

Lecture 1

Solved and unsolved problems in Number Theory

1. ~~What~~ How many prime numbers are there? ∞ (solved)

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

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

It is either a prime or a product of primes 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 $n \in \mathbb{N}$? YES!

$$a+b, 2a+b, 3a+b, \dots$$

Thm: (Dirichlet)

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

?

Legendre (1770)

There are infinitely many n 's so that $n^2 + 1$ is either prime or a product of two primes

$$n^2 + 1 = \begin{cases} p \cdot q \\ p \end{cases}$$

4. Twin primes

$$(p, p+2)$$

$$(3, 5), (17, 19), (5, 7)$$

6. Goldbach's conjecture

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

$$4 = 2 + 2$$

$$6 = 3 + 3$$

$$8 = 3 + 5$$

Two results:

1) Vinogradov: thin (1937?)

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

2) Chen Jing-ran (1966)

Every even number $n \geq 4$ can be written

as $n = p + ce$
prime \nwarrow prime or product of 2 primes

6) Consider $S = N \cup E \cdot N$

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

$$(2k) = E + E + \dots$$

$$2 = 2$$

$$4 = 4$$

$$6 = 2+4, 6$$

$$8 = 2+6, 8$$

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

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

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

$$(2k+1) = O + O + \dots$$

$$3 = 3$$

$$5 = 5$$

$$7 = 7_1, 7_2$$

$$9 = 5+3+1, 9$$

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

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

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

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

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

$$\begin{array}{ccccccc}
 \mathbb{N} & \subset & \mathbb{N}_0 & \subset & \mathbb{Z} & \subset & \mathbb{Q} \\
 \downarrow & & \parallel & & \uparrow & & \uparrow \\
 \text{Positive integer} & & \mathbb{N} \cup \{0\} & \text{"whole numbers"} & \text{ring of integers} & \text{field of rationals} & \text{field of real #s} \\
 & & & & \uparrow & & \uparrow \\
 & & & & \mathbb{R} & & \mathbb{C} \\
 & & & & & & \\
 & & & & & & \mathbb{C}[i]
 \end{array}$$

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

$\cdot : G \times G \rightarrow G$ 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) $\forall a \in G \quad \exists b \in G$ s.t. $ab = ba = e$

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

If also:

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

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

Körper

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

II. $(F \setminus \{0\}, \cdot)$ is an abelian group (4. axioms)

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

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

- I. (1-4) $(R, +)$ is an abelian group } some authors
 5. $\forall a, b, c \in R \quad (a+b)c = ac+bc$ use only
 6. $\forall a, b, c \in R \quad a(b+c) = ab+ac$ these 6
 (R, \cdot) 7. associativity: $a(bc) = (ab)c$ axioms in
 8. The existence of mult. identity:
 $\exists 1 \in R: \forall a \in R \quad a \cdot 1 = 1 \cdot a = a$ 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	0

*	0	1
0	0	b
1	d	1

Galois Γ anya

Complex Numbers $(C, +, \cdot)$

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

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

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

$$0 = (0, 0)$$

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

$$z_1 = z_2 \Leftrightarrow a_1 = a_2 \\ b_1 = b_2$$

$$a = \operatorname{Re} z \quad b = \operatorname{Im} z$$

Algebraic Form

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

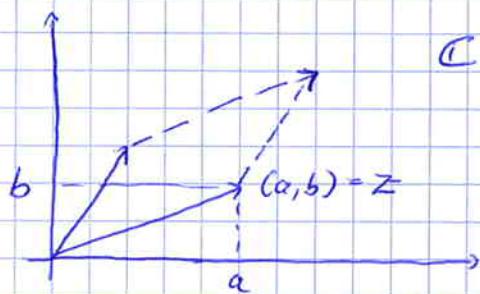
$$\underline{z} = (a, b) = (a, 0) + (0, b) = a \cdot 1 + b \cdot i = a + bi$$

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

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

1. Let $a, n \geq 2$ 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 $k \in \mathbb{N}$



C

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

L

Trigonometric form of complex numbers

right angle

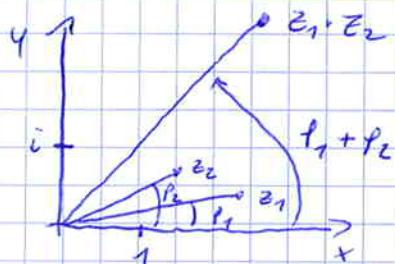
$$z = a + ib = \underbrace{r \cdot \cos \varphi}_{a} + i \cdot r \sin \varphi = \underbrace{r(\cos \varphi + i \sin \varphi)}_{\text{acute}}$$

acute

brackets, parentheses, braces
 [] () { }

\ acute
 abuse

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



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)

$$a^b \cdot a^c = a^{b+c}$$

$$\boxed{|\cos \varphi + i \sin \varphi| = e^{i\varphi}}$$

Euler formula

$$e = 2,7 \underbrace{1828,}_{\text{Leo Tolstoy}} \underbrace{1828}_{\dots} 459045\dots$$

$$z = r \cdot e^{i\varphi}$$

$$e^{ip_1} \cdot e^{ip_2} = e^{i(p_1+p_2)}$$

$$z_1 \cdot z_2 = (r_1 e^{ip_1}) \cdot (r_2 e^{ip_2}) = r_1 \cdot r_2 \cdot e^{i(p_1+p_2)}$$



What is algebraic Number Theory?

I Elementary Number Theory.

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

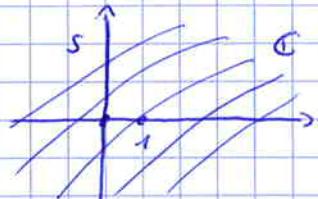
divisibility, congruences, prime #'s
Euclidean algorithm, ...

II. Analytic Number Theory.

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

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

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



Theorem 1 (prime number Theorem)

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \cdot \ln x}{x} = 1 \quad \left| \begin{array}{l} x \in \mathbb{R}; \pi: \mathbb{N} \rightarrow \mathbb{N}_0 \\ \pi(x) = \#\{p \leq x \mid p \text{ is prime}\} \\ = 1 \{ \dots \} \end{array} \right.$$

Ex. $\pi(20) = 8$

Theorem 2 (divergence of the series of reciprocals to primes)

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

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

Reminder:

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

$$\geq 1 + \underbrace{\frac{1}{2}}_1 + \underbrace{\frac{1}{4} + \frac{1}{4}}_2 + \underbrace{\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}}_4 + \underbrace{\frac{1}{16} + \dots + \frac{1}{2^n}}_8 + \dots$$

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

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

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

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

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 $Q := p_1 \cdot p_2 \cdots p_N$ and consider for all $n \in \mathbb{N}$
 $1 + n \cdot Q$

What can we say about the series

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

From the above information we can evaluate:

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

} p_{N+R} is the biggest prime of those dividing $1+nQ$, $1 \leq n \leq t$

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

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

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

$t=1$

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

$t=2$

$$(\dots) \cdot (\dots) = \frac{1}{P_{N+1}^2} + \frac{1}{P_{N+1}P_{N+2}} + \dots$$

$t=3$

$$\dots = \frac{1}{P_{N+1}^3} + \dots$$

(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

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

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:

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

$$\begin{array}{l} 20 \in \mathbb{Z} \\ 20 = 2 \cdot 10 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5 \\ 20 = 5 \cdot 4 = 5 \cdot 2 \cdot 2 \end{array}$$

|

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

(Def) A ring R has no zero division if
 $a \cdot b = 0 \Rightarrow a = 0 \text{ or } b = 0$)
(nonzero)

Divisibility

Ring $(R, +, \cdot)$

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

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

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

Examples of rings

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

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

If in a ring $1=0$, then all its elements $a=0$

Proof $a \in R$, then $a = 1 \cdot a = 0 \cdot a \stackrel{*}{=} 0$

$$(0+0) \cdot a = 0 \cdot a \cancel{+} a \cdot 0$$

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

3. Any field K is a ring

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

$$\tilde{i} \left(\begin{array}{c} \\ \end{array} \right)_{n \times n} \left(\begin{array}{c} \\ \vdots \\ \end{array} \right)^j = \tilde{j} \left(\begin{array}{c} \\ \vdots \\ \end{array} \right)_{n \times n}^i$$

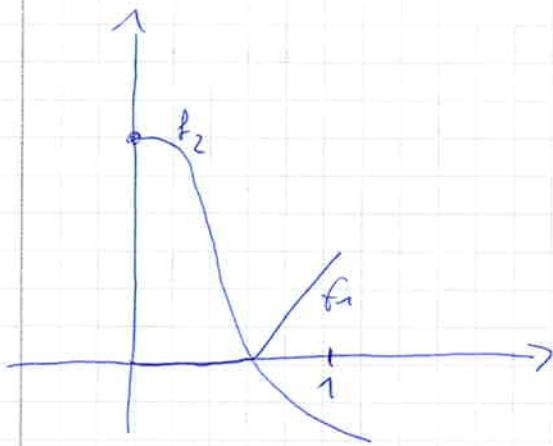
5. $\mathbb{Z}_n = \mathbb{Z}/n \quad \mathbb{Z} = (\{0, 1, 2, \dots, n-1\}, +, \cdot), \quad \begin{matrix} n \in \mathbb{N} \\ n \geq 2 \end{matrix}$

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

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

$\begin{matrix} 1 \cdot 1=1 \\ 2 \cdot \cancel{1} \end{matrix} \quad \text{5)} \quad \text{If } n=p \text{ ist prime, then } \mathbb{Z}_p$
is a field \mathbb{F}_p

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



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

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

$n \in \mathbb{N}, n \geq 2, n$ is square free ($n \neq n_1^2 \cdot m, n_1, m \in \mathbb{N}, n_1 \geq 2$)

8) $\mathbb{Z}[\sqrt{-1}] \subset \mathbb{C}$

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 $a \in R$ divides an element $b \in R$, if $b = a \cdot c$ for some $c \in R$ ($a \neq 0$)

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

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

where u is a unit

$$(a+bi)(c+di) = 1$$

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

$$\begin{aligned} c+di &= \frac{(a-bi)}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \left(\frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2} \right) \\ &\stackrel{\text{if } a \neq 0}{=} \frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2} \end{aligned}$$

$$\begin{matrix} a & b \\ c & d \end{matrix}$$

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 $a|x_1b + yc$ for all $x_1, y \in R$
3. If $a|b$ and $b|a$ $\Rightarrow a = ub$ for some $u \in R^*$
4. $a|b \Leftrightarrow ca|cb$ for some $c \neq 0 \Leftrightarrow ca|cb \wedge c \in R$

Def: An element $\bullet \neq p \in R \setminus R^*$ 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 rands)
- 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 $p|r \cdot s$. 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 $\bullet \neq x \in R$.

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

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

$$(*) \Rightarrow p - pxs = 0 \Rightarrow p \cdot (1 - xs) = 0 \xrightarrow[\substack{p \neq 0 \\ R \text{ without zero}}]{\quad} \\ \Rightarrow 1 - xs = 0 \Rightarrow xs = 1 \Rightarrow x \text{ and } s \text{ are units} \quad \square$$

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

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

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

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

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 ~~of $R \setminus R^*$~~ ~~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) $a = p_1 \dots p_n$, where all p_i are prime by definition, this is a factorisation into irreducibles.

ii) uniqueness

Suppose $a = q_1 q_2 \dots q_m$ (F2)

is a factorisation of a into irreducibles.

By (F4) we see that $p_1 | a \Rightarrow p_1 | q_1 \cdot q_2 \cdots q_m$
 $\Rightarrow p_1 | \text{one of } q_i$
 Since p_1 is prime

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

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

$p_1 \cdot p_2 \cdots p_n \Rightarrow p_1 \cdot p_2 \cdots p_n | q_1 \cdot q_2 \cdots q_m$

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

$$\left\{ p_1(p_2 \cdots p_n - (x \cdot q_2) \cdots q_m) = 0 \right\} \text{ After } n \text{ steps}$$

Since q_1 is irred.
 p_1 or x must
 be a unit. p_1 is
 not a unit (p_1 is
 prime)
 $\Rightarrow x$ is a unit
 impossible $n > 4$
 $n \in m$
 $m = m$

(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 $p | r \cdot s$, then

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

(if r and s are not units)

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

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

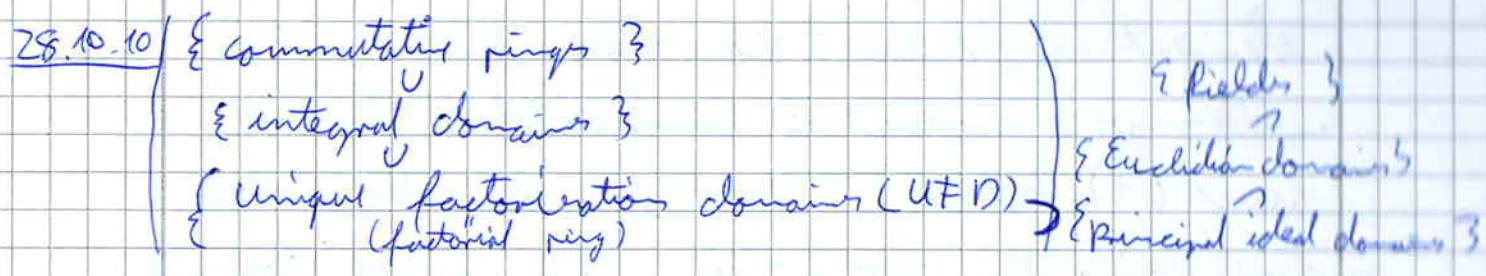
If $p | r_i \Rightarrow p | r$

If $p | s_j \Rightarrow p | s$

(3) \Rightarrow (1) trivial

Remark In a unique factorization 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.



- (1) \exists a factorization into primes
- (2) \nexists fact. into irreducibles
- (3) \exists fact. into irreducibles and prime = irreducible

Example: \mathbb{Z} Primes here $\pm 1, \pm 2, \pm 3, \pm 5, \pm 7$

Principal ideal domains (PID) and Euclidean domains

Reminder: $(R, +, \circ)$ (non-right)

Def. Let R be a ring. A left 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 ^{non-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.

And 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 $p|ab$.

If $p|a$, then we are done.

If $p \nmid a$, then consider $I = (p, a) := \{xp + ya \mid x, y \in R\}$.

$\exists g \in I$ s.t. $I = (g) \Rightarrow g \mid p$ and $g \mid a$ ($p, a \in I$)

Since p is irreducible and $g \mid p$, we know that

either g and p are associates or g is a unit.

The former (1) is impossible (otherwise p would divide a), so g is a unit, and, therefore $I = (g) = R$.

$[g \in (g) \Rightarrow gg^{-1} \in (g) \Rightarrow g \cdot (g^{-1} \cdot 1) = 1 \in (g) \Rightarrow (g) = R]$

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

$\Rightarrow \bar{x}pb + \bar{y}ab = b \Rightarrow p \mid b$.

\cancel{R} p divides this product

(2) We must show that every $a \in R$ is a product of irreducibles. If a is irreducible, then stop (it is already ~~at~~ a factorisation with just one factor). 9

If not, then $a = a_1 \bar{a}_2$, where both a_1 and \bar{a}_2 are non-units. If both a_1 and \bar{a}_2 are irreducibles, we stop. If not, we proceed with factorisation of reducible elements.

If after finitely many steps we have a factorisation into irred. If not, then there is with a sequence of elements a, a_1, a_2, \dots so that

$(a) \subset (a_1) \subset (a_2) \subset \dots \subset (a_n) \subset \dots$

\nwarrow

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

- | i) if $a, b \in I \Rightarrow \exists n \text{ s.t. } a, b \in (a_n)$
- | ii) if $a \in I, r \in R \Rightarrow ar \in I.$

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

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

$$I = (a_n) = (a_{n+1}) = \dots$$

□

Lecture 7

The greatest common divisor.

The Euclidean algorithm in Euclidean domains.

{ commutative ring with 1 }

U

\mathbb{Z}_n , $n \geq 4$ is composite

{ integral domain }

X

U

{ unique factorization domain }

X

{ principal ideal domains }

X

$\mathbb{Z}[\sqrt{5}]$

{ Euclidean domains }

U

{ fields }

$\mathbb{Z}[X] := \{a_0 + a_1 X + a_2 X^2 + \dots | a_i \in \mathbb{Z}\}$

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 greatest common divisor of a and b , if both of the fol. conditions hold:

(1) $c|a$ and $c|b$

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

Notation: $\text{gcd}(a, b)$

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 .
 $\text{gcd}(a_1, \dots, a_n)$.

Exercise:

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

How can we find the gcd?

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

Example: $a = 2 \cdot 3^2 \cdot 5$, $b = (-2)^3 \cdot 3 \cdot (-7)$
 $\text{gcd}(a, b) = 2 \cdot 3$ or -6

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

Properties of the gcd:

- 1° $\gcd(a, b) = \gcd(b, a)$
- 2° $\gcd(a, 0) = 0$ ($a \neq 0$), $\gcd(a, 1) = 1$
- 3° $\gcd(ca, cb) = c \cdot \gcd(a, b)$, $c \neq 0$
- 4° $\gcd(a, b) = a \Leftrightarrow a \mid b$
- 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° $\gcd(a, b) = 1 \Leftrightarrow \gcd(a^i, b^j) = 1 \quad i, j \in \mathbb{N}$
- 9° $a \mid bc \text{ & } \gcd(a, b) = 1 \Rightarrow a \mid c$
 $= \gcd(a, c) = a$
- 10° $\gcd(a, b) = 1 \Rightarrow \gcd(a, bc) = \gcd(a, c)$

Euclidean domains

Def

let R be an integral domain.

A Euclidean function (a norm) is a function
 $f: R \setminus \{0\} \rightarrow \mathbb{N}_0$.

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

- $\forall a, b \in R$ with $b \neq 0 \exists g, r \in R$
 s.t. $a = q \cdot b + r$ and either $r = 0$ or $r \neq 0$ and $f(r) < f(b)$

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

Example: (1) \mathbb{Z} , $f(a) = |a|$

(2) Gaussian integers $\mathbb{Z}[i] := \left\{ \frac{x}{a+bi} \mid \frac{x}{a}, \frac{y}{b} \in \mathbb{Z} \right\}$

$$f(a+bi) = \sqrt{x^2 + y^2}$$

} Euclidean
domains

Example

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

$$a = q \cdot b + r$$

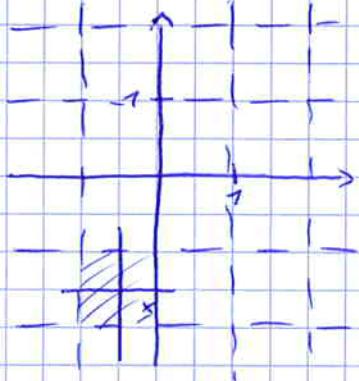
$$f(r) < f(b)$$

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

$$q = -2$$

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

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



$$(5-2i) = (-2i) \cdot (1+3i) - 1$$

$$\begin{matrix} a \\ "q \end{matrix}$$

$$r \neq 0$$

$$1 = f(r) \in f(b) = 10$$

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

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

(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

$b = q^R \cdot a + r$ and either $r = 0$ (then we are done)

or $r \neq 0$ with $f(r) < f(a)$. Since $r = b - qa \in I$

this is a contradiction

\square $\mathbb{Z}[\sqrt{-5}]$

NT

4.11.10

$\gcd(a, b)$ \rightarrow 1) $\gcd(a, b) \mid a$, $\gcd(a, b) \mid b$
 \rightarrow 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? \rightarrow 1) $a = r \cdot g$, $r \in R$ some for. s.

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

In particular, $d \mid xa + yb = g$

□

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 a Euclidean domain called

if we can find a function $f: R \setminus \{0\} \rightarrow \mathbb{N}_0$ 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 $\underbrace{f(d_0+a_1X+\dots+a_nX^n)}_{P(X)} = n = \deg(P(X))$

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

$$(b=) \quad x^2 + 1 \quad \overline{x^3 + 2x - 1} \quad \leftarrow a$$

$$\frac{x^3 + x}{x} + (-1) (= r)$$

Euklidian Algorithm

Example

gcd (84, 57)

~~$\frac{84}{57} = 1 \cdot 27 + 15$~~

$|27| < |57|$

$$\begin{array}{r} a \\ b \\ \hline 84 & 57 & r \\ \hline 1 & 1 & \\ \end{array}$$

$$84 = 1 \cdot 57 + 27$$

$$57 = 2 \cdot 27 + 3 \quad \leftarrow \text{gcd}(a, b)$$

$$27 = 9 \cdot 3 + 0 \quad \boxed{0} \leftarrow \text{stop}$$

$a \mid a \quad d \mid b \quad a = a_0, b = a_1$

$\Rightarrow d \mid a_n$ where $f(a_2) < f(a_1)$

$a_0 = q_1 \cdot a_1 + r_1$

$a_1 = q_2 \cdot a_2 + r_2$

...

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

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

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

Extended EA.

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

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

Fibonacci numbers:

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

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

$$55 = 1 \cdot 34 + 21$$

$$34 = 1 \cdot 21 + 13$$

$$21 = 1 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1 \leftarrow$$

$$2 = 2 \cdot 1 + 0$$

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

Proof

$$\begin{aligned} F_{n+5} &= F_{n+4} + F_{n+3} = (F_{n+3} + F_{n+2}) + F_{n+3} \\ &= 2F_{n+3} + F_{n+2} = 2(F_{n+2} + F_{n+1}) + F_{n+2} \\ &= 3F_{n+2} + 2F_{n+1} = 3(F_{n+1} + F_n) + 2F_{n+1} \\ &= 5F_{n+1} + 3F_n = 5(F_n + F_{n-1}) + 3F_n \\ &= 8F_n + 5F_{n-1} > 8F_n + 4F_{n-1} \end{aligned}$$

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

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

$$\text{Ex } b = 23578$$

Proof

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

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

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

$b = a_1 \geq F_{n+1}$. If we have $n \geq 5k$ ($n \geq 5k+1$) then we would have $b \geq F_{5k+2} \geq 10 \cdot F_{5(k-1)+2} \geq 10^2 \cdot F_{5(k-2)+2} \geq \dots \geq 10^k F_2 = 10^k$
(b would have more than 10 digits)

Contradiction

II

Lecture 5 Modular arithmetic. \mathbb{Z}_m .

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

Notation

$$a \equiv b \pmod{m} \quad \text{or} \quad a = b \pmod{m}$$

Example

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

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

Remark

We almost always assume that $m \in \mathbb{N}$ ($m > 0$)

because $a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{-m}$

Properties

1. $a \equiv b \pmod{m} \Leftrightarrow a = b + mk$ for some k

2. $a \equiv b \pmod{m} \Leftrightarrow a$ and b have the same remainder when divided by m .

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

$\stackrel{\text{"is a}}{=} \stackrel{\text{equivalence relation}}{\text{relation}}$

$4.$ $a \equiv a \pmod{m}$ (reflexive)
$5.$ $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ (symmetric)
$6.$ $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ (transitive)

$\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} := \{0, 1, \dots, m-1\}$ with "+" and " \cdot " 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

$a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$. Then

$$(1) \quad a+c \equiv b+d \pmod{m}$$

$$(2) \quad a \cdot c \equiv b \cdot d \pmod{m}$$

Proof

We have $a \equiv b \pmod{m} \Rightarrow a = b + m \cdot k$ for some $k \in \mathbb{Z}$

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

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

$$ac = bd \pmod{m} \quad (\text{see Property 1.})$$

□

Corollary

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

Example

1. Determine whether 2758152 is divisible by 3.

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

$$\left[\begin{array}{l} 10 \equiv 1 \pmod{3} \\ 10^2 \equiv 1^2 \equiv 1 \pmod{3} \end{array} \right]$$

—

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

$$\equiv 2 + 6 + 2 + 2 + 1 + 2 + 2$$

$$\equiv 0 \pmod{3}$$

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

$$2^4 = 16 \equiv -1 \pmod{17}$$

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

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

II Linear congruences.

$$ax \equiv b \pmod{m}$$

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

$$(1) \quad ax \equiv b \pmod{m} \quad (*)$$

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

Examples

$$(1) \quad 4x \equiv 3 \pmod{2}$$

$\gcd(4, 2) = 2 = d$
 $d \nmid b \quad (2 \nmid 3)$

Def. p. 14

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

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

$$x \equiv 5 \pmod{3}$$

Def

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

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

then $ax \equiv b \pmod{m}$ has a unique solution $(\bmod m)$

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

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

$$\begin{aligned} k \cdot ax &\equiv k \cdot b \pmod{m} \\ &\equiv 1 \pmod{m} \end{aligned}$$

or

$$x \equiv k \cdot b \pmod{m}$$

Uniqueness

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

$$\text{Then } ax' \equiv b \equiv ax'' \pmod{m}$$

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

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

$$\text{or } x' \equiv x'' \pmod{m}$$

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 $a\bar{x} \equiv b \pmod{m}$

that is, $a\bar{x} - b = m \cdot l$ for some $l \in \mathbb{Z}$

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

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

$$\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \quad (***)$$

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 $\frac{a}{d} \cdot y \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

$$\left[\Rightarrow a \cdot y \equiv b \pmod{\frac{m}{d}} \xrightarrow{?} ay \equiv b \pmod{m} \right]$$

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

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

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

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

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

$$\left. \begin{array}{l} ax \equiv b \pmod{m} \\ \gcd(a, m) = d \end{array} \right\} \begin{array}{l} \text{if } d \nmid b, \text{ then stop. No solution!} \\ \text{if } d \mid b, \text{ then there are } d \\ \text{solutions (congruent mod } m) \end{array}$$

Example:

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

$$x \equiv 2 \pmod{5}$$

$$\text{Answer: } x = 2, 7$$

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

$$2x \equiv 1 \pmod{5}$$

$$z^{-1}(5)$$

$$1 = R_2 z + n \cdot 5$$

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

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

Thm 1

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:

$$\left\{ \begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{array} \right. \quad \begin{array}{l} \text{has a unique solution modulo} \\ (10.*) \quad m_1 \cdot m_2 \cdots m_k. \end{array}$$

Proof: (Constructive!)

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

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

$$\uparrow \quad \downarrow$$

$$\gcd(M_i, m_i) = 1$$

We claim that $x = \underbrace{\alpha_1 x_1 m_1 + \alpha_2 x_2 m_2 + \alpha_3 x_3 m_3 + \dots + \alpha_k x_k m_k}_{\equiv \sum \alpha_i x_i m_i \pmod{m_1}} = \alpha_1 (m_1)$
 is a solution to (10.*).

Example

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{9} \end{cases} \quad \begin{aligned} M &= 4 \cdot 5 \cdot 9 = 180 \\ M_1 &= 45 \\ M_2 &= 36 \\ M_3 &= 20 \end{aligned}$$

$$45x_1 \equiv 1 \pmod{4} \Rightarrow x_1 \equiv 1 \pmod{1} \quad (\text{need only one solution})$$

$$36x_2 \equiv 1 \pmod{5} \Rightarrow x_2 \equiv 1 \pmod{1}$$

$$20x_3 \equiv 1 \pmod{9} \Rightarrow x_3 \equiv 5 \pmod{1}$$

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

$$= 135 + 72 + 100 = 307 \equiv 127 \pmod{180}$$

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

Then

$$x \equiv \alpha_1 \equiv y \pmod{m_1} \Rightarrow m_1 \mid (x-y)$$

$$\vdots \qquad \vdots$$

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

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

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

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

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

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

Finish yourself (complete the induction)

□

Example

$$1) \begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 0 \pmod{8} \end{cases} \quad \begin{matrix} 8, 32 \\ 4(6) \\ \cancel{0, 8, 16, 24, 32, 40} \end{matrix} \quad (\text{mod } 48)$$

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

~~0, 8, 16, 24, 32, 40~~
no solutions.

II Fermat's Little Theorem (FLT)

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

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

<u>$p=3$</u>	a	a^2	a^3	a^4
0	0	0	0	0
1	1	1	1	1
2	1	2	1	1

<u>$p=5$</u>	a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	4	3	1	2	4	1
3	4	2	1	3	4	1
4	1	4	1	4	1	1

$p=7$

	a^1	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 (FCLT)

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

Proof

let p be prime and $a \not\equiv 0 \pmod{p}$.

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

We claim that

1) all elements of S are different mod p

2) none of them $\equiv 0 \pmod{p}$ (all $i \cdot a \not\equiv 0 \pmod{p}$)

Indeed, to prove 1) assume $i \cdot a \equiv j \cdot a \pmod{p}$

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

or $p \mid (i-j) \cdot a \Rightarrow p \mid (i-j) \underset{\text{since } i \neq j \mid p-1}{\Rightarrow i=j}$

If $i \cdot a \equiv 0 \pmod{p}$, then $p \mid a$, which is wrong because $p \nmid a$

Claims 1) & 2) mean that

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

$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$

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

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

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

Example

1) $p=5, \alpha = 2$

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

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

2)

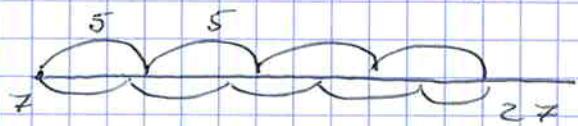
The Chinese Remainder Theorem

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \quad \begin{matrix} \nearrow \text{pairwise rel.} \\ \nwarrow \text{prime} \end{matrix} \Rightarrow \exists! x$$

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.

$$2^{52632} \equiv 1 \pmod{52633} \quad \text{divisible by } 7$$

$(P \Rightarrow Q)$ (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

$$R_1 \times R_2 \times \dots \times R_K := \{(r_1, r_2, \dots, r_K) \mid r_i \in R_i, 1 \leq i \leq K\}$$

with $+$: $(r_1, \dots, r_K) + (s_1, \dots, s_K) = (r_1 + s_1, \dots, r_K + s_K)$

and with \circ : $(r_1, \dots, r_K) \circ (s_1, \dots, s_K) = (r_1 \cdot s_1, \dots, r_K \cdot s_K)$

Thm:

Let $m = m_1 \circ m_2 \circ \dots \circ m_K$, where $m_{1,1}, m_K$ are pairwise relatively prime. Then

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_K}.$$

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

T

epimorphism = homo + surjection

mono = " + injection

iso = " + bijection

|

Proof:

Let Φ be defined as follows

$$\Phi: \mathbb{Z}_m \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_K}$$

$$\begin{array}{ccc} \Phi & & \\ x & \longrightarrow & (\text{Res}_{m_1} x, \text{Res}_{m_2} x, \dots, \text{Res}_{m_K} x), \text{ where} \end{array}$$

$\text{Res}_{m_i} x$ 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 $\Phi(x) = \Phi(y)$

$$\text{Res}_{m_i} x = \text{Res}_{m_i} y \quad \forall 1 \leq i \leq k$$

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 $\Phi(x') = \Phi(x'')$

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

$$x'' \equiv x' \pmod{m} \Rightarrow x'' \equiv x' \pmod{m_i} \quad \forall i$$

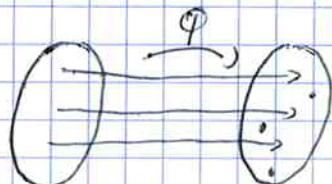
2) surjective.

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) $\Rightarrow \Phi$ is bijective

3) Φ is a homomorphism

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

can be rewritten as

$$\text{Res}_{m_i}(x+y) = \text{Res}_{m_i}(\text{Res}_{m_i} x + \text{Res}_{m_i} y)$$

To see this, consider

$$(x+y) - (\underbrace{\text{Res}_{m_1} x + \text{Res}_{m_2} y}_{\text{Indeed } \hookrightarrow}) \quad \text{and prove that it is divisible by } m_1 m_2$$

$$\begin{aligned} b) \quad & (x \cdot y) - (\text{Res}_{m_1} x \cdot \text{Res}_{m_2} y) \\ & = (x - \text{Res}_{m_1} x) \cdot y + \text{Res}_{m_1} x (y - \text{Res}_{m_2} y) \end{aligned}$$

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

$$\begin{array}{ccc} \varphi: & \mathbb{N} & \rightarrow \mathbb{N} \\ & n & \mapsto \# U_n & \varphi(1) = 1 \end{array}$$

Example:

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

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

Thm Euler $\varphi(n) = \# U_n$ 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 $\varphi(n)$:

$$\text{1. } \varphi(p) = p-1, \text{ if } p \text{ is prime.}$$

□

Wir betrachten das folgende gestörte Optimalitätsystem

16.11.10

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

wobei $t \geq 0$. $x \geq 0$ heißt $x_i \geq 0, i=1, \dots, n$.

Ist (x_c, λ_c, s_c) eine (möglichst eindeutige) Lösung von (7.1), so heißt die Abbildung $t \mapsto (x_t, \lambda_t, s_t)$ der zentrale Pfad und die Bedingungen in (7.1) heißen zentrale Pfad-Bedingungen. Die Idee der Inneren-Punkte-Methode besteht darin, den Pfad $t \rightarrow 0$ zu verfolgen.

Beispiel 7.1 Das Problem $\begin{array}{ll} \min & x_1 + x_2 \\ \text{u.d.N.} & x_1 + x_2 = 0 \\ & x_1 \geq 0, x_2 \geq 0 \end{array}$

hat eine nichtleere zulässige Menge. Trotzdem sind die zentralen Pfad-Bedingungen nicht erfüllt, unabhängig davon, wie $t \geq 0$ 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 (3.4) gehörige primale logarithmische Barrier-Problem ein:

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

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

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

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:

- Das primale Problem (7.2) besitzt eine Lösung x_τ .
- Das duale Problem (7.3) besitzt eine Lösung (λ_τ, s_τ) .
- Das System (7.7) besitzt eine Lösung $(x_\tau, \lambda_\tau, s_\tau)$.

Beweis: Folgt anhand der Karush-Kuhn-Tucker-Bedingungen für konvexe restriktive Optimierungsaufgaben. \square

Definition 7.1 (Primal-dual zulässige Menge)

Die Menge $E = \{(x, \lambda, s) : Ax = b, A^T \lambda + s = c, x \geq 0, s \geq 0\}$

heißt die (primal-dual) zulässige Menge,

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

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

Satz 7.2 Die Menge E° sei nicht leer. Dann besitzt das primale Barrieren-Problem für jedes $\tau > 0$ eine optimale Lösung x_τ .

18.11.10 Beweis: $\tau > 0$, sei $(\hat{x}, \hat{\lambda}, \hat{s}) \in E^\circ \Leftrightarrow \begin{aligned} A\hat{x} &= b \\ A^T \hat{\lambda} + \hat{s} &= c \\ \hat{x} &> 0, \hat{s} > 0 \end{aligned}$

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

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

Wir zeigen, dass L_τ kompakt ist.

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

$\Rightarrow L_\tau$ abgeschlossen ✓

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

mit $Ax = b$

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

18.11.10

$$\Rightarrow \forall x \in L_T : B_T(x) = \hat{s}^T x + \hat{\lambda}^T b - \tau \sum_{i=1}^n \log(x_i) \quad (\checkmark)$$

Wir nehmen an, dass die Menge L_T unbeschränkt ist.

$$\Rightarrow \exists \{x^k\}_{k \geq 1} \subset L_T : \|x^k\| \rightarrow +\infty$$

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

$$\Rightarrow B_T(x^k) \leq B_T(\hat{x}) \stackrel{(\checkmark)}{\Leftrightarrow}$$

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

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

$$\lim_{k \rightarrow +\infty} \left(\sum_{i=1}^n \underbrace{\hat{s}_i x_i^k}_{>0} - \tau \log(x_i^k) \right) \rightarrow +\infty \quad \left| \begin{array}{l} \text{(da } \lim_{t \rightarrow +\infty} (st - \tau \log(t)) = +\infty : \\ \lim_{t \rightarrow +\infty} \underbrace{\log(t)}_{\rightarrow +\infty} \left[s \frac{t}{\log(t)} - \tau \right] = \infty \\ - \lim_{t \rightarrow +\infty} \frac{1}{t} = \lim t = +\infty \end{array} \right)$$

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

ist t nach unten beschränkt

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

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

$\Rightarrow L_T$ beschränkt $\Rightarrow L_T$ kompakt

$$\Rightarrow \exists x_T \in L_T : B_T(x_T) = \min_{x \in L_T} B_T(x) \quad (\checkmark)$$

$$Ax_T = b, x_T > 0 \text{ falls nicht } \Rightarrow B_T(x_T) = +\infty \wedge B_T(x_T) \leq B_T(\hat{x})$$

$\Rightarrow x_T$ zulässig für (7.2)

Gibt es ein x zulässig für (7.2) so, dass $B_T(\hat{x}) < B_T(x_T)$

$$\Rightarrow x \in L_T \quad \square \quad (\checkmark)$$

$\Rightarrow x_T$ opt. Lsg. von (7.2)

\square

$$(7.2): \min_{\substack{Ax=b \\ x \geq 0}} B_T(x)$$

Satz 7.3 (Existenz des zentralen Pfades)

Die strikt zulässige Menge E^0 sei nicht leer.

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^\top eindeutig bestimmt.

Beweis: Sei $\tau > 0$. Laut Satz 7.2

$\Rightarrow \exists x_\tau$ opt. (sg. von (7.2)). Laut Satz 7.1

$\Rightarrow \exists (\lambda_\tau, s_\tau)$ opt. (sg. 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

$\Rightarrow x_\tau$ eindeutig bestimmt.

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

$$f(\lambda x + (1-\lambda)y) < \lambda f(x) + (1-\lambda)f(y)$$

$$B_\tau(x) = c^\top x - \tau \sum_{i=1}^n \log(x_i) - \text{strikt konvex}$$

Sei x_τ nicht eindeutig bestimmt. $\Rightarrow \exists \bar{x}_\tau$ Lösung von (7.2), $\bar{x}_\tau \neq x_\tau$

$\Rightarrow \frac{1}{2}x_\tau + \frac{1}{2}\bar{x}_\tau$ - zulässig für (7.2)

$$B_\tau\left(\frac{1}{2}x_\tau + \frac{1}{2}\bar{x}_\tau\right) < \frac{1}{2}B_\tau(x_\tau) + \frac{1}{2}B_\tau(\bar{x}_\tau) = B_\tau(x_\tau) \quad \square$$

$$\text{Da } (x_\tau)_i, (s_\tau)_i = \tau \quad \forall i = 1, \dots, n$$

$\Rightarrow s_\tau$ eindeutig bestimmt.

Sei $\text{rang}(A) = m \Rightarrow AA^\top$ regulär.

$$A^\top \lambda_\tau + s_\tau = c \Rightarrow AA^\top \lambda_\tau + As_\tau = Ac$$

$$\Leftrightarrow (AA^\top) \lambda_\tau = Ac - As_\tau$$

$$\Leftrightarrow \lambda_\tau = (AA^\top)^{-1} A(c - s_\tau) \Rightarrow \lambda_\tau \text{ eindeutig bestimmt.} \quad \square$$

$$(7.1): \begin{array}{l} Ax = b \\ A^\top \lambda + s = c \\ x, s \geq 0, i = 1, \dots, n \\ x, s \geq 0 \end{array}$$

Definition 7.2 (strikte komplementäre Lösung)

18.11.10

Eine Lösung (x^*, λ^*, s^*) der Optimalitätsbedingungen (5.3) heißt strikte komplementär, falls für alle $i=1, \dots, n$, entweder $x_i^* = 0$ oder $s_i^* = 0$.

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

Die strikt zulässige Menge \mathcal{E}^0 sei nicht leer.

für $\{\tau_k\}_{k=1}^\infty \downarrow 0$ seien $(x_{\tau_k}, \lambda_{\tau_k}, s_{\tau_k})$

Lösungen des ZPB (7.1). Dann ist die Folge

$\{(x_{\tau_k}, s_{\tau_k})\}_{k=1}^\infty$ beschränkt und besitzt daher eine konvergente Teilfolge. Jeder Häufungspunkt dieser Folge gehört zu einer strikt komplementären Lösung von (7.1).

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

$$\begin{aligned} (\underbrace{x_\tau - x^0}_\parallel)^T (\underbrace{s^0 - s^0}_\parallel) &= (x_\tau - x^0)^T (c - A^T \lambda_\tau - c + A^T \lambda^0) \\ &= (x_\tau - x^0)^T A^T (\lambda^0 - \lambda_\tau) \\ &= (A(x_\tau - x^0))^T (\lambda^0 - \lambda_\tau) \\ &= (b - b)^T (\lambda^0 - \lambda_\tau) = 0 \end{aligned}$$

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

$$\Leftrightarrow \underbrace{x_\tau^T s^0}_0 + \underbrace{(x^0)^T s_\tau}_0 = \underbrace{x_\tau^T s_\tau}_n + (x^0)^T s^0 = n\tau + (x^0)^T s^0$$

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

$$\underbrace{x_\tau^T s^0}_0 + \underbrace{(x^0)^T s_\tau}_0 \leq \underbrace{n\bar{\tau}}_0 + \underbrace{(x^0)^T s^0}_0 \Rightarrow (x_\tau)_{\tau \geq 0}, (s_\tau)_{\tau \geq 0} \text{ beschränkt}$$

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

$$\begin{aligned} x_{\tau_k}^T s^0 + (x^0)^T s_{\tau_k} &\leq n\tau_1 + (x^0)^T s^0 \\ &\Rightarrow (x_{\tau_k}, s_{\tau_k}) \text{ beschränkt} \end{aligned}$$

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

$$x_{\tau_k} := x_{\tau_k} \rightarrow x^* \geq 0 \quad A x_{\tau_k} = b \Rightarrow A x^* = b$$

$$s_{\tau_k} := s_{\tau_k} \rightarrow s^* \geq 0 \quad A^T s_{\tau_k} = A^T \lambda_{\tau_k} \in A^T(\mathbb{R}^m) = \text{Bild}(A^T)$$

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

$$\Rightarrow c - s_{t_k} \rightarrow c - s^* \in A^T(\mathbb{R}^m)$$

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

$$A^T \lambda^* + s^* = c \quad \checkmark$$

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

Satz 5.3

x^* opt Lsg von (3.4)

(λ^*, s^*) opt Lsg von (5.2)

Strikte Komplementarität:

$$\text{Für } t > 0: \underbrace{(x_t - x^*)^T}_{\text{P}} (s_t - s^*)^T = (x_t - x^*)^T A^T (\lambda^* - \lambda_t) \\ = (b - b^*)^T (\lambda^* - \lambda_t) = 0$$

$$x_t^T s^* + (x^* s_t) = \underbrace{x_t^T s_t}_{=n} + \underbrace{(x^*)^T s^*}_{=0}$$

$$\Leftrightarrow \frac{1}{t} \cdot x_t^T s^* + \frac{1}{t} (x^*)^T s_t = n$$

$$\forall k' \geq 1: \tau := t_{k'} : \sum_{i=1}^n \underbrace{\frac{(x_{t_{k'}})_i \cdot s_i^*}{t_{k'}}}_{\text{neu}} + \sum_{i=1}^n x_i^* \cdot \left(\frac{(s_{t_{k'}})_i}{t_{k'}} \right) = n \\ \stackrel{1}{=} \frac{1}{(s_{t_{k'}})_i};$$

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

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

Ich nehme an, dass für $\tau \in \{1, \dots, n\} : x_\tau^* = s_\tau^* = 0$

$$k \rightarrow \infty : \frac{s_i^*}{(s_{t_{k'}})_i} \rightarrow 1 \Rightarrow \text{entweder } x_i^* = 0 \text{ oder } s_i^* = 0. \quad \square$$

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: (IA 2)

7.2. Innere-Punkte-Methoden via Newton-Verfahren

Wir wollen die Lösung der 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:

$$X = \text{diag}(x_1, \dots, x_n)$$

$$S = \text{diag}(s_1, \dots, s_n)$$

$$e = (1, \dots, 1)^T \in \mathbb{R}^n$$

Dann lässt sich (7.1) wie folgt äquivalent schreiben:

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

$$\text{wobei } F_t(x, \lambda, s) := \begin{pmatrix} A^T \lambda + s - c \\ A x - b \\ X S e - t e \end{pmatrix} \quad \left| \quad \begin{array}{l} X S e = \begin{pmatrix} x_1 s_1 \\ \vdots \\ x_n s_n \end{pmatrix}, t e = \begin{pmatrix} t \\ \vdots \\ t \end{pmatrix} \end{array} \right. \quad (7.4)$$

Die Jacobi-Matrix hat die folgende Darstellung

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

Satz 7.6 Sei $(x, \lambda, s) \in \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^n$ mit $x > 0$ und $s > 0$ gegeben.

Besitzt A vollen Rang, dann ist die Jacobi-Matrix $DF_t(x, \lambda, s)$ regulär.

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

$$\Leftrightarrow \begin{cases} A^T p_2 + p_3 = 0 & | \cdot p_1^T \Rightarrow p_1^T A^T p_2 + p_1^T p_3 = 0 \Leftrightarrow \underbrace{(A p_1)^T p_2}_{=0} + p_1^T p_3 = 0 \Rightarrow p_1^T p_3 = 0 \quad \checkmark \\ A p_1 = 0 \\ S p_1 + X p_3 = 0 \end{cases}$$

$$\Rightarrow S p_1 = -X p_3 \Leftrightarrow p_1 = -S^{-1} X p_3 \stackrel{V}{\Rightarrow}$$

$$\Rightarrow 0 = -p_1^T (\underbrace{S - X}_{\text{pos. def.}}) p_3 \Rightarrow p_3 = 0$$

$$\begin{cases} A^T p_2 = 0 \\ \text{rang}(A) = m \end{cases} \Rightarrow p_2 = 0 \quad \Rightarrow p_1 = 0$$

□

Satz 7.6 rechtfertigt die Anwendung des Newton-Verfahrens auf (7.4).

Der Newton-Schritt bei dem Iteranten (x^k, λ^k, s^k)

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

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

wobei $X^k = \text{diag}(x_1^k, \dots, x_n^k)$ und $S^k = \text{diag}(s_{11}, \dots, s_{nn})$.

Unter Satz 6.1 ist das Newton-Verfahren lokall konvergent.

Zwecks Globalisierung dieses Verfahrens bestimmt man eine Schrittwerte $t_k > 0$ 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 $A x^k = b$ erfüllt. Aus (7.5):

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

$$A \Delta x^k = 0$$

Dann gilt $A^T \lambda^{k+1} + s^{k+1} - c = A^T(x^k + t_k \Delta \lambda^k) + s^k + t_k A \Delta x^k - c$
 $= \underbrace{A^T \lambda^k + s^k}_c + t_k (A^T \Delta \lambda^k + \Delta s^k) - c = 0$

$$A x^{k+1} = A(x^k + t_k \Delta x^k) = \underbrace{A x^k}_0 + t_k \underbrace{A \Delta x^k}_0 = b$$

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

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 Innen-Punkte-Verfahren an, welches eine strikt zulässige Lösung als Startvektor verwendet und setzt voraus, dass $\text{rang}(A) = m$.

Algorithmus 7.1 (Allgemeines Innere-Punkte-Verfahren)

23.11.10

1. Wähle $(x^0, \lambda^0, s^0) \in E^\circ$, $\varepsilon > 0$ 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

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

4. Bestimme die Schrittwerte $t_k > 0$ 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) ~~Bi~~ $(x^0, \lambda^0, s^0) \in E^\circ$ laut Bemerkung 7.1 und Schritt 4 folgt, dass $(x^k, \lambda^k, s^k) \in E^\circ \forall k \geq 1$.

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 Zentriierungsparameters 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 näher 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) $\mu_k(t) = (1 - t(1 - \sigma_k)) \mu_k$.

NT Def:

23.11

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

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

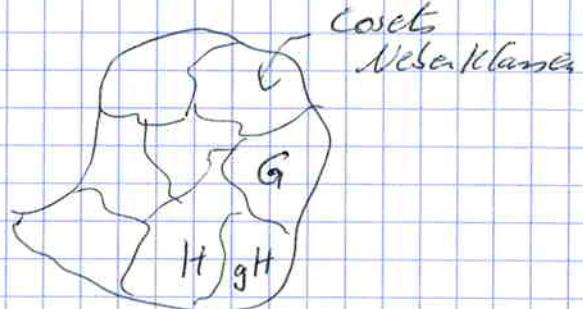
Lemma

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

Proof Ideen:

$$|H| \mid |G|$$

$$|G| = k \cdot |H|$$



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

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

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

$$\begin{array}{l} H = \{0, 2, 4\} \\ \text{cosets: } \rightarrow 1+H = \{1, 3, 5\} \end{array}$$

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

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

Lemma 2

Let $a \in (\mathbb{Z}_n, \cdot)$ and $a^x = 1$, then $\text{ord}_n a | x$.

Proof

Denote $\text{ord}_n a = n$ and write

$$x = q \cdot n + r, \text{ where } 0 \leq r < n.$$

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

$$\text{If } r > 0, \text{ then } \downarrow \Rightarrow r = 0 \Rightarrow x = q \cdot n \Rightarrow n | x$$

□

Reminder: If $g \in \mathbb{Z}_n^*$

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$$

we denote $\text{ord}_n g$ by $\text{ord}_n g$

$$a \cdot x \equiv 1 \pmod{n}$$

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

Lemma 3

$$\text{ord}_m a^k = \frac{\text{ord}_m a}{\gcd(k, \text{ord}_m a)} \quad \left(\text{ord}_m 8 = \frac{\text{ord}_2 8}{\gcd(3, \text{ord}_2 8)} \right)$$

Proof

Denote R.H.S by x .

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

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

2) that x is the smallest such #

Indeed:

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

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

$$\Rightarrow \text{ord}_m a | ky \Rightarrow ky = \text{ord}_m a \cdot b$$

Lemma 2

$$\Rightarrow ky = \text{ord}_m a \cdot \ell \Rightarrow \frac{ky}{\gcd(k, \text{ord}_m a)} = \frac{\text{ord}_m a \cdot \ell}{\gcd(k, \text{ord}_m a)}$$

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

$$\& \gcd(x, \frac{k}{\gcd(k, \text{ord}_m a)}) = 1$$

$\Rightarrow x \mid y \Rightarrow x$ is smallest

□

Corollary

If $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ $\text{ord}_n a \mid f(n)$.
 $\Rightarrow (\mathbb{Z}_n^*)$

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

Lemma 4

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

Lemma 5

If $p \geq 3$ is prime, then the congruence
 $x^d \equiv 1 \pmod{p}$ has exactly d solutions mod p .

Proof

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

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

$$0 \equiv x^{d \cdot \ell} - 1 \equiv (x^d - 1)(x^{d(\ell-1)} + x^{d(\ell-2)} + \dots + x^d + 1) \pmod{p}$$

has exactly $\underbrace{= 0}_{p-1 \text{ solutions}} \at most \underbrace{= 0}_{d \text{ solutions}}$ at most $d(\ell-1)$ solutions

$$= p-1$$

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

$$\leq d \cdot \ell$$

□

Then

let $p \geq 3$ be prime and $d \mid p-1 (d > 0)$

then in \mathbb{Z}_p^* there are exactly $\varphi(d)$ elements of order d .

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

$$\text{ord}_5 1 = 1$$

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

$$\text{ord}_5 3 = 4$$

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

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

$\varphi(2)$ elements of order 2

$\varphi(4)$ elements of order 4

Proof

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

We subdivide this set into the following subsets

here $d \mid p-1$

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

Then the set

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

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

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

Note that

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

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

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

We will prove now that $\psi(d) \subseteq f(d)$ (***)

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

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

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

$\Rightarrow a^d \equiv 1 \pmod{p}$ and the congruence

$x^d \equiv 1 \pmod{p}$ has solutions $L\{a, a^2, \dots, a^{d-1}\}$ and all these numbers 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

$\text{ord}_p a^k = \text{ord}_p a = d$ this is those with $\gcd(k, d) = 1$. There are exactly

$\varphi(d)$ such elements in the list L (and $\Rightarrow n \in A(d)$)

Q.E.D.

UT

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

Proof

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

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

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^*

$$\mathbb{Z}_p^* = \{0, g^2, g^3, \dots, g^{p-1} = 1\}$$

1) $g^{\frac{p-1}{2}}$ is a QR, because $(g^{\frac{p-1}{2}})^2 = g^p \equiv g \pmod{p}$.

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

$$\text{FLT} \quad 1 \equiv c^{p-1} = (c^2)^{\frac{p-1}{2}} \equiv (g^{2k+1})^{\frac{p-1}{2}} \stackrel{\text{FLT}}{\equiv} (g^{p-1})^k \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod{p}$$

So we have $g^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ $\quad \text{y} \quad \square$

Corollary

$$\text{QR} \cdot \text{QR} = \text{QR}$$

$$\text{NR} \cdot \text{NR} = \text{QR}$$

$$\text{QR} \cdot \text{NR} = \text{NR}$$

Example

Find all Quadratic Residues modulo 13.

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

$$1^2 \equiv 1 \pmod{13}$$

$$12^2 \equiv 1$$

$$2^2 \equiv 4$$

$$11^2 \equiv 4$$

$$c^2$$

$$3^2 \equiv 9$$

$$10^2 \equiv 9$$

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

$$4^2 \equiv 3$$

$$9^2 \equiv 3$$

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

$$5^2 \equiv 12$$

$$8^2 \equiv 13$$

$$x^2 \equiv a \pmod{p}$$

$$6^2 \equiv 10$$

$$7^2 \equiv 10$$

Def

The Legendre symbol of a modulo p

\leftrightarrow

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

Properties

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

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

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 $b \not\equiv 0 \pmod{p}$)

Thm (Euler's criterion)

Let p be an odd prime. Then

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

Proof

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

2) $a \in \mathcal{O}$ OR $a \in \mathcal{N}$ mod p , then $\left(\frac{a}{p}\right) = 1$, $a^{\frac{p-1}{2}} = (c^2)^{\frac{p-1}{2}} = c^{\frac{p-1}{2}} \stackrel{\text{FT}}{=} 1$

3) $a \in \mathcal{NR}$ mod p , then $\left(\frac{a}{p}\right) = -1$ $c \not\equiv 0 \pmod{p}$

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

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

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

II

Example

$$1 = \frac{-1}{8753} = (-1) \quad \begin{array}{c} 8752 \\ \hline 2 \end{array} = (-1)^{\frac{4376}{2}} = 1 \quad (\cancel{\text{mod } 8753})$$

Theorem

(Quadratic Reciprocity Law)

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

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

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

Example 1

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

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

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

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

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

Proof Q R L I

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad (\text{Euler's criterion})$$

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

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

I. 5 proved.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \equiv c^2 \pmod{p} \\ -1, & \text{else} \\ 0, & \text{p|a} \end{cases}$$

THEOREM QRL

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

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

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

In order to prove (2) we need the following lemma:

Lemma (Gauss)

Let p be an odd prime, ~~not~~
 $a \neq \varphi(p)$. 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 $\pmod{\frac{p}{2}}$

Example $\left(\frac{3}{13}\right)$, $S = \{3, 6, 9, 12, 15, 18\}$
 $\stackrel{\text{mod } 13}{\equiv} \{3, 6, 9, 12, 2, 5\}$

$$\rightarrow h = 2$$

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 $j^2 \neq k^2 \pmod{p}$

If they were equal, then $(j-a)a \equiv 0 \pmod{p}$

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

Also $ja \not\equiv -ha \pmod{p}$, because otherwise $p \mid (j+h)a$

It means, that if $S' \equiv S \pmod{p}$ and $S' \subset (-\frac{P}{2}, \frac{P}{2})$,
then ~~all numbers in~~ S' the absolute values of
all numbers in S' are different.

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

$\nearrow P$
only one of this signs!

Multiply

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

$$a^{\frac{P-1}{2}} \cdot \left(\frac{P-1}{2}\right)! \stackrel{\substack{\text{Euler} \\ \text{ criterion}}}{=} \left(\frac{a}{p}\right) \cdot \left(\frac{P+1}{2}\right)! \pmod{p}$$

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

$h = \# \text{ of } \cancel{\text{elements}} \text{ in } S \text{ and in } \left(\frac{P}{2}, p\right)$

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

$= \# \text{ of integers in } \left(\frac{P}{4}, \frac{P}{2}\right)$

(1) $p \equiv 1 \pmod{8}$, then $p = 1 + 8h$ for some h

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

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

$= 2h, h \text{ is even}$

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

(2) - (4) are similar

To prove III-

Get

Lemma

Let p be an odd prime and $a \neq 0 \pmod{p}$

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

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

From Gauss'

lemma

$h_p = \# \text{ of elements in } S_p \text{ whose}$

least residues $\geq \frac{p}{2}$

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

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

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

(i) $q \equiv p \pmod{4a} \Rightarrow q = p + 4ah \text{ for some}$
 $h \in \mathbb{Z}$

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

and in $(\frac{P}{2a} + 2h, \frac{P}{a} + 4h) \cup (\frac{3P}{2a} + 6h, \frac{2P}{a} + 8h)$

The general fact: The # of integers in

$(x, y), (x, y+2), (x+2h, y+2a)$

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.

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

Proof III Part of THM

Case $p \equiv q \pmod{4}$

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

$$\text{and: } \left(\frac{P}{q}\right) = \left(\frac{4h+q}{q}\right) = \left(\frac{4h}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{h}{q}\right) = \left(\frac{h}{q}\right) \quad (*)$$

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{p-4h}{p}\right) = \left(\frac{-4h}{p}\right) = \left(\frac{-h}{p}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{h}{p}\right) \stackrel{\substack{\text{Lemma} \\ \text{above}}}{=} \left(\frac{-1}{p}\right)\left(\frac{h}{q}\right) \stackrel{(*)}{=} \left(\frac{-1}{p}\right)\left(\frac{P}{q}\right) \end{aligned}$$

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

Case 2 $p \equiv q + 2 \pmod{4} \Rightarrow p \equiv -q \pmod{4}$

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

$$\left(\frac{P}{q}\right) = \left(\frac{4h-q}{q}\right) = \left(\frac{h}{q}\right); \left(\frac{q}{p}\right) = \left(\frac{4h-p}{p}\right) = \frac{h}{p} \stackrel{\substack{\text{Lemma} \\ \text{QRL}}}{=} \frac{h}{q} = \frac{P}{q} \quad \text{by } (*)$$

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

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

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

Example

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

$$1. \quad p \equiv 1(4)$$

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

$$2. \quad p \equiv -3(4)$$

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

Exercise

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

The Jacobi-Symbol

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

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

$$\left(\frac{a}{u}\right) := \left(\frac{a}{p_1}\right)^{e_1} \cdots \cdots \left(\frac{a}{p_n}\right)^{e_n}$$

Properties

(u, v are odd integers)

$$1) a \equiv b \pmod{u}$$

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

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

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

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

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

Warning

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

Example

$$\left(\frac{41}{57}\right) = \left(\frac{41}{3 \cdot 17}\right) \stackrel{(5)}{=} \left(\frac{41}{3}\right) \cdot \left(\frac{41}{17}\right) = \left(\frac{2}{3}\right) \left(\frac{7}{17}\right)$$

$$= -1 \cdot \left(\frac{17}{7}\right) = -1 \left(\frac{3}{7}\right) = \left(\frac{2}{3}\right) \left(\frac{-1}{3}\right) = -1$$

Suppose 41 is a square mod 57

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

$$41 \equiv c^2 \pmod{57}$$

$$\Rightarrow 41 \equiv c^2 \pmod{3}$$

$$\left[c^2 = 41 + h \cdot 57 = 41 + (h \cdot 17) \cdot 3 \right]$$

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

Example

Does the congruence

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

$\overset{\text{prime}}{\text{prime}}$

$$\begin{aligned} \left(\frac{888}{1999}\right) &= \left(\frac{2^3 \cdot 111}{1999}\right) \stackrel{(4)}{=} \left(\frac{2}{1999}\right) \left(\frac{111}{1999}\right) \\ \text{Legendre-} & \\ \text{symbol} & \stackrel{(2)}{=} 1 + \left(\frac{1999}{111}\right) = -\left(\frac{1}{111}\right) = -\left(\frac{1}{p \cdot q \dots}\right) = \\ &= -1 \cdot 1 \cdot \dots = -1 \end{aligned}$$

Proposition

Let p be prime and $p \equiv 3 \pmod{4}$

and let a be a QR mod p $\left\{ \left(\frac{a}{p}\right) = 1 \right\}$
 Then $c = a^{\frac{p+1}{4}}$ is a solution to $x^2 \equiv a \pmod{p}$

Proof

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

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

Euler's criterion

Remark

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

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

$$\dots a_i \dots a_2 a_1 a_0$$

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

If n is a natural number, and

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

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 $\overline{0}$) 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 sequence (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:

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

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) :

$$\begin{array}{r} \dots & 0 & 0 & 0 & 0 & 0 & 0 \\ - & \dots & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline \dots & 6 & 6 & 6 & 6 & 6 & 6 \end{array}$$

(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 $n\alpha = \alpha + \dots + \alpha$ (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 $p = \dots 0010$ 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 $\alpha_0, \alpha_1, \alpha_2, \dots$ 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 $\alpha_1, \alpha_2, \dots$ all end in zero), the second-last is the second-last digit of $\alpha_0 + \alpha_1$ (because $\alpha_2, \alpha_3, \dots$ 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:

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

(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 $\alpha = \dots 333334$ is the number "one half" by adding it to itself:

$$\begin{array}{r} \dots & 3 & 3 & 3 & 3 & 3 & 4 \\ + & \dots & 3 & 3 & 3 & 3 & 4 \\ \hline \dots & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

Thus, in the 7-adic integers, "one half" is an *integer*. And so are "one third" ($\dots 444445$), "one quarter" ($\dots 1515152$), "one fifth" ($\dots 541254125413$), "one sixth" ($\dots 55556$), "one eighth" ($\dots 0606061$), "one ninth" ($\dots 3613613614$), "one tenth" ($\dots 462046205$), "one eleventh" ($\dots 162355043116235504312$) and so on. But "one seventh", "one fourteenth" 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 $\beta = 1 + \alpha + \alpha^2 + \dots$ 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 $(1 - \alpha)\beta = 1 - \alpha + \alpha - \alpha^2 + \alpha^2 - \dots = 1$. 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 p -adic number 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 integer, 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 .

\mathbb{F} -adic numbers

Motivation

$$\frac{x^2 - 2 \equiv 0 \pmod{\mathbb{F}^k}}{x_0^2 - 2 \equiv 0 \pmod{\mathbb{F}}}$$

$$x_0^2 - 2 \equiv 0 \pmod{\mathbb{F}}$$

$$x_0 = 3$$

$$\frac{x_1^2 - 2 \equiv 0 \pmod{\mathbb{F}^2}, \quad x_1 \equiv x_0 \pmod{\mathbb{F}}}{x_1 = x_0 + \mathbb{F}a_1}$$

$$\begin{aligned} 0 \equiv (x_0 + \mathbb{F}a_1)^2 - 2 &= x_0^2 + \cancel{2x_0\mathbb{F}} + \mathbb{F}^2a_1 \cdot x_0 \\ &\quad + \mathbb{F}^2a_1^2 - 2 \\ &\equiv \mathbb{F}(1 + 6a_1) \equiv 0 \pmod{\mathbb{F}} \end{aligned}$$

$$\Rightarrow 1 + 6a_1 \equiv 0 \pmod{\mathbb{F}}$$

$$\Rightarrow a_1 \equiv 1 \pmod{\mathbb{F}}$$

$$x_1 = 3 + \mathbb{F} \cdot 1 = 10$$

$$\frac{x_2^2 - 2 \equiv 0 \pmod{\mathbb{F}^3}, \quad x_2 \equiv x_1 \pmod{\mathbb{F}^2}}{x_2 = x_1 + \mathbb{F}^2a_2}$$

$$\begin{aligned} 0 \equiv (x_1 + \mathbb{F}^2a_2)^2 - 2 &\equiv x_1^2 + 2 \cdot \mathbb{F}a_2 \cdot x_1 \\ &\quad + \mathbb{F}^4a_2^2 - 2 \\ &= 2 \cdot \mathbb{F}^2(1 + 10a_2) \equiv 0 \pmod{\mathbb{F}^3} \end{aligned}$$

$$2 \cdot (1 + 10a_2) \equiv 0 \pmod{\mathbb{F}}$$

$$a_2 = 2$$

$$x_2 = 10 + \mathbb{F}^2 \cdot 2 = 108$$

$$x_3 = 3 + \mathbb{F} + 2 \cdot \mathbb{F}^2 + 6 \cdot \mathbb{F}^3 = 2166$$

$$x_0 = \lim_{n \rightarrow \infty} x_n := \sum_{k=0}^{\infty} a_k \cdot p^k \quad (\text{p-adic integers})$$

$$\mathbb{Z}_p := \left\{ (x_0, x_1, x_2, \dots) \in \prod_{k=0}^{\infty} \mathbb{Z}/p^{k+1}\mathbb{Z} \mid x_{k+1} \equiv x_k \pmod{p^{k+1}} \right\}$$

Read at home again:

- principal ideal ring
- integral domain
- groups of units of a ring
- prime vs. irreducible elements
- maximal ~~into~~ ideal

$$c_k = \frac{x_k - x_{k-1}}{p}$$

Example
 $p = 7$

$$x = 4 \cdot 7^3 + 3 \cdot 7^2 + 0 \cdot 7 + 1 = 6301$$

$$y = 16 \cdot 7^2 + 17 = 610$$

$$x+y = 4301 + 610 = 4911$$

$$x-y = 3361$$

$$x-y: \begin{array}{r} 4301 \\ - 610 \\ \hline 3690 \end{array}$$

Let $p \in \{2, 3, 5, \dots\}$ be a fixed prime.

A formal series

$$x := \sum_{i=0}^{\infty} a_i p^i \text{ where } a_i \in \{0, 1, \dots, p-1\}$$

is called a p -adic integer.

Denote partial sums of this series by

$$s_h = \sum_{i=0}^{p^{h-1}} a_i p^i = a_0 + a_1 p + \dots +$$

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 $s_h \in \{0, 1, \dots, p^{h-1}\}$ & $h \geq 1, \dots$

then $a_h = \frac{s_{h+1} - s_h}{p^h}$ satisfies $0 \leq a_h < p$
and is determined uniquely for given

$$(s_h)_{h \in \mathbb{N}}$$

$$x \in \prod_{h=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

Consider the mapping

$$\begin{aligned} \mathbb{Z}_p &\rightarrow \mathbb{Z}_p \\ x &\mapsto (s_1, s_2, \dots) \end{aligned}$$

where $s_h \equiv x \pmod{p^h}$

THM (properties of \mathbb{Z}_p and \mathbb{Z}_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 \mathcal{E} as a subset of \mathcal{E}_p

3) The group of units $(\mathbb{Z}_p)^{\times} = \mathbb{Z}_p^{\times} / p\mathbb{Z}_p$

That is, \mathcal{C}^* consists of the elements

$$x = \sum_{i=0}^r a_i p^i \text{ with } a_0 \neq 0$$

Q1 Every element $x \in \mathbb{R}_p \setminus \{0\}$ can be written uniquely in the form

$$x = p^n \cdot u \quad \text{with } n \in \mathbb{N}_0 \text{ and } u \in \mathbb{Z}_p^+$$

5) In particular $x=p$ is the only prime irreducible (and the only prime) in \mathbb{Z}_p^\times up to multiplication by an associate.

5) All ideals in \mathbb{Z}_p are the following:

$q_i \in p_i, p''_i \in p$ for all $n \in N$

In particular the only maximal ideal in \mathbb{H}_p is $p \oplus p^\perp$.

Example

$$p = 7 \quad x = 2 + 4 \cdot 7 + 3 \cdot 7^2 + \dots$$

$$y = 2 + 5 \cdot 7 + 2 \cdot 7^2$$

$$\begin{aligned}
 (11) \quad x+y &= 4 + (4+5) \cdot 7 + (3+2) \cdot 7^2 \\
 &= 4 + (2+7) \cdot 7 + (3+2) \cdot 7^2 \\
 &= 4 + 2 \cdot 7 + 6 \cdot 7^2
 \end{aligned}$$

$$(2) x \cdot y = 6 + (2 \cdot 4 + 2 \cdot 5) \cdot 7 + (2 \cdot 2 + 4 \cdot 5 + 3 \cdot 4) \cdot 7^2 + \dots$$

$$= 6 + 4 \cdot 7 + 4 \cdot 7^2 + \dots$$

$$(3) \frac{1}{z} = z^{-1} \quad z^{-1} \cdot z = 1$$

205

$$\dots \underset{5}{\cancel{a_2}} \underset{5}{\cancel{a_1}} \underset{5}{\cancel{a_0}} \dots \underset{5}{\cancel{a_2}} \underset{5}{\cancel{a_1}} \underset{5}{\cancel{a_0}} \dots$$

Proof

1a) We'll first prove, that \mathbb{Z}_p is an integral domain.

Take $x, y \in \mathbb{Z}_p \setminus \{0\}$, then

~~$x=y$~~ we shall prove that

$$x \cdot y \neq 0$$

Find non-zero coefficients

\Rightarrow their product is not zero

(because $\mathbb{Z}_p = \mathbb{F}_{p^2}$ is a field)

2) Here we prove that

$$\ker \varphi_p = \{0\}$$

3) Let $x = \sum_{i=0}^{\infty} a_i p^i$

i) $a_0 = 0$, then $p|x \Rightarrow x \equiv 0 \pmod{p}$ but

$$\nexists y : x \cdot y \equiv 1 \pmod{p},$$

in other words $x \cdot y = \begin{pmatrix} 0, 5, \dots, 5 \dots \\ s \end{pmatrix}$

$$\neq (1, 1, \dots, 1)$$

Def: $X = (F, +, \cdot)$ a field \nleftrightarrow Eine Norm von X

$\| \cdot \| : X \rightarrow \mathbb{R}$

(1) $\|x\| \geq 0 \quad \forall x \in X$, moreover $\|x\| = 0 \Leftrightarrow x = 0$

(2) $\|x \cdot y\| = \|x\| \cdot \|y\| \quad \forall x, y \in X$

(3) $\|x + y\| \leq \|x\| + \|y\|$

$d(x, y) = \|x - y\|$

Def: The p -adic valuation is the map

$$v_p: \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{\infty\}$$
$$\begin{cases} v_p^m u & \mapsto m, \quad (m \in \mathbb{Z}, u \in \mathbb{Z}_{(p)}^*) \\ 0 & \mapsto \infty \end{cases}$$

Examples: $v_5 = 5$ $\frac{5^2 - 2}{5^2} = 2$ $x \in \mathbb{Z}_5^* = \left\{ \sum_{i=0}^{\infty} a_i p^i, a_0 \neq 0 \right\}$
 $x = 50$ $v_5(50) = 2$

- If m is an integer, then $v_p(m)$ is the highest p power of p so that $p^k \mid m$

- let $m = a \cdot b$, then $v_p(a \cdot b) = v_p(a) + v_p(b)$

- Let $\frac{a}{b} \in \mathbb{Q}$, then $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$

$$v_5(250) = 3$$

$$v_5(125) = 3$$

$$v_5(249) =$$

$$249 = 4 + 245 = 4 + 5 \cdot (\dots)$$

$$a_0 + 5 \cdot (a_1 + 5 \cdot (\dots))$$

—

M-5,

Pontryagin

Chapter 13 (14?)

... hkg.pdf

p -adic.pdf.

—

Properties of $v_p(x)$:

1. $v_p(x) = \infty \iff x = 0$
2. $v_p(x \cdot y) = v_p(x) + v_p(y)$
3. $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$
 $v_p(x+y) = \min\{v_p(x), v_p(y)\}$, if $v_p(x) \neq v_p(y)$
4. $\mathbb{Z}_p = \{z \in \mathbb{Q}_p \mid v_p(z) \geq 0\}$
5. $\mathbb{Z}_p^* = \{z \in \mathbb{Q}_p \mid v_p(z) = 0\}$

Proof

1° and 2° are obvious.

$$3. x, y \in \mathbb{Q}_p; x = p^m u, y = p^n v$$

WLOG we assume that $v_p(y) = n \leq m = v_p(x)$

$$x+y = p^n (v + p^{m-n} \cdot u)$$

$$1) \text{ If } m > n, \text{ then } v + p^{m-n} u \in \mathbb{Z}_p^* \text{ and}$$

$$v_p(x+y) = n = v_p(y) = \min(v_p(x), v_p(y))$$

$$2) \text{ If } m = n \quad \begin{cases} v+u \text{ is a unit} \Rightarrow \dots = \dots \\ v+u \text{ is not a unit} \Rightarrow v_p(x+y) > n \\ -a_0 + p \sim a_0 + p \end{cases}$$

Def A p -adic norm is defined as:

$$1. \quad \lvert \rvert_p : \mathbb{Q}_p \rightarrow \mathbb{R}$$

$$x \stackrel{v}{\mapsto} p^{-v_p(x)} \quad (p^{-\infty} := 0)$$

Example

$$|250|_5 = \frac{1}{250} \cdot \frac{1}{125}$$

$$|-25|_5 = \frac{1}{125}$$

$$|249|_5 = \left(\frac{1}{5}\right)^0 = 1$$

$$d_5(250, -125) = |250 - (-125)|_5 = |375|_5 = \frac{1}{125}$$

$$d_5(250, 249) = |250 - 249|_5 = |1|_5 = 1$$

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \dots$$

~~a_2, a_0~~

$$p = 7 \quad x = \dots \underline{1} \underline{2} \underline{0} \underline{2} \underline{1} \underline{0} \underline{4} \underline{2} \underline{1}$$

$$y = \dots \underline{1} \underline{2} \underline{0} \underline{2} \underline{1} \underline{3} \underline{0} \underline{2} \underline{1}$$

$$z = \dots \underline{1} \underline{2} \underline{0} \underline{2} \underline{1} \underline{0} \underline{4} \underline{2} \underline{2}$$

$$d_7(x, y) = d_7(y, x) = 1$$

$$d_7(x, z) = 1$$

Lemma: A p -adic norm is a norm, moreover

$$|x+y|_p \leq \max\{|x|_p, |y|_p| y \in |x|_p + |y|_p$$

$$\text{If } |x|_p \neq |y|_p, \text{ then } |x+y|_p = \max\{|x|_p, |y|_p\}$$

Remark: A norm that satisfies (*) is called non-Archimedean

Def: Let (X, d) be a metric space. Then a sequence $\{x_i\}_{i \in \mathbb{N}} = \{x_1, x_2, \dots | x_i \in X, i=1, 2, \dots\}$ is called a Cauchy sequence, if $\forall \varepsilon > 0 \exists N \in \mathbb{N}$ s.t.

$$\forall n, m \geq N \quad d(x_m, x_n) < \varepsilon$$

p -adic integers

$$\mathbb{Z}_p = \left\{ x = (s_k)_{k \in \mathbb{N}} \mid s_k \in \mathbb{Z}/p^k \mathbb{Z}, s_k \equiv s_{k+1} \pmod{p^k} \right\}$$

In other words, $x \in \prod_{k=1}^{\infty} \mathbb{Z}/p^k \mathbb{Z}$, and if we denote $x(k) := s_k$ then $x(k) \equiv x(k+1) \pmod{p^k}$.

Example

$x = 123 \in \mathbb{Z}$, write this number as an element of \mathbb{Z}_5

$$x(1) = 3$$

$$x(2) = 23.$$

$$x(3) = 123$$

$$x(4) = 123$$

:

$$x(k) = 123$$

$$(3, 23, 123, \dots, 123) \in \mathbb{Z}_5$$

p -adic numbers

$$\mathbb{Q}_p = \{ p^m \cdot u \mid m \in \mathbb{Z}, u \in \mathbb{Z}_p^* \}$$

$$x = \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p$$

$$= a_0 + a_1 p + a_2 p^2 + \dots$$

$$a_0 \neq 0 \Rightarrow x \in \mathbb{Z}_p^*$$

$$(s_1, s_2, \dots)$$

$$x = \underbrace{(x(1),}_{\text{if } 0} \dots$$

]

$$= \{$$

p -adic valuation:

$$v_p: \mathbb{Q}_p \rightarrow \mathbb{Z}$$

$$\begin{matrix} \Downarrow \\ p^m u \rightarrow m \\ (0 \rightarrow \infty) \end{matrix}$$

p -adic norm

$$\begin{matrix} |\cdot|_p: \mathbb{Q}_p \rightarrow \mathbb{R}_{>0} \\ \begin{matrix} \Downarrow \\ x \rightarrow p^{-v_p(x)} \\ \Downarrow \\ p^m u \rightarrow \frac{1}{p^m} \end{matrix} \end{matrix}$$

p -adic distance

$$d_p(x, y) = |x - y|_p$$

Example:

$$\left| \frac{3}{5} \right|_7 = 1, \text{ b/c } v_p\left(\frac{3}{5}\right) = v_p(3) - v_p(5) = 0 - 0 = 0$$

Consider \mathbb{Q} , the set of rational numbers

Def A trivial norm on a field K is $|x|=1$ for all $0 \neq x \in K$

$$1) |x| \geq 0, |x|=0 \Leftrightarrow x=0$$

$$2) |x \cdot y| = |x| \cdot |y|$$

$$3) |x+y| \leq |x| + |y|$$

Thm (Ostrowski)

On the set of rational numbers, there are only the following norms up to equivalence

- 1) the trivial norm
- 2) the abs. value $\| \cdot \| = \| \cdot \|_\infty$
- 3) p -adic norms $\| \cdot \|_p$, for all primes p .

Def

Two norms $\| \cdot \|_1$ and $\| \cdot \|_2$ are called equivalent,

$$\text{if } \exists m, M > 0 \text{ s.t. } m\| \cdot \|_2 \leq \| \cdot \|_1 \leq M\| \cdot \|_2$$

Example

$$\|x\|_1 = |x|_p := \frac{1}{p^{v_p(x)}}, \quad \|x\|_2 = \alpha^{v_p(x)}, \text{ where } 0 < \alpha < 1$$

$$\text{Then } \| \cdot \|_1 \sim \| \cdot \|_2 \quad \text{Indeed since} \quad \left[\alpha^{v_p(x)} = \frac{1}{p} \right]$$

$$(\alpha)^{v_p(x)} = \left(\frac{1}{p} \log_p \alpha \right)^{v_p(x)}$$

Def

let X be a metric space. A sequence

$$x_1, x_2, \dots, x_n, \dots \quad (x_n \in X)$$

is called a Cauchy sequence on X if

$\forall \epsilon > 0 \exists N \in \mathbb{N}$ so that

$$d(x_i, x_j) < \epsilon \text{ whenever } i, j \geq N$$

Thm The field of p -adic numbers \mathbb{Q}_p is complete w.r.t. p -adic norm, that is, every Cauchy sequence in \mathbb{Q}_p is convergent (= has a limit in \mathbb{Q}_p)

Proof Consider a Cauchy sequence in \mathbb{Q}_p :

$$x_1, x_2, \dots, x_n, \dots \quad (x_n \in \mathbb{Q}_p) \quad (*)$$

1) First we show that $\{|x_n|_p | n \in \mathbb{N}\}$ is bounded from above. If not, then $\forall m \in \mathbb{N}, \forall N \in \mathbb{N}$ we would have $\exists i, j > N$ we would have $\cancel{\exists c_i, j > N}$ s.t. $|x_i|_p > |x_j|_p \geq p^m$

$$\begin{aligned} \text{Then we would have } |x_i - x_j|_p &= |x_i|_p \geq p^m \\ &= \max\{|x_i|_p, |x_j|_p\} \end{aligned}$$

Properties of p -adic norm:

$$|x+y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p \quad \cancel{\text{if } x, y \neq 0}$$

Therefore $\exists m \in \mathbb{N}$ s.t. $\forall n \in \mathbb{N} \quad |x_n|_p \leq p^m$.

2) For such an m the sequence

$$p^m x_1, p^m x_2, \dots, p^m x_n, \dots \quad (**)$$

is in \mathbb{Z}_p . Moreover, $(**)$ is Cauchy $\Leftrightarrow (x)$ is Cauchy

$$|p^m \cdot x_n|_p = |p^m|_p \cdot |x_n|_p \leq \frac{1}{p^m} \cdot p^m = 1$$

$$\Rightarrow p^m \cdot x_n \in \mathbb{Z}_p = \{x \in \mathbb{Q}_p | |x|_p \leq 1\}$$

3) So we assume wlog, that the sequence $(*)$ is in \mathbb{Z}_p

We will prove that $\exists z \in \mathbb{Z}_p$ which is the limit of the sequence $(*)$

For each $k \in \mathbb{N}$ we can find $N_k \in \mathbb{N}$ so that

$$|x_i - x_j|_p < p^{-k} \text{ whenever } i, j \geq N_k \quad (***)$$

Moreover, the sequence N_k can be chosen to be increasing. In particular, $N_k \leq k$.

Notice that $(***) \Leftrightarrow v_p(x_i - x_j) > k$

$$\Leftrightarrow p^{k+1} \mid (x_i - x_j)$$

$$\Leftrightarrow x_i - x_j \in p^{k+1} \cdot \mathbb{Z}_p$$

$$x_1, x_2, \dots, x_{N_1}, \dots, x_{N_2}, \dots, x_{N_k}, \dots$$

$$z_1 \equiv x_{N_1}(1) \pmod{p}$$

$$z_2 \equiv x_{N_2}(2) \pmod{p^2}$$

:

$$z_k \equiv x_{N_k}(k) \pmod{p^k}$$

Then we denote $z = (z_k)_{k \in \mathbb{N}}$.

$$\text{Then } 1) z \in \mathbb{Z} \quad z_k \equiv z_{k+1} \pmod{p^k}$$

2) the sequence $\{x_n\} \subset \mathbb{Z}_p$ is convergent to z .

Complex Numbers

$$x^2 + 1 = 0$$

$$i^2 = -1 \Rightarrow P(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_n x^n, c_j \in \mathbb{C} \quad \forall j \in \{0, \dots, n\}$$

$$c_n \neq 0 \Rightarrow n =: \deg P(x)$$

Thm (Fundamental thm of algebra)

Any polynomial $P(x)$ of degree $n \geq 1$ with complex coefficients has a root (=a zero) in \mathbb{C} . Moreover there are exactly n roots counting multiplicity.

x_0 is a root of $P(x)$ if $P(x_0) = 0$

What about \mathbb{Q}_p ?

Does every polynomial with coefficients in \mathbb{Q}_p have a root in \mathbb{Q}_p ?

WLOG:

$$P(x) = c_0 + c_1 x + \dots + c_n x^n \text{ with } c_i \in \mathbb{Z}_p, 0 \leq i \leq n.$$

Does $P(x)$ always have a root in \mathbb{Z}_p ?

Answer: No, not necessary.

$$x^2 - 7 = 0 \text{ has no solution in } \mathbb{Q}_5.$$

Thm (Hensel's lemma)

Let $P(x) = c_0 + c_1 x + \dots + c_n x^n$ be a polynomial of deg n in $\mathbb{Z}_p[x]$

let $P'(x) = c_1 + 2c_2 x + \dots + nc_n x^{n-1}$ be its derivative.

If $\exists \tilde{x} \in \mathbb{Z}_p$ with $P(\tilde{x}) \equiv 0 \pmod{p}$, but $P'(\tilde{x}) \not\equiv 0 \pmod{p}$ then

$\exists! x \in \mathbb{Z}_p$ s.t.

$$P(x) = 0 \text{ and } x \equiv \tilde{x} \pmod{p}$$

Proof

We claim that $\exists!$ sequence of integers $s_1, s_{2^n}, (s_k \in \mathbb{Z})$
s.t. $\forall K \geq 1$:

$$1) P(s_k) \equiv 0 \pmod{p^k} \quad 1') P(s_{k+n}) \equiv 0 \pmod{p^{k+1}}$$

$$2) s_{k+1} \equiv s_k \pmod{p^k}$$

$$3) 0 \leq s_k < p^k$$

$$3') 0 \leq s_{k+1} < p^{k+1}$$

We construct the sequence $\{s_k\}_{k=1}^\infty$ that satisfies
(1)-(3) by induction:

$K=1$

$$s_1 \equiv x \pmod{p}$$

$$\text{check (1): } P(s_1) = P(x) \equiv 0 \pmod{p}$$

(2): There is nothing to be checked.

(3): and we choose $0 \leq s_1 < p$

$K=2$

$$(2) \& (3) \Rightarrow 0 \leq s_2 < p^2, \quad s_2 \equiv s_1 \pmod{p}$$

$$s_2 = s_1 + b_1 p \quad \text{where } 0 \leq b_1 \leq p-1$$

$$\begin{aligned} \text{Now } P(s_2) &= P(s_1 + b_1 p) && \text{we think } \pmod{p^2} \text{ and ignore terms which are divisible by } p^2 \\ &= \sum_{i=0}^n c_i (s_1 + b_1 p)^i && \\ &= \sum_{i=0}^n c_i (s_1^i + i s_1^{i-1} \cdot b_1 p + \text{terms divisible by } p^2) && \\ &\equiv \sum_{i=0}^n c_i s_1^i + \sum_{i=1}^n c_i s_1^{i-1} b_1 p && \\ &= P(s_1) + P'(s_1) \cdot b_1 p \\ &\stackrel{(*)}{=} 0 \pmod{p^2} \end{aligned}$$

We have $P(s_1) \equiv 0 \pmod{p}$, so $P(s_1) = d_1 \cdot p$ for some ~~$d_1 \in \mathbb{Z}$~~
 $\pmod{p^2}$ $0 \leq d_1 < p-1$

Then (*) becomes

$$\begin{aligned} d_1 p + p'(s_1) \cdot b_1 p &\equiv 0 \pmod{p^2} \\ \Leftrightarrow d_1 + \underbrace{p'(s_1)}_{\equiv p'(\tilde{x}) \not\equiv 0 \pmod{p}} \cdot b_1 &\equiv 0 \pmod{p} \end{aligned}$$

$$b_1 \equiv -d_1 \cdot (P'(s_1))^{-1} \pmod{p} \quad \text{such a } b_1 \text{ is unique.}$$

$K \rightarrow K+1$

Let us assume that we already constructed s_1, s_2, \dots, s_k . We want to construct s_{k+1} that satisfies 1'), 2), 3').

$$2) \& 3') \Rightarrow 0 \leq s_{k+1} < p^{k+1}, \quad s_{k+1} \equiv s_k \pmod{p^k}$$

$$\Rightarrow s_{k+1} = s_k + b_k \cdot p^k, \quad \text{where } 0 \leq b_k \leq p-1.$$

$$\begin{aligned} \text{Now } P(s_{k+1}) &= P(s_k + b_k \cdot p^k) \quad \{ \text{think mod } \cancel{p^{k+1}} \} \\ &= \sum_{i=0}^n c_i (s_k + b_k \cdot p^k)^i \\ &= \sum_{i=0}^n c_i (s_k^i + i \cdot s_k^{i-1} \cdot b_k \cdot p^k + \text{term divisible by } p^{k+1}) \\ &\equiv P(s_k) + P'(s_k) \cdot b_k \cdot p^k \pmod{p^{k+1}} \end{aligned}$$

Again, since $P(s_k) \equiv 0 \pmod{p^k}$, we have

$$P(s_k) \equiv d_k \cdot p^k \pmod{p^{k+1}} \quad \text{with } 0 \leq d_k \leq p-1.$$

$$\Rightarrow b_k \equiv -d_k \cdot (P'(s_k))^{-1} \pmod{p} \quad 0 \leq b_k \leq p-1$$

Again b_k is uniquely determined.

Together with the sequence s_1, s_2, \dots we actually constructed $x = (s_1, s_2, \dots) \in \mathbb{Z}$. For this element x and every $k \in \mathbb{N}$, we have $P(x) \equiv 0 \pmod{p^k}$ $P(s_k) \equiv 0 \pmod{p^k}$

$$\Rightarrow p(x) = 0 \quad S_k = \tilde{x} + b_1 p + b_2 p^2 + \dots + b_{k+1} p^{k+1}$$

□

Examples

$$1) x^2 - 7 = 0 \text{ in } \mathbb{Z}_5$$

If $x \in \mathbb{Z}_5$, which is a solution, exists then we should have $x^2 - 7 \equiv 0 \pmod{5}$ is solvable in $\mathbb{Z}/5\mathbb{Z}$

$x^2 \equiv 2 \pmod{5}$ have no solution in $\{0, 1, 2, 3, 4\}$ and therefore $x^2 - 7 = 0$ has no solution in \mathbb{Z}_5 .

$$2) x^2 - 6 = 0 \text{ in } \mathbb{Z}_5$$

$$\text{a)} s_1 = 1 \Rightarrow x = (1, \dots)$$

$$\text{b)} s_1 = 4 \Rightarrow x = (4, \dots)$$

Quadratic residues over different fields:

$\mathbb{F}_p, \mathbb{R}, \mathbb{Q}, \mathbb{Q}_p$.

(\mathbb{F}_p^*, \cdot) d is a QR in $\mathbb{F}_p^* \iff$

\iff a solution to equation $x^2 = d$ in \mathbb{F}_p^*

\iff a solution to the congruence $x^2 \equiv d \pmod{p}$

\iff the Legendre symbol $\left(\frac{d}{p}\right) = 1$.

In general,

K^* - the group of units of $(K, +, \cdot)$ w.r.t. " \cdot ".

let's denote

$$K^{*2} = \{a^2 \mid a \in K^*\},$$

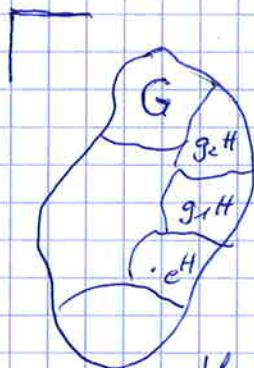
then

$$K^{*2} \trianglelefteq K^*. \text{ Indeed,}$$

sub-group $\begin{cases} 1) \text{ If } a^2 \in K^{*2}, b^2 \in K^{*2} \Rightarrow a^2 \cdot b^2 = (ab)^2 \in K^{*2} \\ 2) \text{ If } a^2 \in K^{*2} \Rightarrow (a^2)^{-1} = (a^{-1})^2 \in (K^*)^2 \end{cases}$

normal $\begin{cases} 3) \text{ If } a^2 \in K^{*2} \Rightarrow \forall b \in K^*, ba^2b^{-1} = b(b^{-1}a^2)b = a^2 \in K^{*2} \end{cases}$

$\cancel{\frac{K^*}{K^{*2}}}$. What is the structure of this quotient group
 (= factor group)



either $g_i H = g_j H \iff g_j \in g_i H \iff g_i^{-1}g_j \in H$
or $g_i H \cap g_j H = \emptyset \iff g_i^{-1}g_j \notin H$.

$$G/H = \{g \cdot H \mid g \in G\}$$

If $\{g_1, \dots, g_k\}$ is the set of elements in case G/H is finite

one of each coset, then it is called the system of representatives for G/H .

$$|G:H| = k \quad G = \bigcup_{i=1}^k g_i H, \quad g_i H \cap g_j H = \emptyset \text{ for } i \neq j$$

Goal: determine K^*/K^{*2} for all fields we know.

Notation:

Denote by

$$\log_{-1} : (\{\pm 1\}, \cdot) \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z}, +)$$

$$-1 \longrightarrow 1$$

$$1 \longrightarrow 0$$

This is an isomorphism.

Let $P = \{2, 3, 5, 7, 11, \dots\}$ be the set of all primes in \mathbb{N} .

I. $K = \mathbb{F}_p$:

Thm (about the structure of $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$)

- If $p \in \mathbb{P} \setminus \{2\}$, then the map

$$\begin{aligned} P_{\mathbb{F}_p} : \mathbb{F}_p^*/(\mathbb{F}_p^*)^2 &\longrightarrow \mathbb{Z}/2\mathbb{Z} \\ b \cdot \mathbb{F}_p^{\times 2} &\mapsto \log_{-1}\left(\frac{b}{p}\right) \end{aligned}$$

is an isomorphism.

- If $p=2$, then

$$\begin{aligned} P_{\mathbb{F}_2} : \mathbb{F}_2^*/\mathbb{F}_2^{\times 2} &\longrightarrow (\{\pm 1\}, \cdot) \\ &\quad (\{0\}, +) \end{aligned}$$

is an isomorphism.

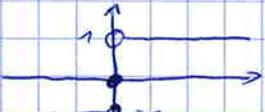
II $K = \mathbb{R}$

Thm The map

$$\Phi_{\mathbb{R}} : \mathbb{R}^*/(\mathbb{R}^*)^2 \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

$$x \cdot \mathbb{R}^{\times 2} \longrightarrow \log_{-1}(\operatorname{sgn} x)$$

$$\operatorname{sgn} x = \begin{cases} 1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases}$$



is an isomorphism. In particular $\{1, -1\}$ is the system of representatives

Remark

Sometimes you can see a generalisation of the Legendre symbol to $R = \mathbb{Q}_\infty$

$$\left(\frac{x}{\infty} \right) = \text{sgn } x$$

III $K = \mathbb{Q}$

$$\text{Thm } \Phi_{\mathbb{Q}} : \mathbb{Q}^*/(\mathbb{Q}^*)^2 \rightarrow \mathbb{Z}/2\mathbb{Z} \times \bigoplus_{p \in \mathbb{P}} \mathbb{Z}/2\mathbb{Z}$$

$$x \cdot \mathbb{Q}^{*2} \rightarrow (\log_-, \text{sgn } x, (v_p(x) + 2\mathbb{Z})_{p \in \mathbb{P}})$$

Example

$$x = -\frac{3}{5}$$

$$\Phi_{\mathbb{Q}}\left(-\frac{3}{5} \cdot \mathbb{Q}^{*2}\right) = (1, v_2\left(\frac{3}{5}\right) \bmod 2, v_3\left(\frac{3}{5}\right) \bmod 2, v_5\left(\frac{3}{5}\right) \bmod 2, \dots)$$

$$= (1, 0, 1, 1, \underbrace{0, \dots, 0}_{\text{only zeros}})$$

$$\boxed{v_p(x \cdot (y)^2) = v_p(x) + v_p(y)^2 = v_p(x) + 2v_p(y) \equiv v_p(x) \bmod 2}$$

Reminder:

$$\bigoplus_{i \in I} \mathbb{G}_i = \left\{ (g_i)_{i \in I} \in \prod_{i \in I} \mathbb{G}_i \mid \text{only finitely many of } g_i \neq 0 \right\}$$

$$(G_i, +) \quad \begin{matrix} (g_1, g_2, \dots, g_n, \dots) \\ + \\ (h_1, h_2, \dots, h_n, \dots) \end{matrix}$$

Proof

$$\tilde{\Phi}_Q : Q^* \xrightarrow[\psi]{} \mathbb{Z}/2\mathbb{Z} \times \bigoplus_{p \in P} \mathbb{Z}/2\mathbb{Z}$$

$x \longrightarrow$ same

- 0) $\tilde{\Phi}_Q$ is well defined
 - 1) $\tilde{\Phi}_Q$ is a homomorphism
 - 2) $\tilde{\Phi}_Q$ is surjective.
- 1 $\rightarrow (1, 0, 0, 0, \dots)$
 2 $\rightarrow (0, 1, 0, \dots)$
 3 $\rightarrow (0, 0, 1, 0, \dots)$

3) Calculate $\ker \tilde{\Phi}_Q$.

i) $Q^{*2} \subseteq \ker \tilde{\Phi}_Q$, because if $x \in Q^{*2}$, then $x > 0$
 and $\sigma_p(x)$ is even. ($\equiv 0 \pmod{2}$) $\Rightarrow \tilde{\Phi}_Q(x) = (0, 0, \dots)$
 $\Rightarrow x \in \ker \tilde{\Phi}_Q$

ii) $\ker \tilde{\Phi}_Q \subseteq Q^{*2}$. We take $x \in \ker \tilde{\Phi}_Q$
 $\Rightarrow x > 0$, if $x = \prod_{p \in P} p^{r_p}$, $r_p \in \mathbb{Z}$.
 with even $r_p \forall p$. $\Rightarrow x = \left(\prod_{p \in P} p^{\frac{r_p}{2}} \right)^2 \in Q^{*2}$

i) & ii) $\Rightarrow \ker \tilde{\Phi}_Q = Q^{*2}$

By the first isomorphism theorem \Rightarrow

□

Remark:

Then (first isomorphism thm)

If $\varphi: G \rightarrow G'$ is a group homomorphism, then

- 1) $\ker \varphi \trianglelefteq G$
- 2) $\text{Im } \varphi \leq G'$
- 3) $G / \ker \varphi \cong \text{Im } \varphi$

$K = \mathbb{F}_p, \mathbb{R}, \mathbb{Q}, \mathbb{Q}_{\neq p}$

$$\frac{K^*}{K^{*2}} = \{b \in K^* \mid b \in K^*\}$$

I. $K = \mathbb{F}_p$

II. $K = \mathbb{R}$

III. $K = \mathbb{Q}$

IV. $K = \mathbb{Q}_p, p \in \mathbb{P} \setminus \{2\}$,

V. $K = \mathbb{Q}_2$

VI. Then $(\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2, p \geq 3)$

If $p \in \mathbb{P} \setminus \{2\}$, then the map

$$\varphi_p: \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$u p^n \cdot \mathbb{Q}_p^* \mapsto (\log_{-1} \left(\frac{u}{p} \right), n - 2\pi) \text{ where } u \in \mathbb{Z}_p^*$$

$$\text{and } \left(\frac{u}{p} \right) = \left(\frac{a_0}{p} \right) \text{ if } u = a_0 + a_1 p + a_2 p^2 + \dots$$

In particular, for each $\varepsilon \in \mathbb{Z}_p^*$ with $(\frac{\varepsilon}{p}) = -1$, the set $\{1, \varepsilon, p, \varepsilon p\}$ is a system of representatives for $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$

Example

1) Is $x = 833$ a square in \mathbb{Q}_7 ? $x = 17 \cdot 7^2$

$$\tilde{\Phi}_7(17 \cdot 7^2) = (1, 0)$$

$$\begin{array}{c} u = 3 + 2 \cdot 7 \in \mathbb{Z}_7^* \\ \parallel \\ a_0 \quad a_1 \\ x_0 \end{array}$$

$$\left(\frac{17}{7} \right) = \left(\frac{3}{7} \right) = - \left(\frac{7}{3} \right) = - \left(\frac{1}{3} \right) = -1 \quad 833 \text{ is not a square in } \mathbb{Q}_7$$

2) $x = 15 \cdot 7^2 \rightarrow$ this is a square in \mathbb{Q}_7

Proof

Again first 4

$$\tilde{\Phi}_p: \mathbb{Q}_p^* \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$u p^n \mapsto (\log_{-1} \left(\frac{u}{p} \right), n+2\mathbb{Z})$$

a) well-defined

b) homomorphism \rightarrow epimorphism

c) surjective

$$p \mapsto (0, 1)$$

$$\varepsilon \mapsto (1, 0), \text{ where } \varepsilon \in \mathbb{Z}_{p, \mathbb{Z}}$$

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

d) calculate $\ker \tilde{\Phi}_p$.

(i) $\mathbb{Q}_p^{*2} \subseteq \ker \tilde{\Phi}_p$. Indeed for $x \in \mathbb{Q}_p^{*2}$ we can write it as $x = u^2 \cdot p^{2n}$, so $\tilde{\Phi}_p(u^2 \cdot p^{2n}) = (\log_{-1} \left(\frac{u^2}{p} \right), 0) = (0, 0)$

$$\Rightarrow x \in \ker \tilde{\Phi}_p$$

(ii) $\ker \tilde{\Phi}_p \subseteq \mathbb{Q}_p^{*2}$. Take $u p^n \in \ker \tilde{\Phi}_p$

$$\Rightarrow \tilde{\Phi}_p(u p^n) = (0, 0) \Rightarrow \underbrace{\left(\frac{u}{p} \right)}_{} = 1 \text{ and } 2|n$$

$$\Rightarrow u p^n \in \mathbb{Q}_p^{*2} \quad \text{is a square mod } p$$

$$(i) \& (ii) \Rightarrow \ker \tilde{\Phi}_p = \mathbb{Q}_p^{*2}$$

□

$$\text{IV. } K = \mathbb{Q}_2$$

$$U_n = (\mathbb{Z}/n\mathbb{Z})^*$$

$$U_8 = (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$$

Thm

If $p=2$, then the map

$$\Phi_2 : \frac{\mathbb{Q}_2^*}{\mathbb{Q}_2^{*2}} \rightarrow (\mathbb{Z}/8\mathbb{Z})^* \times \mathbb{Z}/2\mathbb{Z}$$

$$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$a \cdot 2^n \cdot \mathbb{Q}_2^{\times 2} \longrightarrow (a \bmod 8, n+2\mathbb{Z})$$

$$\{\pm 1, \pm 5, \pm 2, \pm 10\}$$

Thm (Hasse-Minkowski, Part 0).

The equation $x^2 = d$ [with $d \in \mathbb{Q}^*$] has a solution in $\mathbb{Q} \iff$ it has a solution in \mathbb{Q}_p^* for all $p \in \mathbb{P} \cup \{\infty\}$
 (as usual $\mathbb{Q}_{\infty}^* := \mathbb{R}$)

Proof \Rightarrow " $\mathbb{Q} \subset \mathbb{R}$ & $\mathbb{Q} \subset \mathbb{Q}_p^*$ $\forall p \in \mathbb{P}$.

\Leftarrow from theorems in parts II, III, IV, d is a square
 $\Rightarrow d \geq 0, 2 \mid v_p(d) \Rightarrow$ by thm in Part III.

$$\Phi_Q : \mathbb{Z}/2\mathbb{Z} \setminus \{0\} \rightarrow (\log_{-1}(\operatorname{sgn} d), (v_p(d) + 2\mathbb{Z})_{p \in \mathbb{P}})$$

$$Q(x, y, z) = 4x^2 - 3xy + 5y^2 + 5xz - 11yz + z^2$$

$$Q(x, y, z) = ax^2 + by^2 + cz^2 = 0 \quad x = 5x + 1$$

$$ax^2 + by^2 = z^2$$

Def

let $p \in \mathbb{P} \cup \{\infty\}$ and $a, b \in \mathbb{Q}_p^*$ ($\mathbb{Q}_\infty^* := \mathbb{R}$)

The Hilbert symbol

$$\left(\frac{a, b}{p}\right) := \begin{cases} 1, & \text{if } ax^2 + by^2 = z^2 \text{ has a non-trivial solution } (x, y, z) \in \mathbb{Q}_p^3 \\ -1, & \text{otherwise.} \end{cases}$$

Hilbert symbol

25.01.11

Def

let p be prime or $p = \infty$ and let $a, b \in \mathbb{Q}_p^*$

(here $\mathbb{Q}_\infty := \mathbb{R}$) Then the Hilbert symbol

$$\left(\frac{a, b}{p} \right) := \begin{cases} 1 & \text{if } ax^2 + by^2 = z^2 \text{ has a nontrivial } \neq (0,0,0) \\ & \text{solution } (x,y,z) \in \mathbb{Q}_p^3 \\ -1 & \text{otherwise} \end{cases}$$

Properties

$$1^\circ \quad \left(\frac{a, b}{p} \right) = \left(\frac{b, a}{p} \right)$$

2° - 5° Homework

$$5^\circ \quad \left(\frac{a \cdot b, a \cdot c}{p} \right) = \left(\frac{a, b, -bc}{p} \right), \quad a, b, c \in \mathbb{Q}_p^*$$

$$6^\circ \quad \text{If } \left(\frac{a, c}{p} \right) = 1, \text{ then } \left(\frac{a, b}{p} \right) = \left(\frac{a, bc}{p} \right)$$

Proof of 6°

Assume $\left(\frac{a, c}{p} \right) = 1$ Idea is to show that $\left(\frac{a, b}{p} \right) = 1 \iff \left(\frac{a, bc}{p} \right) = 1$

\Rightarrow so we assume that $\left(\frac{a, c}{p} \right) = \left(\frac{a, b}{c} \right) = 1$

This means that $\exists (0,0,0) \neq (x_1, y_1, z_1) \in (\mathbb{Q}_p)^3$ and

$(0,0,0) \neq (\tilde{x}, \tilde{y}, \tilde{z}) \in (\mathbb{Q}_p)^3$ so that $ax^2 + cy^2 = z^2$ (1) and

$$a\tilde{x}^2 + b\tilde{y}^2 = \tilde{z}^2. \quad (2)$$

$$\boxed{ax^2 + bcy^2 = z^2 \quad (3)}$$

If $y=0$ then the solution (x, y, z) of (1) is also a solution of (3).

If $\tilde{y}=0$ then $(\tilde{x}, \tilde{y}, \tilde{z})$ is a solution of both (2) & (3)

So we consider $y \neq 0, \tilde{y} \neq 0$. WLOG we assume that

$$y = \tilde{y} = 1.$$

$a\left(\frac{x}{y}\right)^2 + c \cdot 1^2 = \left(\frac{z}{y}\right)^2$, (x, y, z) is a solution of (1) $\Leftrightarrow \left(\frac{x}{y}, \frac{z}{y}\right) \dots$

$(x, 1, z)$ or $(z, 1, x)$ \Rightarrow (1) & (2) resp.

Then

$$c = z^2 - ax^2, \quad b = \tilde{z}^2 - a\tilde{x}^2$$

FOIC (First outside, inside last)

$$\begin{aligned} bc &= (\tilde{z}^2 - ax^2)(\tilde{z}^2 - a\tilde{x}^2) & Q_p(\sqrt{a}) &= Q_p + Q_p \cdot \sqrt{a} \\ &= (\tilde{z} - \sqrt{a}x)(\tilde{z} + \sqrt{a}x)(z - \sqrt{a}x)(z + \sqrt{a}x) \\ &= ((\tilde{z} \cdot z + a\tilde{x}x) - \sqrt{a}(\tilde{z}x + \tilde{x}z)) \cdot ((\tilde{z} \cdot z + a\tilde{x}x) + \sqrt{a}(\tilde{z}x + \tilde{x}z)) \\ b_c &= (\tilde{z}z + a\tilde{x}x)^2 - a(\tilde{z}x + \tilde{x}z)^2 \end{aligned}$$

So, we have found that $(\tilde{z}x + \tilde{x}z, 1, \tilde{z}z + a\tilde{x}x)$ is a nontrivial solution to (3), and therefore $\left(\frac{a, bc}{p}\right) = 1$.

(2), \Leftarrow Now we start with the assumption

$$\left(\frac{a, c}{p}\right) = \left(\frac{a, bc}{p}\right) = 1. \quad \text{Then}$$

$$\left(\frac{a, b}{p}\right) \stackrel{\substack{4^0 \\ (1) \\ \text{(HK)}}}{=} \left(\frac{a, b \cdot c^2}{p}\right) = \left(\frac{a, (bc)c}{p}\right) \stackrel{(1)}{=} 1$$

Thm (Calculation of the H.s. in Q_p for p an odd prime.)

Let p be an odd prime. Then

$$\Rightarrow \left(\frac{u \cdot p^n, v \cdot p^m}{p}\right) = (-1)^{n \cdot m \cdot \frac{p-1}{2}} \cdot \left(\frac{u}{p}\right)^m \cdot \left(\frac{v}{p}\right)^n, \text{ where } u, v \in \mathbb{Z}_p^* \text{ and } n, m \in \mathbb{Z}$$

In particular

$$i) \quad \left(\frac{u, v}{p} \right) = 1$$

$$ii) \quad \left(\frac{u, vp}{p} \right) = \left(\frac{vp, u}{p} \right) = \left(\frac{u}{p} \right)$$

$$iii) \quad \left(\frac{up, vp}{p} \right) = \left(\frac{-uv}{p} \right) \quad \left\{ = (-1)^{\frac{p-1}{2}} \left(\frac{u}{p} \right) \cdot \left(\frac{v}{p} \right) = \left(\frac{-1}{p} \frac{u \cdot v}{p} \right)$$

Proof

We prove only i), ii) and iii)

i) We must prove that $\left(\frac{u, v}{p} \right) = 1$, that is, that $ux^2 + vy^2 = z^2$ has a nontrivial solution.

I claim that there is a solution (x, y, z) with $x, y \in \mathbb{Q}_p$. To see this, I start with thinking about \mathbb{F}_p .

$$\mathcal{M}_1 = \{ ux^2 + v \pmod{p} \mid x \in \mathbb{F}_p \} \subseteq \mathbb{F}_p,$$

$$\#\mathcal{M}_1 = \frac{p+1}{2}$$

$$\mathcal{M}_2 = \{ \tilde{z}^2 \pmod{p} \mid \tilde{z} \in \mathbb{F}_p \} \subseteq \mathbb{F}_p,$$

$$\#\mathcal{M}_2 = \frac{p+1}{2}$$

$$\mathcal{M}_1 \cap \mathcal{M}_2 \neq \emptyset$$

$\exists \tilde{x} \in \mathbb{F}_p$ and $\tilde{z} \in \mathbb{F}_p$ so that $u \cdot \tilde{x}^2 + v \cdot 1^2 = \tilde{z}^2$

for example
 Let $\tilde{z}_0 = \tilde{z} + \sum_{n=1}^{\infty} 0 \cdot p^n \in \mathbb{Z}_p \quad \mathbb{Z}_p \subset \mathbb{Q}_p$

At least one of \tilde{z} or \tilde{x} is nonzero.

Otherwise we would have $0 \cdot 1^2 = 0 \pmod{p} \Rightarrow v = 0 \pmod{p}$

WLOG assume that $\tilde{x} \neq 0$

$\therefore (v \in \mathbb{Z}_p^*)$

Consider

$$p(x) = ux^2 + v - z_0^2$$

We know that

$$p(\tilde{x}) \equiv 0 \pmod{p},$$

$$p'(\tilde{x}) = 2ux \not\equiv 0 \pmod{p}$$

By Hensel's Lemma $\Rightarrow \exists! x \in \mathbb{Z}_p$ s.t. $p(x) = 0$ and $x \equiv \tilde{x} \pmod{p}$

Therefore, $\exists (x, y, z)^1 \neq (0, 0, 0)$

$$\text{with } ux^2 + vy^2 = z^2.$$

Thm.

Let p be an odd prime, then

$$\left(\frac{up^nvp^n}{p} \right) = (-1)^{n \cdot m \cdot \frac{p-1}{2}} \cdot \left(\frac{u}{p} \right)^m \cdot \left(\frac{v}{p} \right)^n, u, v \in \mathbb{Z}_p^*, n, m \in \mathbb{Z}$$

$$\Leftrightarrow (i) \quad \left(\frac{u, vp}{p} \right) = 1$$

$$(ii) \quad \left(\frac{u, vp}{p} \right) = \left(\frac{u}{p} \right)$$

$$(iii) \quad \left(\frac{up, vp}{p} \right) = \left(\frac{-uv}{p} \right)$$

$$\left(\frac{u, vp^2}{p} \right) = \left(\frac{u, v}{p} \right) = 1$$

Proof

$$(ii) \quad \text{We will show } \left(\frac{u, vp}{p} \right) = 1 \Leftrightarrow \left(\frac{u}{p} \right) = 1$$

\Rightarrow Assume that $\left(\frac{u, vp}{p} \right) = 1 \Rightarrow ux^2 + vp^2y^2 = z^2$ has a nontrivial solution $(x, y, z) \in \mathbb{Q}_p^3 \setminus \{(0, 0, 0)\}$, so that

$(p^n x, p^n y, p^n z) \in \mathbb{Z}_p^3$, moreover at least one of three $p^n x, p^n y$ or $p^n z$ is in \mathbb{Z}_p^* . I denote this new solution again by $(x, y, z) \in (\mathbb{Z}_p)^3$ and one of $x, y, z \in \mathbb{Z}_p^*$

I claim that $x \in \mathbb{Z}_p^*$. If not, then $x \in p \cdot \mathbb{Z}_p$, that is

$$p|x \Rightarrow p^2|x^2 \Rightarrow p|ux^2 + vp^2y^2$$

$$\Rightarrow p|z^2 \quad \boxed{\Rightarrow p|z \Rightarrow p|u \cdot x^2 (= z^2 - vp^2y^2)}$$

$$p^2 | vp^2y^2 (= z^2 - ux^2) \Rightarrow p|v \cdot y^2 \Rightarrow p|y \quad \boxed{y}$$

So $x \in \mathbb{Z}_p^*$ and since $ux^2 = z^2 - vp^2y^2$,

we have $p|z \Rightarrow z \in \mathbb{Z}_p^*$

$$\text{we have } ux^2 \equiv z^2 \pmod{p} \Rightarrow u \equiv \left(\frac{z}{x} \right)^2 \pmod{p}$$

$$\Rightarrow u \text{ is a QR mod } p \Rightarrow \left(\frac{u}{p} \right) = 1$$

\Leftarrow Assume $(\frac{u}{p}) = 1 \Rightarrow u \text{ is a QR mod } p \Rightarrow u = (\tilde{z})^2 \text{ mod } p, \tilde{z} \in \mathbb{F}_p^*$

By Hensel's Lemma, $u = z^2$ has a solution in \mathbb{Z}_p ,
if $\exists \tilde{z}$ $\tilde{z}^2 - u \equiv 0 \pmod{p}$ and $2\tilde{z} \not\equiv 0 \pmod{p}$
 $\Rightarrow \exists z \in \mathbb{Z}_p$ so that $u = z^2$.

With the found z , (x_1, z) is a nontrivial solution
to $ux^2 + vpy^2 = z^2$.

$$(iii) \quad \left(\frac{u_p, v_p}{p} \right) \stackrel{5^0}{=} \left(\frac{u_p, -uv}{p} \right) \stackrel{10^0}{=} \left(\frac{-uv, u_p}{p} \right) \stackrel{(ii)}{=} \left(\frac{-uv}{p} \right)$$

Exercise Which of the following equations has a nontrivial
solutions $\neq 0$ in \mathbb{Q} ?

$$i) 3x^2 + 5y^2 = 7z^2$$

$$ii) 5x^2 + 7y^2 = 3z^2$$

$$iii) 7x^2 + 3y^2 = 5z^2$$

Thm

$$p=2, \quad \mathbb{Q}_2$$

$$\left(\frac{u \cdot 2^n, v \cdot 2^m}{2} \right) = (-1)^{\frac{u-1}{2} \cdot \frac{v-1}{2}} \cdot (-1)^{\frac{n \cdot v^2 - 1}{8}} \cdot (-1)^{\frac{m \cdot u^2 - 1}{8}}, \text{ where}$$

$$\frac{u-1}{2}, \frac{v-1}{2}, \frac{v^2-1}{8}, \frac{u^2-1}{8} \text{ are taken mod 2.}$$

$$\boxed{u = u_0 + 2(\dots)}$$

$$\boxed{\frac{u-1}{2} = (a_1 + 2a_2 + \dots)}$$

Idea of proof

Since the H.s. depends only on cosets $\mathbb{Q}_2/\mathbb{Q}_2^{*2}$ and we know $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ is the system of representatives we can calculate it for all 64 pairs.

For ex.,

$$\left(\frac{-1, 5}{2}\right) = 1 \quad -1x^2 + 5y^2 = z^2 \quad (-1, 1, 1)$$

$$\left(\frac{5, 5}{2}\right) = \begin{matrix} \text{properties} \\ \text{and} \end{matrix} \nearrow = \text{exercise} = 1$$

$$\left(\frac{-1, -1}{2}\right) = -1 \Rightarrow \left(\begin{array}{c} \quad \\ +1 \end{array} \right) = -1$$

Thm

The H.s. $f_p(a, b) = \left(\frac{a, b}{p}\right)$ is bimultikative,

that is

$$f_p(a, bc) = f_p(a, b) \cdot f_p(a, c)$$

$$f_p(ax+by) = a f_p(x) + b f_p(y)$$

$$f(x)$$

$$f(x \cdot y) = f(x) \cdot f(y)$$

Thm

For $a, b \in \mathbb{Q}^*$

$\{Q \subset \mathbb{Q}_p \mid p \in P \cup \{\infty\}\}$

$$\prod_{p \in P \cup \{\infty\}} \left(\frac{a, b}{p}\right) = 1$$

Thm (Hausse-Minkowski, Part 1)

The equation $ax^2 + by^2 = z^2$ with $a, b \in \mathbb{Q}^*$ has a nontrivial solution $(x, y, z) \in \mathbb{Q}^3 \Leftrightarrow$ there are nontrivial solutions of it in $(\mathbb{Q}_p)^3 \mid p \in P \cup \{\infty\}$

Number Theory

Wiederholung

field (+, ·)

Euclidean domain

Principal ideal domain

unique factorization domain

integral domain

ring (+, ·)

irreducible but not prime \Rightarrow not a unique factorization domain

Euclidean domain \Rightarrow principal ideal domain

II Congruences (linear)

$$ax \equiv b \pmod{n}$$

~~gcd d | b~~ \rightarrow has d solutions

Chinese remainder theorem

III φ -function

$$\varphi(n) = \#\left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

format: $a \not\equiv 0 \pmod{p}$:

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

Faul's Theorem:

$$a^{\frac{\phi(n)}{\text{gcd}(a,n)}} \equiv 1 \pmod{n} \quad \text{if } \text{gcd}(a,n)=1$$

$$\frac{41}{1} \stackrel{3}{\overline{2010}} \equiv ? \pmod{100}$$

$$\frac{3}{1} \stackrel{3}{\overline{2010}} \equiv ? \pmod{\varphi(100)}$$

III The structure of \mathbb{Z}_n and \mathbb{Z}_n^*

When is \mathbb{Z}_n^* cyclic? (if n prime)

generator \Leftrightarrow primitive root mod n

γ is a generator of $(\mathbb{Z}/q\mathbb{Z})^*$

$\gamma^h, \quad 1 < h < \phi(q-1) \text{ and } \gcd(h, \phi(q-1)) = 1$

$$\gamma^1, \gamma^2, \dots, \gamma^{q-1} = 1$$

not a generator, $\gcd(\gamma^2, q-1) \neq 1$

Theorems for $\gamma \rightarrow \gamma^2 \rightarrow \gamma^4 \dots$

generators in groups with higher exponent

IV Quadratic residue

a is a quadratic residue modulo p

$\Leftrightarrow a \neq 0$ and \exists a solution to

$$x^2 \equiv a \pmod{p}$$

Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a qr} \\ -1 & a \text{ is not a qr (nonresidue)} \\ 0 & \text{if } a \text{ is divisible by } p \end{cases}$$

Jacobi symbol (b not prime)

$$\left(\frac{a}{b}\right) = \prod_{j=1}^h \left(\frac{a}{p_j}\right)^{e_j}$$

$b = p_1^{e_1} \cdots p_h^{e_h}$ prime factorization, $p \geq 3$ (odd b)

~~Reversible~~

Caution:

$\left(\frac{a}{b}\right) = 1$, then it may happen that a is a nonresidue modulo b. (or a residue)

$$\begin{cases} x \equiv 13 \pmod{15} \\ x \equiv 10 \pmod{21} \\ x \equiv 3 \pmod{35} \end{cases}$$

1. Consider only two congruences

$$\begin{cases} x \equiv 13 \pmod{15} \\ x \equiv 10 \pmod{21} \end{cases}$$

See whether $13 \equiv 10 \pmod{\text{gcd}(15, 21)}$

EFA:

$$21 = 1 \cdot 15 + 6$$

$$15 = 2 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

$$\Rightarrow 3 = 15 - 2 \cdot 6$$

$$13 - 10 - 3 = -2 \cdot 21 + 3 \cdot 15$$

$$\Rightarrow 13 - 3 \cdot 15 = 10 + 2 \cdot 21 = X$$

x is unique mod $\frac{15 \cdot 21}{\text{gcd}(15, 21)}$

$$X = -32 \not\equiv 105 = 73 \pmod{105}$$

Change 2 Equations:

$$\begin{cases} x \equiv 73 \pmod{105} \\ x \equiv 3 \pmod{35} \end{cases}$$

Another way: Introduce new variables:

$$x - 13 \equiv 0 \pmod{15} \quad \text{denote } x - 13 = 3y$$

$$3y \equiv 0 \pmod{15} \quad \sim$$

$$y \equiv 0 \pmod{5}$$

Introduction to Algebraic Number Theory

WS 2010/11

Practice Final Examination, Part I

WARNING: These practice problems are intended to give you a flavor of the kinds of questions I will ask and the kinds of things I expect you to be able to do. The actual questions on the final exam may or may not actually look like this.

Before you try the problems below, I strongly recommend that you read all relevant topics we have considered in the course.

1. Give a definition of principal ideal domain. Is $\mathbb{Z}[\sqrt{-5}]$ a principal ideal domain? Is $\mathbb{Z}\left[\frac{1 + \sqrt{-5}}{2}\right]$ a principal ideal domain?
2. A group of 15 bandits steal a pile of gold coins. When they try to divide the coins into equal parts, there are 9 left over. They fight over the extra coins, and one bandit is killed. They try to divide the coins equally again, and there are now 5 left over. They fight again and another bandit is killed. When they divide the coins equally again, there are none left over. What are the different possible numbers of coins that there could be?
3. Let φ be the Euler phi function.
 - (a) What does the number $\varphi(n)$ represent?
 - (b) Find all integers n such that $\varphi(n) = n/2$.
 - (c) For each integer $k > 2$, find all integers n such that $\varphi(n) = n/k$.
4. Find the last two digits of the number $7^{3^{2010}}$.
5. It is known that $n = 229783171$ is the product of two distinct primes and that its Euler phi function $\varphi(n) = 229752712$. What is the factorization of n ?
6. Find all solutions to the following congruences or explain why no solution exist:
 - (a) $x^2 \equiv 31 \pmod{55}$
 - (b) $x^2 \equiv 51 \pmod{143}$
 - (c) $x^2 \equiv 143 \pmod{51}$

*Cirr. falls west
d~comi*
7. The prime $p = 71$ has 7 as a primitive root. Find *all* primitive roots modulo 71 and also find a primitive root modulo 71^2 and modulo 71^3 .

Introduction to Algebraic Number Theory

WS 2010/11

Practice Final Examination, Part I

WARNING: These practice problems are intended to give you a flavor of the kinds of questions I will ask and the kinds of things I expect you to be able to do. The actual questions on the final exam may or may not actually look like this.

Before you try the problems below, I strongly recommend that you read all relevant topics we have considered in the course.

1. Give a definition of principal ideal domain. Is $\mathbb{Z}[\sqrt{-5}]$ a principal ideal domain? Is $\mathbb{Z}\left[\frac{1+\sqrt{-5}}{2}\right]$ a principal ideal domain?
2. A group of 15 bandits steal a pile of gold coins. When they try to divide the coins into equal parts, there are 9 left over. They fight over the extra coins, and one bandit is killed. They try to divide the coins equally again, and there are now 5 left over. They fight again and another bandit is killed. When they divide the coins equally again, there are none left over. What are the different possible numbers of coins that there could be?
3. Let φ be the Euler phi function.
 - (a) What does the number $\varphi(n)$ represent?
 - (b) Find all integers n such that $\varphi(n) = n/2$.
 - (c) For each integer $k > 2$, find all integers n such that $\varphi(n) = n/k$.
4. Find the last two digits of the number $7^{3^{2010}}$.
5. It is known that $n = 229783171$ is the product of two distinct primes and that its Euler phi function $\varphi(n) = 229752712$. What is the factorization of n ?
6. Find all solutions to the following congruences or explain why no solution exist:
 - (a) $x^2 \equiv 31 \pmod{55}$
 - (b) $x^2 \equiv 51 \pmod{143}$ *no solution*
 - (c) $x^2 \equiv 143 \pmod{51}$ *no " "*
7. The prime $p = 71$ has 7 as a primitive root. Find *all* primitive roots modulo 71 and also find a primitive root modulo 71^2 and modulo 71^3 .

Introduction to Algebraic Number Theory

WS 2010/11

Practice Final Examination, Part II

WARNING: These practice problems are intended to give you a flavor of the kinds of questions I will ask and the kinds of things I expect you to be able to do. The actual questions on the final exam may or may not actually look like this.

In the following problems we denote by \mathbb{Q}_p p -adic numbers and by \mathbb{Z}_p p -adic integers. Before you try these problems, I strongly recommend that you read all relevant topics we have considered in the course.

1. Which of the rational numbers $1, -2, 5, 1/3, 4/15$ belong to:

(a) \mathbb{Z}_5 ? (b) \mathbb{Z}_5^* ? (c) \mathbb{Q}_5^* ? Explain.

For each number you have found in (a), give its 5-adic expansion.

2. Give an example of a number in $\mathbb{Q}_7 \setminus \mathbb{Q}$. Explain why the number belongs to this set.
3. Determine the set of all primes p for which $5/9$ is a square in \mathbb{Q}_p .
4. Let $f \in \mathbb{Z}_5[x]$ be defined by $f(x) = x^2 - 5x - 1$. How many roots does f have in \mathbb{Z}_5 ? Find the values of all these roots modulo 5^4 .
5. Let the sequence $\{x_n\}_{n=1}^\infty$ be defined as follows:

$$x_n = \begin{cases} \frac{(-1)^n}{n} & \text{if } n \equiv 1 \pmod{3} \\ 5n - 13 & \text{if } n \equiv 2 \pmod{3} \\ n^2 + 11 & \text{if } n \equiv 0 \pmod{3} \end{cases}$$

Find (with proof!) at least one subsequence of $\{x_n\}_{n=1}^\infty$ which is a Cauchy sequence with respect to the 7-adic norm $| \cdot |_7$.

6. Two of the following equations have only the trivial solution $(x, y, z) = (0, 0, 0)$ in \mathbb{Z}^3 :

$$3x^2 + 5y^2 = 7z^2, \quad 5x^2 + 7y^2 = 3z^2, \quad 7x^2 + 3y^2 = 5z^2.$$

Prove that this is really the case and find a nontrivial solution of the third equation.

Theorem of a number is a square

NT

PFE I

$$6^{\circ} \quad \text{a) } x^2 \equiv 31 \pmod{55}$$

$$x^2 = 31 + k \cdot 55 = 31 + (11k) \cdot 5$$

$$\begin{array}{l} \xrightarrow{\text{and}} x^2 \equiv 31 \pmod{5} \\ \xrightarrow{\text{and}} x^2 \equiv 31 \pmod{11} \end{array} \quad \begin{array}{l} \xrightarrow{\text{Chinese}} \\ \xrightarrow{\text{Pellonize}} \\ \xrightarrow{\text{Then}} \end{array} \quad x^2 \equiv 31 \pmod{55}$$

$$\begin{cases} x \equiv c \pmod{5} \\ x \equiv d \pmod{11} \end{cases}$$

$$1) \quad c^2 \equiv 31 \pmod{5} \quad \Rightarrow \quad c^2 \equiv 1 \pmod{5}$$

$$\left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = -1 \quad c_1 \equiv 1 \pmod{5}$$

$$c_2 \equiv -1 \pmod{5} \quad = 4 \pmod{5}$$

$$2) \quad d^2 \equiv 31 \pmod{11}$$

$$\text{Legendre's symbol} \quad \left(\frac{31}{11}\right) = \left(\frac{9}{11}\right) = -1 \quad \Rightarrow \quad d^2 \equiv 9 \pmod{11}$$

$$d_1 \equiv 3 \pmod{11}$$

$$d_2 \equiv -3 \pmod{11} = 8 \pmod{11}$$

Four solutions

One of them:

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{11} \end{cases}$$

$$x = 1 + 5k$$

$$1 + 5k \equiv 3 \pmod{11}$$

$$5k - 2 \equiv 0 \pmod{11} \quad \Rightarrow \quad k = 7$$

$$x = 1 + 5 \cdot 7 = 36$$

Chech: $(36^2 - 31) \div 55$

In general

$$\left(\frac{31}{55}\right) = \left(\frac{31}{5}\right) \cdot \left(\frac{31}{11}\right) \quad (= -1)$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$\xrightarrow{-1 \Rightarrow \text{Step}}$

10 Solutions

Part II

$$\text{Q}^0 \quad 3x^2 + 5y^2 = 7z^2 \quad \text{nontrivial solution in } \mathbb{Z}$$

Thm (Hausse-Matkowski, Part I)

$a x^2 + b y^2 = z^2$, where $a, b \in \mathbb{Q}^*$, has a solution $(x, y, z) \in \mathbb{Q}^3$

\Leftrightarrow it has a nontrivial solution in all $(\mathbb{Q}_p)^3$, $p \in \mathbb{P} \cup \{\infty\}$.

$$1) \frac{3}{7} \cdot x^2 + \frac{5}{7} \cdot y^2 = z^2 \Rightarrow \frac{3 \cdot 7}{7^2} \cdot x^2 + \frac{5 \cdot 7}{7^2} \cdot y^2 = z^2$$

$$\left(\frac{21, 35}{p} \right) = \left(\frac{21 \cdot \left(\frac{1}{7}\right)^2, 35 \cdot \left(\frac{1}{7}\right)^2}{p} \right)$$

$$2) 3 \cdot 7 x^2 + 5 \cdot 7 y^2 = (7z)^2$$

1) or 2) we need to know

$$\left(\frac{21, 35}{p} \right) \quad \forall p \in \mathbb{P} \cup \{\infty\}$$

Thm p an odd prime $u, v \in \mathbb{Z}_p^*$

$$\left(\frac{u, v}{p} \right) = 1 \quad \left(\frac{u, vp}{p} \right) = \left(\frac{u}{p} \right) \quad \boxed{1}$$

$$21 = a_0 + a_1 p + a_2 p^2 + \dots$$

$\frac{1}{p}$

If $p \mid 21 \Rightarrow a_0 = 0$ and 21 is not a unit in this case.

For $p \neq$ an odd prime, both 21 and 35 are units

Therefore for $p \neq$ $\left(\frac{21, 35}{p} \right) = 1$, that is, equation 1)
has a nontrivial solution in $(\mathbb{Q}_p)^3$ for such p

$$p=3 \quad \left(\frac{21, 35}{3} \right) = \left(\frac{73, 35}{3} \right) = \left(\frac{35}{3} \right) = \left(\frac{2}{3} \right) = -1$$

Stop! no solutions.

Hensel Lemma

If $f \in \mathbb{Z}_p[x]$ and $\tilde{x} \in \mathbb{Z}_p$ so that $f(\tilde{x}) \equiv 0 \pmod{p^2}$ but $f'(\tilde{x}) \not\equiv 0 \pmod{p}$

\Rightarrow If solution x to $f(x) = 0$ in \mathbb{Z}_p so that $x \equiv \tilde{x} \pmod{p}$

Aufg 4

$$f(x) = x^2 - 5x - 1$$

$$x^2 \equiv 1 \pmod{5}$$

$$x \equiv 1 \text{ or } 4 \pmod{5}$$

$$f'(x) = 2x - 5 \equiv 2x \pmod{5}$$

$$x = a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + a_3 \cdot 5^3 + \dots : x^2 - 5x - 1 \equiv 0 \quad x \equiv 1 \pmod{5}$$

$$x_0 = 1 \Rightarrow x = 1 + a_1 \cdot 5 \pmod{5^2}$$

$$(1 + a_1 \cdot 5)^2 - 5 \cdot (1 + a_1 \cdot 5) - 1 \equiv 0 \pmod{5^2}$$

$$1 + 10a_1 - 5 - 1 \equiv 0 \pmod{5^2}$$

$$10a_1 - 5 \equiv 0 \pmod{5^2}$$

$$2a_1 - 1 \equiv 0 \pmod{5}$$

$$a_1 = 3, \quad a_0 = 1$$

$$x \equiv 1 + 3 \cdot 5 + a_2 \cdot 5^2 \pmod{5^3}$$

$$x \equiv 16 + a_2 \cdot 5^2 \pmod{5^3}$$

Introduction to Algebraic Number Theory

WS 2010/11

Practice Final Examination, Part I

WARNING: This practice problems are intended to give you a flavor of the kinds of questions I will ask and the kinds of things I expect you to be able to do. The actual questions on the final exam may or may not actually look like this.

Before you try the problems below, I strongly recommend that you read all relevant topics we have considered in the course.

1. Give a definition of principal ideal domain. Is $\mathbb{Z}[\sqrt{-5}]$ a principal ideal domain? Is $\mathbb{Z}\left[\frac{1+\sqrt{-5}}{2}\right]$ a principal ideal domain?
2. A group of 15 bandits steal a pile of gold coins. When they try to divide the coins into equal parts, there are 9 left over. They fight over the extra coins, and one bandit is killed. They try to divide the coins equally again, and there are now 5 left over. They fight again and another bandit is killed. When they divide the coins equally again, there are none left over. What are the different possible numbers of coins that there could be?
3. Let φ be the Euler phi function.
 - (a) What does the number $\varphi(n)$ represent?
 - (b) Find all integers n such that $\varphi(n) = n/2$.
 - (c) For each integer $k > 2$, find all integers n such that $\varphi(n) = n/k$.
4. Find the last two digits of the number $7^{3^{2010}}$.
5. It is known that $n = 229783171$ is the product of two distinct primes and that its Euler phi function $\varphi(n) = 229752712$. What is the factorization of n ?
6. Find all solutions to the following congruences or explain why no solution exist:
 - (a) $x^2 \equiv 31 \pmod{55}$
 - (b) $x^2 \equiv 51 \pmod{143}$
 - (c) $x^2 \equiv 143 \pmod{51}$
7. The prime $p = 71$ has 7 as a primitive root. Find *all* primitive roots modulo 71 and also find a primitive root modulo 71^2 and modulo 71^3 .

Introduction to Algebraic Number Theory

WS 2010/11

Practice Final Examination, Part II

WARNING: This practice problems are intended to give you a flavor of the kinds of questions I will ask and the kinds of things I expect you to be able to do. The actual questions on the final exam may or may not actually look like this.

In the following problems we denote by \mathbb{Q}_p p -adic numbers and by \mathbb{Z}_p p -adic integers. Before you try these problems, I strongly recommend that you read all relevant topics we have considered in the course.

- Which of the rational numbers $1, -2, 5, 1/3, 4/15$ belong to:

$$(a) \mathbb{Z}_5 ? \quad (b) \mathbb{Z}_5^* ? \quad (c) \mathbb{Q}_5^* ? \quad \text{Explain.}$$

For each number you have found in (a), give its 5-adic expansion.

- Give an example of a number in $\mathbb{Q}_7 \setminus \mathbb{Q}$. Explain why the number belongs to this set.
- Determine the set of all primes p for which $5/9$ is a square in \mathbb{Q}_p .
- Let $f \in \mathbb{Z}_5[x]$ is defined by $f(x) = x^2 - 5x - 1$. How many roots does f have in \mathbb{Z}_5 ? Find the values of all these roots modulo 5^4 .
- Let the sequence $\{x_n\}_{n=1}^\infty$ be defined as follows:

$$x_n = \begin{cases} \frac{(-1)^n}{n} & \text{if } n \equiv 1 \pmod{3} \\ 5n - 13 & \text{if } n \equiv 2 \pmod{3} \\ n^2 + 11 & \text{if } n \equiv 0 \pmod{3} \end{cases}$$

Find (with proof!) at least one subsequence of $\{x_n\}_{n=1}^\infty$ which is a Cauchy sequence with respect to the 7-adic norm $| \cdot |_7$.

- Two of the following equations have only the trivial solution $(x, y, z) = (0, 0, 0)$ in \mathbb{Z}^3 :

$$3x^2 + 5y^2 = 7z^2, \quad 5x^2 + 7y^2 = 3z^2, \quad 7x^2 + 3y^2 = 5z^2.$$

Prove that this is really the case and find a nontrivial solution of the third equation.