MATH 361: NUMBER THEORY — SIXTH LECTURE SUPPLEMENT

1. Computation of $\sqrt{-1}$ in $\mathbb{Z}_5$

Let $p = 5$. Let

$$f(x) = 1 + x^2, \qquad f'(x) = 2x.$$

The condition $f(x) = 0$ is $x^2 = -1$. That is, finding a root of f amounts to finding a square root of -1.

Let $\boxed{x_1 = 2.}$ Thus

$$f(x_1) = 5, \qquad f'(x_1) = 4,$$

and so

$$f(x_1) = 0 \bmod 5^1, \qquad f'(x_1) = 0 \bmod p^0, \quad f'(x_1) \neq 0 \bmod p^1.$$

Here we have $n = 1$, $k = 0$, and $2k \leq n - 1$.

Let $x_2 = x_1 + 5^1 k = 2 + 5k$, with k to be determined. Compute

$$f(x_2) = 1 + 2^2 + 2 \cdot 2 \cdot 5k + 5^2 k^2 = 5(1 + 4k) \bmod 5^2.$$

This is 0 mod 5^2 if $1 + 4k = 0 \bmod 5$, or $1 = k \bmod 5$, so take $k = 1$. Now $\boxed{x_2 = 7}$. Thus

$$f(x_2) = 50, \qquad f'(x_2) = 14.$$

So $x_2 = x_1 \bmod 5^1$ and

$$f(x_2) = 0 \bmod 5^2, \qquad f'(x_2) = 0 \bmod p^0, \quad f'(x_2) \neq 0 \bmod p^1.$$

Now we have $n = 2$, $k = 0$, and still $2k \leq n - 1$.

Let $x_3 = x_2 + 5^2 k = 7 + 25k$, with k to be determined. Compute

$$f(x_3) = 1 + 7^2 + 2 \cdot 7 \cdot 5^2 k + 5^4 k^2 = 5^2(2 + 14k) \bmod 5^3.$$

This is 0 mod 5^3 if $2 + 4k = 0 \bmod 5$, or $2 = k \bmod 5$, so take $k = 2$. Now $\boxed{x_3 = 57}$. Thus

$$f(x_3) = 3250 = 26 \cdot 5^3, \qquad f'(x_2) = 114.$$

So $x_3 = x_2 \bmod 5^2$ and

$$f(x_3) = 0 \bmod 5^3, \qquad f'(x_3) = 0 \bmod p^0, \quad f'(x_3) \neq 0 \bmod p^1.$$

Now we have $n = 3$, $k = 0$, and still $2k \leq n - 1$.

Let $x_4 = x_3 + 5^3 k = 57 + 125k$, with k to be determined. Compute

$$f(x_4) = 1 + 57^2 + 2 \cdot 57 \cdot 5^3 k + 5^6 k^2 = 5^3(26 + 2 \cdot 57k) \bmod 5^4.$$

This is 0 mod 5^4 if $1 + 4k = 0 \bmod 5$, or $1 = k \bmod 5$, so take $k = 1$. Now $\boxed{x_4 = 182}$. So $x_4 = x_3 \bmod 5^3$, and we can confirm that

$$f(x_4) = 0 \bmod 5^4, \qquad f'(x_4) = 0 \bmod p^0, \quad f'(x_4) \neq 0 \bmod p^1.$$

And now we have $n = 4$, $k = 0$, and still $2k \leq n - 1$.

We can continue indefinitely in this fashion. At each step, no matter how large n is, the congruence to solve for k will take the form $a+4k = 0 \bmod 5$, or $a = k \bmod 5$, so we take $k = a$ and then $x_{n+1} = x_n + 5^n k$.

2. p-adic valuation and absolute value

Fix a prime p. Every nonzero rational number x uniquely takes the form

$$x = p^e \frac{m}{n}, \quad e \in \mathbb{Z},\ m, n \in \mathbb{Z} - \{0\},\ p \nmid mn,\ n > 0,\ \gcd(m, n) = 1.$$

Here we crucially use unique factorization in $\mathbb{Z}^+$. The *p-adic valuation function on $\mathbb{Q}$* is

$$\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{-\infty\}$$

given by

$$\nu_p(x) = \begin{cases} e & \text{if } x = p^e m/n \\ -\infty & \text{if } x = 0. \end{cases}$$

For $x = p^e m/n$ and $x' = p^{e'} m'/n'$, compute

$$\nu_p(xx') = \nu_p\left(p^{e+e'} \frac{mm'}{nn'}\right) = e + e' = \nu_p(x) + \nu_p(x').$$

And if at least one of x and x' is 0 then, again,

$$\nu_p(xx') = \nu_p(0) = -\infty = \nu_p(x) + \nu_p(x').$$

(Here $-\infty + e' = -\infty$ for all $e' \in \mathbb{Z} \cup \{-\infty\}$.) That is, for all $x, x' \in \mathbb{Q}$,

$$\boxed{\nu_p(xx') = \nu_p(x) + \nu_p(x').}$$

As an application, if $r \in \mathbb{Q}$ squares to 2 then

$$2\nu_2(r) = \nu_2(r^2) = \nu_2(2) = 1,$$

giving $\nu_2(r) = 1/2 \notin \mathbb{Z}$, impossible. So no rational number can square to 2.

Again for $x = p^e m/n$ and $x' = p^{e'} m'/n'$, now take $e' > e$ so that $e' = e + \delta$ where $\delta > 0$. Because $p \nmid mn' + p^\delta m'n$ we have

$$\nu_p(x + x') = \nu_p\left(p^e \frac{mn' + p^\delta m'n}{nn'}\right) = e = \min\{\nu_p(x), \nu_p(x')\}.$$

But if instead $e' = e$, so that now $\delta = 0$ and possibly $p \mid mn' + m'n$, we have only

$$\nu_p(x + x') = \nu_p\left(p^e \frac{mn' + m'n}{nn'}\right) \geq e = \min\{\nu_p(x), \nu_p(x')\}.$$

If $x \neq 0$ as above but now $x' = 0$ then

$$\nu_p(x + x') = \nu_p(x) = e > -\infty = \min\{\nu_p(x), \nu_p(x')\},$$

and if $x = x' = 0$ then

$$\nu_p(x + x') = \nu_p(0) = -\infty = \min\{\nu_p(x), \nu_p(x')\}.$$

That is, overall, for all $x, x' \in \mathbb{Q}$,

$$\boxed{\nu_p(x + x') \geq \min\{\nu_p(x), \nu_p(x')\}, \quad \text{with equality if } \nu_p(x) \neq \nu_p(x').}$$

As an application, for any integer $n \geq 2$ let 2^s be the biggest power of 2 that lies in $\{1, \dots, n\}$; thus $2^{s+1} > n$ and so no proper integer multiple of 2^s lies in $\{1, \dots, n\}$. Consequently

$$\begin{aligned} \nu_2(1/2^s) &= -s \\ \nu_2(1/k) &> -s \quad \text{for all } k \neq 2^s \text{ in } \{1, \dots, n\}. \end{aligned}$$

It follows that

$$\nu_2\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \frac{1}{2^s}\right) > -s$$

and therefore that

$$\nu_2\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right) = -s < 0.$$

Thus $1 + 1/2 + \cdots + 1/n$ is not an integer.

The *p-adic absolute value on* $\mathbb{Q}$ is

$$|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$$

given by

$$|x|_p = p^{-\nu_p(x)}.$$

This formula is understood to connote that $|0|_p = p^{-\infty} = 0$; for all nonzero $x \in \mathbb{Q}$ the absolute value $|x|_p$ is positive. The two boxed formulas above give for all $x, x' \in \mathbb{Q}$,

$$\boxed{|xx'|_p = |x|_p |x'|_p}$$

and

$$\boxed{|x + x'|_p \leq \max\{|x|_p, |x'|_p\}, \quad \text{with equality if } \nu_p(x) \neq \nu_p(x').}$$

This last relation is called the *ultrametric inequality* because it is stronger than the usual metric inequality $|x + x'| \leq |x| + |x'|$. Because the ultrametric inequality applies with $-x'$ in place of x', and because $|-x'|_p = |-1|_p |x'|_p = |x'|_p$, this says that p-adically all triangles are isosceles.