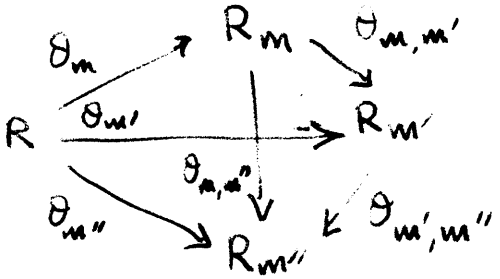
p-ADIC NUMBERS

Paul Taylor.

1. Consider the positive integers written base p, ie
$$n = a_m p^m + a_{m-1} p^{m-1} + \ldots + a_0 p + a_0$$
where $a_r \in \{0,1,2,\ldots,p-1\}$ for $r = 0,1,\ldots,m$. What is the algorithm for adding or multiplying two such numbers, in terms of (a_r)?
2. Suppose you were to consistently ignore the (coefficients of) powers of p from p^m upwards. Does it matter whether you curtail the sequence before or after adding (or multiplying)? If you curtail to m places and then add and then curtail to m' ($\leq m$), does it matter what the value of m is?
3. Show that the addition and multiplication with curtailment to m places gives a ring [addition forms an abelian group with identity "0" and inverse "$-$"; multiplication is associative and has identity "1"; multiplication distributes over addition from both sides] and that this is just the ring of integers modulo p^m. Call this ring R_m.
4. Show that curtailment from m to m' places ($m' \leq m$) gives a ring homomorphism [preserves addition, multiplication, 0, $-$ and 1] $\theta_{m,m'} : R_m \to R_{m'}$. What is its kernel [inverse image of 0]?
5. Suppose we now allow infinite sequences. How do you define addition and multiplication for these? How are negative integers represented? Show that we have a ring, R.
6. Show that curtailment to m places gives a ring homomorphism $\theta_m : R \to R_m$. Also, show that for $m \geq m' \geq m''$ the following diagram commutes [any ~~two~~ two routes between given points yield the same map]:



7. Now let S be any ring and let $(\phi_m)_{m=0}^{\infty}$ be a collection of ring homomorphisms $\phi_m : S \to R_m$ such that the above diagram (with R, θ_m replaced by

S, φ_m) commutes. Show that there is a unique ring homomorphism $\varphi: S \to R$ such that the obvious diagram with both S and R in it also commutes.

8. Let $(a_m), (b_m)$ be two elements of R. Define the distance $d((a_m),(b_m))$ between them to be $\inf\{p^r : a_m = b_m \text{ for } 0 \le m \le r\}$. Show that this is a metric, ie $d(\underline{a},\underline{b}) \ge 0$, $d(\underline{a},\underline{b}) = d(\underline{b},\underline{a})$, $d(\underline{a},\underline{c}) \le d(\underline{a},\underline{b}) + d(\underline{b},\underline{c})$ and $d(\underline{a},\underline{b}) = 0 \Leftrightarrow \underline{a} = \underline{b}$.

9. Show that $d(\underline{a},\underline{b}) = d(\underline{a}+\underline{c}, \underline{b}+\underline{c})$ and ~~$d(\underline{a},\underline{b}) = d(\underline{c},\underline{0}) d($~~ $d(\underline{a}\underline{c}, \underline{b}\underline{c}) = d(\underline{a},\underline{b}) d(\underline{c},\underline{0})$. Hence show that $+, -$ and $*$ are continuous with respect to this metric; show that the same is true of $\theta_{m,m'}$ and θ_m.

10. Hence show that R is an integral domain, ie $\underline{a}\underline{b} = 0 \Rightarrow$ either $\underline{a} = 0$ or $\underline{b} = 0$.

11. Show that $\underline{a}$ is invertible iff $d(\underline{a},\underline{0}) = 1$. With $p = 2$, what is the value of $1 + 2 + 4 + 8 + 16 + \ldots$?

12. Let $(\underline{a}_i)$ be a Cauchy sequence in R, so $d(\underline{a}_i, \underline{a}_j) < \varepsilon$ if $i \ge j \ge n(\varepsilon)$. Show that $\underline{a}_i \to \underline{a} \in R$ for some $\underline{a}$ [hint: apply θ_m].

13. Show that $\mathbb{Z}$ is dense in R, ie given $\underline{a} \in R$ and $\varepsilon > 0$ there's some $n \in \mathbb{Z}$ with $d(n, \underline{a}) < \varepsilon$. R is called the (metric space) completion of $\mathbb{Z}$.

14. How do you represent the field of fractions of R? R is usually called $\mathbb{Z}_{(p)}$ and its field of fractions $\mathbb{Q}_p$.

FINITE FIELDS.

A field is a set, K, with operations $+$ $*$ and special elements $0,1 \in K$ $(0 \neq 1)$ s.t. $(K,+,0)$ is an Abelian group, $(K^*,*,1)$ is a (commutative) group, where $K^* = K \setminus \{0\}$ and $*$ distributes over $+$ (ie $a*(b+c) = a*b+a*c$).
A field homomorphism is a map preserving $0,1,+,*,-,^{-1}$.
A field has characteristic zero if $0,1,2 \equiv 1+1, 3 \equiv 1+1+1, 4, 5, \ldots$ are distinct; it has characteristic p if $p \equiv 1+1+\cdots+1$ (p times) $= 0$ and p is the smallest positive integer for which this is so.

1. Show that any field homomorphism is injective
2. [Difficult] Let $\theta : K \to L$ be a field hom. s.t. whenever $\varphi, \psi : L \to M$ are field. homs. s.t. $\varphi \cdot \theta = \psi \cdot \theta : K \to M$ then $\varphi = \psi$ are equal. Is it true that θ is always surjective?
3. (i) Show that the characteristic of a field is either zero or a prime (ii) Show that there is no hom. between fields of different char. (iii) Show that every field has a unique subfield isomorphic to $\mathbb{Q}$ or $\mathbb{F}_p$, where $\mathbb{F}_p$ is the set $\{0,1,\ldots,p-1\}$ under addition and multiplication modulo p. this is the prime subfield (iv) Show that the characteristic of a finite field is nonzero.
4. Show that an equation of the form
$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$
with coeffs. in K has at most n solutions in K.
5. (i) Let K be a field and F a subfield. Show how to make K into a vector-space over F. (ii) Hence show that if K is finite it has p^n elements with p prime and n an integer. (iii) Find an example with $n \geq 2$.
6. Let K be a field of characteristic p. (i) Show that $\varphi : x \mapsto x^p$ is an endomorphism of K and (ii) that this is an automorphism for K finite, the Frobenius automorphism (iii) Hence show that $x^m - x = 0$ for all $x \in K$ (for some integer $m \geq 2$). (iv) What is the least value of m? [at least put a lower bound on it]
7. The exponent of a group G is the lcm of the orders of its elements (i) If G is Abelian, show that some element has order equal to the exponent (ii) but that this is not necessarily so otherwise. (iii) Hence show that $(K^*,*)$ is cyclic (a generator is called a primitive root in classical number theory).
8. Show that there is a unique (up to isomorphism) field of order p^n. [I'm not sure whether you have the machinery to do this]
9. Show that the group of field automorphisms of K is cyclic and generated by φ $(q^n 6)$. [ditto]
10. Find the orders of the groups $GL_n(K)$ and $SL_n(K)$ (sometimes written $GL(n,q)$, $SL(n,q)$) where K is a field of order $q = p^n$.

RINGS & IDEALS.

A ring is a set R with (possibly equal) special elements $0, 1$ and associative binary operations $+, *$ s.t. $(R,+,0)$ is an Abelian group, $(R,*,1)$ is a monoid [ie $a*1=1*a=a \ \forall a\in R$] and $*$ distributes over $+$, so $0*a=a*0=0 \ \forall a$.
A ring homomorphism is a map preserving $0,1,+,-,*$.

(1) $0=1$ iff $R=\{0\}$, the zero ring. Also, given any ring R, $\exists!\ \varphi: R\to 0$ [easy]

(2) List the kinds of ring you've encountered in IA (including Applied); does the 1 always arise directly in the naïve definition?

The kernel of a ring homomorphism $\varphi: R\to S$ is the set $\ker\varphi = \{r\in R : \varphi(r)=0_S\}$. A (two-sided) ideal of a ring is a subset J which is a subgroup under addition (ie $x,y\in J \Rightarrow x-y\in J$) and is closed under multiplication by R on either side (ie $x\in J,\ r\in R \Rightarrow rx, xr\in J$). Write $J\lhd R$

(3) $J=R$ iff $1\in J$ [easy]

(4) $\ker\varphi \lhd R$ for any $\varphi: R\to S$ [easy]

(5) if $\varphi,\psi: R\twoheadrightarrow S$ and $\ker\varphi=\ker\psi$ then $\exists!\ \theta: S\xrightarrow{\sim} S$ st. 

(6) if $J\trianglelefteq R$ then $J=\ker\varphi$ for some $\varphi: R\twoheadrightarrow S$
(S is called the quotient of R by J, written R/J)

(7) If $\varphi: R\to S$ is bijective (as a set map) then it's invertible.

(8) $n\mathbb{Z}=\{nz : z\in\mathbb{Z}\}\trianglelefteq\mathbb{Z}$ $(\forall n\in\mathbb{Z})$. What is the quotient? Does $\mathbb{Z}$ have any other ideals? [Hint: Euclidean algorithm]

(9) Let K be a field and $K[t]$ the ring of polynomials in one variable over K. Classify the ideals of $K[t]$ [Hint: 9.8] Does this work for $K[t_1,t_2]$?

(10) A division ring R [in which every $a\neq 0$ is invertible] has no ideals apart from $0, R$ [easy]

(11) A nontrivial ring with no nontrivial ideals is a division ring.

An ideal J is maximal if $J\neq R$ and $J\subseteq I\trianglelefteq R \Rightarrow I=J$ or $I=R$.

(12) Every ring has a maximal ideal [using Zorn's lemma]
An ideal J is principal if $J=rR$, ie it consists only of multiples of some element. This is also written $\langle r\rangle$
[Assume R commutative henceforward].
An element $r\in R$ is irreducible if $r=ab \Rightarrow$ either a or b is invertible; it is prime if $r\mid ab \Rightarrow r\mid a$ or $r\mid b$.
An ideal J is prime if $ab\in J \Rightarrow a\in J$ or $b\in J$.

(13) A principal ideal is prime iff it's generated by a prime element.

(14) Every prime is irreducible, but by considering $\mathbb{Z}[\sqrt{-5}]\subset\mathbb{C}$, not conversely.

(15) Every maximal ideal is prime

(16) If $I, J \trianglelefteq R$ with $I \subseteq J$ then $I \trianglelefteq J$ and $J/I \trianglelefteq R/I$. Also $(R/I)/(J/I) \cong R/J$

(17) If $J \lhd R$ is maximal and R is commutative, then R/J is a field.

(18) If $J \neq \lhd R$ is prime and R is commutative, then R/J is an integral domain [$ab=0 \Rightarrow a=0$ or $b=0$]

A principal ideal domain is an integral domain in which every ideal is principal. A unique factorization domain is an integral domain in which every irreducible is prime and every element can be expressed as a product of primes in a unique way in the sense that if $x = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ then $n=m$ & $q_i = u_i p_{\pi(i)}$ for some invertible elements [unit] u_i and permutation $\pi \in S_n$

(19) Every PID is a UFD, but, by considering $\mathbb{Z}[t]$ or $K[t_1, t_2]$, not conversely. [Hint: maximal, prime & irreducible coincide].

(20) Construct a field of order p^n and show it's unique.

(21) Let R be an integral domain [such as $\mathbb{Z}$]. Construct a field K [such as $\mathbb{Q}$] in which R is embedded, such that every $k \in K$ is of the form r/s for $r, s \in R$.

(22) Let $\varphi: R \hookrightarrow L$ be an injective map of an integral domain into a field. Show that there's a unique $\bar{\varphi}: K \to L$ extending φ (ie s.t. $\bar{\varphi}|_R = \varphi$).
K is called the field of fractions of R, $\mathrm{fof}(R)$.
$\mathrm{fof}(K[t])$ is written $K(t)$: it consists of the rational functions in one variable over K.

(23) Let $K \subset L$ be fields with $\alpha \in L \setminus K$ s.t. L is generated as a field by (K, α). Show that $L \cong K(t)$.

(24) [Hard] Using Zorn's lemma, construct an algebraically closed field $\bar{K}$ [every polyn. has a root] containing a given field K, s.t. every $a \in \bar{K}$ is algebraic over K [satisfies a polyn. eqn. with coeffs. in K]