \mathbb{P}$, $\alpha \in \mathbb{N}$

0.5.1 Case 1: $\alpha = 1$

Theorem 0.5.1. *$\mathbb{Z}_p^\times$ is cyclic, i.e. $\mathbb{Z}_p^\times \cong \mathbb{Z}_{(p-1)}$*

Proof. Use structure theorem for finite abelian groups. If G is a finite abelian group then $\exists d_1, \dots d_l \in \mathbb{N}$ such that $1 < d_1 \mid d_2 \mid d_3 \mid \dots \mid d_l$, and $G \cong \mathbb{Z}_{d_1}^\times \times \dots \times \mathbb{Z}_{d_l}^\times$ thus, $\mathbb{Z}_p^\times \cong \mathbb{Z}_{d_1}^\times \times \dots \times \mathbb{Z}_{d_l}^\times$ (every element $x \in \mathbb{Z}_{d_1}^\times \times \dots \times \mathbb{Z}_{d_l}^\times$ satisfies $d_l x = 0 \Rightarrow$ every $x \in \mathbb{Z}_p^\times$ satisfies $x^{d_l} = 1$). $x^{d_l} - 1$ is a polynomial of degree d_l over the field $\mathbb{Z}_p \Rightarrow x^{d_l} - 1$ has $\leq d_l$ roots $\Rightarrow p - 1 \leq d_l$, but $p - 1 = d_1 \dots d_l \Rightarrow l = 1, p - 1 = d_l$ □

Remark 9. *The same proof shows: Let F be a field, $G \leq F^\times$, $|G| < \infty$. Then G is cyclic.*

0.5.2 Case 2: $\alpha \geq 2$; $p \geq 3$

Denote $|x|$ as the order of x in $\mathbb{Z}_{p^\alpha}^\times$; i.e. $|x| = \min\left\{l \in \mathbb{N} : x^l \equiv 1 \mod p^\alpha\right\}$

$\left|\mathbb{Z}_{p^\alpha}^\times\right| = \phi(p^\alpha) = p^{\alpha-1}(p-1)$, find $x, y \in \mathbb{Z}_{p^\alpha}^\times$ such that $|x| = p^{\alpha-1}$, $|y| = p - 1$ then $|xy| = |x||y| = p^{\alpha-1}(p-1)$, since $\gcd(|x|, |y|) = 1$

Lemma 0.5.2.

$$(1+p)^{p^{n-1}} \begin{cases} \equiv 1 & \mod p^n \\ \not\equiv 1 & \mod p^{n+1} \end{cases}$$

Proof. Proof by induction

$n = 1$ ✓

$n \to n+1$

$$\begin{aligned}(1+p)^{p^{n-1}} &= 1 + ap^n, p \nmid a\\ (1+p)^{p^n} &= (1+ap^n)^p\\ &= 1 + pap^n + \sum_{i=2}^{p-1}\binom{p}{i}(ap^n)^i + (ap^n)^p\end{aligned}$$

$$p^{np} \mid \bullet, \quad np \geq n+2, \quad (\text{or } p \geq 3), \quad p^{2n+1} \mid \bullet, \quad 2n+1 \geq n+2$$

$$p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}, 1 \leq i < p \Rightarrow (1+p)^{p^n} \equiv 1 + ap^{n+1} \pmod{p^{n+2}}, p \nmid a$$

□

2× Lemma: $x = 1+p$ satisfies $|x| = p^{\alpha-1}$, now find y.

1. $\exists z \in \mathbb{Z} : |\bar{z}| = p-1$ is $\mathbb{Z}_p^\times$
2. let $l := |E|$ is $\mathbb{Z}_{p^\alpha}^\times$
3. Then $p^\alpha \mid z^l - 1 \Rightarrow z^l \equiv 1 \mod p$
4. $\Rightarrow p-1 \mid l$.
5. Let $y := z^{\frac{l}{p-1}}$, then $|\bar{y}| = p-1$.

We have proven: Theorem: $\mathbb{Z}_{p^\alpha}^\times$ is cyclic, i.e. $\mathbb{Z}_{p^\alpha}^\times \cong \mathbb{Z}_{p^{\alpha-1}(p-1)}$, if $p \geq 3, \alpha \geq 1$.
$p = 2$: $\mathbb{Z}_{2^\alpha}^\times \cong \{0, \alpha = 1 \quad \mathbb{Z}_2, \alpha = 2 \quad \mathbb{Z}_2 \times \mathbb{Z}_{p^{\alpha-2}}, \alpha \geq 3\}$

Corollary 0.5.3. *Let $m \in \mathbb{N}$. Then $\mathbb{Z}_m^\times$ is cyclic iff m has one of the following forms:*

- $m = 2$
- $m = 4$
- $m = p^\alpha, p \geq 3, \alpha \in \mathbb{N}$
- $m = 2p^\alpha, p \geq 3, \alpha \in \mathbb{N}$

In these cases a generator of $\mathbb{Z}_m^\times$ is called *a primitive root modulo m.*

New Lecturer

Chapter 1:

1. Approximation to algebraic numbers; Wolfgang M. Schmidt, 1972 L'Ehseignement Mathématique
2. Lectures Notes in Mathematics 785; W.M.Schmidt, Springer
3. LNM 1467, W.M.S., Springer
4. For section 2 (continued fractions) he will strictly follow the lecture notes of MT421 of Professor James McKee

1 Diophantine Approximation

1.1 Dirichlet's Theorem

Let $\alpha \in \mathbb{R}$. As $\mathbb{Q}$ is dense in $\mathbb{R}$ any $\alpha \in \mathbb{R}$ can be approximated arbitrarily well, by rational numbers p/q ($p \in \mathbb{Z}, q \in \mathbb{N} = \{1, 2, 3, \dots\}$).
The question is how well can we approximate α in terms of the denominator q, e.g., is it true that for every $\alpha \in \mathbb{R}$ there esist infinitly many $p/q \in \mathbb{Q}$ $q \in \mathbb{N}$) such that $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$?

The answer is no!
Take $\alpha = r/s(s \in \mathbb{N})$ a rational number. Then

$$|\alpha - \frac{p}{q}| = |\frac{r}{s} - \frac{p}{q}| = |\frac{qr - ps}{sq}| \overset{\geq}{\text{provided}}\ \alpha \neq \frac{p}{q} \frac{1}{sq} > \frac{1}{q^2} \text{ provided } q > s.$$

This shows that we habe only finitly many solutions $p/q \in \mathbb{Q}$ for $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.

Theorem 1.1.1 (Dirichlet's Theorem)**.** *Suppose $\alpha, Q \in \mathbb{R}$ and $Q > 1$. Then $\exists p, p \in \mathbb{Z} s.t. 0 < q < Q$ and $|q\alpha - p| \leq \frac{1}{Q}$.*

Proof. for $\xi \in \mathbb{R}$ put $\{\xi\} = \xi - \lfloor \xi \rfloor$. so $0 \leq \{\xi\} \leq 1$. First suppose $Q \in \mathbb{Z}$. Consider the $Q + 1$ numbers $0, 1, \{\alpha\}, \{2\alpha\}, \dots, \{(Q-1)\alpha\}$.
They all lie in $[0, 1]$. We split it up in Q subintervals:

$$[0, 1] = [0, \frac{1}{Q}] \cup \left[\frac{1}{Q}, \frac{2}{Q}\right] \cup \dots \cup \left[\frac{Q-1}{Q}, 1\right]$$

By the pigeon hole principle two of the previous numbers lie in the same subinterval. Thus $\exists r_1, r_2, s_1, s_2 \in \mathbb{Z}$ with $0 \leq r_1 < r_2 \leq Q - 1$ such that $|(r_1\alpha - s_1) - (r_2\alpha - s_2)| \leq \frac{1}{Q}$. Then with $q = r_2 - r_1$ and $p = s_2 - s_1$ we get $|q\alpha - p| \leq \frac{1}{Q}$ and $0 < q < Q$. This proves the Theorem when $Q \in \mathbb{Z}$. Now suppose $Q \notin \mathbb{Z}$. We apply the previous with $Q' = \lfloor Q \rfloor + 1 > 1$. Hence, $\exists p, q \in \mathbb{Z}$ with $|q\alpha - p| \leq \frac{1}{Q'}$ and $0 < q < Q'$, and so $|q\alpha - p| \leq \frac{1}{Q}$ and $0 < q < Q$. □

Corollary 1.1.2. *Suppose $\alpha \in \mathbb{R}/\mathbb{Q}$. Then there exist infinitly many solutions $p/q \in \mathbb{Q}$ $(q \in \mathbb{N})$ of $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.*

Proof. Take $Q_1 > 1$. By Theorem 1.1.1 we get $(p_1, q_1) \in \mathbb{Z}^2$ with $0 < q_1 < Q$, and $|q_1\alpha - p_1| \leq \frac{1}{Q_1}$. Thus $|\alpha - \frac{p_1}{q_1}| \leq \frac{1}{q_1 Q_1} < \frac{1}{q_1^2}$
Next take $Q_2 = |\alpha - \frac{p_1}{q_1}|^{-1} + 1$. Then Thm 1.1.1 again yields $\frac{p_2}{q_2} \in \mathbb{Q}$ with $|\alpha - \frac{p_2}{q_2}| < \frac{1}{q^2}$ and $|\alpha - \frac{p_2}{q_2}| \leq \frac{1}{q_r Q_2} \leq \frac{1}{Q_2} < |\alpha - \frac{p_1}{q_1}|$. So $\frac{p_2}{q_2}$ is a better approx then $\frac{p_1}{q_1}$. Repeating this process indefinitely proves the claim. □

Theorem 1.1.3 (Pell-equation)**.** *Suppose $m \in \mathbb{N}$ is not a square (i.e., $m \neq n^2 \forall n \in \mathbb{Z}$).*
Then

$$x^2 - my^2 = 1$$

has infinitely many solutions $(x, y) \in \mathbb{Z}^2$.

Proof. Apply Corollary 1.1.2 with $\alpha = \sqrt{m}$. So $\alpha \in \mathbb{R}/\mathbb{Q}$. We get $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$ and $|\alpha + \frac{p}{q}| \overset{\leq}{triangleinequality} 1 + 2\alpha$. Thus

$$|p^2 - mq^2| = q^2|\alpha - \frac{p}{q}| \cdot |\alpha + \frac{p}{q}| < 1 + 2\sqrt{m}.$$

Hence, there exists $k \in \mathbb{Z}$ with $|k| < 1 + 2\sqrt{m}$. such that $p^2 - mq^2 = k$ for infinitly many $(p,q) \in \mathbb{Z}^2$ and p/q all distinct.
As m is not a square we have $k \neq 0$.

Let S be the set of solutions $(p,q) \in \mathbb{Z}^2$ of $p^2 - mq^2 = k$. The map $S \to (\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/k\mathbb{Z})$. This map is not injective ($S = \infty$) hence, $\exists (p_1, q_1) \neq (p_2, q_2)$ both in S such that $p_1 \cong p_2, q_1 \cong q_2 \pmod{k}$. (MOD)
Now we compute

$$\begin{aligned} k^2 &= (p_1^2 - mq_1^2)(p_2^2 - mq_2^2) && (12)\\ &= (p_1 + \sqrt{m}q_1)(p_2 - \sqrt{m}q_2) && (13)\\ &= (r - \sqrt{m}s)(r + \sqrt{m}s) = r^2 - ms^2 && (14)\\ \text{where } r &= p_1p_2 - mq_1q_2 && (15)\\ s &= p_1q_2 - q_1p_2 = \frac{1}{q_1q_2}(\frac{p_1}{q_1} - \frac{p_2}{q_2}) \neq 0. && (16) \end{aligned}$$

because of (MOD) $k \mid s$. Hence, $k^2 \mid s^2$. Thus $k^2 \mid r^2$. Hence $k \mid r$. Then $x = \frac{r}{k}$ and $y = \frac{s}{k}$ are both integers and

$$x^2 - my^2 = 1.$$

We have one solution but we need infinitely many! To this end we replace m by md^2 ($d \in \mathbb{N}$). The above argument yields a solution $(x', y') \in \mathbb{Z}^2$ of ${x'}^2 - md^2{y'}^2 = 1$. Thus, $(x,y) = (x', dy')$ is a new lolution of $x^2 - my^2 = 1$.
(Critical: $s \neq 0$) □

1.2 Continued fractions

Let $\theta \in \mathbb{R}$. Put $a_0 = \lfloor \theta \rfloor$. If $a_0 \neq \theta$ then we find $\theta_1 > 1$ such that

$$\theta = a_0 + \frac{1}{\theta_1}$$

and we put $a_1 = \lfloor \theta_1 \rfloor$. If $a_1 \neq \theta_1$ then we can find $\theta_2 > 1$ such that

$$\theta_1 = a_1 + \frac{1}{\theta_2}$$

and we put $a_= \lfloor \theta_2 \rfloor$. This process can be continued indefinitely, unless $a_n = \theta_n$ for some n. Note that a_0 can be zero or negative but $a_1, a_2, a_3, \ldots$ are all positive integers.
We call this process the *continued fraction process*. The a_i are called *partial quatients* of θ.

Example.

$$\theta = \frac{19}{11}$$

Then $a_0 = \lfloor\theta\rfloor = 1$
Now $\theta = \frac{19}{11} = a_0 + \frac{1}{\theta_1} = 1 + \frac{8}{11} = 1 + \frac{1}{\frac{11}{8}}$
So $\theta_1 = \frac{11}{8}$.
Thus $a_1 = \lfloor\theta_1\rfloor = 1$.
Now

$$\theta_1 = \frac{11}{8} = a_1 + \frac{1}{\theta_2} = 1 + \frac{3}{8} = 1 + \frac{1}{\frac{8}{3}}$$

Thus $\theta_2 = \frac{2}{3}$ *and* $a_2 = \lfloor\theta_2\rfloor = 2$
and so on...

If the continued fraction process terminates then we have

$$\theta = a_0 + \frac{1}{\theta_1} \tag{17}$$

$$= a_0 + \frac{1}{a_2 + \frac{1}{\theta_2}} \tag{18}$$

$$= a_0 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\theta_3}}} \qquad \ldots = a_0 + \frac{1}{a_1 + \frac{1}{\ddots}} \tag{19}$$

In this case we write $\theta = [a_0, \ldots, a_n]$.
We use the same notation when the a_i *are any real numbers, not necessarily integers.*
In particular

$$\theta = [a_0, \ldots, a_i, \theta_{i+1}]$$

where $a \le i < n$.

If the continued fraction process does not terminate then we write $\theta = [a_0, a_1, a_2, \ldots]$.
Note that in this case, for every $n \ge 0$, we have

$$\theta = [a_0, \ldots, a_n, \theta_{n+1}]$$

where $a_0, \ldots, a_n$ are integers but θ_{n+1} is not! For $n \ge 0$ we set

$$\frac{p_n}{q_n} = [a_0, \ldots, a_n]$$

where $\gcd(p_n, q_n) = 1$. We shall say that $\frac{p_n}{q_n}$ is the n-th convergent of θ. We will prove that $\frac{p_n}{q_n} \to \theta$ as $n \to \infty$. Next we shall see that $p_n, q_n > 0$ both satisfy the same simple recurrence relation $x_n = a_n x_{n-1} + x_{n-2}$ with different starting values.

Lemma 1.2.1. *Let* $a_0, a_1, a_2, \ldots$ *be a sequence of integers with* $a_i > 0$ $(i > 0)$.

Define p_n, q_n:

$$p_0 = a_0 \tag{20}$$
$$q_0 = 1 \tag{21}$$
$$p_1 = a_0 a_1 + 1 \tag{22}$$
$$q_1 = a_1 \tag{23}$$
$$p_n = a_n p_{n-1} + p_{n-2} \text{ for } n \geq 2 \tag{24}$$
$$q_n = a_n q_{n-1} + q_{n-2} \text{ for } n \geq 2. \tag{25}$$

Then:

1. $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$
2. $\gcd(p_n, q_n) = 1$
3. $p_n / q_n = [a_0, \dots, a_n]$
4. *If the a_i are produced by the continued fraction process for θ, then, for every $n \geq 1$, $\frac{p_n}{q_n}$ is the n-th convergent of θ and*

$$\theta = \frac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n-1}}$$

Proof. 1. We use induction on n. For $n = 0$ we note that

$$p_0 q_1 - p_1 q_0 = a_0 a_1 - a_0 a_1 - 1 = -1.$$

So the result holds for $n = 0$.
Now suppose result holds for $n = m - 1$.
consider case $n = m$. Using the recurrence relation, we set

$$p_m q_{m+1} - p_{m+1} q_m = p_m (a_m q_m + q_{m-1}) - q_m (a_m p_m + p_{m-1}) \tag{26}$$
$$= p_m q_{m-1} - p_{m-1} q_m = -(-1)^m = (-1)^{m+1}. \tag{27}$$

This proves claim for $n = m$.

2. Immedate from (a)

3. (c) + (d):
Remark about $\frac{p_n}{q_n}$ in (d) follows directly from (c). We prove the rest of (d), along with (c), using induction on n. Remember that (c) a priori does not require that the a_i are produced by the continued fraction process.
Consider base case $n = 1$. For (c) note that $\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = [a_0, a_1]$. For (d) we note that

$$\frac{p_1 \theta_2 + p_0}{q_1 \theta_2 + q_0} = \frac{(a_0 a_1 + 1)\theta_2 + a_0}{a_1 \theta_2 + 1} = a_0 + \frac{\theta_2}{a_1 \theta_2 + 1} = a_0 + \frac{1}{a_1 + \frac{1}{\theta_2}} = \theta$$

Next suppose (c) and (d) both hold for $n = m - 1$, and consider $n = m$. Using (d) with $n = m - 1$ we get

$$[a_0, \dots, a_m] = \frac{p_{m-1} a_m + p_{m-2}}{q_{m-1} a_m + q_{m-2}} = \frac{p_m}{q_m} \text{ by recurrence ralation.}$$

This proves (c) for $n = m$.
To prove (d) with $n = m$ we observe that

$$\theta = [a_0, \dots, a_m, \theta m + 1] \tag{28}$$

$$= [a_0, \dots, a_m + \frac{1}{\theta_{m+1}}] \tag{29}$$

$$(d) forn \overset{=}{=} m - 1 \frac{p_{m-1}(a_m + \frac{1}{\theta_{m+1}}) + p_{m-2}}{q_{m-1}(a_m \frac{1}{\theta_{m-1}}) + q_{m-2}} \tag{30}$$

$$\overset{=}{rec.rel} \frac{p_m + p_{m-1}(\frac{1}{\theta_{m+1}})}{q_m + q_{m-1}(\frac{1}{\theta_{m+1}})} \tag{31}$$

$$= \frac{p_m \theta_{m+1} + p_{m-1}}{q_m \theta_{m+1} + q_{m-1}} \tag{32}$$

which is (d) for $n = m$.

□

Next we deduce some properties of continued fraction convergents.

Theorem 1.2.2. *Let $\theta = [a_0, a_1, a_2, \dots]$ with convergents $\frac{p_n}{q_n}$. For (a) - (d) we assume that the continued fraction proves does not terminate*

1. *For all $n \in \mathbb{N}_0$, θ lies between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$.*
2. *For all $n \in \mathbb{N}_0 : |\theta - \frac{p_n}{q_n}| \leq \frac{1}{q_n q_{n+1}}$*
3. *For $n \geq 1$ we have $q_{n+2} \geq 2 \cdot q_n$*
4. *$\frac{p_n}{q_n} \to \theta$ as $n \to \infty$*
5. *The continued fraction process terminates if and only if θ is rational.*

Proof.

1. Note $\theta = [a_0, \dots, a_n, \theta_{n+1}] = [a_0, \dots, a_n + \frac{1}{\theta_{n+1}}$ where $0 < \frac{1}{\theta_{n+1}} < \frac{1}{a_{n+1}}$. So that θ lies between $[a_0, \dots, a_n]$ and $[a_0, \dots, a_n + \frac{1}{a_{n+1}}]$. But $[a_0, \dots, a_n + \frac{1}{a_{n+1}} = [a_0, \dots, a_{n+1}]$. This shows (a).
2. By (a) we have $|\theta - \frac{p_n}{q_n}| \leq |\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}| = |\frac{p_n q_{n+1} - p_{n+1} q_n}{q_n q_{n+1}}| \underset{=}{Lemma 1.2.1(a)} \frac{1}{q_n q_{n+1}}$
3. Follws from the fact that $a_i > 0 (i > 0)$ using Lemma 1.2.1.
4. Follows from (b) and (c)
5. Only if part is obvious.
Conversely suppose $\theta = \frac{a}{b} \in \mathbb{Q}$ but the process does *not* terminate. Taking n such that $q_n > b$ yields

$$|\theta - \frac{p_n}{q_n}| \frac{a}{b} \neq \frac{p_n}{q_n} \underset{\geq}{as q_n > b and} \gcd(p_n, q_n) = 1 \frac{1}{b q_n} > \frac{1}{q_n q_{n+1}}$$

contradicting (b).

□

Example. *Take* $\theta = \frac{16}{9}$*. We have* $a_0 = 1$*. Then* $\theta = 1 + \frac{7}{9}$ *so* $\theta_1 = \frac{9}{7}$ *and* $a_1 = 1$*. From* $\theta_1 = \frac{9}{7} = 1 + \frac{2}{7}$ *we get* $\theta_2 = \frac{7}{2}$ *and* $a_2 = 3$*. Form* $\theta_2 = \frac{7}{2} = 3 + \frac{1}{2}$ *we get* $\theta_3 = 2$ *and* $a_3 = 2$*. Thus* $\theta = \frac{16}{9} = [1, 1, 3, 2]$ *and the convergents are* $\frac{p_0}{q_0} = \frac{1}{1}$, $\frac{p_1}{q_1} = 1 + \frac{1}{1} = \frac{2}{1}$, $\frac{p_2}{q_2} = 1 + \frac{1}{1+\frac{1}{3}} = 1 + \frac{1}{\frac{4}{3}} = \frac{7}{4}$ *and* $\frac{p_3}{q_3} = \frac{16}{9}$*.*
Let's check some of the properties claimed.
$p_1q_2 + p_2q_1 = 2\cdot4 - 7\cdot1 = 1\checkmark$, $p_2q_3 - p_3q_2 = 7\cdot9 - 16\cdot4 = -1\checkmark$, $\frac{p_2\theta_3+p_1}{q_2\theta_3+q_1} = \frac{7\cdot2+2}{4\cdot2+1} = \frac{16}{9} = \theta\checkmark$

We now show that convergents give best-possible rational approximations.

Theorem 1.2.3. *Let* θ *be an irrational real number, and let* $\frac{p_n}{q_n}$ *be the convergents* $(n \geq 0)$ *with partial quotients* $a_n (n \geq 0)$*.*
Then

1. $|\theta - \frac{p_n}{q_n}|$ *strictly decreases as* n *increases.*
2. *the convergents give successively closer approximations to* θ*.*
3. $\frac{1}{(a_{n+1}+2)q_n^2} < |\theta - \frac{p_n}{q_n}| < \frac{1}{a_{n+1}q_n^2} \leq \frac{1}{q_n^2}$
4. *If* $p, q \in \mathbb{Z}$ *with* $0 < q < q_{n+1}$ *then*
$$|q\theta - p| \geq |q_n\theta - p_n|$$
Moreover, "=" only if $(p, q) = (p_n, q_n)$*.*
(In this sense convergents are best-possible approximations.)
5. *If* $(p, q) \in \mathbb{Z} \times \mathbb{N}$ *and* $|\theta - \frac{p}{q}| < \frac{1}{2\cdot q^2}$ *then* $\frac{p}{q}$ *is a convergent to* θ*.*

Proof. 1. From Lemma 1.2.1(d) we have $\theta = \frac{p_n\theta_{n+1}+p_{n-1}}{q_n\theta_{n+1}+q_{n-1}}$. Using Lemma 1.2.1(a) we get

$$\begin{aligned}
|q_n\theta - p_n| &= |\frac{q_np_n\theta_{n+1} + q_np_{n-1} - p_nq_n\theta_{n+1} - p_nq_{n-1}}{q_n\theta_{n+1} + q_{n-1}}| && (33)\\
&= \frac{1}{q_n\theta_{n+1} + q_{n-1}} && (34)\\
&< \frac{1}{q_n + q_{n-1}} && (35)\\
&= \frac{1}{(a_n + 1)q_{n-1} + q_{n-2}} && (36)\\
&< \frac{1}{\theta_nq_{n-1} + q_{n-2}} && (37)\\
&= |q_{n-1}\theta - p_{n-1}| && (38)
\end{aligned}$$

This shows (a) and (b) because the q_n are increasing.

c We use $a_{n+1}q_n^2 < \theta_{n+1}q_n^2 + q_nq_{n-1} < (a_{n+1} + 2)q_n^2$ and combine it with the equation (proof part (a)),

$$|\theta - \frac{p}{q}| = \frac{1}{q_n^2\theta_{n+1} + q_nq_{n-1}}$$

d) By Lemma 1.2.1(a) we can find $\begin{pmatrix} u \\ v \end{pmatrix}$ $in\mathbb{Z}^2$ such that

$$\begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}.$$

As $0 < q < q_{n+1}$ we have $u \neq 0$. If $v = 0$ then $(p, q) = u \cdot (p_n, q_n)$ and the claim is trivial. ($u = 1 \Rightarrow$ equality, $u > 1 \Rightarrow$ strictly ¿)
So let's assume $v \neq 0$. Then u and v cannot both be negative (as $q > 0$) nor both be positive (as $q < q_{n+1}$). So they have opposite signs.
By Theorem 1.2.2(a) also $q_n\theta - p_n$ and $q_{n+1}\theta p_{n+1}$ have opposit signs. Hence, $|q\theta - p| = |u(q_n\theta p_n) + v(q_{n+1}\theta - p_{n+1}| > |q_n\theta - p_n|$.

e) Take n with $q_n \leq q < q_{n+1}$. Then

$$\begin{aligned} |\frac{p}{q} - \frac{p_n}{q_n}| &\leq |\theta - \frac{p}{q}| + |\theta - \frac{p_n}{q_n}| \\ &= \frac{|q\theta - p|}{q} + \frac{|q_n\theta - p_n|}{q_n} \\ &\overset{\leq}{(d)} (\frac{1}{q} + \frac{1}{q_n})|q\theta - p| \\ &\leq \frac{2}{q_n}\frac{1}{2q} \\ &= \frac{1}{qq_n} \end{aligned}$$

Hence, $\frac{p}{q} = \frac{p_n}{q_n}$.

□

Remark 10. • *(d) implies that if $p, q \in \mathbb{Z}$, $0 < q \leq p_n$ then*

$$\begin{aligned} |\theta - \frac{p}{q}| &\geq |\theta - \frac{p_n}{q_n}| \cdot \frac{p_n}{q} \\ &\geq |\theta - \frac{p_n}{q_n}| \end{aligned}$$

with "=" only if $\frac{p}{q} = \frac{p_n}{q_n}$.

- *We say $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ is* badly approximable *if*

$$\exists c > 0 \textit{ such that } |\alpha - \frac{p}{q}| > \frac{c}{q^2} \forall (p, q) \in \mathbb{Z} \times \mathbb{N}$$

- *By (c) and (d) we see that $\theta = [a_0, a_1, a_2, \dots]$ is badly approximable if and only if the partial quotients a_i are uniformly bounded, i.e., $\exists M > 0$ such that $a_i < M \forall i$.*

- *(c) suggests that the "worst-approximable" number is $\theta = [1, 1, 1, \dots]$. That's indeed the case c.f Exercise sheet 2 # 5,6 (using that $\theta = 1 + \frac{1}{1 + \frac{1}{1 + \dots}} = 1 + \frac{1}{\theta}$. So $\theta^2 - \theta - 1 = 0$.
So $\theta = \frac{1 \pm \sqrt{5}}{2}$ but $a_0 = 1$ so $\theta = \frac{1 + \sqrt{5}}{2}$.*

Counting Diophantine approximations 1:
Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and let $\phi : [1,\infty) \to (0,\infty)$ be decreasing. Consider the number of "ϕ-good" approximations:

$$N_\alpha(\phi, Q) = \#\{\frac{p}{q} \in \mathbb{Q}; |\alpha - \frac{p}{q}| < \phi(q), 1 \leq q \leq Q\}$$

We put $S_\alpha(\phi, Q) = \{(x,y) \in \mathbb{R}^2 : |\alpha - \frac{x}{y}| < \phi(y), 1 \leq y \leq Q\}$. Then

$$N_\alpha(\phi, Q) = \#\{(p,q) \in \mathbb{Z} \times \mathbb{N} : \gcd(p,q)\} \cap S_\alpha(\phi, Q)$$

Note that by Corollary 1.1.2 we have $N_\alpha(\phi, Q) \to \infty$ as $Q \to \infty$ provided $\phi(y) \geq \frac{1}{y^2}$, and by Exercise sheet 2, even when $\phi(y) \geq \frac{1}{\sqrt{5}y^2}$. If ϕ decays slowly enough then one can easily show that

$$N_\alpha(\phi, Q) = 2 \cdot \underbrace{\int_1^Q y\phi(y)dy}_{} VolS_\alpha(\phi, Q) (\text{It } \underbrace{o(1)}_{} \text{ tends to } 0 \text{ as } Q \to \infty) \text{ as Q } \to \infty$$

More specifically, using tools we develp in Chapter 3, one can easily show that

$$\#\mathbb{Z}^2 \cap S_\alpha(\phi, Q) = 2 \cdot \int_1^Q y\phi(y)dy + \mathcal{O}(Q),$$

using Möbius-inversion, one can show that

$$N_\alpha(\phi, Q) = \frac{2}{S(2)} \cdot \int_1^Q y\phi(y)dy + \mathcal{O}(Q \log Q).$$

So we get an asymptotic formula

$$N_\alpha(\phi, Q) \sim \frac{2}{S(2)} VolS_\alpha(\phi, Q)$$

provided

$$\frac{Q \log Q}{\int_1^Q y\phi(y)dy} \to 0 \text{ as } Q \to \infty.$$

So, e.g., if $\phi(y) \geq \frac{(\log y)^2}{y}$.

However, the case when $\phi(y)$ decays much quicker is more interesting. Serge Lang in 1967 proved that if α is reals quadratic then

$$N_\alpha(\frac{1}{x^2}, Q) = c_\alpha \cdot \log(Q) + \mathcal{O}(1). \; (c_\alpha > 0).$$

He mentioned that it would seem quite difficult to prove an asymptotic result por algebraic α, let alone transcendend.
Adams showed

$$N_e(\frac{1}{x^2}, Q) = c_e \cdot \frac{\log Q}{\log \log Q} + \mathcal{O}(1)(c_e > 0)$$

where $e = 2.7122\ldots$
Lang and Adams both used continuous fractions expansion. How can one prove asymptotics for $N_\alpha(\phi, Q)$? Here is an example.

Example 6. *Suppose $\phi(x) = \frac{1}{2x^2}$. Consider the continuous fraction expansion $\alpha = [a_0, a_1, a_2, \dots]$. By Theorem 1.2.3 we know $|\alpha - \frac{p}{q}| < \phi(q) \Rightarrow \frac{p}{q}$ is a convergent. Moreover, if $\frac{p}{q} = \frac{p_n}{q_n}$ is the n-th convergent then $|\alpha - \frac{p}{q}| < \frac{1}{a_{n+1}q^2}$. So if all $a_i > 1$ then $|\alpha - \frac{p}{q}| < \phi(q) \forall$ convergent $\frac{p}{q}$.*
Hence, $N_\alpha(\phi, Q) = \#\{n : q_n \le Q\}$.
So, we need to compute the number of convergents $\frac{p_n}{q_n}$ with $q_n \le Q$. We shall soon see that this is rather simple if $\alpha = [b, a, b, a, b, a, \dots]$ with $a \mid b$.
We will get back to this after Theorem 1.2.5.

A continued fraction $[a_0, a_1, a_2, \dots]$ is called *periodic* if

$$\exists k \in \mathbb{N} \text{ and } L \in \mathbb{N}_0 \text{ such that } a_{k+l} a_l \forall l \ge L.$$

In this case we write $[a_0, a_1, a_2, \dots] = [a_0, \dots, a_L, \overline{a_{L+1}, \dots, a_{L+k-1}}]$.

Theorem 1.2.4. *$\theta = [a_0, a_1, a_2, \dots]$ is periodic $\iff$ θ is real quadratic (θ is real quadratic means $\exists D \in \mathbb{Z}[x] \setminus 0$ with $D(\theta) = 0$, but $\theta \notin \mathbb{Q}$ and $\theta \in \mathbb{R}$)*

See Ex Sheet 2 #3 for a special instance.
A proof can be found, e.g., in Hardy & Wright "The Theory of numbers", Oxford University press

Let's go back to the problem of computing p_n, q_n of the n-th convergent. The general recursion formula is unhandy. But in certain cases there is a simple explicit formula. Consider $\theta = [b, a, b, a, \dots] = [\overline{b, a}]$ and suppose $b = a \cdot c$ for some $c \in \mathbb{N}$. Now $\theta = b + \frac{1}{a + \frac{1}{b + \frac{1}{\dots}}} = b + \frac{1}{a + \frac{1}{\theta}}$. Thus $\underbrace{a\theta^2 - ab\theta - b}_{} \theta^2 - b\theta - c = 0$, so $\theta = \frac{b + \sqrt{b^2 + 4c}}{2}$ and we put $\bar{\theta} = \frac{b - \sqrt{b^2 + 4c}}{2}$.

Theorem 1.2.5. *The p_n and q_n of the n-th convergent $\frac{p_n}{q_n}$ of $\theta = [\overline{b, a}] (b = ac)$ are give by*

$$p_n = c^{-\lfloor \frac{n+1}{2} \rfloor} \cdot U_{n+2}, q_n = c^{-\lfloor \frac{n+q}{2} \rfloor} \cdot u_{n+1}$$

where

$$u_n = \frac{\theta^n - \bar{\theta}^n}{\theta - \bar{\theta}}.$$

(Recall: $\theta = \frac{b + \sqrt{b^2 + 4c}}{2}, \bar{\theta} = \frac{b - \sqrt{b^2 + 4c}}{2}$, so $\theta - b\theta - c = 0, \bar{\theta}^2 - b\bar{\theta} - c = 0$)

Proof. For $n = 0, 1$ we note that

$$q_0 = q = u_1 \tag{39}$$

$$q_1 = a = \frac{b}{c} = \frac{u_2}{c} \tag{40}$$

$$p_0 = b = \theta + \bar{\theta} = u_2 \tag{41}$$

$$p_1 = ab + 1 = \frac{b^2 + c}{c} = \frac{(\theta + \bar{\theta})^2 - \theta\bar{\theta}}{c} = \frac{u_3}{c} \tag{42}$$

Put $\omega_{n+2} = c^{-\lfloor \frac{n+1}{2} \rfloor} u_{n+2}$.
So we need to show that $p_n = \omega_{n+2}$.
Using that $\theta^{n+2} = b\theta^{n+1} + c\theta^n$ and $\bar{\theta}^{n+2} = b\bar{\theta}^{n+1} + c\bar{\theta}^n$ and hence $u_{n+2} = \frac{\theta^{n+2} - \bar{\theta}^{n+2}}{\theta - \bar{\theta}} = bu_{n+1} + cu_n$.

Moreover, $u_{2m+2} = c^m \omega 2m + 2$, $u_{2m+1} = c^m \omega_{2m+1}$. Inserting this into the above, distinguishing n even or odd yields:

$$\omega_{2m+2} = b\omega_{2m+1} + \omega_{2m} \tag{43}$$

$$\omega_{2m+1} = a\omega_{2m} + \omega_{2m-1} \tag{44}$$

Hence, p_n and ω_{n+2} satisfy the same recurrence relation. and here the same two starting values, so $p_n = \omega_{n+2}$.
Similar for q_n. $\square$

Counting Diophantine Approximation 2:
We can use Theorem 1.2.5 to show that if $\theta = [\overline{b, a}]$ with $b = ac, a > 1$ then

$$N_\theta(\frac{1}{2x^2}, Q) = \frac{\log Q}{\log(\frac{Q}{\sqrt{c}})} + \mathcal{O}(1)$$

Indeed, we have already seen, that

$$N_\theta(\frac{1}{2x^2}, Q) = \#\{n : q_n \leq Q\}$$

By Theorem 1.2.5 we know

$$q_n \leq Q \iff c^{-\lfloor \frac{n+1}{2} \rfloor} \frac{\theta^n - \bar{\theta}^n}{\theta - \bar{\theta}} = \left(\frac{\theta}{\sqrt{c}}\right)^n \left(1 - \left(\frac{\bar{\theta}}{\theta}\right)^n\right) \epsilon \leq Q$$

where $\epsilon = \begin{cases} \frac{1}{\theta - \bar{\theta}} & 2 \mid n \\ \frac{1}{\sqrt{c}(\theta - \bar{\theta}} & 2 \nmid n \end{cases}$

$$\iff n \log\left(\frac{\theta}{\sqrt{c}}\right) + \log\left(1 - \left(\frac{\bar{\theta}}{\theta}\right)^n\right) + \log \epsilon \leq \log Q$$

Using Taylor series expansion we see that

$$|\log\left(1 - \left(\frac{\bar{\theta}}{\theta}\right)^n\right)| \leq |\frac{\bar{\theta}}{\theta - \bar{\theta}}|$$

This proves the claim.

2 Liouville's Theorem

Let $\alpha \in \mathbb{C}$. If $\exists D(x) \in \mathbb{Z}[x]$, $D \neq 0$ and $D(\alpha) = 0$ then we say α is *algebraic*. In this case $\exists D(x) = a_0 x^d + \cdots + a_d \in \mathbb{Z}[x]$ with

- $D(\alpha) = 0$
- $a_0 > 0$
- $\gcd(a_0, \ldots, a_d) = 1$
- $\deg D(x)$ minimal

Imposing all these condition renders D unique; We write $D_\alpha(x)$ and call this the *minimal polynomial* of α. If α is algebraic then we say $\deg D_\alpha$ is the *defree of* α.

Example 7.

- $\alpha = 0, D_\alpha(x) = x$
- $\alpha = \sqrt{2} + 1, D_\alpha(x) = (x-1)^2 - 2 = x^2 - 2x - 1$
- $\alpha = \frac{1}{\sqrt{2}}, D_\alpha(x) = 2x^2 - 1$

Theorem 2.0.6 (1.3.1 Liouville's Theorem)**.** *Suppose α is a real, algebraic number of degree d. Then $\exists c(\alpha) > 0$ such that*

$$|\alpha - \frac{p}{q}| > \frac{c(\alpha)}{q^d}$$

for every $(p,q) \in \mathbb{Z} \times \mathbb{N}$ with $\alpha \neq \frac{p}{q}$.

Proof. Suppose $|\alpha - \frac{p}{q}| > 1$ then the claim holds for every $c(\alpha) > 1$. Now suppose $|\alpha - \frac{p}{q}| \leq 1$. Taylor series expansion at D_α about α gives:

$$D_\alpha(x) = \sum_{i=1}^{d} (x-\alpha)^i \frac{1}{i!} D_\alpha^{(i)}(\alpha)$$

Hence,

$$|D_\alpha\left(\frac{p}{q}\right)| = |\sum_{i=1}^{d} \left(\frac{p}{q} - \alpha\right)^i \frac{1}{i!} D_\alpha^{(i)}(\alpha)| \overset{\leq}{(D)label} |\frac{p}{q} - \alpha| \frac{1}{c(\alpha)}$$

where

$$c(\alpha) = \left(1 + \sum_{i=1}^{d} \frac{1}{i!} |D_\alpha^{(i)}(\alpha)|\right)^{-1}$$

Now if D_α has a rational root then it must have degree one, so have only *one* root. Thus $D_\alpha\left(\frac{p}{q}\right) \neq 0$ unless $\alpha = \frac{p}{q}$. Hence, if $\alpha \neq \frac{p}{q}$ we get

$$|D_\alpha\left(\frac{p}{q}\right)| = |\frac{\text{non-zero integer}}{q^d} \geq \frac{1}{q^d}.$$

Combing this with (D)label yields

$$|\alpha - \frac{p}{q}| > \frac{c(\alpha)}{q^d}.$$

□

We say a real number α is a *Liouville number* if for every $n \in \mathbb{N}$

$$0 < |\alpha - \frac{p}{q}| < \frac{1}{q^n}$$

has a solution. $p, q \in \mathbb{Z}$ with $q > 1$.

Example 8. $\alpha = \sum_{k=1}^{\infty} 10^{-k^k}$ *is a Liouville number. Let $n \in \mathbb{N}$ and put $p = \sum_{k=1}^{n} 10^{n^n - k^k}$ and $q = 10^{n^n}$. Then $0 < |\alpha - \frac{p}{q}| = \sum_{k>n} 10^{-k} \leq 2 \cdot 10^{-(n+1)^{(n+1)}} < 10^{-n^{(n+1)}} = q^{-n}$*

Corollary 2.0.7 (1.3.2)**.** *Every Liouville number is trancendental (i.e., not algebraic).*

Proof. Immediate from Theorem 1.3.1 (Liouville's Theorem). □

Algebraic numbers are enumerable and thus have Lebesgue measure zero. It's not difficlut to show that the set of Liouville numbers, while *not* enumberable, also has measure zero. In fact "most" real numbers are "not very far" from badly approximable as the following theorem shows.

Theorem 2.0.8 (Khintchine)**.** *Suppose $\psi : \mathbb{N} \to (0, \infty)$ is monotone decreasing (not necessarily strictly). The set*

$$A_\psi = \{\alpha \in \mathbb{R} : |\alpha - \frac{p}{q}| < \frac{\psi(q)}{q} \text{ has } \infty\text{-many solutions } (p, q) \in \mathbb{Z} \times \mathbb{N}\}$$

has a Lebesgue measure zero of $\sum_{q=1}^{\infty} \psi(q)$ converges and has full Lebesgue measure (i.e. the complement has measure zero) if $\sum_{q=1}^{\infty} \psi(q)$ diverges.

We will not prove this Theorem. (For a proof see e.g. Glyn Harman "Metric number theory".)

Example 9.

- *Take $\psi(q) = \frac{1}{q}$. We already know that $A_\psi = \mathbb{R} \setminus \mathbb{Q}$. And indeed $\sum \psi(q)$ divergers...*
- *$\psi(q) = \frac{1}{q \log(q-1)}$. Then $\sum \psi(q)$ diverges and thus A_ψ has full measure.*
- *$\psi(q) = \frac{1}{q(\log(q+1))^{1+\epsilon}} (\epsilon > 0)$ then $\sum \psi(q)$ converges, so A_ψ has measure zero.*

3 4 Theorems of Thue- Siegel and Poth

In Section 1 we have seen that ∞-many solutions $\frac{p}{q}$ to $\left|\sqrt{2} - \frac{p}{q}\right| < \frac{1}{q^2}$ leads to ∞-many solutions $(x, y) \in \mathbb{Z}^2$ of $x^2 - 2y^2 = 1$. What about $x^3 - 2y^3 = 1$? Starting as for $x^2 - 2y^2$ we get

$$y^3 \left|\frac{x}{y} - 2^{1/3}\right| \underbrace{\left|\frac{x}{y} - 2^{1/3}\omega\right|}_{\geq \operatorname{Im} \omega} \underbrace{\left|\frac{x}{y} - 2^{1/3}\omega^2\right|}_{\geq (\operatorname{Im} \omega)^2}$$

where $\omega = e^{\frac{2\pi i}{3}}$.

So to get boundedness of $x^3 - 2y^3$ for ∞-many (x, y) we need $\exists c > 0$ such that

$$\left|\frac{x}{y} - 2^{1/3}\right| < \frac{c}{y^3}$$

has ∞-many solutions $(x, y) \in \mathbb{Z} \times \mathbb{N}$.

Theorem 1.3.3 tells us that we would be extremely lucky if that were the case. And erven if so, we still would lack the group structure for $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ (closed under multiplication but $\mathbb{Z} + 2^{1/3}\mathbb{Z}$ is not). On the other hand, suppose we could show that

$$\left|\frac{x}{y} - 2^{1/3}\right| < 1/y^\lambda$$

has only finitely many solutions $(x,y) \in \mathbb{Z}\times\mathbb{N}$ for some fixed $\lambda < 3$. As $x^3-2y^3 = 1$, and $y \neq 0$ yields:

$$\left|\frac{x}{y} - 2^{1/3}\right| < \frac{1}{2^{1/3}(\operatorname{Im}\omega)^2 y^3}$$

We would conclude that $x^3 - 2y^3 = 1$ has only finitely many solutions $(x,y) \in \mathbb{Z}^2$. Note that "deg"$2^{1/3} = 3(D(x) = x^3 - 2)$ and so Liouville's Theorem yields only $\lambda = 3$ not $\lambda < 3$. So the big challenge is to improve Liouville's Theorem. After Liouville it has taken 65 years until the first breakthrough was obtained by Axel Thue in 1909.

Theorem 3.0.9 (1.4.1 Thue)**.** *Let α be a real algebraic number of degree $d \geq 2$, and let $\lambda > \frac{d}{2} + 1$. Then $\exists c = c(\alpha,\lambda) > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^\lambda}, \quad \forall (p,q) \in \mathbb{Z}\times\mathbb{N}.$$

- Note that for $d = 2$ Liouville is stronger
- Given α and λ there is no method to determine a feasible value for c. This is in stark contrast to Liouville's Theorem.

Just as for $x^3 - 2y^2 = 1$ one can now very easily show that if $f(X,Y) = a_0(X-\alpha_1 Y)\cdots(X-\alpha_d Y) \in \mathbb{Q}[X,Y]$ with $a_0 \neq 0, d \geq 3$, and $\alpha_1,\ldots,\alpha_d$ pairwise distinct, and $b \in \mathbb{Q}\setminus\{0\}$, then

$$f(x,y) = b$$

has only finitely many solutions $(x,y) \in \mathbb{Z}^2$.
Wrong if $d = 2$:

$$X^2 - 2Y^2 = 1$$

or $b = 0$:

$$X^3 - Y^3 = 0$$

or $\alpha_1,\ldots,\alpha_d$ not pairwise distinct:

$$(X-Y)^5 = 1$$

We will show that Theorem 1.4.1 implies even the following stronger result.

Theorem 3.0.10 (1.4.2 Generalized Thue equations)**.** *Let $f(X,Y) = a_0\,(X-\alpha_1 Y)\cdots(X-\alpha_d Y) \in \mathbb{Q}[X,Y]$ with $a_0 \neq 0, d \geq 3$ and $\alpha_1,\cdots,\alpha_d$ pairwise distinct. Let $g(X,Y) \in \mathbb{Q}[X,Y]$ of total degree $< \frac{d}{2} - 1$.*
Then there are only finitely many $(X,Y) \in \mathbb{Z}^2$ with

$$f(x,y) = g(x,y)$$

and $g(x,y) \neq 0$.

Example 10.

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

has only finitely many solutions $(x,y) \in \mathbb{Z}^2$. Indeed if $x - y = 0$ then $x^5 - 2y^5 = 0$ thus $x = y = 0$. Note Theorem can go wrong if $\alpha_1 = \alpha_2$:

$$(X^2 - 2Y^2)^2 = 1.$$

(assuming Theorem 1.4.1). If $y = 0$ then we have at most d possibilities for x. So we can assume $y \neq 0$. We claim that

$$|x| \leq c_1|y|$$

for some $c_1 = c_1(f,g)$. Clearly true when $|x| \leq |y|$, so let's assume $|x| > |y|$. Then we write

$$f(x,y) = \sum_{i=0}^{d} a_i x^{d-i} y^i = \sum_{j+k \leq d-1} b_{jk} x^j y^k = g(x,y)$$

Dividing by x^{d-i} yields

$$a_0 x = -\sum_{i=0}^{d} a_i \frac{y^i}{x^{i-1}} + \sum_{j+k \leq d-1} b_{jk} x^{j-d+1} y^k$$

We have

$$\left| \frac{y^i}{x^{i-1}} \right| \leq |y|$$

and

$$\left| \frac{y^k}{x^{d-1-j}} \right| \leq |y|^{j+k-(d-1)} \leq 1$$

Therefore $|x| \leq c_1|y|$, e.g. with $c_1 = \frac{1}{|a_0|}\left(\sum|a_i| + \sum|b_{jk}|\right) + 1$. From

$$f(x,y) = g(x,y), (\star)$$

we get

$$|\alpha_0| \prod_{j=1}^{d} \left| \frac{x}{y} - \alpha_i \right| \leq c_2 |y|^{e-d}$$

where $c_2 = c_2(c_1, g)$ and $e < \frac{d}{2} - 1$. So assume $(\star)$ has ∞-many solutions $(x,y) \in \mathbb{Z}^2$. Then $\exists i$, say $i = 1$, such that $\left|\frac{x}{y} - \alpha_1\right| \leq \mu := \frac{1}{2}\min_{j \neq i}\{|\alpha_j - \alpha_1|\} > 0$ for ∞-many (x,y) of these solutions of $(\star)$. Now

$$\left| \frac{x}{y} - \alpha_j \right| \geq \left| |\alpha_j - \alpha_i| - \left| \frac{x}{y} - \alpha_1 \right| \right| \geq 2\mu - \mu = \mu > 0$$

Hence, we conclude

$$\left| \frac{x}{y} - \alpha_1 \right| \leq \frac{c_2}{|a_0|} \mu^{1-d} |y|^{e-d}, (\star\star)$$

for these solutions (x,y). Here we can assume $y > 0$ (just replace x by $-x$). Now let d_1 be the degree of α_1. As $f(x,1) \in \mathbb{Q}[x]$, $f(x,1) \neq 0$ and $f(\alpha_1, 1) = 0$. Thus $d_1 \leq d$. Moreover, $d - e > \frac{d}{2} + 1$ and this $\exists \lambda$ such that

$$d - e > \lambda > \frac{d_1}{2} + 1.$$

If $d_1 \geq 2$ then Theorem 1.4.1 implies that $(\star)$ has only finitely many solutions $(x,y) \in \mathbb{Z}^2$. Finally suppose $d_1 = 1$. Then $\alpha_1 = \frac{p}{q}$, and $(\star\star)$ yields:

$$\left| x - \frac{p}{q} y \right| \leq c_3 y^{e-d+1} \leq c_3 y^{-\frac{d}{2}}.$$

Thus $x = \frac{p}{q} y = \alpha_1 y$ for y large enough. But then $0 = f(x,y) = g(x,y)$ a contradiction. $\square$

After Thue came Siegel (1921) who improved the exponent $\frac{d}{2}+1$ to $2\sqrt{d}$. This was slightly improved by Dyson and Gelfand (1947) to $\sqrt{2d}$. Finally in 1955 came Roth:

Theorem 3.0.11 (1.4.3 (Roth))**.** *Let α be a real, algebraic irrational number, and $\lambda > 2$. Then $\exists c = c(\alpha, \lambda) > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^{\lambda}}, \quad \forall (p,q) \in \mathbb{Z} \times \mathbb{N}.$$

By Corollary 1.1.2 $\lambda > 2$ is best-possible. But if we allow more general functions $\phi(q)$, not only powers of q, then an improvement might be possible. However, since 1955 nobody was able to replace $q^{-\lambda}$ by a function $\phi(q)$ that decays more slowly, e.g. $\phi(q) = q^{-2}(\log q)^{-1}$.
However, back to the case where $\phi(q)$ is a power of q.
From Theorem 1.3.3. we know that for a generic real α

$$\left|\frac{p}{q} - \alpha\right| < q^{-\lambda}$$

has only finitely many solutions $p, q \in \mathbb{Z} \times \mathbb{N}$ provided $\lambda > 2$. Any by Corollary 1.1.2 every irrational real number has ∞-many solutions when $\lambda = 2$. And so from Roth's Theorem we see an algebraic irrational behaves "essentially" like a generic number.

Roth's Theorem has various new applications to, e.g., Diophantine equations and transcendence. Let's consider just one now trancendence result:
Take $\alpha = \sum_{k=1}^{\infty} 2^{-3^k}$; put $q_n = 2^{3^n}$ and $p_n = q_n \sum_{k=1}^{n} 2^{-3^k}$. Then $0 < \left|\alpha - \frac{p_n}{q_n}\right| = \sum_{k=n+1}^{\infty} 2^{-3^k} < 2 \cdot 2^{-3^{n+1}} = 2 \cdot 2 \cdot q_n^{-1}$ so by Roth's Theorem α is transcendental.

How does one prove results like Roth's Theorem of the kind

$$\left|\alpha - \frac{p}{q}\right| \geq \phi(q)?$$

The idea is to find good rational approximations.

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \delta_n$$

with δ_n "pretty small". Then

$$\left|\alpha - \frac{p}{q}\right| \geq \left|\frac{p_n}{q_n} - \frac{p}{q}\right| - \left|\alpha - \frac{p_n}{q_n}\right|$$

If

$$\frac{p_n}{q_n} \neq \frac{p}{q} \tag{45}$$

then

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{qq_n} - \delta_n.$$

If we are lucky then $\delta_n < \frac{1}{qq_n}$ and we get a positive lower bound. How do we find these $\frac{p_n}{q_n}$?

Usually this is a difficult task, but sometimes one can easily see these approximations $\frac{p_n}{q_n}$. Here is an example.

Take again $\alpha = \sum_{k=1}^{\infty} 2^{-3^k}$. Then we can take again $q_n = 2^{3^n}$, $p_n = q_n \sum_{k=1}^{n} 2^{-3^k}$; so $\left|\alpha - \frac{p_n}{q_n}\right| < 2 \cdot q_n^{-3}$. Hence, if

$$\frac{p_n}{q_n} \neq \frac{p}{q}$$

then

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{qq_n} - \frac{2}{q_n^3}$$

If $q_n > 4 \cdot q$ then

$$\frac{1}{qq_n} - \frac{2}{q_n^3} \geq \frac{q}{2 \cdot qq_n}$$

As $\frac{p_n}{q_n}$ tends strictly monotonously to α, we have $\frac{p_n}{q_n} \neq \frac{p}{q}$ or $\frac{p_{n+1}}{q_{n+1}} \neq \frac{p}{q}$ Let m be minimal with $q_m > 4 \cdot q$. Hence

$$q_m^{\frac{1}{3}} = q_{m-1} \leq 4 \cdot q < q_m$$

If $\frac{p_m}{q_m} \neq \frac{p}{q}$ we take $n = m$ and $n = m + 1$ else. We conclude

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{2qq_n} \geq \frac{1}{2qq_{m+1}} \geq \frac{1}{2q}\frac{1}{q_m^3} \geq \frac{1}{2q}\frac{1}{(4q)^{\frac{9}{2}}} = 2^{-10}q^{-\frac{11}{2}}$$

In this example everything works out nicely, e.g., (ref*) could easily be guaranteed by using $\frac{p_n}{q_n}$ tending strictly monotonously to α. However, in Roth's Theorem (ref*) becomes the major-problem.

3.1 5 Simultaneous Diophantine approximation and the Subset Theorem

Suppose $\alpha_1, \ldots, \alpha_n$ are real numbers. Theorem 1.1.1 can be generated to yield a solution $(x_1, \ldots, x_n, y) \in \mathbb{Z}^n \times \mathbb{N}$ at the system

$$\left|\frac{x_i}{y} - \alpha\right| \leq \frac{1}{y \cdot Q}(1 \leq i \leq n), 0 < y < Q.$$

(c.f. Exercise sheet 4). This in turn yields ∞-many solutions $(x_1, \ldots, x_n, y) \in \mathbb{Z}^n \times \mathbb{N}$ of the system

$$\left|\frac{x_i}{y} - \alpha_i\right| < \frac{1}{y^{1+\frac{1}{n}}}(1 \leq i \leq n).$$

provided at least one of the α_i's is irrational. So Corollary 1.1.2 extends to simultaneous approximation. A much deeper fact is that Roth' Theorem also extends to simultanious approximation.

For $\underline{x} \in \mathbb{R}^n$ we write $\|\underline{x}\| = (\sum_{i=1}^{n} x_i^2)^{\frac{1}{2}}$ for the Euclidean length.

Theorem 3.1.1 (Subspace Theorem, Schmidt)**.** *Suppose $L_i(\underline{x}) = \sum_{j=1}^{n} a_{ij}x_j (1 \leq i \leq n)$ are linearly independent linear forms with algebraic coefficients a_{ij}. Let $\delta > 0$. Then the solutions $\underline{x} \in \mathbb{Z}^n \setminus \underline{0}$ of*

$$|L_1(\underline{x}) \ldots L_n(\underline{x})| < \|\underline{x}\|^{-\delta}$$

lie in finitely many proper subspaces of $\mathbb{Q}^n$.

Remark 11. *linearly independent linear forms means the coefficient vectors* $(a_{i1}, \dots, a_{in})$ *are linearly independent over* $\mathbb{C}$.

Corollary 3.1.2 (1.5.2)**.** *Let* $\delta > 0$, *suppose* $\alpha_1, \dots, \alpha_n$ *are algebraic and* $1, \alpha, \dots, \alpha_n$ *are linearly independentn over* $\mathbb{Q}$. *Then there are only finitely many* $(x_1, \dots, x_n, y) \in \mathbb{Z}^n \times \mathbb{N}$ *with*

$$(5.1)\left|\frac{x_i}{y} - \alpha_i\right| < \frac{1}{y^{1+\frac{1}{n}+\delta}}(1 \le i \le n) \tag{46}$$

Proof. (assuming Theorem 1.5.1) Put $\underline{X} = (X_1, \dots, X_n, Y)$, $L_i(\underline{X}) = \alpha_i Y - X_i (1 \le i \le n)$, $L_n(\underline{X}) = Y$. These $n+1$ linear forms in $n+1$ unknowns are linarly independet. With $\underline{x} = (x_1, \dots, x_n, y)$ the solutions of (5.1) yield

$$|L_1(\underline{x}) \dots L_{n+1}(\underline{x})| < \frac{1}{y^\delta} < \frac{1}{\|\underline{x}\|^{\frac{\delta}{2}}}$$

if y is large enough. so by Theorem 1.5.1 (in $n+1$ dimensions), we set that the solutions lie in finitely many prober subspeced at $\mathbb{Q}^{n+1}$. Pick one of these (of codimension I say). It is giben by an equation $c_1x_1 + \dots + c_nx_n + c_{n+1}y = 0$ where $c_i \in \mathbb{Q}$ not all zero. On this subspace we have

$$(c_1\alpha_1 + \dots + c_n\alpha_n + c_{n+1})y = c_1(\alpha_1 y - x_1) + \dots + c_n(\alpha_n y - x_n).$$

Put $\gamma = c_1\alpha_1 + \dots + c_n\alpha_n + c_{n+1}$. By $\mathbb{Q}$-linearly independence of $1, \alpha_1, \dots, \alpha_n$ we have $\gamma \ne 0$. Hence,

$$|\gamma||y| \le |c_1||\alpha_1 y - x_1| + \dots + |c_n||\alpha_n y - x_n| \le (|c_1| + \dots + |c_n|)\frac{1}{y^{1+\frac{1}{n}+\delta}} \le |c_1| + \dots + |c_n|$$

So $|y|$ is bounded and we are done. □

In applications one sometimes needs a "p-adic" version of the subspace Theorem in which one approximates with respect to also the so called p-adic absolute values.

Definition (Absolute values)**.** *An absolute value on a field* K *is a map* $|\bullet| : K \to [0, \infty)]$ *such that*

- $|x| = 0 \iff x = 0$
- $|x \cdot y| = |x| \cdot |y|$
- $|x + y| \le |x| + |y|$

Example.

- *K arbitrary.* $|x| = \begin{cases} 0 & x = 0 \\ 1 & x \ne 0 \end{cases}$ *the* trivial absolute value.
- $K = \mathbb{Q}$, $|\bullet|$ = standatd absolute value *on* $\mathbb{Q}$. *To distinguish it from other absolute values let's write it as* $|\bullet| = |\bullet|_\infty$.
- $K = \mathbb{Q}$ *and let* $p \in \mathbb{N}$ *be a prime number. If* $x \in \mathbb{Q}, x \ne 0, \pm 1$, *then* $\exists$ *a unique prime factoriation* $x = \pm p_1^{a_1} \dots p_s^{a_s}$ *where* $p_1, \dots, p_s$ *primes and* $a_i \in \mathbb{Z} \setminus 0$. *For any prime* $p \in \mathbb{N}$ *write* $ord_p(x)$ *for the exponent of* p *in the*

primfractorisation of x *(e.g.* $ord_{p_i} x = a_i$*). For* $x = \pm 1$ *we put* $ord_p x = 0 \forall p_i$*.*
The p-adic absolute vlaue $1 \cdot 1_p$ *on* $\mathbb{Q}$ *is defined by*

$$|x|_p = \begin{cases} 0 & : x = 0 \\ p^{-ord_p(x)} & : x \neq 0 \end{cases}$$

The multiplicativity is clear. Note that $ord_p(x_1+x_2) \geq \min\{ord_p(x_1), ord_p(x_2)\}$*.*
Hence, $|x_1 + x_2|_p = p^{-ord_p(x_1+x_2)} \leq p^{-\min\{ord_p(x_1), ord_p(x_2)\}} \underbrace{=} strongtriangleinequality \max |x_1|_p, |x_2|_p\}$

$|x_1|_p + |x_2|_p$ *An absolute value that satisfies the srtong triange inequality is called non-Archimedean.*

Definition 3.1.3. *We set* $M_{\mathbb{Q}} = \{primes\ in\ \mathbb{N}\} \cup \{\infty\}$*. Then for each* $v \in M_{\mathbb{Q}}$ *we get an absolute value* $|\cdot|_v$*. Note that if* $v \in M_{\mathbb{Q}}$ *and* p *a prime,* $a \in \mathbb{Z}$*, then*

$$|\pm p^a|_v = \begin{cases} p & : v = p \\ p^a & : v = \infty \\ 1 & : v \neq p, v \neq \infty \end{cases}$$

Hence

$$\prod_{v \in M_{\mathbb{Q}}} |1 \pm p^a|_v = 1$$

and so vy multiplicativity we conclude

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1$$

for all $x \in \mathbb{Q}$*,* $x \neq 0$*. (PF) Thsi is the so-called producct formula (PF) on* $\mathbb{Q}$*.*