Number Theory, Algebra and Analysis

William Yslas Vélez

Department of Mathematics

University of Arizona

O_F denotes the ring of integers in the field *F*, it mimics Z in Q

How do primes factor as you consider them in the larger ring?

P — O_F — F

p — Z — Q

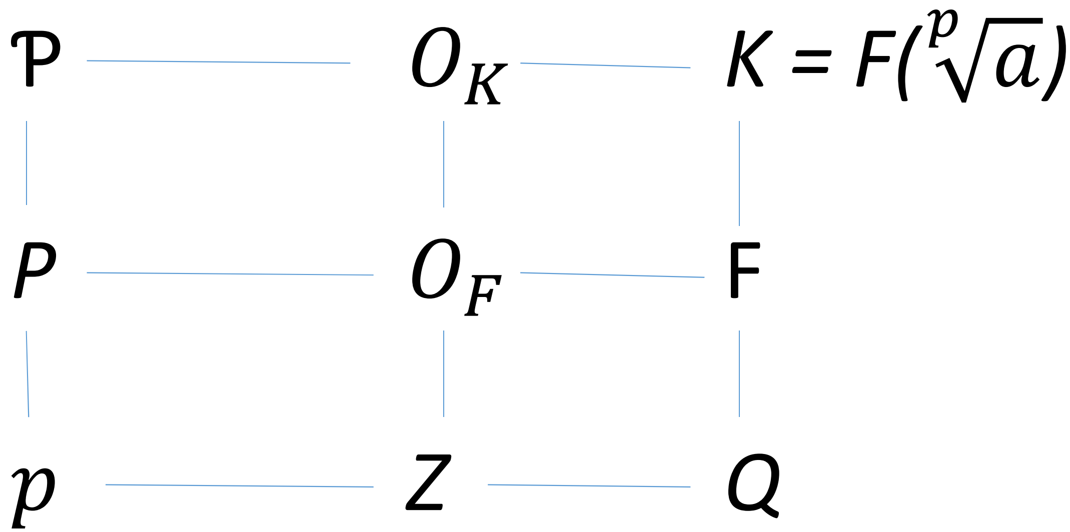
Examples

2 = ($\sqrt{2}$) ($\sqrt{2}$) in Q($\sqrt{2}$)

and more subtly

2 = (1 + i)(1 – i) in Q($\sqrt{-1}$)

Thesis Problem



If $x^p - a$ is irreducible over *F*, and *K* = *($\sqrt[p]{a}$)*, how do the prime divisors of p in O_F factor in O_K?

The number theoretic tools

The division algorithm

Given integers m and n, with $n > 0$, there exist unique integers, q & r, with $0 \le r < n$, so that $m = q*n + r$.

q is called the quotient and r is called the remainder.

With m = 88, n = 7,   88 = 12*7 + 4

$$
\begin{array}{r|l}
 & \;\;12 \\ \hline
7 & \;\;88 \\
 & -84 \\ \hline
 & \;\;\;\;4
\end{array}
$$

This is the algorithm you learned in grade school.

If we only want the remainder, it is called modular arithmetic.

Modular arithmetic

Given integers *m* and *n*, with *n > 0*, there exist unique integers, *q* & *r*, with *0 ≤ r < n*, so that *m = q*n + r*.

We define: *m ≡ r (mod n)* if the remainder is *r*, when *m* is divided by *n*.

In modular arithmetic we can multiply, add, subtract in the usual way.

88 ≡ 4 (mod 7), 32 ≡ 5 (mod 7) and

88 + 32 = 120 ≡ 4 + 5 ≡ 2 (mod 7)

88 * 32 = 2816 ≡ 4*5 ≡ 6 (mod 7)

Modular arithmetic – Dividing?????

The remainders when we divide by 7 are {0, 1, 2, 3, 4, 5, 6}

The 0 acts like the zero in ordinary arithmetic.

The 1 acts like the unit in ordinary arithmetic.

Can we divide? Instead of taking about dividing, let's ask for the multiplicative inverse of a number (mod 7).

- **Notice: $2*4 \equiv 1 \pmod 7$**
- **$3*5 \equiv 1 \pmod 7$**
- **$6*6 \equiv 1 \pmod 7$**

(mod 9), the remainders are: {0, 1, 2, 3, 4, 5, 6, 7, 8}

0, 3 & 6 have no multiplicative inverses (mod 9)

2*5 ≡ 1 (mod 9)   4*7 ≡ 1 (mod 9)   8*8 ≡ 1 (mod 9)

The remainders *(mod n)* are *{0, 1, 2, …, n-1}.* A number *a* has a multiplicative inverse iff *a* and *n* have no factors in common.

Notice that if *a* and *b* have inverses *(mod n),* then *a*b* has an inverse.

The subset of *{0, 1, 2, …, n-1}* that have inverses is called the group of units *(mod n).*

An important function in number theory is the Euler φ function which counts the number of elements which have no factors with n.

An aside: The Euler $\boldsymbol{\varphi}$ function

We talked about working (mod n) and pointed out that we can essentially work with the set *{0, 1, …, n-1}*

$\boldsymbol{\varphi(n) = |\{a: 0 \leq a < n}$: ***a* and *n* have no factors in common}|**

Properties: For *p* a prime, $\boldsymbol{\varphi\left(p^f\right) = (p-1) * p^{f-1}}$

and $\boldsymbol{\varphi(m * n) = \varphi(m)\varphi(n)}$ **if m and n have no factors in common**

Lehmer's Conjecture (1940's): $\boldsymbol{\varphi(n) |\ n-1}$ **iff *n* is prime**

Let *p, q* be primes. If we could calculate $\varphi(p * q)$ we could factor *p*q*

Algebraic tools

We have to deal with the holes

$X^2 – 3$ has no rational solutions, but we routinely do algebraic calculations with its roots.

We can take a + b*$\sqrt{3}$, where and b are rational numbers and compute.

{a + b*$\sqrt{3}$: a, b are rational numbers} forms a field, just like Q.

We need to be able to deal with roots of equations.

The general construction

Let $f(x) = x^k + a_{k-1} x^{k-1} + \dots + a_0$ be an irreducible polynomial with integer coefficients and let ϑ denote a root of this equation.

Let $F = Q(\vartheta)$ denote

$\{ b_{k-1} \vartheta^{k-1} + b_{k-2} \vartheta^{k-2} + \dots + b_1 \vartheta + b_0 : b_i$ are rational$\}$

***F* is a field, like *Q*, and you can also see that it is a k-dimensional vector space over *Q*.**

The integers in a field

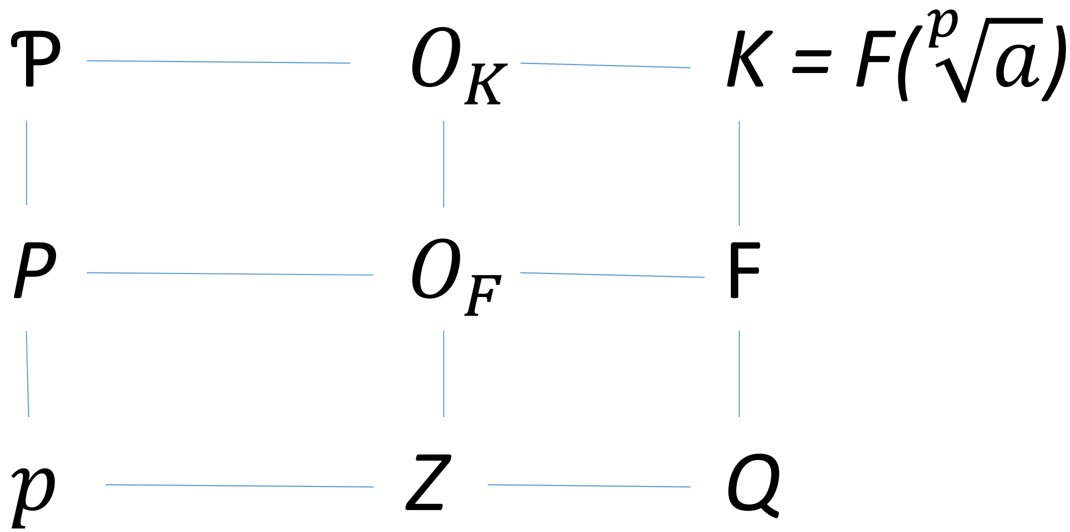
Let $f(x) = x^k + a_{k-1} x^{k-1} + \dots + a_0$ be an irreducible polynomial with integer coefficients and let ϑ denote a root of this equation.

Let $F = Q(\vartheta) = \{ b_{k-1} \vartheta^{k-1} + b_{k-2} \vartheta^{k-2} + \dots + b_1 \vartheta + b_0 : b_i$ are rational$\}$

O_F will denote the ring of integers in F. In many instances O_F = $\{ c_{k-1} \vartheta^{k-1} + c_{k-2} \vartheta^{k-2} + \dots + c_1 \vartheta + c_0 : c_i$ are integers$\}$

Notice: $f(\vartheta) = \vartheta^k + a_{k-1} \vartheta^{k-1} + \dots a_1 \vartheta + a_0 = 0$

Thesis Problem



If $x^p - a$ is irreducible over *F*, and *K* = ($\sqrt[p]{a}$), how do the prime divisors of p in O_F factor in O_K?

Tools from analysis

Q **has an absolute value, | |, with the properties that**

1. $|x| \geq 0$**, and** $|x| = 0$**, only for and** $x = 0$

2. $|x + y\ | \leq |x| + |y|$**, for all** $x, y\ \in Q$

This absolute allows us to define the limit concept and from there we can construct *R,* the real numbers, via equivalence classes of Cauchy sequences, thereby filling in all of the holes in *Q.* This is called the completion of Q with respect to | |

An algebraic construction,$\{a + b\ i\colon a, b\ are\ real\}$ **then yields the complex numbers and we now have a structure in which to work with solutions of ALL polynomial equations, plus other things.**

Cauchy sequences

Let $\{x_k\}$ and $\{y_k\}$ be sequences of rational numbers

$\{x_k\}$ is said to be a Cauchy sequence if given ε *> 0*, there exists a positive integer M so that $|x_r - x_s| < ε$, for all *r, s > M*

Two Cauchy sequences, $\{x_k\}$ and $\{y_k\}$, are said to be equivalent if $\{x_k - y_k\}$ goes to 0 as k goes to infinity

Other absolute values on *Q*

Let *p* be a prime number in *Z.* Any rational number *x* in *Q* has a unique representation

$x = p^k * \frac{a}{b}$**, where *a, b* are integers, have no common factors, and have no common factors with *p***

The p-adic absolute value is defined by $|x|_p = p^{-k}$. This satisfies

1. $|x|_p \geq 0$, and define $|0|_p = 0$

2.$|x + y|_p \leq \max\{|x|_p, |y|_p\}$ for all $x, y \in Q$

This inequality is stronger than the triangle inequality

What do we do with an absolute value?

We can define convergence of a sequence

With that we can define Cauchy sequences

We then take equivalence classes of Cauchy sequences

We now form the completion of Q with respect to $| \ |_p$ denoted by Q_p

Notice: $\lim_{n\to\infty} p^n = 0$

Just as for the reals we can do limits, infinite series, etc in Q_p

Theorem: **For $c_i \in Q_p$, the series $\sum_{i=1}^{\infty} c_i$ converges iff $\lim_{i\to\infty} c_i = 0$**

What do elements in $\boldsymbol{Q_p}$ look like?

The elements (mod p^{k+1}) are $a_0 + a_1 p + \ \dots + \ a_k p^k$,
where $a_i \in \{0, 1, \dots p-1\}$ and the elements of Q_p are

$$\sum_{i=l}^{\infty} a_i p^i \text{ where l is an integer}$$

The set of integers in Q_p are those elements where $l \geq 0$, that is

$$a_0 + a_1 p + \ \dots + \ a_k p^k + \dots$$

Bonus: Q_p has a structure analogous to *Z* in *Q*, whereas *R* does not

Amazing Theorems

Let $f(x) = x^k + a_{k-1}\, x^{k-1} + \ldots + a_0$ be an irreducible polynomial with integer coefficients, ϑ a root,

$$F = Q(\vartheta) = \{\, b_{k-1}\, \vartheta^{k-1} + b_{k-2}\, \vartheta^{k-2} + \ldots + b_1\, \vartheta + b_0 : b_i \text{ are rational}\}.$$

THEOREM 1: For almost all primes of *p* of Z, the number of prime factors of *p* in O_F is the number of irreducible factors of *f(x)* (mod *p*), and more…

THEOREM 2: For ALL primes of *p* of Z, the number of prime factors of *p* in O_F is the number of irreducible factors of *f(x)* in Q_p, and more…

$x^p - a$ is irreducible over *F*, and *K* = $(\sqrt[p]{a})$

We want to determine how a prime P, a divisor of *p* in O_F factors.

THEOREM 2: For ALL primes of *p* of Z, the number of factors of *p* in O_F is the number of irreducible factors of *f(x)* in Q_p, and more…

A generalization of the above theorem says that we need to factor the binomial in the p-adic field, F_P.

The binomial is reducible iff a is a p-th power!

Help is on the way: power series in p-adic fields.

Power series in *p*-adic fields

There are power series expansions for *e*^{x}*, log (1 + x)* in p-adic fields

I am interested in

$(\mathbf{1}+\boldsymbol{x})^{\mathbf{1}/\boldsymbol{p}} = \sum_{\boldsymbol{n}=\mathbf{1}}^{\infty} \frac{\mathbf{1}/\boldsymbol{p}}{\boldsymbol{n}} \boldsymbol{x}^{\boldsymbol{n}}$ **converges in Q_p if $|\boldsymbol{x}|_{\boldsymbol{p}} < \frac{\mathbf{1}}{\boldsymbol{p}}$, for *p* odd**

For the experts: In F_P the radius of convergence is *ef*

$$(1+x)^{1/p} = \sum_{n=1}^{\infty} \frac{1/p}{n} x^n$$ **converges in Q_p if $|x|_p < \frac{1}{p}$**

Here is how we use this to factor $x^p - a$, where *p* does not divide *a*

If $a \equiv b^p \ (mod\ p^2)$, then let b^{-1}denote the multiplicative inverse of b (*mod p).* So, b^{-1} is an integer and $ab^{-p} \equiv 1(mod\ p^2)$

Let $x = ab^{-p} - 1$, then p^2 divides x, that is $|x|_p \le (\frac{1}{p})^2 < \frac{1}{p}$

So, $(1+x)^{1/p}$ exists in Q_p and $a = (b(1+x)^{1/p})^p$ and $x^p - a$ can be factored in Q_p.

In fact $x^p - a$ factors into a linear factor and a irreducible factor of degree *p-1*

A story from my advisor

Klein

Hensel

Furtwängler

H. B. Mann

W. Y. Vélez

Thesis results

I had to go back to H. B. Mann's thesis

He studied the units in the system $(mod\ P^n)$

He was able to complete a basis for this system, except in one case.

I had look at his thesis and was able to complete his problem because I used p-adic methods.

H. B Mann has claimed that p-adic methods did not give new information.

I showed that in the case he left, there was a root of unity in the P-adic completion that completed the work in his thesis

H. B. Mann retired in 1976

- In his last year he taught the graduate course in algebra and presented p-adic methods

- One last problem about the Euler problem

Champions of Arithmetic functions

Ramanujan's early paper was on the number of divisors function

d(n) = # of divisors of n

n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 12, 13, ….

d(n)= 1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2 , ….

The champions of a function are the largest value up to that point.

- **What are the champions of the Euler φ function?**