NT

12.10

Lecture 1

Solved and unsolved problems in Number Theory

1. ~~Euclid~~ How many Prime numbers are there? ∞ (solved)

$S = \{p_1, \dots, p_N\}$

consider $n = p_1 \cdot p_2 \cdots p_N + 1$

It is either a prime or a product of prime that are not in the list S.

2. Choose $a, b \in \mathbb{N}$, $\gcd(a,b) = 1$.

Are there infinitely many primes of the form $\boxed{an+b}$ where $n \in \mathbb{N}$? $\quad Y \in S!$

$n+1$

$a+b,\ 2a+b,\ 3a+b, \dots$ Thm: (Dirichlet)

3. Are there ∞ prime of the form n^2+1? nobody knows

Iwaniec (1978)

There are infinitely many n's so that n^2+1 is either prime or a product of two primes $\quad n^2+1 = \begin{cases} p \cdot q \\ p \end{cases}$

4. Twin primes

$(p, p+2) \qquad (3,5)\ (17,19),\ (5,7)$

6. Goldbach's conjecture

Every even number $n \neq 4$ is a sum of two primes.

$4 = 2+2$
$6 = 3+3$
$8 = 3+5$

Two results:

1) Vinogradov: then (1937 ?)

Every sufficient large odd number is the sum of three primes.

2) Chen Jing-run (1966)

Every even number $n \geq 4$ can be written as $n = p + d$

(p: prime; d: prime or product of 2 primes)

6) Consider $S = \mathbb{N} \cup 7 \cdot \mathbb{N}$

$= \{1, 2, 3, 4, 5, 6, 7_1, 7_2, 8, 9, 10, 11, 12, 13, 14_1, 14_2, 15 \ldots\}$

$\in \cup \mathcal{O}$

$(2k) = \in + \in + \ldots$ $\quad$ $(2k+1) = \mathcal{O} + \mathcal{O} + \mathcal{O} \ldots$

$2 = 2$

$4 = 4$

$6 = 2+4, 6$

$8 = 2+6, 8$

$10 = 2+8, 4+6, 10$

$12 = 2+10, 4+8, 12, 2+4+6$

$14 = 2+4+8, 12+2^*, 10+4, 14_1, 14_2, 6+8$

$3 = 3$

$5 = 5$

$7 = 7_1, 7_2$

$9 = 5+3+1, 9$

$11 = 3+7_1+1, 3+7_2+1, 11$

$13 = 3+9+1, 7_1+5+1, 13, 1+5+7_2$

$15 = 1+5+9, 1+3+11, 1+7_1+7_2$

$3+5+7_1, 3+5+7_2, 15$

H. Farkas, I. Kra Theta constants, Riemann surfaces and the modular group AMS, 2001

NT

14.10.10

$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

↑	=	↑	↑	↑	↑	↑
Positive integer	$\mathbb{N} \cup \{0\}$ "whole numbers"	ring of integers	field of rationals	field of real #'s	field of complex #'s	$\mathbb{Z}[i]$

Def A group $(G, \cdot)$ is a set G with a binary operation $\leftarrow$ (closed = defined for all pairs (a,b) given a unique $a \cdot b \in G$)

$\cdot : G \times G \to G$, $(a,b) \to ab$ with the following properties

1) associativity: $\forall a,b,c \in G \quad (ab)c = a(bc)$

2) $\exists e \in G : \forall a \in G \quad ae = ea = a$ (e is called the identity, or neutral element)

3) $\forall a \in G \ \exists b \in G$ s.t. $ab = ba = e$

We denote $b = a^{-1}$

// also:

4) commutatively: $\forall a,b \in G$ $ab = ba$ holds, then the group is called abelian (or commutative)

Def A field (Körper) $(F, +, \cdot)$ is

I. $(F, +)$ is an abelian group (4 axioms)

II. $(F_{\neq 0}, \cdot)$ is an abelian group (4. axiom)

III. Distributivety: $\forall a,b,c \in F : (a+b)c = ac + bc$

Def. A ring $(R, +, \cdot)$

I. (1-4) $(R, +)$ is an abelian group

5. $\forall a, b, c \in R \quad (a+b)c = ac + bc$

6. $\forall a, b, c \in R \quad a(b+c) = ab + ac$

$(R, \cdot)$ 7. associativity: $a(bc) = (ab)c$

8. The existence of mult. identity:

$\exists\, 1 \in R: \quad \forall a \in R \quad a \cdot 1 = 1 \cdot a = a$

} some authors use only these 6 axioms in the definition of a ring

—

We can talk about commutative rings, division rings (= skew fields) "almost" a field, without commutativity

Example of a field $F = \{0, 1\}$

+	0	1
0	0	1
1	1	a

·	0	1
0	b	c
1	d	1

Galois Галуа

Complex Numbers $(\mathbb{C}, +, \cdot)$

$z = (a, b)$, where $a, b \in \mathbb{R}$

$z_1 + z_2 = (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

$z_1 \cdot z_2 = (a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$

$0 = (0, 0)$

$1 = (1, 0) \qquad (z \cdot 1 = (a, b)(1, 0) = (a, b))$

$z_1 = z_2 \iff a_1 = a_2,\ b_1 = b_2$

$a = \mathrm{Re}\, z \quad b = \mathrm{Im}\, z$

Algebraic Form

Denote $i = (0, 1) \qquad (a, 0) = a(1, 0) = a \cdot 1$

$z = (a, b) = (a, 0) + (0, b) = a \cdot 1 + b \cdot i = a + bi$

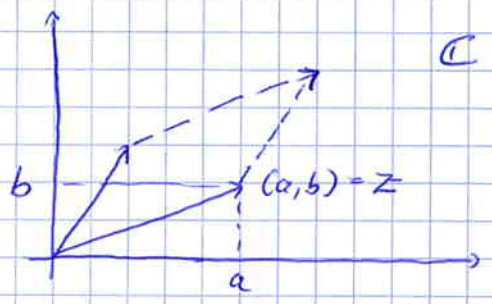
$z_1 \cdot z_2 = (a_1 + b_1 i)(a_2 + b_2 i) = a_1 a_2 + a_1 b_2 i + b_1 a_2 i + b_1 b_2 i^2$

"Foil method" $= (\quad) + (\quad) \cdot i$

1. Let $a, n > 2$ be positive integers so that $\boxed{a^n + 1 \text{ is prime}}$

Prove that 1) a is even (gerade)

2) $n = 2^k$ for some $k \in \mathbb{N}$



$r = |z| = \sqrt{a^2 + b^2}$


right angle

Trigonometric form of complex numbers

$z = a + ib = \underbrace{r \cdot \cos\varphi}_{a} + i \cdot r \sin\varphi = \underline{\underline{r(\cos\varphi + i \sin\varphi)}}$

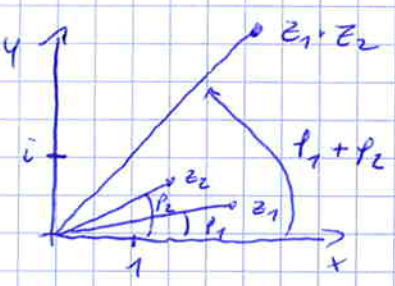

acute

brackets, parantheses, braces

[ ] ( ) { }


obtuse

$$z_1 \cdot z_2 = r_1(\cos\varphi_1 + i\sin\varphi_1) \cdot r_2(\cos\varphi_2 + i\sin\varphi_2)$$
$$= r_1 \cdot r_2 \underbrace{(\cos\varphi_1 \cdot \cos\varphi_2 - \sin\varphi_1 \sin\varphi_2)}_{\cos(\varphi_1+\varphi_2)} + (\cos\varphi_1 \sin\varphi_2 + \sin\varphi_1 \cos\varphi_2)i$$
$$= r_1 \cdot r_2 \cdot (\cos(\varphi_1 + \varphi_2) + \sin(\varphi_1 + \varphi_2) \cdot i)$$



4. (a) $\sin(\varphi_1 + \varphi_2) = \sin\varphi_1 \cdot \cos\varphi_2 + \sin\varphi_2 \cdot \cos\varphi_1$

(b) $\cos(\varphi_1 + \varphi_2) = \cos\varphi_1 \cdot \cos\varphi_2 - \sin\varphi_1 \cdot \sin\varphi_2$

Exponential Form (r, φ) $\quad a^b \cdot a^c = a^{b+c}$

$\cos\varphi + i\sin\varphi = e^{i\varphi}$ Euler formula

$e = 2,7\ \underbrace{1828}_{\text{Leo Tolstov}}\ \underbrace{1828}_{\text{Leo Tolstov}}\ 45\,90\,45\ldots$

$z = r \cdot e^{i\varphi}$ $\qquad e^{i\varphi_1} \cdot e^{i\varphi_2} = e^{i(\varphi_1+\varphi_2)}$

$z_1 \cdot z_2 = (r_1 e^{i\varphi_1}) \cdot (r_2 \cdot e^{i\varphi_2}) = r_1 \cdot r_2 \cdot e^{i(\varphi_1+\varphi_2)}$

NT

19.10.10

What is algebraic Number Theory?

I Elementary Number Theory.

$\mathbb{N}_1$, $\mathbb{N}_0$
$\{1,2,3,\dots\}$ $\{0,1,2,\dots\}$

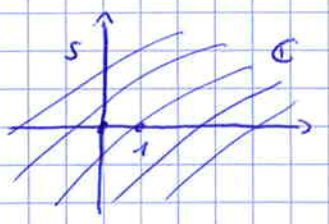
divisibility, congruences, prime #'s
Euclidean algorithm, ...

II Analytic Number Theory.

Riemann zeta function $\zeta(s)$, $s \in \mathbb{C} \setminus \{1\}$

If $\mathrm{Re}(s) > 1$, then $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$

for $s=2$: $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$



Thm 1 (prime number Theorem)

$$\lim_{x \to \infty} \frac{\pi(x) \cdot \ln x}{x} = 1$$

$$\pi(x) \sim \frac{x}{\ln x}$$

$x \in \mathbb{R}$; $\pi : \mathbb{R} \to \mathbb{N}_0$

$\pi(x) = \#\{p \le x \mid p \text{ is prime}\}$
$= |\{\dots\}|$

Ex. $\pi(20) = 8$

Thm 2 (divergence of the series of reciprocals to primes).

The series $\sum_{k=1}^{\infty} \frac{1}{p_k}$ is divergent.

$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots$

Remarks:

1) $\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots$

$\geq 1 + \underbrace{\frac{1}{2}}_{1} + \underbrace{\frac{1}{4} + \frac{1}{4}}_{2} + \underbrace{\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}}_{4} + \dots \underbrace{\frac{1}{16} + \dots + \frac{1}{16}}_{8}$

$+ \dots + \underbrace{\frac{1}{2^{k+1}} + \dots + \frac{1}{2^{k+1}}}_{2^k} + \dots$

$$= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots = \infty$$

You show here that the partial sums of the series $\sum_{n=1}^{\infty} \frac{1}{n}$ are unbounded, so the series is divergent.

2) $\sum_{n=1}^{\infty} \frac{1}{n^s}$, $s > 1$ is convergent

$s = 2$: $\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \dots$

Remark

The meaning of Thm 2 and the above example is: the prime numbers appear more often among positive integers, than square #'s

Proof of Thm 2

By contradiction

Suppose that $\sum_{k=1}^{\infty} \frac{1}{p_k}$ is convergent.

Then $\exists N \in \mathbb{N}$ so that $\sum_{k=N+1}^{\infty} \frac{1}{p_k} < \frac{1}{2}$ (1)

Denote by $Q := p_1 \cdot p_2 \cdot \dots \cdot p_N$ and consider for all $n \in \mathbb{N}$

$1 + n \cdot Q$

What can we say about the series

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ} \quad ? \qquad (2)$$

From the above information we can evaluate:

(3) $$\sum_{n=1}^{r} \frac{1}{1+nQ} \leq \sum_{t=1}^{r} \left(\sum_{k=N+1}^{N+R} \frac{1}{p_k} \right)^t \underset{(1)}{\leq} \sum_{t=1}^{r} \left(\frac{1}{2} \right)^t \leq \sum_{t=1}^{\infty} \left(\frac{1}{2} \right)^t = 1$$

p_{N+R} is the biggest prime of those dividing

$1 + nQ$, $1 \leq n \leq r$

T is the biggest # of prime factors of each of $1+n$ Q.

$$1+Q = p_{N+2} \cdot p_{N+5}$$

$$1+5Q = p_{N+3}^2 \cdot p_{N+7} \cdot p_{N+9}$$

$t=1$

$$\frac{1}{p_{N+1}} + \frac{1}{p_{N+2}} + \dots + \frac{1}{p_{N+R}}$$

$t=2$

$$(\dots) \cdot (\quad) = \frac{1}{p_{n+1}^2} + \frac{1}{p_{N+1}p_{N+2}} + \dots$$

$t=3$

$$\dots = \frac{1}{ppp} + \dots$$

(3) shows that the partial sums of the series (2) are all bounded by 1 from above.
Therefore, (2) must be convergent.

On the other hand, if we denote by $a_n = \frac{1}{1+nQ}$ and by $b_n = \frac{1}{n}$ we see that

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{n}{1+nQ} = \frac{1}{Q} \neq 0 \quad \neq \infty$$

and by the limit comparison test, the series $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ are convergent or divergent together.
Since we know that $\sum_{n=1}^{\infty} \frac{1}{n} = b_n$ is divergent,
$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} \frac{1}{1+nQ}$ must be divergent. We arrived at a contradiction.

III Algebraic Number Theory

Def An *algebraic number* α is a root of a monic polynomial with rational coefficients:

$$x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = 0 \quad \text{for some } a_1, \dots, a_n \in \mathbb{Q}.$$

$20 \in \mathbb{Z}$

$20 = 2 \cdot 10 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$

$20 = 5 \cdot 4 = 5 \cdot 2 \cdot 2$

Def An *integral Domain* is a commutative (assoc) ring with the mult identity $1 \neq 0$ that does not have zero divisors.

(**Def** A ring R has *no zero divisors* (nonzero) if $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$)

Divisibility

Ring $(R, +, \cdot)$

1 – 4. $(R, +)$ is an abelian group.

5. $\forall a, b, c \in R \quad a(b+c) = (a+b)c =$

6. $\forall a, b, c \in R \quad (ab)c = a(bc)$

Examples of rings

1) $\mathbb{Z}$, commutativ with $1 \neq 0$

2) Trivial ring $R = \{0\}$

If in a ring $1 = 0$ (1: multi. id., 0: add. id.), then all its elements $a = 0$

Proof $a \in R$, then $a = 1 \cdot a = 0 \cdot a \overset{\text{?}}{=} 0$

$(0+0) \cdot a = 0 \cdot a + a \cdot 0$

$0 \cdot a \; [= 0 \cdot a + (-0 \cdot a) = 0 \cdot a + 0 \cdot a + (-0a) = 0 \cdot a + 0 = 0 \cdot a.$

3. Any field K is a ring

4. Square Matrices $M(n, K)$

$$i \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}_{n \times n} \begin{pmatrix} j \\ \vdots \\ \end{pmatrix} = i \begin{pmatrix} & j & \\ & & \\ & & \end{pmatrix}_{n \times n}$$

5. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = (\{0, 1, 2, \ldots, n-1\}, +, \cdot)$, mod n, $n \in \mathbb{N}$, $n \geq 2$

Example. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ mod 6

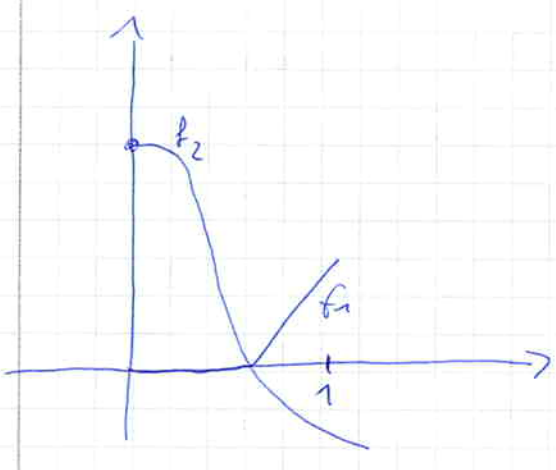
$4 + 5 = 3 \quad 4 \cdot 5 = 2$

$1 \cdot 1 = 1$

$2 \cdot \; \neq 1$

5') If $n = p$ ist prime, then $\mathbb{Z}_p$ is a field $\mathbb{F}_p$

6. Continuous functions on $[0,1] \leftarrow C[0,1]$



$f: [0,1] \longrightarrow \mathbb{R}$

7) $\mathbb{Z}[\sqrt{u}] := \mathbb{Z} + \mathbb{Z}\cdot\sqrt{u} := \{a + b\sqrt{u} \mid a, b \in \mathbb{Z}\}$

$u \in \mathbb{N}$, $u \geq 2$, u is square free ($u \neq u_1^2 \cdot m$, $u_1, m \in \mathbb{N}$, $u_1 \geq 2$)

8) $\mathbb{Z}[a\sqrt{a}] \subset \mathbb{Q}$

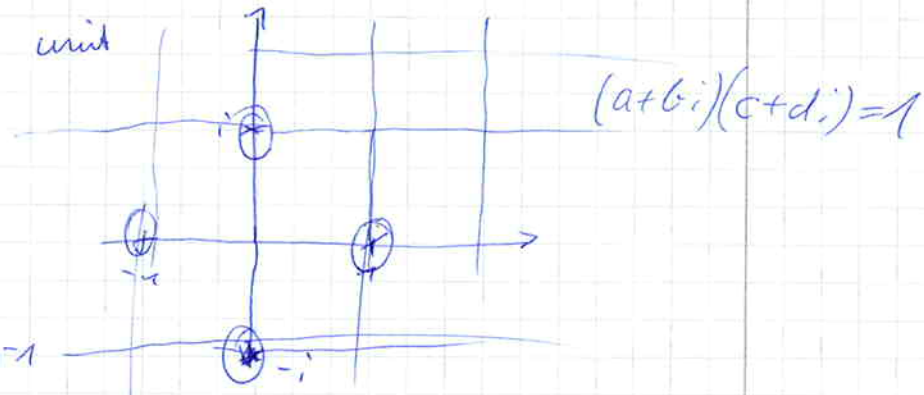
Def An *integral domain* is a commutative ring with mult. identity $1 \neq 0$ without zero divisions (i.e. $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

Let R be an integral domain

Def • We say that $0 \neq a \in R$ divides an element $b \in R$, if $b = a \cdot c$ for some $c \in R$ ($a \mid b$)

• We say that a is a unit of R if it ~~divides~~ divisides $1 (\neq 0)$

• We say that a and b are associates if $a = u \cdot b$ where u is a unit



$(c + di) = 1\,(a+bi)^{-1}$

$$c + di = \frac{(a - bi)}{(a+bi)(a-bi)} = \frac{a - bi}{a^2 + b^2} = \left(\frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2}\right)$$

$$= \underbrace{\frac{a}{a^2+b^2}}_{c} - \underbrace{\frac{b}{a^2+b^2}}_{d} \cdot i$$

1) If $|b| > 0$ then $a = 0$ $\Rightarrow b = \pm 1$

2) $b = 0$, then $a = \pm 1$

Let R be an integral domain. We know the meaning of.

$a|b$ $(b = a \cdot x)$, a unit (= invertible element = division of 1)

a and b are associates ($b = u \cdot a$ for some $u \in R^*$)

Properties:

1. If $a|b$ and $b|c$, then $a|c$.
2. If $a|b$ and $a|c$, then $a | xb + yc$ for all $x, y \in R$
3. If $a|b$ and $b|a$ $\Leftrightarrow$ $a = ub$ for some $u \in R^*$
4. $a|b \Leftrightarrow ca | cb$ for some $c \neq 0 \Leftrightarrow ca | cb \ \forall c \in R$

Def: An element $0 \neq p \in R \setminus R^*$ is called

- prime, if whenever $p | r \cdot s$ for $r, s \in R$ we have $p|r$ or $p|s$ (or p divides both r and s)
- irreducible, if from $p = r \cdot s$ $(r, s \in R)$ it follows that either r or s is a unit (or, equivalently, p and s (resp. p and r) are associates.
- if p is not irreducible, it is reducible

Proposition If p is prime, p is irreducible.

Proof Assume p is prime. We want to prove that p is irreducible. Suppose $p = r \cdot s$ for some $r, s \in R$. We see that $p | rs$. Since p is prime $p|r$ or $p|s$. WLOG (without loss of generality) we can assume that $p|r$. Therefore, $r = x \cdot p$ for $0 \neq x \in R$.

We substitute r to $p = r \cdot s$ to get

$$p = x \cdot p \cdot s = p \cdot x \cdot s \quad (*)$$

$(*) \Rightarrow p - pxs = 0 \Rightarrow p \cdot (1 - xs) = 0 \overset{\text{R without zero p.t.o. divisors}}{\Rightarrow}$

$\Rightarrow 1 - xs = 0 \Rightarrow x \cdot s = 1 \Rightarrow$ both x and s are units $\square$

Remarks: The converse to the above Proposition is not necessary true. There are integral domains that contain irreducible elements that are not prime.

Example $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

$(1 - \sqrt{-5})(1 + \sqrt{-5}) = 6 = 2 \cdot 3$

$(1 - \sqrt{-5})(a + c \cdot \sqrt{-5}) = 2$

It is clear that $1 - \sqrt{-5} \mid 2 \cdot 3$. But it can be shown that $1 - \sqrt{-5} \nmid 2$, $1 - \sqrt{-5} \nmid 3$ so $1 - \sqrt{-5}$ is not prime

§ Unique factorization domains

Def: Let R be an integral domain
R is called a unique factorisation domain.
if one of the following (equivalent) statements hold:

(1) every element $0 \neq a \in R \setminus R^*$ can be written as a product of primes.

(2) every element $0 \neq a \in R \setminus R^*$ can be written as a product of irreducibles uniquely up to the order of factors and the change of the factors by their associates.

(3) Every irreducible element ~~$0 \neq a \in R \setminus R^*$ can be~~ in R is prime and every element $0 \neq a \in R \setminus R^*$ can be written as a product of irreducibles.

Proof (1) $\Rightarrow$ (2).

Let $0 \neq a \in R \setminus R^*$ be an arbitrary element.

i) we want to show that a can be written as a product of irreducibles.
Since (1) holds (F1) $a = p_1 \cdots p_n$, where all p_i are prime by preparation, this is a factorisation into irreducibles

ii) uniqueness

suppose $a = q_1 q_2 \cdots q_m$ (F2)
is a factorisation of a into irreducibles

By (FA) we see that $p_1 \mid a \Rightarrow p_1 \mid q_1 \cdot q_2 \cdot \ldots \cdot q_m$

$\Rightarrow$ (p_1 is prime) $p_1 \mid$ one of q_i

WLOG $p_1 \mid q_1$, that is $q_1 = x \cdot p_1$

We have $a = p_1 \cdot x \cdot q_2 \cdot \ldots \cdot q_m$

$p_1 \cdot p_2 \cdot \ldots \cdot p_n \Rightarrow p_2 \cdot \ldots \cdot p_n = (x \cdot q_2) \cdot \ldots \cdot q_m$ (q_2)

$\{ p_1 (p_2 \cdot \ldots \cdot p_n - (x \cdot q_2) \cdot \ldots \cdot q_m) = 0 \}$ After n steps $1 = \{ q_{n+1} \cdot \ldots \cdot q_m$

(q_1 is irred. p_1 or x must be a unit, p_1 is not a unit (it is prime) $\Rightarrow x$ is a unit)

impossible $m > n$, $n \in m$, $n = m$

(2) $\Rightarrow$ (3). We assume (2) and must prove that every irreducible in such a ring is prime.

Let $0 \neq p \in R \setminus R^*$ be irreducible and $p \mid r \cdot s$, then

$\underbrace{r \cdot s}_{a} = \underbrace{p \cdot x}_{a} = p \cdot \underbrace{(x_1 \cdot \ldots \cdot x_k)}_{\text{factorisation of } x \text{ into irreducibles}}$

(if r and s are not units)

$(r_1 \cdot \ldots \cdot r_e) \cdot (s_1 \cdot \ldots \cdot s_m)$

Because of (2), the number of factors in both sides is the same and p is an associate of (at least) one of $r_1, \ldots, r_e, s_1, \ldots, s_m$. If p is an associate of such factor, it divides it.

If $p \mid r_i \Rightarrow p \mid r$

If $p \mid s_j \Rightarrow p \mid s$

(3) $\Rightarrow$ (1) trivial

Remark In a unique factorisation domain factorization into primes is also unique in the same sense

Remark: In a unique factorization domain factorization into primes is also unique in the same sense.

28.10.10

{commutative rings}
∪
{integral domains}
∪
{unique factorization domains (UFD)} = {factorial ring}
→ {Principal ideal domains} ← {Euclidian domains} ← {fields}

UFD

(1) ∃ a factorization into primes
⇓
(2) ∃! fact. into irreducibles
⇓
(3) ∃ fact. into irreducibles and prime = irreducibles

Example: $\mathbb{Z}$ Primes here $\{\pm 1, -5, -3, -2, 2, 3, 5, \dots\}$

Principal ideal domains (PID) and Euclidian domains

Reminder:

Def. Let R $(R,+,\cdot)$ be a ring. A left (resp. right) ideal I is a subset of R if the following statements hold:
(1) $(I,+)$ is a group of $(R,+)$. $\{\forall a,b \in I \Rightarrow a-b \in I$
(2) I is "stable" w.r.t. left (resp. right) multiplication, that is,
$\forall i \in I, r \in R \Rightarrow r \cdot i \in I$.

Def: If I is a left and right ideal, we call it two-sided ideal or just ideal.

Since we work with integral domains, we talk about ideals.

Def: An integral domain at which all ideals are principal, is called principal ideal domain.

Def An ideal $I \subset R$ is called principal, if $\exists g \in I$ s.t. $I = \{g \cdot r \mid r \in R\}$ (I is generated by g and denote this by $I = (g)$)

Example: $R = \mathbb{Z}$, $I_2 = 2 \cdot \mathbb{Z} := \{2 \cdot a \mid a \in \mathbb{Z}\}$.

$I_n = n \cdot \mathbb{Z}$

Thm. (PID is UFD)

Proof: Let R be a principal ideal domain. To show that this is a unique fact. domain, we use definition (3).

(1) We show that every irreducible is prime. Indeed, let p be an irreducible and let $p \mid ab$. If $p \mid a$, then we are done. If $p \nmid a$, then consider $I = (p, a) := \{xp + ya \mid x, y \in R\}$. $\exists\, q \in I$ s.t. $I = (q) \Rightarrow q \mid p$ and $q \mid a$ ($p, a \in I$). Since p is irreducible and $q \mid p$, we have that either q and p are associates (I) or q is a unit (R). The former (I) is impossible (otherwise p would divide a), so q is a unit, and, therefore $I = (q) = R$.

[$q \in (q) \Rightarrow q q^{-1} \in (q) \Rightarrow q \cdot (q^{-1} \cdot r) = r \in (q) \Rightarrow (q) = R$.]

So, we have, in particular, $1 \in I \Rightarrow \exists\, \bar{x}, \bar{y}$ s.t. $\bar{x}p + \bar{y}a = 1$.

$\Rightarrow \bar{x}pb + \bar{y}ab = b \Rightarrow p \mid b$.
(p divides this product)
$p(\bar{x}b + \bar{y}s)$ ✓

(2) We must show that every $0 \neq a \in R$ is a product of irreducibles. If a is irreducible, then stop (it is already a factorization with just one factor). ✓

If not, then $a = a_1 \cdot a_2$, where both a_1 and a_2 are non-units. If both a_1 and a_2 are irreducibles, we stop. If not, we proceed with factorization of reducible elements.

If after finitely many steps we have a factorization into irred. if not, then there exists a sequence of elements $a, a_1, a_2, \ldots$ so that

(a) $\subset (a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots$
$\|_{\infty}$

$I = \bigcup_{i=0}^{\infty} (a_i)$ 1) I is an ideal. why?

i) if $a, b \in I \Rightarrow \exists\, n$ s.t. $a, b \in (a_n)$

ii) if $a \in I$, $r \in R \Rightarrow ar \in I$.

2) I is a principal ideal, so $I = (g)$ and since $g \in I$

$\exists\, n$ s.t. $g \in (a_n) \Rightarrow g \in (a_j)$, $j \geq n$ and

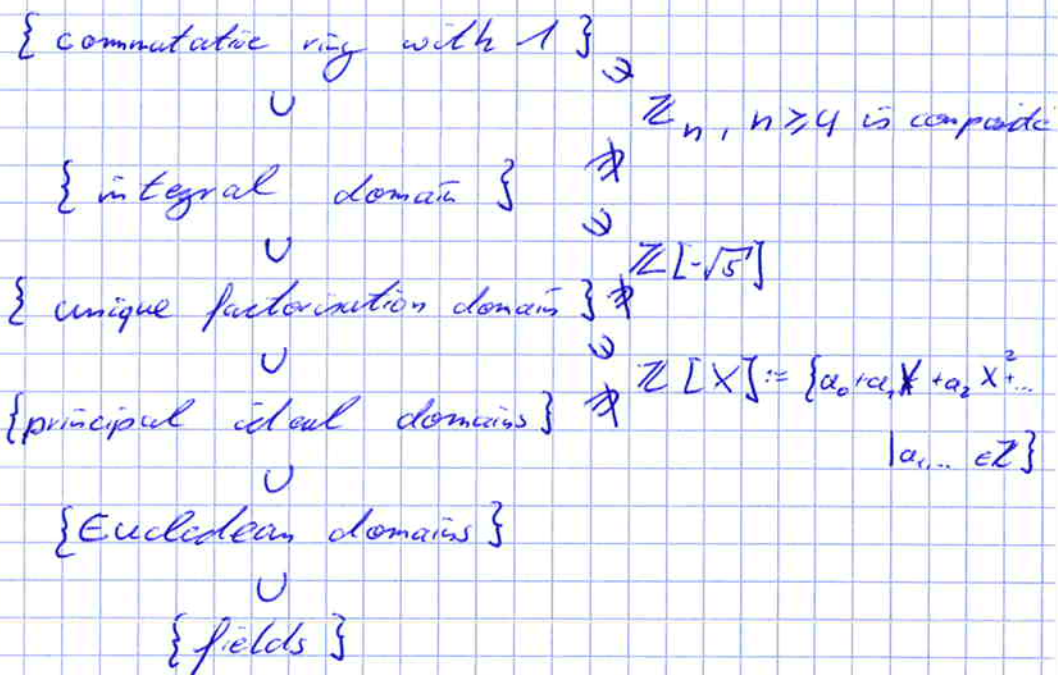
$I = (a_n) = (a_{n+1}) = \dots$ ∎

2.11. '20

Lecture 7

The greatest common divisor

The euclidean algorithm in Euclidean domains



Def

Let R be a UFD and let $a, b \in R$ with at least one of a and b non zero.
Then we say that $c \in R$ is the <u>greatest common divisor</u> of a and b, if both of the fol. conditions hold:

(1) $c \mid a$ and $c \mid b$

(2) if $d \mid a$ and $d \mid b$ for some $d \in R$, then $d \mid c$

Notation: $\gcd(a, b)$

Remarks:

- If c and c' are the g.c. division of a and b, then c and c' are associate.
  So, up to associativity, the gc divisor is unique, that is why we use "the"

- The above definition can be generalized to finitely many elements $a_1, \dots, a_n$.
  $\gcd(a_1, \dots, a_n)$.

Exercise:

Write a definition of $\gcd(a_1, \dots, a_n)$

How can we find the gcd?

I. Use the factorisation of both a and b into primes.

Example: $a = 2 \cdot 3^2 \cdot 5$, $b = (-2)^3 \cdot 3 \cdot (-7)$

$\gcd(a, b) = 2 \cdot 3$ or -6

II. Use the euclidean algorithm in Euclidean domains.
(we will talk about E. domains later today)
(see schnell!)

Properties of the gcd:

1°. $\gcd(a,b) = \gcd(b,a)$

2°. $\gcd(a,0) = 0 \quad (a \neq 0), \quad \gcd(a,1) = 1$

3°. $\gcd(ca, cb) = c \cdot \gcd(a,b) \quad , c \neq 0$

4°. $\gcd(a,b) = a \iff a \mid b$

5°. $\gcd(a,b) \mid \gcd(a,bc)$

6°. $\gcd(a, b+ca) = \gcd(a,b)$

7°. $\gcd(a,b,c) = \gcd(a, \gcd(b,c))$

8°. $\gcd(a,b) = 1 \iff \gcd(a^i, b^j) = 1 \quad i,j \in \mathbb{N}$

9°. $a \mid bc \;\&\; \gcd(a,b) = 1 \Rightarrow a \mid c$

$= \gcd(a,c) = a$

10°. $\gcd(a,b) = 1 \Rightarrow \gcd(a,bc) = \gcd(a,c)$

Euclidean domains

Def Let R be an integral domain.

A <u>Euclidean function</u> (a <u>norm</u>) is a function

$f: R \setminus \{0\} \to \mathbb{N}_0$

that satisfied the following ("division with remainder") property:

- $\forall\, a, b \in R$ with $b \neq 0$ $\exists\, q, r \in R$

s.t. $a = q \cdot b + r$ and either $r = 0$ or $r \neq 0$ and $f(r) < f(b)$

A <u>Euclidean domain</u> is an integral domain that can be endowed with at least one Euclidean function.

<u>Examples</u>: (1) $\mathbb{Z}$, $f(a) = |a|$

(2) Gaussian integers $\mathbb{Z}[i] := \{x + iy \mid x, y \in \mathbb{Z}\}$ } Euclidean domains

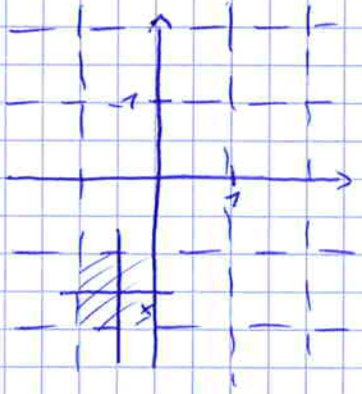
$f(x+iy) = x^2 + y^2$

Example

$a = 5 - 2i \;,\; b = 1 + 3i$

$a = q \cdot b + r \qquad f(r) < f(b)$

$$\frac{a}{b} = \frac{(5-2i)(1-3i)}{(1+3i)(1-3i)} = \frac{5-6-17i}{1+3^2} = \frac{-1}{10} - \frac{17}{10} i$$



$q = -2$

$5 - 2i = -2i(1+3i) + r$

$\quad = 6 - 2i + r \Rightarrow r = -1$

$\underbrace{(5-2i)}_{a} = \underbrace{(-2i)}_{q} \cdot \underbrace{(1+3i)}_{b} \underbrace{-1}_{r}$

$r \neq 0$

$1 = f(r) < f(b) = 10$

Warning: the division with remainder in $\mathbb{Z}[i]$ is not unique

(3) $\mathbb{Z}[\sqrt{-2}] \qquad f(a) = a \cdot \bar{a}$

(4) Not a euclidean domain: $\mathbb{Z}[\sqrt{-5}]$ because:

Thm
Every Euclidean domain is a principal ideal domain.

Proof: Let R be a Euclidean domain and f some E.f. and let $\{0\} \neq I \subset R$ be an ideal. We take $a \in I \setminus \{0\}$ with minimal $f(a)$ (think why such an a exists). We claim that $I = (a)$. Indeed, if we take an arbitrary $b \in I$, then we can find q, r so that $b = q \cdot a + r$ ($q \in R$) and either $r = 0$ (then we are done) or $r \neq 0$ with $f(r) < f(a)$. Since $r = b - qa \in I$ ($b \in I$, $q \in R$, $a \in I$) this is a contradiction ∎

NT

4.11.10

$\gcd(a,b)$ → 1) $\gcd(a,b) \mid a$, $\gcd(a,b) \mid b$

→ 2) If $d \mid a$ & $d \mid b$, then $d \mid \gcd(a,b)$

Thm If R is a principal ideal domain and $a, b \in R$ for which the gcd exists, then $\gcd(a,b) = xa + yb$ for some $x, y \in R$.

Proof Consider $I = (a,b) := \{xa + yb \mid x, y \in R\}$

$I = (g)$. We claim that $g = \gcd(a,b)$.

Why? → 1) $a = r \cdot g$, $r \in R$ same for b.

→ 2) $d \mid a$ & $d \mid b \Rightarrow d \mid xa + yb$

in particular, $d \mid \bar{x}a + \bar{y}b = g$ □

Remark It is not always clear how the gcd can be easily found. There is one case, when it is quick and easy, namely, the case of Euclidean Domains.

Reminder An integral domain is called a Euclidean domain if we can find a function $f: R \setminus \{0\} \to \mathbb{N}_0$ so that $\forall a, b \in R$ $(b \neq 0)$ $\exists q, r \in R$ with $a = q \cdot b + r$ where either $r = 0$ or else $f(r) < f(b)$

Ex

1) $\mathbb{Z}$, $f(n) = |n|$

2) $\mathbb{Z}[i]$, $f(n + im) = n^2 + m^2$

3) $K[x]$, where K is a field $f(\underbrace{a_0 + a_1 X + \dots + a_n X^n}_{P(x)}) = n = \deg(P(x))$ ($a_0 \neq 0$, $a_n \neq 0$, $\deg P(x)$)

Ex $P(x) = x^3 + 2x - 1$; $Q(x) = x^2 + 1$ $\quad P, Q \in \mathbb{Q}[x]$

$$\begin{array}{r|l} x & \leftarrow q \\ \hline x^2+1 & x^3+2x-1 \quad \leftarrow a \\ & x^3 + x \\ \hline & x + (-1) \quad (= r) \end{array}$$

(b=)

Euclidean Algorithm

Example $\quad \gcd(84, 57)$

~~84~~ = 1 · ~~57~~ $\qquad |27| < |54|$

$a \quad q \quad b \quad r$

$84 = 1 \cdot 57 + 27$

$57 = 2 \cdot 27 + 3$ ← $\gcd(a,b)$

$27 = 9 \cdot 3 + \boxed{0}$ ← Stop

$d \mid a \;\&\; d \mid b \quad a = a_0, \; b = a_1 \quad \Rightarrow d \mid a_2$ where $f(a_2) < f(a_1)$

$a_0 = q_1 \cdot a_1 + a_2$

$a_1 = q_2 \cdot a_2 + a_3$

$\dots$

$a_{n-2} = q_{n-1} \cdot a_{n-1} + \boxed{a_n}$ ← $\gcd(a,b)$

$a_n \mid a_{n-1} \quad a_{n-1} = q_n \cdot a_n + 0$

$\gcd(a,b) = x \cdot a + y\,b$

Extended EA.

$$3 = 57 - 2 \cdot 27 = 57 - 2 \cdot (84 - 1 \cdot 57)$$

$$= -2 \cdot 84 + 3 \cdot 57$$

$$\gcd(a,s) = xa + yb = (x + kb) \cdot a + (y - ka) \cdot b$$

Fibonacci numbers:

$F_1\ F_2\ F_3$
1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...

$$\gcd(F_9, F_{10}) = \gcd(34, 55)$$
$b\ ;\ a$

$55 = 1 \cdot 34 + 21$

$34 = 1 \cdot 21 + 13$

$21 = 1 \cdot 13 + 8$

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$ ↩

$2 = 2 \cdot 1 + 0$

Lemma: For $n \geq 2$, we have $F_{n+5} > 10 F_n$

Proof

$$F_{n+5} = F_{n+4} + F_{n+3} = (F_{n+3} + F_{n+2}) + F_{n+3}$$

$$= 2F_{n+3} + F_{n+2} = 2(F_{n+2} + F_{n+1}) + F_{n+2}$$

$$= 3F_{n+2} + 2F_{n+1} = 3(F_{n+1} + F_n) + 2F_{n+1}$$

$$= 5F_{n+1} + 3F_n = 5(F_n + F_{n-1}) + 3F_n$$

$$= 8F_n + 5F_{n-1} > 8F_n + 4F_{n-1}$$

$$(2F_{n-1} \geq F_{n-1} + F_{n-2} = F_n) \geq 8F_n + 2F_n = 10F_n$$

Thm (Lamé) If $a, b \in \mathbb{N}$, $a > b$, then the # of steps (divisions) in the EA is at most $5k$, where k = # of digits in b.

Ex $b = 23578$

Proof $a_n \geq 1 = F_2$, $a_{n-1} > a_n \geq 1$

$\Rightarrow a_{n-1} \geq 2 = F_3$; $a_{n-2} = q_{n-i} \cdot a_{n-1} + a_n \geq a_{n-1} + a_n \geq F_2 + F_3 = F_4$

$\Rightarrow a_{n-3} \geq \dots \geq F_5$

$b = a_1 \geq F_{n+1}$. If we have $n > 5k$ ($n \geq 5k+1$) then we would have $b \geq F_{5k+2} > 10 \cdot F_{5(k-1)+2}$

$> 10^2 \cdot F_{5(k-2)+2} > \dots > 10^k F_2 = 10^k$

(b would have more than 10 digits)

Contradiction

$\square$

NT

9.11.10

Lecture 3 Modular arithmetic. $\mathbb{Z}_m$.

Def Let $a, b, m \in \mathbb{Z}$ $(m \neq 0)$. We say that a is congruent to b modulo m if $m \mid (a-b)$.

Notation $a \equiv b \pmod{m}$ or $a \equiv b \ (m)$

Example

$2 \equiv 17 \pmod{5}$, because $5 \mid (2-17)$

$2 \not\equiv -11 \pmod{5}$, because $5 \nmid (2-(-11))$

Remark

We almost always assume that $m \in \mathbb{N}$ $(m > 0)$ because $a \equiv b \pmod{m} \iff a \equiv b \pmod{-m}$

Properties

1° $a \equiv b \ (m) \iff a = b + mk$ for some k

2° $a \equiv b \ (m) \iff a$ and b have the same remainder when divided by m.

3° Every integer is congruent to exactly one of the #'s in the set $\{0, 1, 2, \dots, m-1\}$

"$\equiv$" is an equivalence relation:

4° $a \equiv a \ (m)$ (reflexive)

5° $a \equiv b \ (m) \Rightarrow b \equiv a \ (m)$ (symmetric)

6° $a \equiv b \ (m)$, $b \equiv c \ (m) \Rightarrow a \equiv c \ (m)$ (transitive)

$\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} := \{0, 1, \dots, m-1\}$ with "+" and "·" that come from $\mathbb{Z} \pmod{m}$.

This operations are well-defined because of:

Prop.

Let $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ and let $a \equiv b \ (m)$, $c \equiv d \ (m)$. Then

(1) $a + c \equiv b + d \ (m)$

(2) $a \cdot c \equiv b \cdot d \ (m)$

Proof

We have $a \equiv b \ (m) \Rightarrow a = b + m \cdot k$ for some k

$c \equiv d \ (m) \Rightarrow c = d + m\ell$ for some $\ell \in \mathbb{Z}$

$$a \cdot c = (b + mk)(d + m\ell) = bd + m(\underbrace{b\ell + kd + mk\ell}_{\in \mathbb{Z}})$$

$\Downarrow$

$ac \equiv bd \ (m)$ (see Property 1°) ☐

Corollary

If $a \equiv b \ (m) \Rightarrow a^k \equiv b^k \ (m)$ for all $k \in \mathbb{N}$

Examples

1. Determine whether 2758152 is divisible by 3.

$$2758152 = 2 \cdot 10^6 + 7 \cdot 10^5 + 5 \cdot 10^4 + 8 \cdot 10^3 + 1 \cdot 10^2 + 5 \cdot 10^1 + 2 \cdot 10^0$$

$\lceil 10 \equiv 1 \ (3)$, $10^2 \equiv 1^2 \equiv 1 \ (3) \rfloor$

$$\equiv 2 \cdot 1 + 7 \cdot 1 + 5 \cdot 1 + 8 \cdot 1 + 1 \cdot 1 + 5 \cdot 1 + 2 \cdot 1$$

$$\equiv 2 + 1 + 2 + 2 + 1 + 2 + 2$$

$$\equiv 0 \ (3)$$

2. What is the remainder when 2^{72} is divided by 17?

$$2^4 = 16 \equiv -1 \ (17)$$

$$2^8 = (2^4)^2 \equiv (-1)^2 = 1 \ (17)$$

$$2^{72} = (2^8)^9 \equiv 1^9 = 1 \ (17)$$

II Linear congruences

$$ax \equiv b \ (m)$$

Thm Let $a, b, m \in \mathbb{Z}$, $\gcd(a, m) = d > 0$. Then

(1) $ax \equiv b \ (m)$ (*)

(2) If $d \mid b$, then there are exactly d incongruent solutions modulo m.

Examples

(1) $\underset{a}{4}x \equiv \underset{b}{3} \pmod{\underset{m}{2}}$ $\quad \gcd(4,2) = 2 = d$, $d \nmid b$ $(2 \nmid 3)$

Def: $a \mid b$

(2) $4x \equiv 5 \pmod 3$ $\quad d = 1 \Rightarrow 1 \mid 5$

$1 \cdot 4x \equiv 1 \cdot 5 \pmod 3$

$x \equiv 5 \pmod 3$

Def

a, b are relatively prime iff (if and only if) $\gcd(a, b) = 1$.

Lemma If $\gcd(a, m) = 1$

then $ax \equiv b \ (m)$ has a unique solution $(\mathrm{mod}\, m)$

Proof **Existence** Since $\gcd(a, m) = 1$, there exist $k, \ell \in \mathbb{Z}$ s.t. $k \cdot a + \ell \cdot m = 1$. In other words

$\exists\, k$: $\quad k \cdot a \equiv 1 \ (m)$

We multiply both sides of $(*)$ by k, then we get

$\underbrace{k \cdot a}_{\equiv 1 (m)} x \equiv k \cdot b \ (m)$

or

$x \equiv k \cdot b \ (m)$

Uniqueness

Suppose x' and x'' are solutions to $(*)$

Then $ax' \equiv b \equiv ax'' \ (m)$

$\Leftrightarrow ax' - ax'' \equiv 0 \ (m) \Leftrightarrow a \cdot (x' - x'') \equiv 0 \ (m)$

multiply by $k \ (= a^{-1}) \Rightarrow x' - x'' \equiv 0 \ (m)$

or $x' \equiv x'' \ (m)$

Proof of the Thm If $d = 1$, see Lemma.

consider $d > 1$

1) $\Rightarrow$ By Contradiction. Let $(*)$ has a solution say $\bar{x}$. but $d \nmid b$. We have that $a\bar{x} \equiv b \ (m)$ that is, $a\bar{x} - b = m \cdot \ell$ for some $\ell \in \mathbb{Z}$

Find $b = a\bar{x} - m\ell = d \cdot (\quad) \Rightarrow d \mid b$ ↯

1. $\Leftarrow$? We assume $d \mid b$ and consider:

$$\frac{a}{d} x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right) \quad (**)$$

In $(**)$, $\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$. We can apply Lemma to $(**)$ and find a solution y to $(**)$ unique modulo $\frac{m}{d}$.

We claim that $y, y+\frac{m}{d}, y+\frac{2m}{d}, \dots, y+\frac{(d-1)m}{d}$ are the only solutions to $(*)$ modulo m.

Indeed, we know that $\frac{a}{d} \cdot y \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

$$\left[\Rightarrow a \cdot y \equiv b \pmod{\tfrac{m}{d}} \overset{i}{\Longrightarrow} ay \equiv b \,(m)\right]$$

$$\frac{a}{d} \cdot y = \frac{b}{d} + i\,\frac{m}{d} \Rightarrow ay = b + im \Rightarrow ay \equiv b \,(m)$$

$$a\left(y + \frac{jm}{d}\right) = ay + a \cdot \frac{jm}{d} \equiv b + \underbrace{\frac{aj}{d}}_{\in \mathbb{Z}} \cdot m \equiv b \pmod{m}$$

The fact that there are no other solutions follows from the uniqueness in the Lemma.

NT

11.11.10

Last Time $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$

Def $a \equiv b \pmod m \iff m \mid (a-b)$

$ax \equiv b \pmod m$

$\gcd(a,m) = d$

If $d \nmid b$, then stop. No solution!

If $d \mid b$, then there are d solutions (incongruent mod m)

Examples:

(1) $2x \equiv 9 \pmod{10}$

$x \equiv 2 \pmod 5$

Answer: $x = 2, 7$

$2, 2+5$

(2) $10x \equiv 5 \pmod{25}$

$2x \equiv 1 \pmod 5$

$3 \cdot 2x \equiv 3 \pmod 5$

$2^{-1} \pmod 5$

$1 = (k) \cdot 2 + 4 \cdot 5$

$x \equiv 3 \pmod 5 \Rightarrow x = 3, 8, 13, 18, 23$

Thm

Simultaneous congruences. Chinese Remainder Theorem (CRT)

Let $m_1, m_2, \dots, m_k$ be pairwise relatively prime integers

$\gcd(m_i, m_j) = 1 \quad (i \neq j)$

Then:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \quad (10.*)$$

has a unique solution modulo $m_1 \cdot m_2 \cdots m_k$.

Proof: (Constructive!)

Existence $M = m_1 \cdot m_2 \cdots m_k$, $M_i = \prod_{j \neq i} m_j = \frac{M}{m_i}$

Then we find $x_1, \dots, x_k$: $x_i M_i \equiv 1 \pmod{m_i} \quad (i = 1, \dots, k)$

$\gcd(M_i, m_i) = 1$

We claim that $x = \underbrace{a_1 x_1 M_1 + a_2 x_2 M_2 + a_3 x_3 M_3 + \dots + a_k x_k M_k}$

is a solution to (10.*) $\equiv \underbrace{a_1 x_1}_{1} M_1 (m_1) \equiv a_1 (m_1)$

Example

$$\begin{cases} x \equiv 3 \ (4) & = m_1 \\ x \equiv 2 \ (5) & = m_2 \\ x \equiv 1 \ (9) & = m_3 \end{cases}$$

$M = 4 \cdot 5 \cdot 9 = 180$

$M_1 = 45$

$M_2 = 36$

$M_3 = 20$

$45 x_1 \equiv 1 \ (4) \Rightarrow x_1 \equiv 1$ (need only one solution)

$36 x_2 \equiv 1 \ (5) \Rightarrow x_2 = 1$

$20 x_3 \equiv 1 \ (9) \Rightarrow x_3 = 5$

$x = 3 \cdot 1 \cdot 45 + 2 \cdot 1 \cdot 36 + 1 \cdot 5 \cdot 20$

$= 135 + 72 + 100 = 307 \equiv 127 \ (180)$

Uniqueness Suppose x and y are two solutions to (10.*)

Then

$$x \equiv a_1 \equiv y \pmod{m_1} \Rightarrow m_1 \mid (x-y)$$

$$\vdots \qquad\qquad \vdots$$

$$x \equiv a_k \equiv y \pmod{m_k} \Rightarrow m_k \mid (x-y)$$

Prove by induction that $M = m_1 \cdots m_k \mid (x-y)$

1) $m_1 \mid (x-y)$ & $m_2 \mid (x-y) \overset{?}{\Longrightarrow} m_1 \cdot m_2 \mid (x-y)$

Indeed, $m_1 \mid (x-y) \Rightarrow x - y = m_1 \cdot k \ (k \in \mathbb{Z})$

Also $m_2 \mid (x-y)$, that is, $\underbrace{m_2 \mid m_1 \cdot k \ \& \ \gcd(m_1, m_2) = 1}_{k = m_2 \cdot \ell}$

$x - y = m_1 \cdot m_2 \cdot \ell \Rightarrow m_1 \cdot m_2 \mid (x-y)$

Finish yourself (complete the induction) □

Example

1) $x \equiv 2 \ (6)$

$x \equiv 0 \ (8)$ ↑ $4 \ (6)$

$\not{0}, 8, \overset{\parallel}{16}, 24, 32, 40$

$8, 32 \qquad (\text{mod } 48)$

2) $\begin{cases} x \equiv 1 \ (6) \\ x \equiv 0 \ (8) \end{cases} \qquad (\text{mod } 48)$

$\not{0}, 8, 16, 24, 32, 40$

no solutions.

II Fermat little Theorem (FLT)

Fix me!! Take $a \in \mathbb{Z}$, then a is congruent to exactly on # from the list $\{0, 1, 2, \ldots, m-1\}$, which is called "the last residue" of a modulo m".

Charts of last residues of a^k modulo $m = p \leftarrow$ prime

$p = 3$

a	a^2	a^3	a^4
0	0	0	0
1	1	1	1
2	1	2	1

$p = 5$

a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0
1	1	1	1	1	1
2	4	3	1	2	4
3	4	2	1	3	4
4	1	4	1	4	1

$p=7$

	a	a^2	a^3	a^4	a^5	a^6	a^7
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2							
3							
4							
5							
6							

Conjecture

$$a^p \equiv a \pmod p$$

Thm (FLT)

If $a \not\equiv 0 \ (p)$ then $a^{p-1} \equiv 1 \ (p)$, where p is prime

Proof

Let p be prime and $a \not\equiv 0 \pmod p$.

Consider the set $S = \{a, 2a, 3a, \dots, (p-1)\cdot a\}$.

We claim that

1) all elements of S are different mod p

2) none of them $\equiv 0$ mod p (all $j \cdot a \not\equiv 0 \bmod p$)

Indeed, to prove 1) assume $i \cdot a \equiv j \cdot a \ (p)$

for some $i, j \in \{1, \dots, p-1\}$. Then $(i-j)\cdot a \equiv 0 \ (p)$

or $p \mid (i-j)\cdot a \underset{p \nmid a}{\Longrightarrow} p \mid (i-j) \underset{0 < |i-j| < p-1}{\Longrightarrow} i = j$

If $i \cdot a \equiv 0 \ (p)$, then $p \mid i$ or $p \mid a$, which is wrong because $p \nmid a$, $p \nmid i$

Claim 1) & 2) mean that

$S \equiv \{1, 2, \dots, p-1\}$ modulo p (up to permutations of elements)

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)\cdot a \equiv 1 \cdot 2 \cdot 3 \cdot \dots (p-1) \text{ modulo } p$$

$$a^{p-1} (p-1)! \equiv (p-1)! \pmod p \quad \Leftarrow \text{ multiply with } ((p-1)!)^{-1}$$

$\ast$ $\gcd((p-1)!, p) = 1$

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

Examples

1) $p = 5$, $a = 2$

$S = \{2, 4, 6, 8\}$

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

2)

NT

16.11.11

The Chinese Remainder Theorem

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

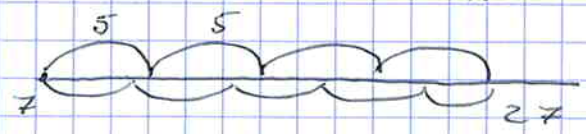
pairwise rel. prime $\Rightarrow \exists! x$

Ex:

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 4$

$x \equiv 7 \pmod{20}$



Fermat's Little Theorem

p is prime and $\gcd(a,p)=1$

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

Q: Is it true that if $a^{n-1} \equiv 1 \pmod n$, then n is prime?

A: No. Not necessarily

$$2^{52632} \equiv 1 \pmod{52633}$$ ← divisible by 7.

$(P \Rightarrow Q)$ (statement)

$(Q \Rightarrow P)$ (converse)

$(\neg Q \Rightarrow \neg P)$ (contrapositive)

$\neg P \Rightarrow \neg Q$ (inverse)

Lecture 11 The ring $\mathbb{Z}_n$

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z}\}$$

Example: $\mathbb{Z}_3 := \{0,1,2\} = \{0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$

Element of $\mathbb{Z}_n$ = Equivalence class modulo n.

Def (Direct sum = Direct product = Cartesian sum/product)
Let $R_1, R_2, \dots, R_k$ be rings

Then *direct product* is the set

$$R_1 \times R_2 \times \dots \times R_k := \{(r_1, r_2, \dots, r_k) \mid r_i \in R_i,\ 1 \le i \le k\}$$

with $+$: $(r_1, \dots, r_k) + (s_1, \dots, s_k) = (r_1 + s_1, \dots, r_k + s_k)$
and with $\cdot$: $(r_1, \dots, r_k) \cdot (s_1, \dots, s_k) = (r_1 \cdot s_1, \dots, r_k \cdot s_k)$

Thm:
Let $n = m_1 \cdot m_2 \cdot \dots \cdot m_k$, where $m_1, \dots, m_k$ are pairwise relatively prime. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}.$$

Example: $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

epimorphism = homo + surjection
mono = " + injection
iso = " + bijection

Proof:
Let Φ be defined as follows

$$\Phi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$$

$$\Psi$$

$$x \longrightarrow (\mathrm{Res}_{m_1} x, \mathrm{Res}_{m_2} x, \dots, \mathrm{Res}_{m_k} x), \text{ where}$$

$Res_{m_i} x$ is the least Residue of x modulo m_i.

We must prove that Φ is:

1) injective

We take $x, y \in \mathbb{Z}_m$ so that $\Phi(x) = \Phi(y)$

$Res_{m_i} x = Res_{m_i} y \quad \forall\, 1 \le i \le k$

By uniqueness in CRT, we have $x \equiv y \pmod m$

0) Φ is well-defined

x' and x'' are two representatives for class "$x + m\mathbb{Z}$", then $\Phi(x') = \Phi(x'')$

$$x'' = x' + m \cdot z \implies x'' = x' + m_i \cdot \underbrace{\left(\frac{m}{m_i} \cdot z\right)}_{\text{integer}}$$

$$x'' \equiv x' \ (m) \implies x'' \equiv x' \ (\text{mod } m_i) \quad \forall i$$

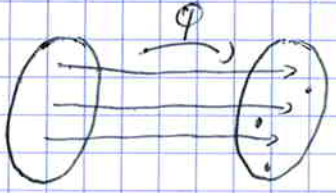
2) surjective.

two ways to show this:

I. Existence in CRT.

II. Φ is injective

- $\#\mathbb{Z}_m = \#(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}) = m$



1) + 2) $\implies$ Φ is bijective

3) Φ is a homomorphism

a) $\Phi(x+y) = \Phi(x) + \Phi(y)$ shall be shown

can be rewritten as

$$Res_{m_i}(x+y) = Res_{m_i}(Res_{m_i} x + Res_{m_i} y)$$

To see this, consider

$(x+y) - (Res_{m_i} x + Res_{m_i} y)$ and prove that it is divisible by m_i

Indeed $= (x - Res_{m_i} x) + (y - Res_{m_i} y)$

b) $(x \cdot y) - (Res_{m_i} x \cdot Res_{m_i} y)$

$= (x - Res_{m_i} x) \cdot y + Res_{m_i} x \cdot (y - Res_{m_i} y)$

The group of units $(\mathbb{Z}_n)^* =: U_n$

$$U_n = \{ a + n\mathbb{Z} \mid \gcd(a,n) = 1 \}$$

$ax \equiv 1 \pmod n$

$\varphi(n) = \# U_n$

Def The Euler phi-function

$$\begin{array}{rccc} \varphi: & \mathbb{N} & \to & \mathbb{N} \\ & \cup & & \\ & n & \to & \# U_n \end{array} \qquad \varphi(1) = 1$$

Examples: $\varphi(5) = \# U_5 = \# (\mathbb{Z}_5)^* = \# \{1,2,3,4\} = 4$

$\varphi(10) = \# \{1,3,7,9\} = 4$

Thm Euler If $\gcd(a,n) = 1$ then.

$$a^{\varphi(n)} \equiv 1 \pmod n$$

Idea of the proof

$U_n = \{b_1, b_2, \dots, b_{\varphi(n)}\}$

$S = \{ab_1, ab_2, \dots, ab_{\varphi(n)}\}$ □

Properties of $\varphi(n)$:

1° $\varphi(p) = p - 1$, if p is prime.

16.11.10

Wir betrachten das folgende gestörte Optimalitätssystem

$$\begin{aligned} Ax &= b \\ A^T\lambda + s &= c \\ x_i s_i &= \tau, \quad i = 1, \dots, n \\ x, s &> 0, \end{aligned}$$

wobei $\tau > 0$. $x > 0$ heißt $x_i > 0$, $i = 1, \dots, n$.

Ist $(x_\tau, \lambda_\tau, s_\tau)$ eine (möglichst eindeutige) Lösung von (7.1), so heißt die Abbildung $\tau \longmapsto (x_\tau, \lambda_\tau, s_\tau)$ der zentrale Pfad und die Bedingungen in (7.1) heißen zentrale Pfad-Bedingungen. Die Idee der Inneren-Punkte-Methoden besteht darin, den Pfad $\tau \searrow 0$ zu verfolgen.

Beispiel 7.1 Das Problem

$$\begin{aligned} \min\ & x_1 + x_2 \\ \text{u.d.N.}\ & x_1 + x_2 = 0 \\ & x_1 \geq 0, x_2 \geq 0 \end{aligned}$$

hat eine nichtleere zulässige Menge. Trotzdem sind die zentralen Pfad-Bedingungen nicht erfüllt, unabhängig davon, wie $\tau > 0$ gewählt wird.

Unser Ziel ist es zunächst, unter gewissen Voraussetzungen die Existenz und die Eindeutigkeit einer Lösung von (7.1) zu garantieren.

Wir führen das zu (5.4) gehörige primale logarithmische Barriere-Problem ein

$$\begin{aligned} \min\ & c^T x - \tau \sum_{i=1}^n \log(x_i) \\ \text{u.d.N.}\ & Ax = b \\ & x > 0 \end{aligned} \qquad (7.2)$$

Das zum dualen Problem (5.2) gehörige Barriere-Problem lautet

$$\begin{aligned} \max\ & b^T\lambda + \tau \sum_{i=1}^n \log(s_i) \\ \text{u.d.N.}\ & A^T\lambda + s = c \\ & s > 0 \end{aligned} \qquad (7.3)$$

Der Zusammenhang zwischen (7.1), (7.2) und (7.3) wird im folgenden Satz dargestellt (Analog zu Satz 5.3).

Satz 7.1 (Notwendige und hinreichende Optimalitätsbedingungen)

Sei $\tau > 0$ gegeben. Dann sind die folgenden Aussagen äquivalent:

a) Das primale Problem (7.2) besitzt eine Lösung x_τ.

b) Das duale Problem (7.3) besitzt eine Lösung (λ_τ, s_τ).

c) Das System (7.1) besitzt eine Lösung $(x_\tau, \lambda_\tau, s_\tau)$

Beweis: Folgt anhand der Karush-Kuhn-Tucker-Bedingungen für konvexe restringierte Optimierungsaufgaben. □

Definition 7.1 (Primal-dual zulässige Menge)

Die Menge $\mathcal{F} = \{(x, \lambda, s) : Ax = b, A^T\lambda + s = c, x \geq 0, s \geq 0\}$ heißt die (primal-dual) zulässige Menge, und die Menge $\mathcal{F}^\circ = \{(x, \lambda, s) : Ax = b, A^T\lambda + s = c, x > 0, s > 0\}$ heißt die (primal-dual) strikte zulässige Menge.

Erfüllt (x, λ, s) die Bedingung (7.1) $\Rightarrow \mathcal{F}^\circ \neq \emptyset$. Als nächstes werden wir die umgekehrte Aussage beweisen.

Satz 7.2 Die Menge $\mathcal{F}^\circ$ sei nicht leer. Dann besitzt das primale Barriere-Problem für jedes $\tau > 0$ eine optimale Lösung x_τ.

18.11.10 **Beweis:** $\tau > 0$ ... sei $(\hat{x}, \hat{\lambda}, \hat{s}) \in \mathcal{F}^\circ \Leftrightarrow A\hat{x} = b$, $A^T\hat{\lambda} + \hat{s} = c$, $\hat{x} > 0, \hat{s} > 0$

Wir bezeichnen mit $B_\tau(x) = c^T x - \tau \sum_{i=1}^{n} \log(x_i)$ die Zielfunktion des Problems (7.2)

Sei $\mathcal{L}_\tau := \{x \in \mathbb{R}^n : Ax = b, x \geq 0, B_\tau(x) \leq B_\tau(\hat{x})\}$ ($\neq \emptyset$, da $\hat{x} \in \mathcal{L}_\tau$)

Wir zeigen, dass $\mathcal{L}_\tau$ kompakt ist.

$\mathcal{L}_\tau = \underbrace{\{x \in \mathbb{R}^n : Ax = b, x \geq 0\}}_{\text{abgeschlossen}} \cap \underbrace{B_\tau^{-1}((-\infty, B_\tau(\hat{x})])}_{\text{abgeschlossen, da } B_\tau \text{ stetig}}$

$\Rightarrow \mathcal{L}_\tau$ abgeschlossen ✓

Es gilt $\forall x \in \mathbb{R}^n$ mit $Ax=b$: $c^T x = c^T x - \hat{\lambda}^T(Ax-b)$

$= c^T x - (\underbrace{A^T\hat{\lambda}}_{=c-\hat{s}})^T x + \hat{\lambda}^T b$

$= c^T x - (c-\hat{s})^T x + \hat{\lambda}^T b$

$= \hat{s}^T x + \hat{\lambda}^T b$

$\Rightarrow \forall x \in \mathcal{L}_\tau : B_\tau(x) = \hat{s}^T x + \hat{\lambda}^T b - \tau \sum_{i=1}^n \log(x_i)$ (✓)

Wir nehmen an, dass die Menge $\mathcal{L}_\tau$ unbeschränkt ist.

$\Rightarrow \exists \{x^k\}_{k\geq 1} \subset \mathcal{L}_\tau : \|x^k\| \to +\infty$

$\Rightarrow \exists j \in \{1,\dots,n\}: \{x_j^k\}_{k\geq 1} \to +\infty$

$\Rightarrow B_\tau(x^k) \leq B_\tau(\hat{x}) \overset{(V)}{\Leftrightarrow}$

$\overset{(✓)}{\Leftrightarrow} \hat{s}^T x^k + \hat{\lambda}^T b - \tau \sum_{i=1}^n \log(x_i^k) \leq B_\tau(\hat{x}),\ \forall k \geq 1$

$\Leftrightarrow \sum_{i=1}^n [\hat{s}_i x_i^k - \tau \log(x_i^k)] \leq B_\tau(\hat{x}) - \hat{\lambda}^T b,\ \forall k \geq 1.$

$\lim_{k\to+\infty} (\underbrace{\hat{s}_j}_{>0} x_j^k - \tau \underbrace{\log(x_j^k)}_{\to+\infty}) \to +\infty$

$\forall i = 1,\dots,n: t \mapsto \hat{s}_i t - \tau\log(t)$ ist nach unten beschränkt

(Minimum wird an der Stelle $\frac{\tau}{\hat{s}_i}$ angenommen)

(da $\lim_{t\to+\infty}(st - \tau\log(t)) = +\infty$:

$\lim_{t\to+\infty} \underbrace{\log(t)}_{\to+\infty}\left[s\frac{t}{\log(t)} - \tau\right] = \infty$

$= \lim \frac{1}{\frac{1}{t}} = \lim t = +\infty$)

$\Rightarrow \lim_{k\to+\infty} \sum_{i=1}^n [\hat{s}_i x_i^k - \tau\log(x_i^k)] = +\infty$ ↯

$\Rightarrow \mathcal{L}_\tau$ beschränkt $\Rightarrow \mathcal{L}_\tau$ kompakt

$\Rightarrow \exists x_\tau \in \mathcal{L}_\tau : B_\tau(x_\tau) = \min_{x\in\mathcal{L}_\tau} B_\tau(x)$ (✓✓)

$Ax_\tau = b$, $x_\tau > 0$ (falls nicht $\Rightarrow B_\tau(x_\tau) = +\infty$ ↯ $B_\tau(x_\tau) \leq B_\tau(\hat{x})$)

$\Rightarrow x_\tau$ zulässig für (7.2)

Gibt es ein x zulässig für (7.2) so, dass $B_\tau(x) < B_\tau(x_\tau)$

$\Rightarrow x \in \mathcal{L}_\tau$ ↯ zu (✓✓)

$\Rightarrow x_\tau$ opt. Lsg. von (7.2)

(7.2): $\min_{\substack{Ax=b \\ x>0}} B_\tau(x)$

□

Satz 7.3 (Existenz des zentralen Pfades)
Die strikt zulässige Menge E^0 sei nichtleer.
Dann besitzen die zentralen Pfadbedingungen (7.1)
für jedes $\tau > 0$ eine Lösung $(x_\tau, \lambda_\tau, s_\tau)$.
Dabei ist die x- und die s-Komponente dieses Vektors eindeutig bestimmt;
besitzt A vollen Rang, so ist auch λ^T eindeutig bestimmt.

(7.1): $Ax = b$, $A^T\lambda + s = c$, $x_i s_i = \tau$, $i = 1, \dots, n$, $x, s > 0$

Beweis: Sei $\tau > 0$. Laut Satz 7.2
$\Rightarrow \exists x_\tau$ opt Lsg von (7.2). Laut Satz 7.1
$\Rightarrow \exists (\lambda_\tau, s_\tau)$ opt. Lsg von (7.3) und
$(x_\tau, \lambda_\tau, s_\tau)$ ist eine Lösung des Optimalitätssystems (7.1)
Die zulässige Menge der Aufgabe (7.2) ist konvex
und die Zielfunktion B_τ ist strikt konvex
$\Rightarrow$ x_τ - eindeutig bestimmt.

f strikt konvex: $\forall x, y \in \mathbb{R}^n$, $x \neq y$, $\forall \lambda \in (0,1)$:
$f(\lambda x + (1-\lambda) y) < \lambda f(x) + (1-\lambda) f(y)$

$B_\tau(x) = c^T x - \tau \sum_{i=1}^{n} \ln(x_i)$ - strikt konvex
Sei x_τ nicht eindeutig bestimmt. $\Rightarrow \exists \overline{x_\tau}$ Lösung von (7.2), $\overline{x_\tau} \neq x_\tau$
$\Rightarrow \frac{1}{2} x_\tau + \frac{1}{2} \overline{x_\tau}$ - zulässig für (7.2)
$B_\tau(\frac{1}{2} x_\tau + \frac{1}{2} \overline{x_\tau}) < \frac{1}{2} B_\tau(x_\tau) + \frac{1}{2} B_\tau(\overline{x_\tau}) = B_\tau(x_\tau)$ ↯

Da $(x_\tau)_i (s_\tau)_i = \tau \quad \forall i = 1, \dots, n$
$\Rightarrow s_\tau$ eindeutig bestimmt.
Sei $\operatorname{rang}(A) = m \Rightarrow \underline{AA^T}$ - regulär.
$A^T \lambda_\tau + s_\tau = c \Rightarrow AA^T \lambda_\tau + A s_\tau = Ac$
$\Leftrightarrow (AA^T) \lambda_\tau = Ac - A s_\tau$
$\Leftrightarrow \lambda_\tau = (AA^T)^{-1} A(c - s_\tau) \Rightarrow \lambda_\tau$ - eindeutig bestimmt. □

18.11.10

Definition 7.2 (strikt komplementäre Lösung)

Eine Lösung (x^*, λ^*, s^*) der Optimalitätsbedingungen (5.3) heißt <u>strikt komplementär</u>, falls für alle $i = 1, \dots, n$,

<u>entweder</u> $x_i^* = 0$ <u>oder</u> $s_i^* = 0$.

Satz 7.4 (Konvergenz für $\tau \searrow 0$)

Die strikt zulässige Menge $\mathcal{F}^0$ sei nichtleer.

Für $\{\tau_k\}_{k=1} \searrow 0$ seien $(x_{\tau_k}, \lambda_{\tau_k}, s_{\tau_k})$ Lösungen des ZPB (7.1). Dann ist die Folge $\{(x_{\tau_k}, s_{\tau_k})\}_{k \geq 1}$ beschränkt und besitzt daher eine konvergente Teilfolge. Jeder Häufungspunkt dieser Folge gehört zu einer strikt komplementären Lösung von (7.1)

<u>Beweis:</u> Sei $\tau > 0$ und $(x^0, \lambda^0, s^0) \in \mathcal{F}^0$.

$$(x_\tau - x^0)^T (s^\tau - s^0) = (x_\tau - x^0)^T \cdot (c - A^T \lambda_\tau - c + A^T \lambda^0)$$

$$= (x_\tau - x^0)^T \cdot A^T (\lambda^0 - \lambda_\tau)$$

$$= (A(x_\tau - x^0))^T (\lambda^0 - \lambda_\tau)$$

$$= (b - b)^T (\lambda^0 - \lambda_\tau) = 0$$

$$x_\tau^T s_\tau - x_\tau^T s^0 - (x^0)^T s_\tau + (x^0)^T s^0 = 0$$

$$\Leftrightarrow \underbrace{x_\tau^T s^0 + (x^0)^T s_\tau}_{} = \underbrace{x_\tau^T s_\tau}_{n\tau} + (x^0)^T s^0 = n\tau + (x^0)^T s^0$$

Sei $\bar{\tau} > 0$ fixiert $\Rightarrow \forall\, \tau \in (0, \bar{\tau}]$:

$$\underbrace{x_\tau^T}_{\geq 0} s^0 + \underbrace{(x^0)^T}_{\geq 0} s_\tau \leq \underbrace{n\bar{\tau} + (x^0)^T s^0}_{\text{konstant}} \Rightarrow (x_\tau)_{\tau > 0},\ (s_\tau)_{\tau > 0} \text{ beschränkt}$$

$\bar{\tau} := \tau_1 \Rightarrow \forall\, k \geq 1 : \tau_k \in (0, \tau_1]$,

$$x_{\tau_k}^T s^0 + (x^0)^T s_{\tau_k} \leq n\tau_1 + (x^0)^T s^0$$

$$\Rightarrow (x_{\tau_k}, s_{\tau_k}) \text{ beschränkt}$$

$\Rightarrow \exists\, \{(x_{\tau_{k'}}, s_{\tau_{k'}})\}_{k' \geq 1}$ Teilfolge, die gegen ein Element (x^*, s^*) konvergiert.

$x_{k'} := x_{\tau_{k'}} \to x^* \geq 0$ ✓ $\quad A \underbrace{x_{\tau_{k'}}}_{\to x^*} = b \Rightarrow Ax^* = b$

$s_{k'} := s_{\tau_{k'}} \to s^* \geq 0$ ✓ $\quad c - s_{\tau_{k'}} = A^T \lambda_{\tau_{k'}} \in A^T(\mathbb{R}^m) = \text{Bild}(A^T)$

Und $A^T(\mathbb{R}^m)$ ist abgeschlossen.

$\Rightarrow c - s_{\tau_{k'}} \longrightarrow c - s^* \in A^T(\mathbb{R}^m)$

$\Rightarrow \exists \lambda^* \in \mathbb{R}^m : c - s^* = A^T \lambda^*$ ✓

$A^T \lambda^* + s^* = c$ ✓

$\Rightarrow (x^*, \lambda^*, s^*)$ - Lösung von (5.3)

Satz 5.3 $\Rightarrow$ x^* opt Lsg von (3.4)

(λ^*, s^*) opt Lsg von (5.2)

$(x_{\tau_{k'}})^T s_{\tau_{k'}} = \tau_{k'} \cdot n$

$\downarrow x^* \quad \downarrow s^*$

$(x^*)^T s^* \quad 0$

$\Rightarrow \boxed{(x^*)^T s^* = 0}$ ✓

$\Leftrightarrow x_i^* s_i^* = 0, i = 1 \to n$

Striktte Komplementarität:

Für $\tau > 0$: $(x_\tau - x^*)^T (s_\tau - s^*)^T = (x_\tau - x^*)^T A^T (\lambda^* - \lambda_\tau)$

$= (b - b^*)^T (\lambda^* - \lambda_\tau) = 0$

$x_\tau^T s^* + (x^* s_\tau) = \underbrace{x_\tau^T s_\tau}_{= n\tau} + \underbrace{(x^*)^T s^*}_{=0}$

$\Leftrightarrow \underline{\frac{1}{\tau} \cdot x_\tau^T s^* + \frac{1}{\tau} (x^*)^T s_\tau = n}$

$\forall k' \geq 1 : \tau := \tau_{k'} : \sum_{i=1}^n \frac{(x_{\tau_{k'}})_i \cdot s_i^*}{\tau_{k'}} + \sum_{i=1}^n x_i^* \left(\frac{(s_{\tau_{k'}})_i}{\tau_{k'}} \right) = n$

$\frac{(x_{\tau_{k'}})_i}{(s_{\tau_{k'}})_i} \to \infty$; $\frac{1}{(x_{\tau_{k'}})_i}$

$\Leftrightarrow \sum_{i=1}^n \frac{s_i^*}{(s_{\tau_{k'}})_i} + \sum_{i=1}^n \frac{x_i^*}{(x_{\tau_{k'}})_i} = n$

$\forall i = 1 \to n : x_i^* s_i^* = 0 \Rightarrow 0 \in \{x_i^* s_i^*\}$

Ich nehme an, dass für $\tau \in \{1 \to n\} : x_i^* = s_i^* = 0$

$k \to +\infty : \frac{s_i^*}{(s_{\tau_{k'}})_i} \to 1 \quad \Rightarrow$ entweder $x_i^* = 0$ oder $s_i^* = 0$. □

23.11.10

Korollar 7.5

Seien (x^*, λ^*, s^*) und $(x^{**}, \lambda^{**}, s^{**})$ zwei strikt komplementäre Lösungen von (5.3). Dann gilt

$$s_i^* > 0 \Leftrightarrow s_i^{**} > 0 \text{ und } x_i^* > 0 \Leftrightarrow x_i^{**} > 0 \quad \forall i = 1, \dots, n.$$

Beweis: ÜA 29

7.2. Innere-Punkte-Methoden via Newton-Verfahren

Wir wollen die Lösung des zentralen Pfad-Bedingungen mithilfe des Newton-Verfahrens beschreiben. Für $x \in \mathbb{R}^n$ und $s \in \mathbb{R}^n$ führen wir die folgenden Berechnungen ein:

$$X = \operatorname{diag}(x_1, \dots, x_n)$$
$$S = \operatorname{diag}(s_1, \dots, s_n)$$
$$e = (1, \dots, 1)^T \in \mathbb{R}^n$$

Dann lässt sich (7.1) wie folgt äquivalent schreiben:

$$F_\tau(x, \lambda, s) = 0, \quad x > 0, s > 0,$$

$$\text{wobei } F_\tau(x, \lambda, s) := \begin{pmatrix} A^T\lambda + s - c \\ Ax - b \\ XSe - \tau e \end{pmatrix} \quad \Big| \quad Xe = \begin{pmatrix} x_1 s_1 \\ \vdots \\ x_n s_n \end{pmatrix}, \ \tau e = \begin{pmatrix} \tau \\ \vdots \\ \tau \end{pmatrix} \Big| \quad (7.4)$$

Die Jacobi-Matrix hat die folgende Darstellung

$$\nabla F_\tau(x, \lambda, s) = \begin{pmatrix} 0 & A^T & I \\ A & 0 & 0 \\ S & 0 & X \end{pmatrix}$$

Satz 7.6 Sei $(x, \lambda, s) \in \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R}^n$ mit $x > 0$ und $s > 0$ gegeben. Besitzt A vollen Rang, dann ist die Jacobi-Matrix $\nabla F_\tau(x, \lambda, s)$ regulär.

Beweis: Wir zeigen, dass aus $\nabla F_\tau(x, \lambda, s) \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} = 0 \quad (p_1, p_2, p_3) = 0$ folgt

$$\Leftrightarrow \begin{cases} A^T p_2 + p_3 = 0 & | \cdot p_1^T \Rightarrow p_1^T A^T p_2 + p_1^T p_3 = 0 \Leftrightarrow \underbrace{(Ap_1)^T}_{=0} p_2 + p_1^T p_3 = 0 \Rightarrow \boxed{p_1^T p_3 = 0} \ \checkmark \\ Ap_1 = 0 \\ Sp_1 + Xp_3 = 0 \Rightarrow Sp_1 = -Xp_3 \Leftrightarrow p_1 = -S^{-1}Xp_3 \overset{\checkmark}{\Rightarrow} \end{cases}$$

$$\Rightarrow 0 = -p_3^T \underbrace{(S^{-1}X)}_{\text{pos. def.}} p_3 \Rightarrow p_3 = 0$$

$$\Rightarrow p_1 = 0$$

$$\left.\begin{matrix} A^T p_2 = 0 \\ \operatorname{rang}(A) = m \end{matrix}\right\} \Rightarrow p_2 = 0$$

□

Satz 7.6 rechtfertigt die Anwendung des Newton-Verfahrens auf (7.4).
Der Newton-Schritt bei dem Iterierten (x^k, λ^k, s^k)

$$DF_t(x^k, \lambda^k, s^k)\begin{pmatrix}\Delta x\\ \Delta\lambda\\ \Delta s\end{pmatrix} = -F_t(x^k, \lambda^k, s^k)$$

liefert $\begin{pmatrix}0 & A^T & I\\ A & 0 & 0\\ S^k & 0 & X^k\end{pmatrix}\begin{pmatrix}\Delta x\\ \Delta\lambda\\ \Delta s\end{pmatrix} = -\begin{pmatrix}A^T\lambda^k + s^k - c\\ Ax^k - b\\ X^k S^k e - t_k e\end{pmatrix}$, (7.5)

wobei $X^k = \operatorname{diag}(x_1^k, \dots, x_n^k)$ und $S^k = \operatorname{diag}(s_1^k, \dots, s_n^k)$.

Laut Satz 6.1 ist das Newton-Verfahren lokal konvergent.
Zwecks Globalisierung dieses Verfahrens bestimmt man eine Schrittweite $t_k > 0$ und man ersetzt die Vorschrift durch

$$(x^{k+1}, \lambda^{k+1}, s^{k+1}) = (x^k, \lambda^k, s^k) + t_k(\Delta x^k, \Delta\lambda^k, \Delta s^k)$$

Bemerkung 7.1 Wir nehmen an, dass die k-te Iterierte die Gleichungen $A^T x^k + s^k = c$ und $Ax^k = b$ erfüllt. Aus (7.5):

$$A^T\Delta\lambda^k + \Delta s^k = 0$$
$$A\,\Delta x^k = 0$$

Dann gilt $A^T\lambda^{k+1} + s^{k+1} - c = A^T(x^k + t_k\Delta\lambda^k) + s^k + t_k\Delta s^k - c$

$$= \underbrace{A^T\lambda^k + s^k}_{=c} + t_k\underbrace{(A^T\Delta\lambda^k + \Delta s^k)}_{=0} - c = 0$$

$$Ax^{k+1} = A(x^k + t_k\Delta x^k) = \underbrace{Ax^k}_{=0} + t_k\underbrace{A\Delta x^k}_{=0} = b$$

$\Rightarrow$ auch $(x^{k+1}, \lambda^{k+1}, s^{k+1})$ genügt den beiden Gleichungen $A^T\lambda + s = c$ und $Ax = b$.

Sofern dies für den Startvektor (x^0, λ^0, s^0) der Fall ist, genügen also alle Iterierten diesen Gleichungen. So können die ersten beiden Blöcke der rechten Seite von (7.5) durch Nullen ersetzt werden.
Als Nächstes geben wir ein allgemeines Innere-Punkte-Verfahren an, welches eine strikt zulässige Lösung als Startvektor verwendet und setzen voraus, dass $\operatorname{rang}(A) = m$.

23.11.10

Algorithmus 7.1 (Allgemeines Innere-Punkte-Verfahren)

1. Wähle $(x^0, \lambda^0, s^0) \in \mathcal{E}^0$, $\varepsilon > 0$ und setze $k = 0$
2. Ist $\mu_k := (x^k)^T s^k / n \leq \varepsilon$: STOP
3. Wähle $\sigma_k \in [0,1]$ und löse

$$\begin{pmatrix} 0 & A^T & I \\ A & 0 & 0 \\ S^k & 0 & X^k \end{pmatrix} \begin{pmatrix} \Delta x^k \\ \Delta \lambda^k \\ \Delta s^k \end{pmatrix} = - \begin{pmatrix} 0 \\ 0 \\ X^k S^k e - \sigma_k \mu_k e \end{pmatrix} \qquad (7.6)$$

4. Bestimme die Schrittweite $t_k > 0$ so, dass $x^k + t_k \Delta x^k > 0$ und $s^k + t_k \Delta s^k > 0$. Und setze:

$$x^{k+1} := x^k + t_k \Delta x^k$$
$$\lambda^{k+1} := \lambda^k + t_k \Delta \lambda^k$$
$$s^{k+1} := s^k + t_k \Delta s^k$$

5. Setze $k = k+1$ und gehe zu Schritt 2.

Bemerkung 7.2

a) $(x^0, \lambda^0, s^0) \in \mathcal{E}^0$ laut Bemerkung 7.1 und Schritt 4 folgt, dass $(x^k, \lambda^k, s^k) \in \mathcal{E}^0 \; \forall k \geq 1$.
Laut Satz 7.6 ist (7.6) eindeutig lösbar. Da $x^k > 0$, $s^k > 0$, so lässt sich ein $t_k > 0$ immer finden so, dass $x^{k+1} > 0$ und $s^{k+1} > 0$. Der Algorithmus 7.1 ist wohldefiniert.

b) Siehe Beweis des Satzes 5.1):

$$(x^k)^T s^k = c^T x^k - b^T \lambda^k$$

Dann bezeichnet man $\mu_k = \frac{(x^k)^T s^k}{n} = \frac{c^T x^k - b^T \lambda^k}{n}$ als gewichtete Dualitätslücke. Diese soll gegen 0 konvergieren.

Bemerkung 7.3

Der auf der rechten Seite von (7.6) auftretende Term $\sigma_k \mu_k$ spielt die Rolle t. Der Algorithmus 7.1 hat zwei Freiheitsgrade:

- in der Wahl des Zentrierungsparameters σ_k
- in der Wahl der Schrittweite t_k

Die Wahl von $\sigma_k = 0$ entspricht einem reinen Newton-Schritt für (5.3). Diese Wahl wird für kleine Schrittweiten sorgen, da wir noch $x^k > 0$ und $s^k > 0$ gewährleisten müssen.

Die Wahl von $\sigma_k = 1$ bringt uns nicht unbedingt dichter an die Lösungsmenge von (6.3), allerdings näher an den zentralen Pfad, was eine größere Schrittweite ermöglicht.

Wir zeigen als Nächstes, dass μ_k in jedem Schritt reduziert werden kann, in Abhängigkeit von t_k und σ_k. Dazu setzen wir:

$$(x^k(t), \lambda^k(t), s^k(t)) = (x^k, \lambda^k, s^k) + t(\Delta x^k, \Delta \lambda^k, \Delta s^k)$$

$$\mu_k(t) = \frac{(x^k(t))^T s_k(t)}{n}$$

Lemma 7.7 Die Lösung des linearen Gleichungssystems (7.6) besitzt die folgenden Eigenschaften

(a) $(\Delta x^k)^T \Delta s^k = 0$

(b) $\mu_k(t) = (1 - t(1 - \sigma_k))\mu_k$.

VT **Def:** 23.11

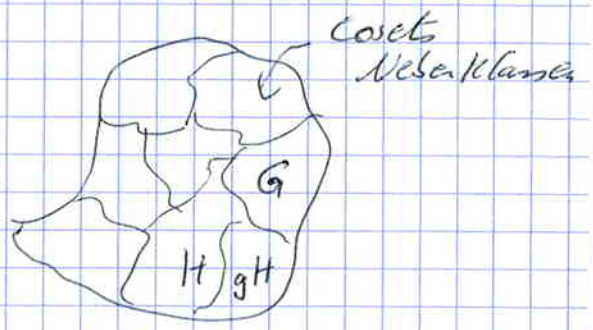
Let G be a group. The Order of G is its cardinality, that is, the # of elements in it, if G is finite or ∞ (in the later case we distinguish countable and uncountable groups)

Notation $|G|$ or $\text{ord}(G)$

Lemma If H is a subgroup of a finite group G then $|H|$ divides $|G|$

Proof Idea:

$|H| \mid |G|$ $\qquad |G| = K \cdot |H|$



$K = [G:H]$ - index of H in G.

$|G| = |H| \cdot [G:H]$ (Lagrange's Theorem)

Example: $(\mathbb{Z}_6, +) = \{0,1,2,3,4,5\} = G$

$H = \{0, 2, 4\}$

cosets $\rightarrow 1 + H = \{1, 3, 5\}$

Last time we defined $\text{ord}\, a$, where $a \in (G, \cdot)$ The smallest k s.t. $a^k = 1$ is called the order of a. In other words, $\text{ord}\, a = |\langle a \rangle|$, where $a \in (G, \cdot)$

Indeed, if $\text{ord}\, a = n$, then

$\langle a \rangle = \{a, a^2, \ldots, a^n = 1\}$

Lemma 2

Let $a \in (G, \cdot)$ and $a^x = 1$, then $\operatorname{ord} a \mid x$.

Proof

Denote $\operatorname{ord} a = n$ and write

$x = q \cdot n + r$, where $0 \le r < n$.

$a^x = 1 \Rightarrow a^{q \cdot n + r} = 1 \Rightarrow (a^n)^q \cdot a^r = 1 \Rightarrow a^r = 1$

If $r > 0$, then $\lightning$ $\Rightarrow r = 0 \Rightarrow x = q \cdot n \Rightarrow n \mid x$ □

Reminder: If $g \in \mathbb{Z}_n^*$ $\quad \mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

we denote $\operatorname{ord} g$ by $\operatorname{ord}_n g$ $\quad a \cdot x \equiv 1 \ (n)$

$|\mathbb{Z}_n^*| = \varphi(n)$

Lemma 3

$$\operatorname{ord}_m a^k = \frac{\operatorname{ord}_m a}{\gcd(k, \operatorname{ord}_m a)} \qquad \left(\operatorname{ord}_m 8 = \frac{\operatorname{ord} 2}{\gcd(3, \operatorname{ord} 2)} \right)$$

Proof

Denote RHS by x.

We want to show that $\operatorname{ord}_m a^k = x$, that is,

we want to show:

1) $(a^k)^x \equiv 1 \pmod m$

2) that x is the smallest such #

Indeed:

1) $$(a^k)^x = (a^k)^{\frac{\operatorname{ord}_m a}{\gcd(k, \operatorname{ord}_m a)}} = \left(a^{(\operatorname{ord}_m a)}\right)^{\frac{k}{\gcd(k, \operatorname{ord}_m a)}} = 1^{\text{integer}} \equiv 1 \pmod m$$

2) Suppose $(a^k)^y \equiv 1 \ (m) \Rightarrow a^{ky} \equiv 1 \ (m)$

$\overset{\text{Lemma 2}}{\Rightarrow}$ $\operatorname{ord}_m a \mid ky \Rightarrow ky = \operatorname{ord}_m a \cdot b$

$$\Rightarrow ky = \operatorname{ord}_n a \cdot b \Rightarrow \frac{ky}{\gcd(k, \operatorname{ord}_n a)} = \frac{\operatorname{ord}_n a \cdot \ell}{\gcd(k, \operatorname{ord}_n a)}$$

$$\Rightarrow x \cdot \ell = \frac{k}{\gcd(k, \operatorname{ord}_n a)} \cdot y \rightarrow x \mid \frac{k}{\gcd(k, \operatorname{ord}_n a)} \cdot y$$

$$\& \quad \gcd\left(x, \frac{k}{\gcd(k, \operatorname{ord}_n a)}\right) = 1$$

$$\Rightarrow x \mid y \Rightarrow x \text{ is smallest}$$

□

Corollary

$\forall a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ $\quad \operatorname{ord}_n a \mid \varphi(n)$.

$\Rightarrow |\mathbb{Z}_n^*|$

$$\boxed{a^{\varphi(n)} \equiv 1 \pmod n \quad \gcd(a, n) = 1}$$

Lemma 4

$$\sum_{d \mid n} \varphi(d) = n$$

Lemma 5

If $p \neq 3$ is prime, then the congruence $x^d \equiv 1 \pmod p$ has exactly d solutions modulo p.

Proof

We know that $x^{p-1} \equiv 1 \pmod p$ has exactly $p-1$ solutions mod p

$$x^{p-1} - 1 \equiv 0 \pmod p \quad \text{and} \quad p - 1 = d \cdot \ell$$

$$\underbrace{0 \equiv x^{d \cdot \ell} - 1}_{\substack{\text{has exactly} \\ p-1 \text{ solutions} \pmod p}} = \underbrace{(x^d - 1)}_{\substack{\equiv 0 \\ \text{at most} \\ d \text{ solutions}}} \underbrace{\left(x^{d(\ell-1)} + x^{d(\ell-2)} + \ldots + x^d + 1\right)}_{\substack{\equiv 0 \\ \text{at most } d(\ell-1) \text{ solutions}}} \text{ no zero divisors mod } p.$$

$$\text{at most } d \cdot d(\ell - 1) = d \cdot \ell$$

$$\leq d \cdot \ell$$

$$= p - 1$$

□

Thm Let $p \neq 3$ be prime and $d \mid p-1 \ (d > 0)$ then in $\mathbb{Z}_p^*$ there are exactly $\varphi(d)$ elements of order d.

Example $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$\operatorname{ord}_5 1 = 1$

$\operatorname{ord}_5 2 = 4$, b/c $2^1 \not\equiv 1 \ (5)$, $2^2 \not\equiv 1 \Rightarrow \operatorname{ord} 2 = 4$

$\operatorname{ord}_5 3 = 4$

$\operatorname{ord}_5 4 = 2$ b/c $4^1 \not\equiv 1$, $4^2 \equiv 1 \pmod 5$

$\varphi(1) = 1$ elements of order 1

$\varphi(2)$ elements of order 2

$\varphi(4)$ elements of order 4

Proof $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$

We subdivide this set into the following subsets here $d \mid p-1$

$$A(d) = \{ a \in \mathbb{Z}_p^* \mid \operatorname{ord}_p a = d \}$$

Then the set

$$\mathbb{Z}_p^* = \bigsqcup_{d \mid p-1} A(d)$$

Denote by $\psi(d) = \# A(d)$

We want to show that $\psi(d) = \varphi(d)$

Note that

1) $\sum_{d \mid p-1} \varphi(d) = p-1$

2) $\sum_{d \mid p-1} \psi(d) = p-1$, b/c $\# (\mathbb{Z}_p^*) = p-1$

$1 \& 2) \Rightarrow \sum_{d \mid p-1} (\varphi(d) - \psi(d)) = 0 \qquad (*)$

We will prove now that $\psi(d) \leq \varphi(d)$ (**)

This (**) and (*) will give that $\psi(d) = \varphi(d)$

To prove (**) we show that either $\psi(d) = 0$ or $\psi(d) = \varphi(d)$.

If $\psi(d) \neq 0$, then $A(d)$ contains at least one element, denote it a ($a \in \mathbb{Z}_p^*$, $\operatorname{ord}_p a = d$).

$\Rightarrow a^d \equiv 1 \pmod p$ and the congruence $x^d \equiv 1 \pmod p$ has solutions $L\{a, a^2, \dots, a^d\}$ and all this numbers(L) are different.

By Lemma 5 there are no other solutions.

What are the elements of $A(d)$ - are those a^k from the list L. For which $\operatorname{ord}_p a^k = \operatorname{ord}_p a = d$ this is there with $\gcd(k, d) = 1$. There are exactly $\varphi(d)$ such elements in the list L (and $\Rightarrow$ in $A(d)$) q.

30.11.10

UT

c) $\langle -1 \rangle \cap \langle 5 \rangle = \{1\}$

Proof

$\langle -1 \rangle = \{-1, 1\}$, if $\langle -1 \rangle \cap \langle 5 \rangle \neq \{1\}$

$\Rightarrow -1 \in \langle 5 \rangle$, that is, $-1 = 5^k$, but this equation modulo 4 is $-1 \equiv 1 \bmod 4$ ↯

Lecture 15 Quadratic residues

The Legendre symbol

Def Let p be prime and $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod p$. Then a is called a quadratic residue (QR) modulo p $\Leftrightarrow \exists\, c \in \mathbb{Z} : c^2 \equiv a \pmod p$

If no such number c exist, then a is called a quadratic nonresidue (NR) modulo p.

Proposition

Let p be an odd prime, then in $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ there are exactly $\frac{p-1}{2}$ QR's and $\frac{p-1}{2}$ NR's.

Proof Let g be a generator of $\mathbb{Z}_p^*$

$$\mathbb{Z}_p^* = \{g, g^2, g^3, \dots, g^{p-1} = 1\}$$

1) $g^{2k}_{=a}$ is a QR, because $(g^k)^2 = g^{2k}_{=a} \bmod p$.

2) To prove that g^{2k+1} is a NR, we suppose that this is not the case. We suppose that $\exists c \in \mathbb{Z}, c \not\equiv 0 (p)$ s.t. $c^2 \equiv g^{2k+1} \bmod p$

$$1 \underset{F.L.T}{\equiv} c^{p-1} = (c^2)^{\frac{p-1}{2}} \equiv (g^{2k+1})^{\frac{p-1}{2}} \equiv (g^{p-1})^k \cdot g^{\frac{p-1}{2}} \underset{FLT}{\equiv} g^{\frac{p-1}{2}} (p)$$

So we have $g^{\frac{p-1}{2}} \equiv 1 (p)$ ↯ □

Corollary

$$QR \cdot QR = QR$$
$$NR \cdot NR = QR$$
$$QR \cdot NR = NR$$

Example

Find all Quadratic Residues modulo 13.

$\mathbb{Z}_{13}^* = \{1, 2, \dots, 12\}$

$1^2 \equiv 1 (13)$	$12^2 \equiv 1$
$2^2 \equiv 4$	$11^2 \equiv 4$
$3^2 \equiv 9$	$10^2 \equiv 9$
$4^2 \equiv 3$	$9^2 \equiv 3$
$5^2 \equiv 12$	$8^2 \equiv 13$
$6^2 \equiv 10$	$7^2 \equiv 10$

c^2

$(p-c)^2 = p^2 - 2pc + c^2$

$\equiv c^2 \pmod p$

$x^2 \equiv a \pmod p$

Def

The Legendre symbol of a modulo p is

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a QR mod } p \\ -1, & \text{NR} \\ 0, & \text{if } p \mid a \quad (\text{i.e. } a \equiv 0 \bmod p) \end{cases}$$

Properties

1°. If $a \equiv b \bmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

2° $\left(\frac{a+kp}{p}\right) \underset{1°}{=} \left(\frac{a}{p}\right)$, $k \in \mathbb{Z}$

3°. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ {follows from corollary}

4° $\left(\frac{a \cdot b^2}{p}\right) = \left(\frac{a}{p}\right)$ if $p \nmid b$ (if $b \not\equiv 0 \bmod p$)

Thm (Euler's criterion)
Let p be an odd prime. Then

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

Proof

1) $a \equiv 0 \bmod p$ then $\left(\frac{a}{p}\right) = 0$ and $a^{\frac{p-1}{2}} = 0 \ (p)$
2) a is a QR $\bmod p$, then $\left(\frac{a}{p}\right) = 1$, $a^{\frac{p-1}{2}} = (c^2)^{\frac{p-1}{2}} = c^{p-1} \underset{\text{FLT}}{=} 1$
3) a is a NR $\bmod p$, then $\left(\frac{a}{p}\right) = -1$ $\quad c \not\equiv 0 \ (p)$

$a = g^{2k+1}$ for $k \in \mathbb{Z}$ and g generator of $\mathbb{Z}^*$.

$$a^{\frac{p-1}{2}} = \left(g^{2k+1}\right)^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \not\equiv 1, \text{ but } \left(g^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod p$$

$$\Rightarrow g^{\frac{p-1}{2}} \equiv -1 \pmod p$$

$\square$

Example

$$1 = \frac{-1}{8753} \equiv (-1)^{\frac{8752}{2}} = (-1)^{4376} = 1 \pmod{8753}$$

Thm (Quadratic Reprocity Law)

I $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv -1 \pmod 4 \end{cases}$

II $\left(\frac{2}{p}\right) = (-1)^{\frac{(p-1)(p+1)}{8}} = \begin{cases} 1, & p \equiv \pm 1 \ (8) \\ -1, & p \equiv \pm 3 \ (8) \end{cases}$

III $\left(\frac{q}{p}\right) = -1^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \frac{p}{q} = \begin{cases} -\left(\frac{p}{q}\right), & \text{if } p \equiv q \equiv 3 \ (4) \\ \frac{p}{q}, & \text{otherwise} \end{cases}$

odd primes

Example 1

1) $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1+3\cdot 2}{3}\right) = -\left(\frac{1}{3}\right) = -1$

2) $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \frac{1}{5} = 1$

3) $\left(\frac{69}{389}\right) = \left(\frac{3\cdot 23}{389}\right) = \left(\frac{3}{389}\right)\left(\frac{23}{389}\right) = \left(\frac{389}{3}\right)\cdot\left(\frac{389}{23}\right)$

$= -\left(\frac{2}{3}\right)\cdot\left(\frac{21}{23}\right) = -1\cdot\left(\frac{3}{23}\right)\cdot\left(\frac{7}{23}\right) = -\frac{23}{3}\cdot\frac{23}{7}$

$= -\left(\frac{2}{3}\right)\cdot\left(\frac{2}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{9}{7}\right) = 1$

Proof QRL I

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \qquad \text{(Eulers Criterion)}$$

$p \equiv 1(4) \Rightarrow p = 4k+1 \Rightarrow \frac{p-1}{2} = 2k$

$p \equiv 3(4) \Rightarrow p = 4k+3 \Rightarrow \frac{p-1}{2} = 2k+1$

I. 5 proved.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \equiv c^2 \not\equiv 0 \ (p) \\ -1, & \text{else} \\ 0, & p \mid a \end{cases}$$

THM QRL

1) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \ (4) \\ -1, & p \equiv -1 \ (4) \end{cases}$

2) $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \ (8) \\ -1, & p \equiv \pm 3 \ (8) \end{cases}$

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

In order to proove (2) we need the following Lemma:

Lemma (Gauss)

Let p be an odd prime, ~~$a \neq 0$~~ $a \not\equiv 0 \ (p)$. Then $\left(\frac{a}{p}\right) = (-1)^h$, where h is the ~~number~~ of integers in $S = \{a, 2a, \dots, \frac{p-1}{2}a\}$ whose least residue $> \frac{p-1}{2}$

Example $\left(\frac{3}{13}\right)$, $S = \{3, 6, 9, 12, 15, 18\}$

$\overset{\text{mod } 13}{\equiv} \{3, 6, \underline{9}, \underline{12}, 2, 5\}$

$\Rightarrow h = 2$

So by Gauss' Lemma $\Rightarrow \left(\frac{3}{13}\right) = (-1)^2 = 1$

Check $\left(\frac{3}{13}\right) = \left(\frac{3+13}{13}\right) = \left(\frac{16}{13}\right) = \left(\frac{4^2}{13}\right) = 1$

Proof

Idea: If j and k are two different integers in $[1, \frac{p-1}{2}]$, then $ja \not\equiv ka \mod p$

// they were equal, then $(j-k)a \equiv 0 \ (p)$

$\Rightarrow p \mid (j-k)a$

Also $ja \not\equiv -ka \ (p)$, because otherwise $p \mid (j+k)a$

it means, that if $S' \equiv S \bmod p$ and $S' \in (-\frac{p}{2}, \frac{p}{2})$, then ~~all numbers in S'~~ the absolut values of all numbers in S' are different.

$S' = \{\pm 1, \pm 2, \dots\}$

only one of this signs!

Multiply

$$a \cdot 2a \cdot \dots \cdot \frac{p-1}{2} a \equiv (-1)^h \cdot \left(\frac{p-1}{2}\right)!$$

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \underset{\text{Kriterion}}{\overset{\text{Eulers}}{\equiv}} \left(\frac{a}{p}\right) \cdot \left(\frac{p+1}{2}\right)! \quad \text{mod } p$$

Now we prove QRL (II.)

II For $\left(\frac{2}{p}\right)$ we have $S = \{2, 4, 6, \dots, p-1\}$

S has already only least residues mod p

h = # of ~~elements~~ elements in S and in $(\frac{p}{2}, p)$

= # of even numbers in $(\frac{p}{2}, p)$

= # of integers in $(\frac{p}{4}, \frac{p}{2})$

(1) $p \equiv 1 \ (8)$, then $p = 1 + 8k$ for some k

h = # of integers in $(2k + \frac{1}{4}, 4k + \frac{1}{2})$, $k \in \mathbb{Z}$

= # $\{2k+1, 2k+2, \dots, 2k+2k\}$

= $2k$, h is even.

$\Rightarrow \left(\frac{2}{p}\right) = 1$ for $p \equiv 1 \ (8)$

(2) - (4) are similar

To prove III:

~~Let~~

Lemma

Let p be an odd prime and $a \not\equiv 0 \ (p)$
Let q be another prime so that
$q \equiv \pm p \pmod{4a}$

Then

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

Proof

$$S_p = \left\{ a, 2a, \ldots, \frac{p-1}{2} a \right\}$$

Ef from Gauss' lemma

h_p = # of elements in S_p whose least residues $> \frac{p}{2}$

= # of elements in S_p and in $\left(\frac{p}{2}, p\right) \cup \left(\frac{3p}{2}, 2p\right) \cup \left(\frac{5p}{2}, 3p\right) \cup \ldots$

= # of integers in $\left[1, \frac{p-1}{2}\right]$ and in $\left(\frac{p}{2a}, \frac{p}{a}\right) \cup \left(\frac{3p}{2a}, \frac{2p}{a}\right), \ldots$

h_q = # of integers in $\left[1, \frac{q-1}{2}\right]$ and in $\left(\frac{q}{2a}, \frac{q}{a}\right) \cup \left(\frac{3q}{2a}, \frac{2q}{2a}\right), \ldots$

(i) $q \equiv p \ (4a) \Rightarrow q = p + 4aqk$ for some $k \in \mathbb{Z}$

h_q = # of integers in $\left[1, \frac{p-1}{2} + 2ak\right]$

and in $\left(\frac{p}{2a}+2k, \frac{p}{a}+4k\right) \cup \left(\frac{3p}{2a}+6k, \frac{2p}{a}+8k\right)$

...

The general fact: The # of integers in

$(x, y), (x, y+2), (x+2k, y+2k)$

have the same parity, i.e.

they are either both even or both odd.

This means, that ~~the parity~~ h_p and h_q have the same parity.

$$\left(\frac{a}{p}\right) = (-1)^{h_p} = (-1)^{h_q} = \left(\frac{a}{q}\right)$$

Proof III Part of Th 19

Case $p \equiv q \ (4)$

$\Rightarrow p = 4k+q$ for some $k \in \mathbb{Z}$

$$\left(\frac{p}{q}\right) = \left(\frac{4k+q}{q}\right) = \left(\frac{4k}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{k}{q}\right) = \left(\frac{k}{q}\right) \quad (*)$$

and:

$$\left(\frac{q}{p}\right) = \left(\frac{p-4k}{p}\right) = \left(\frac{-4k}{p}\right) = \left(\frac{-k}{p}\right)$$

$$= \left(\frac{-1}{p}\right)\left(\frac{k}{p}\right) \overset{\text{Lemma above}}{=} \left(\frac{-1}{p}\right)\left(\frac{k}{q}\right) \overset{(*)}{=} \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right)$$

So we have that if $p \equiv q \equiv 1 \ (4)$, then by I of the lemma QRL we get $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ and if $p \equiv q \equiv 3 \ (4)$, then $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$

Case 2 $p \equiv q+2 \ (4) \ (\Leftrightarrow p \equiv -q \ (4))$

$\Rightarrow p+q = 4k$ for some $k \in \mathbb{Z}$

$$\left(\frac{p}{q}\right) = \left(\frac{4k-q}{q}\right) = \left(\frac{a}{q}\right); \left(\frac{q}{p}\right) = \left(\frac{4k-p}{p}\right) = \frac{k}{p} \overset{\text{Lemma}}{=} \frac{k}{q} = \frac{p}{q}$$ $k \in \mathbb{Z}$ ∎

QRL

I) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 (4) \\ -1, & \text{if } p \equiv -1 (4) \end{cases}$

II) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 (8) \\ -1 & \text{if } p \equiv \pm 3 (8) \end{cases}$

III) $\left(\frac{p}{q}\right) = \begin{cases} -\frac{q}{p} & \text{if } p \equiv q \equiv 3 (4) \\ \left(\frac{q}{p}\right) & \text{if } \sout{p \equiv q \equiv} \text{ otherwise} \end{cases}$

Example

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

1. $p \equiv 1 (4)$

$$\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & p \equiv 1 (3) \\ \left(\frac{2}{3}\right) = -1 & p \equiv 2 (3) \end{cases}$$

2. $p \equiv \sout{-3} (4)$

$$\left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} u & u \\ 0 & p \equiv 3 \end{cases}$$

Exercise

Prove that $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 (12) \\ -1 & \text{if } p \equiv \pm 5 (12) \\ 0 & \text{if } p \equiv 3 (12) \end{cases}$

Final Exam (Klausur) 8.2.2017 11:00

The Jacobi-Symbol

Def Let $a \in \mathbb{Z}$, u be an odd number and let $u = p_1^{e_1} \cdots p_k^{e_k}$ the prime factorization.

Then the Jacobi Symbol $\left(\frac{a}{u}\right)$ is defined as follows

$$\left(\frac{a}{u}\right) := \left(\frac{a}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{e_k}$$

Properties

(u, v are odd integers)

1) $a \equiv b \pmod{u}$
$\Rightarrow \left(\frac{a}{u}\right) = \left(\frac{b}{u}\right)$

2) $\left(\frac{a + ku}{u}\right) = \left(\frac{a}{u}\right)$

3) $\left(\frac{ab}{u}\right) = \left(\frac{a}{u}\right)\left(\frac{b}{u}\right)$

4) $\left(\frac{a \cdot b^2}{u}\right) = \left(\frac{a}{u}\right)$ if $\gcd(u, b) = 1$

5) $\left(\frac{a}{u \cdot v}\right) = \left(\frac{a}{u}\right)\left(\frac{a}{v}\right)$

Warning

If $\left(\frac{a}{u}\right) = 1$ this does not mean anymore, that a is necessarily a QR modulo u.

Example

$$\left(\frac{41}{51}\right)=\left(\frac{41}{3\cdot 17}\right) \overset{(5)}{=} \left(\frac{41}{3}\right)\cdot\left(\frac{41}{17}\right) = \left(\frac{2}{3}\right)\left(\frac{7}{17}\right)$$

$$= -1 \cdot \left(\frac{17}{7}\right) = -1\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right)=\left(\frac{1}{3}\right) = 1$$

Suppose 41 is a square mod 51

$\Rightarrow \exists\, c \in \mathbb{Z}$ such that

$41 = c^2 \pmod{51}$

$\Rightarrow 41 = c^2 \pmod{3}$ $\quad 3\cdot 17$

$\left[c^2 = 41 + k\cdot 51 = 41 + (k\cdot 17)\cdot 3\right]$

$\Rightarrow 41 \equiv 2 \pmod 3$, but 2 is not a square modulo 3 $\left(\left(\frac{2}{2}\right) = -1\right)$

Example

Does the congruence

$x^2 \equiv 888 \pmod{1999}$ have a solution?

1999 prime

$$\left(\frac{888}{1999}\right) = \left(\frac{2^3\cdot 111}{1999}\right) \overset{(4)}{=} \left(\frac{2}{1999}\right)\left(\frac{111}{1999}\right)$$

legendre-symbol

$$\overset{(2)}{=} 1 + \left(\frac{1999}{111}\right) = -\left(\frac{1}{111}\right) = -\left(\frac{1}{p\cdot q\cdot \dots}\right) =$$

$$-1\cdot 1\cdot \dots = -1$$

Proposition

Let p be prime and $p \equiv 3(4)$

and let a be a QR mod p $\left\{\left(\frac{a}{p}\right) = 1\right\}$

Then $c \equiv a^{\frac{p+1}{4}}$ is a solution to $x^2 \equiv a \pmod p$

Proof

Substitute $a^{\frac{p+1}{4}}$ to $x^2 \equiv a \ (p)$

$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \equiv \left(\frac{a}{p}\right) \cdot a = a \pmod p$$

↑ Eulers criterion

Remark

a^n, $a, a^2, a^4, a^8, \ldots$

Example

$n = 14 = 1110$

$a^{14} = a^{2^3} \cdot a^{2^2} \cdot a^1$

The square-and-multiply-method.

A first introduction to p-adic numbers

David A. Madore

Revised 7th december 2000

In all that follows, p will stand for a prime number. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are the sets of respectively the natural numbers (i.e. non negative integers), integers, rational numbers, reals and complex numbers.

In some — but not all — of what follows, we assume the reader is familiar with the notions of "group", "ring" and "field". We assume throughout that the reader knows the basic facts about the b-adic representation (i.e. representation in base b) of integers and reals

Note: I did not aim here at writing a completely rigorous document, but only an easily understandable introduction for those who do not have any idea of what a p-adic is.

1 First definition

We will call p-adic digit a natural number between 0 and $p-1$ (inclusive). A p-adic integer is by definition a sequence $(a_i)_{i\in\mathbb{N}}$ of p-adic digits. We write this conventionally as

$$\cdots a_i \cdots a_2\, a_1\, a_0$$

(that is, the a_i are written from left to right).

If n is a natural number, and

$$n = \overline{a_{k-1}\, a_{k-2} \cdots a_1\, a_0}$$

is its p-adic representation (in other words $n = \sum_{i=0}^{k-1} a_i p^i$ with each a_i a p-adic digit) then we identify n with the p-adic integer (a_i) with $a_i = 0$ if $i \geq k$. This means that natural numbers are exactly the same thing as p-adic integer only a finite number of whose digits are not 0. Also note that 0 is the p-adic integer all of

whose digits are 0, and that 1 is the p-adic integer all of whose digits are 0 except the right-most one (digit a_0) which is 1.

If $\alpha = (a_i)$ and $\beta = (b_i)$ are two p-adic integers, we will now define their sum. To that effect, we define by induction a sequence (c_i) of p-adic digits and a squence (ε_i) of elements of $\{0, 1\}$ (the "carries") as follows:

- ε_0 is 0.
- c_i is $a_i + b_i + \varepsilon_i$ or $a_i + b_i + \varepsilon_i - p$ according as which of these two is a p-adic digit (in other words, is between 0 and $p - 1$). In the former case, $\varepsilon_{i+1} = 0$ and in the latter, $\varepsilon_{i+1} = 1$.

Under those circumstances, we let $\alpha + \beta = (c_i)$ and we call $\alpha + \beta$ the sum of α and β. Note that the rules described above are *exactly* the rules used for adding natural numbers in p-adic representation. In particular, if α and β turn out to be natural numbers, then their sum as a p-adic integer is no different from their sum as a natural number. So $2 + 2 = 4$ remains valid (whatever p is — but if $p = 2$ it would be written $\cdots 010 + \cdots 010 = \cdots 100$).

Here is an example of a 7-adic addition:

$$\begin{array}{rcccccc} & \cdots & 2 & 5 & 1 & 4 & 1 & 3 \\ + & \cdots & 1 & 2 & 1 & 1 & 0 & 2 \\ \hline & \cdots & 4 & 0 & 2 & 5 & 1 & 5 \end{array}$$

This addition of p-adic integers is associative, commutative, and verifies $\alpha + 0 = \alpha$ for all α (recall that 0 is the p-adic integer all of whose digits are 0).

Subtraction of p-adic integers is also performed in exactly the same way as that of natural numbers in p-adic form. Since everybody reading this is assumed to have gone through first and second grade, we will not elaborate further :-).

Note that this subtraction scheme gives us the negative integers readily: for example, subtract 1 from 0 (in the 7-adics) :

$$\begin{array}{rcccccc} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ - & \cdots & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline & \cdots & 6 & 6 & 6 & 6 & 6 & 6 \end{array}$$

(each column borrows a 1 from the next one on the left). So $-1 = \cdots 666$ as 7-adics. More generally, -1 is the p-adic all of whose digits are $p - 1$, -2 has all of its digits equal to $p - 1$ except the right-most which is $p - 2$, and so on. In fact, (strictly) negative integers correspond exactly to those p-adics all of whose digits except a finite number are equal to $p - 1$.

It can then be verified that p-adic integers, under addition, form an abelian group.

We now proceed to describe multiplication. First note that if n is a natural number and α a p-adic integer, then we have a naturally defined $n\alpha = \alpha + \cdots + \alpha$ (n times, with $0\alpha = 0$ of course). If n is negative, we let, of course, $n\alpha = -((-n)\alpha)$. This limited multiplication satisfies some obvious equalities, such as $(m+n)\alpha = m\alpha + n\alpha$, $n(\alpha+\beta) = n\alpha + n\beta$, $m(n\alpha) = (mn)\alpha$, and so on (for those with some background in algebra, this is not new: any abelian group is a $\mathbb{Z}$-module). Note also that multiplying by $p = \cdots 0010$ is the same as adding a 0 on the right.

Multiplying two *p-adic integers* on the other hand requires some more work. To do that, we note that if $\alpha_0, \alpha_1, \alpha_2, \ldots$ are p-adic integers, with α_1 ending in (at least) one zero, α_2 ending in (at least) two zeroes, and so on, then we can define the sum of all the α_i, even though they are not finite in number. Indeed, the last digit of the sum is just the last digit of α_0 (since $\alpha_1, \alpha_2, \ldots$ all end in zero), the second-last is the second-last digit of $\alpha_0 + \alpha_1$ (because $\alpha_2, \alpha_3, \ldots$ all end in 00), and so on: every digit of the (infinite) sum can be calculated with just a finite sum. Now we suppose that we want to multiply α and $\beta = (b_i)$ two p-adic integers. We then let $\alpha_0 = b_0\alpha$ (we know how to define this since b_0 is just a natural number), $\alpha_1 = pb_1\alpha$, and so on: $\alpha_i = p^i b_i \alpha$. Since α_i is a p-adic integer multiplied by p^i, it ends in i zeroes, and therefore the sum of all the α_i can be defined.

This procedure may sound complicated, but, once again, it is still exactly the same as we have all learned in grade school to multiply two natural numbers. Here is an example of a 7-adic multiplication:

$$\begin{array}{cccccccc}
 & \cdots & 2 & 5 & 1 & 4 & 1 & 3 \\
\times & \cdots & 1 & 2 & 1 & 1 & 0 & 2 \\
\hline
 & \cdots & 5 & 3 & 3 & 1 & 2 & 6 \\
+ & \cdots & 0 & 0 & 0 & 0 & 0 & \\
+ & \cdots & 1 & 4 & 1 & 3 & & \\
+ & \cdots & 4 & 1 & 3 & & & \\
+ & \cdots & 2 & 6 & & & & \\
+ & \cdots & 3 & & & & & \\
\hline
 & \cdots & 3 & 1 & 0 & 4 & 2 & 6
\end{array}$$

(of course, it is relatively likely that I should have made some mistake somewhere).

We now have a set of p-adic integers, which we will call $\mathbb{Z}_p$, with two binary operations on it, addition and multiplication. It can be checked — but we will

not do it — that $\mathbb{Z}_p$ is then a commutative ring (for those who don't know what that means, it means that addition is associative and commutative, that zero exists and satisfies the properties we wish it to satisfy, that multiplication is associative and commutative, and distributive over addition, and that 1 exists and satisfies the properties we wish it to satisfy (namely $1\alpha = \alpha$ for all α)).

Now, how about division? First, the bad news: division of p-adics is *not* performed in the same way as division of integers or reals. In fact, it can't always be performed. For example, $1/p$ has no meaning as a p-adic integer — that is, the equation $p\alpha = 1$ has no solution — since multiplying a p-adic integer by p always gives a p-adic integer ending in 0. There is nothing really surprising here: $1/p$ can't be performed in the integers either.

However, what is mildly surprising is that division by p is essentially the only division which cannot be performed in the p-adic integers. This statement (in technical terms "$\mathbb{Z}_p$ is a *local* ring") will not be made precise for the moment; however, we give a concrete example. Suppose p is odd (in other words, $p \neq 2$). And let α be the p-adic integer all of whose digits are equal to $(p-1)/2$ except the last one which is $(p+1)/2$. By performing 2α (in other words, $\alpha + \alpha$), it is clear that every digit will be zero except the last one which is 1. So $2\alpha = 1$, in other words $\alpha = 1/2$.

For example, with our usual example of $p = 7$ we show that the number $\alpha = \cdots 333334$ is the number "one half" by adding it to itself:

$$\begin{array}{rcccccccc} & \cdots & 3 & 3 & 3 & 3 & 3 & 4 \\ + & \cdots & 3 & 3 & 3 & 3 & 3 & 4 \\ \hline & \cdots & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

Thus, in the 7-adic integers, "one half" is an *integer*. And so are "one third" ($\cdots 44445$), "one quarter" ($\cdots 1515152$), "one fifth" ($\cdots 541254125413$), "one sixth" ($\cdots 55556$), "one eighth" ($\cdots 0606061$), "one ninth" ($\cdots 3613613614$), "one tenth" ($\cdots 462046205$), "one eleventh" ($\cdots 162355043116235504312$) and so on. But "one seventh", "one fourtneenth" and so on, are not 7-adic integers.

We now give a way to calculate the inverse (and therefore the quotient) of p-adic integers. Suppose α is a p-adic integer ending in zero (such numbers are called *small* for reasons we will describe later). Then α^i ends in at least i zeros. Therefore, as we have seen, we can calculate $\beta = 1 + \alpha + \alpha^2 + \cdots$ even though it has an infinite number of terms. Multiplying this by $(1-\alpha)$ and expanding out (we shall admit that all the appropriate properties of addition are preserved when dealing with infinite sums) we find that $(1-\alpha)\beta = 1 - \alpha + \alpha - \alpha^2 + \alpha^2 - \cdots = 1$. Therefore we are able to calculate the inverse of $1 - \alpha$, which may be, as is easy

to see, any p-adic integer ending in 1. To summarize: p-adic integers ending in 0 have no inverse; those ending in 1 can be inverted with the formula described above. To inverse a p-adic integer α ending in a digit d other than 0 and 1, we find the (unique) digit f such that df is congruent to 1 mod p (i.e. is equal to 1 plus a multiple of p). In that case, $f\alpha$ ends in 1 so can be inverted, and we then have $1/\alpha = f/(f\alpha)$. To find f for small values of p, I have no better advice than checking successively all digits. Perhaps computer scientists can suggest an altogether faster method for inverting p-adics.

Up to now we have only described p-adic integers, and not p-adic numbers. We now proceed to define the latter. The relation between the set (ring) $\mathbb{Z}_p$ of p-adic integers and the set (field) $\mathbb{Q}_p$ of p-adic numbers is the same as between the set (ring) $\mathbb{Z}$ of integers and the set (field) $\mathbb{Q}$ of rationals. Namely, the second is obtained by taking quotients of an element of the first by a non zero element of the same — or, which amounts to the same, by adding new inverses to some elements of the first. In the case of the rationals, an inverse has to be added to every prime number p. In our case, however, we are fortunate, and adding an inverse to p only will suit our needs. We therefore proceed to do that.

We now define a <u>p-adic number</u> to be a $\mathbb{Z}$-indexed sequence $(a_i)_{i\in\mathbb{Z}}$ of p-adic digits such that $a_i = 0$ for sufficiently small i (explicitly: there exists $i_0 \in \mathbb{Z}$ such that $a_i = 0$ for $i < i_0$). Such numbers are also written from right to left, with a "p-adic dot" after decimal 0. So our condition says: there are a finite number of non zero digits on the right of the p-adic point. We consider p-adic integers as p-adic numbers by identifying $(a_i)_{i\in\mathbb{N}}$ with $(a_i)_{i\in\mathbb{Z}}$ where $a_i = 0$ for $i < 0$, in other words by adding zeros to the right of the point. If $\alpha = (a_i)$ is a p-adic number such that $a_i = 0$ for $i < i_0$ (and we can certainly suppose $i_0 \leq 0$ so we do) then the p-adic number α' obtained by shifting every decimal of α by $-i_0$ places to the left is a p-adic integer. We write $\alpha = \alpha' p^{i_0}$ (or $\alpha = \alpha'/p^{-i_0}$).

p-adic numbers can then be added as follows: if $\alpha = \alpha' p^i$ with α' a p-adic intger, and $\beta = \beta' p^j$ ditto, and suppose moreover $i \leq j \leq 0$, then we let $\alpha + \beta = (\alpha' + \beta' p^{j-i})p^i$ — note that $\alpha' + \beta' p^{j-i}$ is indeed a p-adic integer. This is just a complicated way of saying that we add as usual, starting from the furthest (rightmost) column where there is a non zero digit. Multiplication is easier: under the same notations (except that the condition $i \leq j$ is no longer necessary) we let $\alpha\beta = \alpha'\beta' p^{i+j}$. This says that we multiply "as usual", ignoring the p-adic dot, and then we place the dot in the "obvious" place where it should be.

The set $\mathbb{Q}_p$ of p-adic numbers, with this addition and multiplication, forms a field — in other words, all the properties of a ring are satisfied, and moreover every nonzero element has a multiplicative inverse.

2 Second definition — topology and metric

If n is an integer, recall that its p-adic valuation is the exponent of the greatest power of p that divides n. It is written $v_p(n)$. By convention, $v_p(0) = \infty$. If $r = a/b$ is a rational, its p-adic valuation is defined as $v_p(r) = v_p(a) - v_p(b)$.

For example, the 7-adic valuation of 7 is 1. That of 14 is also 1, as are those of 21, 28, 35, 42 or 56. The 7-adic valuation of 49, on the other hand, is 2, as is that of 98. And the 7-adic valuation of 343 is 3. The 2-adic valuation of an integer is 0 iff it is odd, it is *at least* 1 iff it is even, at least 2 iff the integer is multiple by 4, and so on. The 7-adic valuation of $1/7$ is -1, and so are those of $3/7$, $1/14$, $5/56$. The 7-adic valuation of $1/2$ or $8/3$ is 0. The 7-adic valuation of $7/3$ or $14/5$ is 1. The 7-adic valuation of $48/49$ is -2.

We now define the p-adic absolute value of a rational number r to be $|r|_p = p^{-v_p(r)}$. For example, $|p|_p = \frac{1}{p}$, $|1|_p = 1$, $|2p|_p = \frac{1}{p}$ if p is odd, and $|\frac{1}{p^2}| = p^2$.

We then define the p-adic distance between two rationals r, r' to be $|r' - r|_p$. It is relatively straightforward to check that this indeed defines a distance on the rationals. The rationals are not complete for that distance, in other words, every Cauchy sequence is not convergent. It is possible to define the p-adic numbers as the completion of the p-adic rationals under this metric. General theorems on topological fields ensure that this defines a field, the field of p-adic numbers.

To make the equivalence of both definitions clearer, we say that the valuation of a p-adic number (a_i) is the smallest i_0 (possibly positive) such that $a_i = 0$ for all $i < i_0$. With this terminology, a p-adic integer is exactly a p-adic number with non negative valuation. And a small p-adic integer (one which ends in 0) is one whose valuation is (strictly) positive. It is not hard to check that this definition coincides with the aforementioned one for integers, hence for rationals.

As for rationals, we define the p-adic absolute value and distance by $|\alpha|_p = p^{-v_p(\alpha)}$. Note that the p-adic absolute value of a p-adic number is **real** number (it is also a p-adic, and in fact a rational, but ought not be considered as such). Then $\mathbb{Q}_p$ is a metric space, and the two following facts can be proven:

- $\mathbb{Q}_p$ is complete.
- $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Also note that $\mathbb{Z}_p$ is the unit ball with center 0 in $\mathbb{Q}_p$.

7-adic numbers

Motivation

$$x^2 - 2 \equiv 0 \pmod{7^k}$$

$$x_0^2 - 2 \equiv 0 \pmod 7$$

$x_0 = 3$

$x_1^2 - 2 \equiv 0 \pmod{7^2}$, $x_1 \equiv x_0 \pmod 7$

$x_1 = x_0 + 7a_1$

$$0 \underset{(7^2)}{\equiv} (x_0 + 7a_1)^2 - 2 = x_0^2 + 7 \cdot 2 \cdot a_1 \cdot x_0 + 7^2 a_1^2 - 2$$

$$\equiv 7(1 + 6a_1) \equiv 0 \pmod 7$$

$$\Rightarrow 1 + 6a_1 \equiv 0 \pmod 7$$

$$\Rightarrow a_1 \equiv 1 \pmod 7$$

$x_1 = 3 + 7 \cdot 1 = 10$

$x_2^2 - 2 \equiv 0 \pmod{7^3}$, $x_2 \equiv x_1 \pmod{7^2}$

$x_2 = x_1 + 7^2 a_2$

$$0 \underset{(7^3)}{\equiv} (x_1 + 7^2 a_2)^2 - 2 \equiv x_1^2 + 2 \cdot 7^2 a_2 x_1 + 7^4 a_2^2 - 2$$

$$= 2 \cdot 7^2 (1 + 10 a_2) \equiv 0 \ (7^3)$$

$$2 \cdot (1 + 10 a_2) \equiv 0 \pmod 7$$

$a_2 = 2$

$x_2 = 10 + 7^2 \cdot 2 = 108$

$x_3 = 3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 = 2166$

$$x_0 = \lim_{k \to \infty} x_k := \sum_{k=0}^{\infty} a_k \cdot p^k \quad (p\text{-adic integers})$$

$$\mathbb{Z}_p := \left\{ (x_0, x_1, x_2, \dots) \in \prod_{k=0}^{\infty} \mathbb{Z}/p^{k+1}\mathbb{Z} \;\middle|\; x_{k+1} \equiv x_k \bmod p^{k+1} \right\}$$

Read at home again:
- principal ideal ring
- integral domain
- groups of units of a ring
- prime vs. irreducible elements
- maximal ideal

$$a_k = \frac{x_k - x_{k-1}}{p}$$

Example

$p = 7$

$x = 4 \cdot 7^3 + 3 \cdot 7^2 + 0 \cdot 7 + 1 = 4301$

$y = 6 \cdot 7^2 + 1 \cdot 7 = 610$

$x + y = 4911$

$x - y = 3691$

$x \cdot y$:

$$\begin{array}{r} 4301 \cdot 610 \\ \hline 0000 \\ 43010 \\ 3540600 \\ \hline 3613610 \end{array}$$

Let $p \in \{2, 3, 5, \dots\}$ be a fixed prime

A formal series

$$x := \sum_{i=0}^{\infty} a_i p^i \quad \text{where } a_i \in \{0, 1, \dots, p-1\}$$

is called a p-adic integer.

Denote partial sums of this series by

$$S_n = \sum_{i=0}^{n-1} a_i p^i = a_0 + a_1 p^1 + \dots + a_{n-1} p^{n-1}$$

Then the set of p-adic integers

$$\mathbb{Z}_p := \{x = (S_1, \dots, S_n) \mid S_n \in \mathbb{Z}/p^n\mathbb{Z}, \; S_n = S_{n+1} \pmod{p^n}\}$$

If we take $S_n \in \{0, 1, \dots, p^n - 1\}$ $\forall n = 1, 2, \dots$
then $a_n = \frac{S_{n+1} - S_n}{p^n}$ satisfies $0 \le a_n < p$
and is determined uniquely for given $(S_n)_{n \in \mathbb{N}}$

$$x \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

Consider the mapping

$$\varepsilon_p : \mathbb{Z} \to \mathbb{Z}_p$$
$$x \to (S_1, S_2, \dots)$$

where $S_n \equiv x \pmod{p^n}$

THM (properties of $\mathbb{Z}_p$ and ε_p)
Let p be a prime and $\mathbb{Z}_p$ the set of p-adic integers. Then:

a) $\mathbb{Z}_p$ is an integral domain

b) Moreover, $\mathbb{Z}_p$ is a principal ideal domain, and therefore, $\mathbb{Z}_p$ is a UFD (= a factorial ring)

2) The mapping ε_p is a monomorphism.
So we can regard $\mathbb{Z}$ as a subset of $\mathbb{Z}_p$

3) The group of units $(\mathbb{Z}_p)^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$,
that is, $\mathbb{Z}_p^*$ consists of the elements
$x = \sum_{i=0}^{\infty} a_i p^i$ with $a_0 \neq 0$

4) Every element $x \in \mathbb{Z}_p \setminus \{0\}$ can be ~~written~~ uniquely in the form
$X = p^n \cdot u$ with $n \in \mathbb{N}_0$ and $u \in \mathbb{Z}_p^*$
In particular, $x = p$ is the only ~~prime~~ irreducible (and the only prime) in $\mathbb{Z}_p^*$ up to multiplication by an associate.

5) All ideals in $\mathbb{Z}_p$ are the following:
$0, \mathbb{Z}_p, p^n \mathbb{Z}_p$ for all $n \in \mathbb{N}$
In particular the only maximal ideal in $\mathbb{Z}_p$ is $p\mathbb{Z}_p$.

Example

$p = 7$ $\quad x = 2 + 4 \cdot 7 + 3 \cdot 7^2 + \ldots$
$\quad\quad\quad y = 2 + 5 \cdot 7 + 2 \cdot 7^2$

(1) $x + y = 4 + (4+5) \cdot 7 + (3+2) 7^2 \ldots$
$= 4 + (2+7) \cdot 7 + (3+2) 7^2 \ldots$
$= 4 + 2 \cdot 7 + 6 \cdot 7^2 \ldots$

(2) $x \cdot y = 4 + (2 \cdot 4 + 2 \cdot 5) \cdot 7 + (2 \cdot 2 + 4 \cdot 5 + 3 \cdot 2) \cdot 7^2 \ldots$
$= 4 + 4 \cdot 7 + 4 \cdot 7^2 + \ldots$

(3) $\frac{1}{z} = z^{-1}$ $\quad z^{-1} \cdot z = 1$

$z = 5$ $\quad \ldots a_2 a_1 a_0 \cdot 5 \Leftrightarrow$ $\quad \ldots a_2 a_1 \; 2 \; 3 \cdot 5 = 1$

Proof:

1a) We'll first prove, that $\mathbb{Z}_p$ is an integral domain.

Take $x, y \in \mathbb{Z}_p \setminus \{0\}$, then

~~$x \cdot y$~~ we shall prove that

$x \cdot y \neq 0$

Find non-zero coefficients

$\Rightarrow$ their product is not zero

(because $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is a field)

2) Here we prove that

$\ker \varepsilon_p = \{0\}$

3) Let $x = \sum_{i=0}^{\infty} a_i p^i$

1) $a_0 = 0$, then $p \mid x \Rightarrow x \equiv 0 \pmod{p}$ but

$\nexists y : x \cdot y \equiv 1 \pmod{p}$ ↯,

in other words $x \cdot y = (\underset{s_4}{0}, \underset{s_1}{s}, \ldots, s \ldots)$

$\neq (1, 1, \ldots, 1)$